Thematic Research: Medical

Cybersecurity in Medical

1 October 2020

GDMED-TR-S008

Contents

Executive summary

Cybersecurity is increasingly required for patient safety

The global healthcare industry is increasingly embracing digital technologies, such as cloud, Big Data, Internet of Things (IoT), remote monitoring, and more, to deliver the best patient care. However, as more digital technologies are utilized, the greater potential there is for cyberattack. Healthcare data is particularly sensitive to cyberattack, since healthcare cyber breaches often involve loss of sensitive personal information and medical records. Digitally-connected medical devices are also susceptible to cyberattack, and interference with how these devices operate could potentially lead to patient harm or even death. Health system data breaches have occurred in the past and continue to occur. In 2019, there were 510 healthcare breaches of 500 records or more (up from 371 in 2018) reported to the US Department of Health and Human Services (HHS), which in total affected over 41 million patient records.

Hospitals and health systems have historically been slow to adapt to changing technologies, preferring established methods of practice in most arenas. However, as the importance of cybersecurity in healthcare is becoming increasingly apparent, healthcare providers are now beginning to shift to prioritizing data protection and cybersecurity. As a result, there is a significant market opportunity, and technology vendors can leverage their ecosystems to offer end-to-end security solutions and exploit state-of-the-art technology such as artificial intelligence (AI) and forensics for healthcare purposes.

Forward-thinking healthcare providers are pivoting towards a holistic cybersecurity approach to shore up their current positions. This approach will also ensure strong future-proofing elements by acknowledging ongoing changes that are in line with wider growth strategies. However, achieving a comprehensive cybersecurity approach requires involving people, processes, and technology that are relevant to detection, prediction, prevention, and rapid response in order to safeguard users from the myriad cyber breaches that healthcare players now need to confront.

Leaders and laggards

New AI-infused security companies will either be the standard-bearers of the future or, more likely, become M&A targets for the old guard.

Leaders, both young and old, will include the following:

- **Endpoint security:** Microsoft, CrowdStrike, McAfee, FireEye, Palo Alto Networks, SentinelOne, BlackBerry, Trend Micro.
- **Threat intelligence:** IBM, ThreatQuotient, Darktrace, Recorded Future, Deep Instinct, Anomali.
- **Cloud security:** Microsoft, IBM, Proofpoint, Trend Micro, Fortinet, Palo Alto Networks
- **DevSecOps:** Sumo Logic, Veracode, NTT Security, Red Hat.

Laggards will include those firms that fail to define a clear AI security stance or take the necessary M&A steps to acquire one.

Inside

Related reports

- Thematic Research: Cybersecurity (2020)

Report type

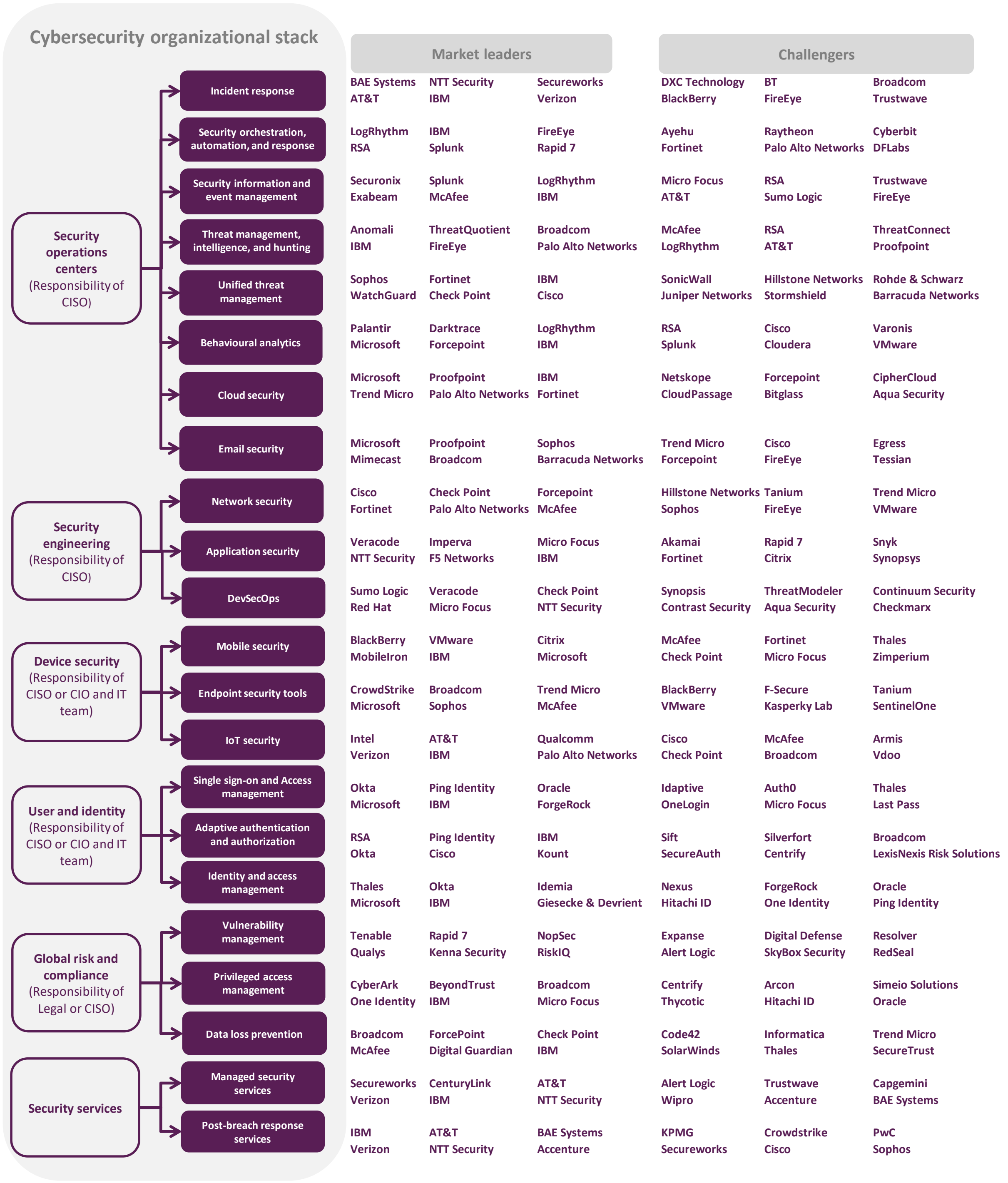
- **Single theme**
- Multi-theme
- Sector Scorecard

Players

This schematic shows the major technology areas that make up the cybersecurity sector and details both the leading companies in each area and some of the most notable challengers.

Who are the leading players in the Cybersecurity theme and where do they sit in the value chain?

This graphic lists the leaders and challengers across the cybersecurity technology stack



Cybersecurity organizational stack		Market leaders			Challengers		
Security operations centers (Responsibility of CISO)	Incident response	BAE Systems AT&T	NTT Security IBM	Secureworks Verizon	DXC Technology BlackBerry	BT FireEye	Broadcom Trustwave
	Security orchestration, automation, and response	LogRhythm RSA	IBM Splunk	FireEye Rapid 7	Ayehu Fortinet	Raytheon Palo Alto Networks	Cyberbit DFLabs
	Security information and event management	Securonix Exabeam	Splunk McAfee	LogRhythm IBM	Micro Focus AT&T	RSA Sumo Logic	Trustwave FireEye
	Threat management, intelligence, and hunting	Anomali IBM	ThreatQuotient FireEye	Broadcom Palo Alto Networks	McAfee LogRhythm	RSA AT&T	ThreatConnect Proofpoint
	Unified threat management	Sophos WatchGuard	Fortinet Check Point	IBM Cisco	SonicWall Juniper Networks	Hillstone Networks Stormshield	Rohde & Schwarz Barracuda Networks
	Behavioural analytics	Palantir Microsoft	Darktrace Forcepoint	LogRhythm IBM	RSA Splunk	Cisco Cloudera	Varonis VMware
	Cloud security	Microsoft Trend Micro	Proofpoint Palo Alto Networks	IBM Fortinet	Netskope CloudPassage	Forcepoint Bitglass	CipherCloud Aqua Security
	Email security	Microsoft Mimecast	Proofpoint Broadcom	Sophos Barracuda Networks	Trend Micro Forcepoint	Cisco FireEye	Egress Tessian
Security engineering (Responsibility of CISO)	Network security	Cisco Fortinet	Check Point Palo Alto Networks	Forcepoint McAfee	Hillstone Networks Sophos	Tanium FireEye	Trend Micro VMware
	Application security	Veracode NTT Security	Imperva F5 Networks	Micro Focus IBM	Akamai Fortinet	Rapid 7 Citrix	Snyk Synopsys
	DevSecOps	Sumo Logic Red Hat	Veracode Micro Focus	Check Point NTT Security	Synopsis Contrast Security	ThreatModeler Aqua Security	Continuum Security Checkmarx
Device security (Responsibility of CISO or CIO and IT team)	Mobile security	BlackBerry MobileIron	VMware IBM	Citrix Microsoft	McAfee Check Point	Fortinet Micro Focus	Thales Zimperium
	Endpoint security tools	CrowdStrike Microsoft	Broadcom Sophos	Trend Micro McAfee	BlackBerry VMware	F-Secure Kasperky Lab	Tanium SentinelOne
	IoT security	Intel Verizon	AT&T IBM	Qualcomm Palo Alto Networks	Cisco Check Point	McAfee Broadcom	Armis Vdoo
User and identity (Responsibility of CISO or CIO and IT team)	Single sign-on and Access management	Okta Microsoft	Ping Identity IBM	Oracle ForgeRock	Idaptive OneLogin	Auth0 Micro Focus	Thales Last Pass
	Adaptive authentication and authorization	RSA Okta	Ping Identity Cisco	IBM Kount	Sift SecureAuth	Silverfort Centrify	Broadcom LexisNexis Risk Solutions
	Identity and access management	Thales Microsoft	Okta IBM	Idemia Giesecke & Devrient	Nexus Hitachi ID	ForgeRock One Identity	Oracle Ping Identity
Global risk and compliance (Responsibility of Legal or CISO)	Vulnerability management	Tenable Qualys	Rapid 7 Kenna Security	NopSec RiskIQ	Expanse Alert Logic	Digital Defense SkyBox Security	Resolver RedSeal
	Privileged access management	CyberArk One Identity	BeyondTrust IBM	Broadcom Micro Focus	Centrify Thycotic	Arcon Hitachi ID	Simeio Solutions Oracle
	Data loss prevention	Broadcom McAfee	ForcePoint Digital Guardian	Check Point IBM	Code42 SolarWinds	Informatica Thales	Trend Micro SecureTrust
Security services	Managed security services	Secureworks Verizon	CenturyLink IBM	AT&T NTT Security	Alert Logic Wipro	Trustwave Accenture	Capgemini BAE Systems
	Post-breach response services	IBM Verizon	AT&T NTT Security	BAE Systems Accenture	KPMG Secureworks	Crowdstrike Cisco	PwC Sophos

Source: GlobalData

Trends

The main trends in the cybersecurity industry over the next 12 to 24 months are shown below. We classify these trends into five categories: the changing nature of cyber threats, evolution of key cybersecurity technologies, industry growth drivers, medical governance trends, and cybersecurity trends in medical.

Changing Nature of Cyber Threats

Trend	What's happening?
Ransomware	Ransomware, in which a victim's most critical files are held hostage, is a form of cyberattack that is on the rise. In 2016, security company Malwarebytes surveyed 500 companies in four countries and found that one-third had been the victim of a ransomware attack. Ransomware refers to malicious software that takes control of a computer and encrypts the data on it, rendering it inaccessible. The hackers then demand a payment, typically in the form of bitcoin, in exchange for handing over the encryption keys. Spear phishing remains the most common entry mechanism, whereby an email from someone known asks the user to inadvertently click on something that downloads the ransomware to the computer. According to cybersecurity company FireEye, there were over 30 ransomware families in 2016, up from just three in 2012. The WannaCry ransomware attack is one of the most high-profile ransomware attacks in recent memory. On May 12, 2017, the attack targeted computers running the Microsoft Windows XP operating system by encrypting data and demanding ransom payments in bitcoin. Within a single day, WannaCry had reportedly infected more than 230,000 computers in over 150 countries. Companies and organizations including Britain's National Health Service (NHS), Spain's Telefónica, FedEx, and Deutsche Bahn were crippled. Another recent and high-profile ransomware was SamSam. This affected the City of Atlanta, Georgia, US, causing digital disruption in five of the city's 13 local government departments. The attack encrypted and renamed files as well as locked out computers. It resulted in a loss of access to files, as well as outages to several online systems and services. The hacker demanded a bitcoin payment of $50,000. The medical sector is not immune to ransomware attacks. In June, 2020, a hospital in Colorado, US reported a ransomware attack that targeted software essential to accessing patient records. Ransomware attacks in the medical sector are especially problematic, as the ransomed files are often critical to patient health and safety.
Insider and privilege misuse	According to a 2016 Data Breach Investigation by Verizon, around 77% of breaches fall within the insider and privilege misuse category. These breaches are caused by an internal party or individual, such as a dissatisfied employee who leaks data on purpose or a careless staff member who unintentionally discloses sensitive data. This could be an indication of a lack of appropriate cybersecurity measures within an organization. Organizations are increasingly looking to restrict access to company-sensitive and key accounts, as well as assigning special account access privileges to authorized individuals. Many organizations have started to offer cybersecurity education and training to employees and staff. Insider breaches are problematic, as 48% of insurers surveyed by Accenture reported experiencing malicious insider threats, while 55% lacked confidence in their internal security monitoring. Insurers will look to track the data flow in all information technology (IT) systems, applications, and components. The 2020 Data Breach Report by Verizon indicates that privilege misuse is also a significant cause of factor in cyber threats in the healthcare sector, with insider and privilege misuse leading to 8.7% of cyberattacks. However, in the previous year, insider and privilege misuse made an even greater contribution to healthcare cyberattacks at 23%. This trend suggests that insiders in the healthcare sector may be granting less and less malicious access over time.

Trend	What's happening?
Denial of service	A Denial of Service (DoS) attack is a form of cyber-attack that aims to shut down a network, application, or machine, or make them inaccessible to users such as employees, members, or account holders. This can be accomplished by flooding the targeted network with traffic or sending information that causes a crash, thus interrupting the network service. Victims of DoS attacks are typically players from the banking, media, commerce, government, and trading sectors. One type of DoS attack is Distributed Denial of Service (DDoS), which occurs when multiple systems organize a synchronized DoS attack on one target. An example of a DDoS attack was that suffered by the British Broadcasting Corporation (BBC) website in January 2016. Botnets (also known as "robot networks") are also on the rise. Botnets are created when a hacker temporarily takes control of millions of internet-enabled devices such as security cameras or TV set-top boxes by remotely infecting them with hidden malware. The botnet can then be used to mount DDoS attacks by instructing the infected devices to send simultaneous data requests en masse to a single server, causing the server to overload and crash. On October 21, 2016, a number of popular US websites—including Airbnb, Amazon, Spotify, Netflix, and Twitter—were rendered inaccessible following a massive DDoS attack on the Domain Name Service (DNS) servers of Dyn, a company that manages website domains and routes internet traffic. It marked one of the largest DDoS attacks ever launched. The attackers had infected tens of millions of internet-connected devices with the Mirai botnet, a form of malware that scours the web for IoT devices protected only by factory-default usernames and passwords, and then assumes control of these enlisted devices to launch DDoS attacks. The compromised IoT devices flooded Dyn's computers with junk data, causing them to overload and eventually fail. This led to legitimate users, who used Dyn's servers to direct their URL requests, being denied access to their intended websites. The webcams of Chinese electronics manufacturer Xiongmai were linked to the attack. The attack on Dyn shows the weakness of the internet's underlying infrastructure and the relative ease with which large-scale attacks can be implemented with impunity. It also shows that manufacturers of IoT devices are an integral part of the security equation and need to take appropriate steps to ensure security needs are met. DoS and DDoS attacks also occur in the healthcare sector, and are particularly problematic when they occur in hospitals since access to critical patient information can be compromised, according to the Center for Internet Security (CIS). One example of a large DDoS attack that occurred in the healthcare sector was the attack of Boston Children's Hospital in 2014. A DDoS attack against the hospital resulted in network outages affecting not only this hospital, but also other hospitals using the same network, including Harvard University and all its affiliated hospitals. As a result of the attack, there was a period of time where patient information including appointment times and test results could not be accessed, and the hospitals had to spend significant resources in both time and money to restore access.
Hacktivist groups	Increasingly, more sophisticated hacking has been perpetrated by groups of hackers against governments, nations, and states rather than against an individual. Anonymous and Lulz Security are two of the most widely known hacktivist groups. They use sophisticated hacking methods to bring down large institutions via DDoS attacks that temporarily eliminate the availability of web or email servers. Anonymous, in alliance with Ghost Squad Attackers, claims to have brought down several central banks in this way, including the Bank of Greece, the Federal Reserve Bank of Boston, the Bank of England, and the Bank of France. The group also claims to have brought down the London Stock Exchange for over two hours in early June 2017. Hactivist groups also target healthcare facilities, and Anonymous has also been credited with the DDoS attack against Boston Children's Hospital described above.
Online fraud	Online fraud is on the rise on the back of technology cycles such as peer-to-peer (P2P) lending, mobile banking, e-commerce, and the IoT. Social media encourages the reckless dissemination of personal information on the web, which facilitates identity theft. Moreover, hackers have access to low-cost tools and methodologies on the internet and little prospect of being caught. As more personal data ends up stored in the databases of

Trend	What's happening?
	internet companies, specialist data resellers can create more and more Big Data algorithms that dissect this data for resale. Credit profilers such as Experian and Equifax are one set of beneficiaries, and online fraud detection companies such as IBM, Guardian Analytics, RSA (Dell/EMC), and Kount are another. With telehealth on the rise in the healthcare sector, more and more personal health information also continues to be shared online, making this sensitive information vulnerable to cyberattack through online fraud. Online fraud in healthcare often takes one of three primary forms: provider fraud, cyber scams, and medical identity theft. In provider fraud, healthcare providers use online billing systems to commit fraud, such as charging for more expensive procedures than were actually provided. Cyber scams include marketing ads targeting patients and/or providers with fake products or other scams. Medical identity theft occurs when someone's personal information is stolen and used to fraudulently obtain medical services. All three forms of online fraud are likely to rise with the increasing use of telemedicine and sharing of medical information through IoT devices.

Source: GlobalData

Evolution of Cybersecurity Technologies

Trend	What's happening?
Prevention, detection and response	There has been a move away from a prevention-based approach to cyberattacks towards active detection and timely responses. This approach uses three levels of cybersecurity: people, process, and technology. The prevention approach is futile unless it is combined with detection and rapid response approaches. Many Chief Information Security Officers (CISOs) and security executives are investing in detection and response-based technologies such as deception, endpoint detection and response, software defined segmentation, and behavior analytics. CISOs and security executives are looking to achieve and optimize visibility across their infrastructure to ensure an adequate protection from security incidents. Detection and response-based technologies are also extremely useful in healthcare, with some companies directly marketing this approach to the healthcare industry. For example, LastLine (recently acquired by VMware) advertised detection and response technologies to healthcare industry users on their website in 2019.
Unified threat management	In recent years, multiple vendors have sold a patchwork of security products to corporations without considering how well they work together. The result has been a lack of strategic direction and co-ordination within many companies' IT departments. This could be reworked so that unified threat management systems powered by intelligence engines that take a risk-based approach to security are in the lead. By automating threat discovery, investigation, and response, unified threat management can reduce incident response times and enhance overall threat detection rates. The leading companies in unified threat management are Check Point Software, Fortinet, IBM, SecureWorks, Sophos, and WatchGuard. Hospitals and other healthcare providers will also benefit from unified threat management, for the same reasons as corporations would.
Behavioral Analytics	Some breaches are caused by insider threats—whether through malicious intent or negligence—so behavioral analytics are critically important as a cyber defense. AI leaders IBM, Google, Microsoft, Splunk, and Palantir are among the best-placed companies to exploit this trend. However, there are also a number of start-ups specializing in behavioral analytics in the cybersecurity sector, including Cloudera, Bay Dynamics, Carbon Black (acquired by VMware), E8 Security, and Securonix. In 2017, Cybraics used behavioral analytics to identify cyberattacks that had previously been missed within a large health system in the US.
Biometric security	Amazon and Mastercard are among the first major payment players to use selfies as an alternative to security passwords. In October 2016, Mastercard announced the European rollout of Identity Check Mobile, a new payment technology application that uses biometrics such as fingerprints or facial recognition to verify a card holder's identity. Passwords offer poor security for most digital transactions and are overdue to be replaced. Facial recognition and fingerprint technology companies should be a major beneficiary of this trend. Leaders in this space include Clarifai, 3M Cogent, and Safran. In healthcare, biometric authentication could significantly improve security in electronic patient records. Currently, biometrics are being used in hospitals across the US for a variety of reasons, such as during patient registration. For example, the University of Pittsburgh Medical Center first implemented finger scanners in 2016, and by the end of 2019 boasted a total of 3,800 biometric readers across 68 sites, according to HealthTechMagazine.net. In the future, biometric security will likely be used for other healthcare applications as well, such as to access records or submit claims.
Incidence response services	British telecom operator TalkTalk was fined £400,000 ($521,294) for security failings by the Information Commissioner's Office in the aftermath of its October 2015 cyber-attack. There is a growing market for post-breach strategy consultancy services. Post-breach strategy focuses on gathering information about the cyber-attack as quickly as possible after the event and formulating a credible public relations (PR) strategy to demonstrate that company management remains in control of their business and have taken all actions possible to protect critical digital assets. The leading post-breach consultancy services companies include IBM, Accenture, KPMG, PwC, FireEye, Herjavec Group, and root9B. These services are also critical for healthcare services as they continue to face cyber threats.

Trend	What's happening?
Managed security services	Few organizations have the necessary skill base to build cybersecurity defenses themselves or even make effective use of cybersecurity technology. This tilts the balance in favor of managed security services, whereby a single security vendor manages an organization's cloud applications, compliance with data protection laws, and other cybersecurity risks. Leaders in managed security services include IBM, Symantec, SecureWorks, WIPRO, BAE Systems, HP Enterprise, and Trustwave (SingTel). Telecommunications companies (telcos) like AT&T, BT, CenturyLink, NTT, Orange, and Verizon also operate in the space. Some companies, such as Securitas, offer managed security services in packages specific to healthcare needs.
Security as a service	Cybersecurity is also moving from the purchase of one-off software products (such as downloading Norton anti-virus software) to security as a service. This is because one-off security products are designed for a specific purpose, while the threat environment is constantly changing. Security as a service replaces the one-off cost of purchasing on premises equipment with a monthly subscription. It also enables corporations to ensure their IT security is constantly up to date without having to manually replace equipment or download the latest security patches. Many security-managed service providers offer security services on the cloud, including Barracuda Networks, Fortinet, Imperva, Qualys, Trustwave (SingTel), CloudPassage, and CliQr. Similarly to managed security services, some companies that offer security as a service offer healthcare-specific packages that are intended to be tailored to healthcare provider needs.
The network segmentation imperative	The increase of connectivity and interconnected digitized networks—whereby organizations are moving data in and out of the enterprise network—has led to cyberattacks such as the recent WannaCry ransomware attack. There is a growing trend among enterprises to separate their enterprise network from their external network. Splitting the network into a subnetwork or separating a group of systems and applications can prevent hackers from pivoting from one vulnerable system to allow malware or a virus to propagate across the whole organization network. While security experts consider network segmentation to be an essential security measure, organizations are lagging behind in terms of implementation. This includes healthcare organizations: a 2019 study by security firm Forescout reported that only 49% of medical devices were deployed across 10 virtual local access networks (VLANs) or fewer, which indicates a lack of network segmentation. However, organizations are being educated on better protection mechanisms for the outer perimeter in order to guard internal infrastructure, workloads, and data, as well as to support their organizational systems. The concept of micro-segmentation—segregating all critical applications into a secure core network with different architectural zones, with different levels of security applied through configured firewalls, and VLANs—ensures that data cannot randomly be moved from one network zone to another. Some examples of vendors delivering this type of segmentation include VMware, Juniper, and Cisco.
Risk-based security approach	Risk-based strategies allow businesses and organizations to adopt strategies that are tailored to their unique operating models and their environments, threat landscapes, and business objectives. This approach delivers better value to organizations, allowing them to understand the impact of risk mitigation initiatives and providing a comprehensive view of their risk. A risk-based approach fits and complements the enterprise risk management framework adopted by the organization. It allows organizations to assess and carefully consider policies, process, and technology solutions and services that provide a comprehensive defense approach to cyber risks. Healthcare facilities would equally benefit from a risk-based security approach.

Source: GlobalData

Industry Growth Drivers

Trend	What's happening?
Cloud	Large corporations are building private and hybrid clouds while small-to-medium enterprises (SMEs) are spending significantly on public cloud services. Both activities could open companies up to a higher risk of cyber-attack, and could also increase the demand for cloud security and web application security services. The healthcare industry is employing cloud technology more and more abundantly for a variety of usages, including data storage, device interconnectivity, and communication. Protecting this type of data stored in clouds is of utmost importance, as this data is often sensitive and personal in nature. The leading cybersecurity companies that specialize in this field are Akamai, Barracuda Networks, Citrix Systems, F5 Networks, Fortinet, HP Enterprise, IBM, Imperva, Qualys, Rapid7, Trend Micro, CloudFlare, NSFocus, Trustwave (SingTel), Cyren, CloudPassage, CliQr, and WhiteHat Security.
Dwell times	Dwell time refers to the time from compromise to detection. Reducing the dwell time is important because it reduces the risk of a zero-day threat (a vulnerability that is exploited by a hacker before the security vendor becomes aware of its existence). Most corporations (and their insurers) are expected to get dwell times as close to zero as possible. The fact that dwell times remain high demonstrates that growth prospects for the security industry remain extremely positive.
IoT	As more things become connected to the internet, cybercrime could shift to connected fridges, connected cars, drones, and industrial machines. In the race to create an app for every physical product, many companies are overlooking basic security features. Medical devices also employ IoT technology for connectivity and data sharing. The IoT could lead to a dramatic extension of the attack surfaces that hackers can target within a typical company. The Dyn attack is a possible example of things to come.
Cloud Security Alliance	The Cloud Security Alliance, a group that most major technology companies are a part of, now operates in almost every country. It is an industry body that aims to share intelligence on cybersecurity issues in an open environment and to jointly create large-scale, self-learning cybersecurity systems based on open standards. This could enable its collaborators to build a collective wall against emerging cyber threats. The Cloud Security Alliance regularly publishes learning materials targeted at the healthcare industry, and is a solid resource for healthcare cybersecurity awareness.
Android fragmentation	Android handsets have long been susceptible to serious security breaches because Android is open source and Google does not control the software update process for most of the world's Android smartphones. As such, when a security breach occurs, Google's ability to quickly patch the breach is limited. Instead, it is the device makers or telecom operators that decide if, when, and how to release software updates. In October 2016, Google took a big step to fix this Android fragmentation problem by introducing Pixel, a smartphone with hardware and software that is entirely controlled by Google. It is expected that Google will make Android proprietary, just like Microsoft Windows or Apple iOS, but that option is likely several years away. In the meantime, hundreds of millions of Android smartphones remain vulnerable to attack because their owners have not or cannot download the latest Android software updates from Google. By the end of 2019, Android fragmentation was still a problem, with a large number of software versions being utilized. Android is gaining popularity as a platform for mobile health, and as such, this fragmentation will be a cybersecurity issue until it is dealt with.
Mergers and acquisitions	The larger software conglomerates—IBM, Oracle, SAP, Microsoft, and Alphabet—are all in a race to build software ecosystems. Cybersecurity remains their weakest link. For networking equipment makers like Cisco, security is also seen as a weak spot in their offering. There have been continued mergers and acquisitions (M&As) in this sector among the big software houses, internet ecosystems, and networking equipment makers, thus strengthening their cybersecurity capability, especially in unified threat management and AI. The following cybersecurity companies are expected to be acquired within the next few years: Barracuda Networks, Check Point Software, FireEye, Fortinet, Imperva, Palo Alto Networks, Qualys, Rapid7, SecureWorks, Sophos, and TrendMicro.

Trend	What's happening?
Geopolitics	Geopolitical tensions in the South China Sea, the Middle East, Ukraine, and elsewhere mean that the world is likely to witness a new wave of cyberattacks. Many could be zeroday attacks, including some that may be state-sponsored. In October 2016, the US government formally accused Russia of interfering in the US presidential election held on November 8, 2016, by hacking into Democratic Party emails and releasing them on WikiLeaks in advance of the vote. Several governments are setting up new military cyber command divisions that could put cyber warfare on an equal footing with combat divisions in air, land, sea, and space. The Edward Snowden revelations forced Silicon Valley's technology firms to show the world that they are not controlled by the US military. The result is that Silicon Valley now co-operates much less with the US Department of Defense than at any time since before the Vietnam War. Military contractors see this as an opportunity. The two military contractors branching out the fastest in the commercial cybersecurity space are BAE Systems and Raytheon (which owns ForcePoint). In the healthcare sphere, geopolitics impacts cyber risk when medical devices become involved; for example, opposing parties could use cyber-vulnerabilities within medical devices to bring down the device and assassinate its user, thereby committing "cyber-assassination".
Bug bounty programs	In August 2016, Apple became the latest big tech company to introduce a bug bounty program. It will pay cybersecurity professionals for finding holes in Apple's software and reporting these vulnerabilities to Apple so it can fix them before criminals use them to hack into Apple devices. Other companies such as Google, Microsoft, and Facebook all have their own bug bounty programs, and healthcare systems are beginning to adopt them as a security measure as well. As the IoT gains traction, more and more non-tech companies could become vulnerable to cyber hacking. The scale of bug bounty programs is expected to rise in the coming years. The larger, cash-rich tech titans are able to pay bigger bounties, enabling them to patch up holes in their software quicker than smaller rivals.

Source: GlobalData

Corporate Governance Trends

Trend	What's happening?
California's own GDPR	The May 2018 introduction of Europe's GDPR has proved to be a worldwide catalyst for data protection regulation, with several countries following suit. From 1 January 2020, Californian consumers, vendors, and foreign companies selling into the state have to respect the new California Consumer Privacy Act (CCPA). The act has teeth, and its introduction will be monitored closely by tech companies operating in Silicon Valley. However, as with GDPR, corporate lawyers will do their level best to test its scope or find ways around it. Whatever the potential of California's new act, you can bet someone will be working hard to undermine it.
Regulation in Europe	The EU's Directive on Security of Network and Information Systems (NIS) was adopted by the European Parliament on July 6, 2016. Member states had 21 months to transpose the directive into their national laws, and an additional six months to identify operators of essential services to whom the law applies. The EU NIS Directive harmonizes EU cybersecurity regulations. It stipulates that breaches must be notified to a competent authority within 72 hours. The goal was that within two years, Europe could have had the strictest cybersecurity compliance laws in the world. Companies could be fined up to 2%, or revenues of up to €20M ($26M) for breaches of this directive, which could lead to a significant rise in EU cybersecurity expenditure. The directive provides regulations meant to apply to the healthcare sector as well. In addition, the General Data Protection Regulation (GDPR) was approved by the European Parliament on April 14, 2016, and came into effect on May 25, 2018. GDPR sought to protect and empower EU citizen data privacy and enforce structural changes in the way that organizations approach customer data privacy and protection. In order to align with GDPR regulations, health systems have had to make operational and technological advancements. Under GDPR, non-compliant organizations could suffer fines of 4% of their annual turnover or €20M ($26M), whichever is highest. Healthcare facilities have not been exempt from these fines: the first GDPR fine issued was a 400,000 Euro fine against a Portuguese hospital, for three violations of the GDPR.
Regulation in China	China's new national security law aims to foster a secure and controllable internet infrastructure. Initially, it was thought that the law would force many foreign technology companies to hand over their source code and submit to intrusive product testing. Some US companies indicated they would pull out of China altogether to avoid this. Since then, the Chinese government has loosened its proposals somewhat. If such laws are eventually enforced, the main beneficiaries would be domestic Chinese technology companies, who would be operating in an even more protected environment than they have so far enjoyed. China has also implemented specific rules surrounding collection and security of healthcare-related data. These regulations focus on collection, localisation, storage, and transfer of personal health information. In some cases, even the collection alone of personal data is subject to strict authorization.
US federal plan will drive more government cyber spending	A bipartisan commission charged with recommending a reorganization of the US federal government's cybersecurity operations wants to see the appointment of a national cyber director. The recommendation for the new position comes from the Cyberspace Solarium Commission, which has argued the appointment is needed to ensure federal agencies are adequately protecting themselves against cyberattacks. However, the White House is expected to veto the idea, having eliminated a cybersecurity coordinator position in 2018. Among its other recommendations, the Commission wants to reform the US government's structure and organization for cyberspace. It also recommends Congress create a cyber state of distress that is accompanied by a cyber response and recovery fund. The Commission's recommendations are likely to lead to an increase in both US government cybersecurity spending and the speed at which software can be procured.
Cyber bills pass through US Congress	The US government has stepped up its legislative activity and enacted several laws to try and reduce its vulnerability to cyberattacks. Cybersecurity-related bills for Washington departments and agencies to prevent cyber breaches include the Cybersecurity Vulnerability Remediation Act, which would allow the Department of Homeland Security's Cybersecurity Agency to issue protocols to mitigate vulnerabilities, the Federal Risk Authorization and

Trend	What's happening?
	Management Program, which enables the US federal government to access cloud computing services using a risk-based approach, and the 2019 IoT Cybersecurity Improvement Act, which gives the National Institute of Standards and Technology the authority to manage IoT cybersecurity risks for devices acquired by the federal government. According to a report published in June 2020 under the Federal Information Security Modernization Act of 2014, the number of cybersecurity incidents recorded at US federal agencies in 2019 was down by 8%, at 28,581. However, not all agencies could claim to be successful in their efforts. The National Aeronautics and Space Administration (NASA) had 1,468 cyber incidents in 2019, compared with 317 in 2018.
CISO	Many established enterprises and data-driven start-ups have recently appointed their first CISO. A CISO's role is to protect a company's assets (both physical and digital) from cyber-attack. JP Morgan did not have a CISO when it was breached in 2014. Sony's CISO had only been in the job three months when its media arm was hacked. Many hospitals have also appointed CISOs to oversee cyber risk management within health systems. Larger hospitals are more likely to have appointed a CISO, as they have more data to protect and are more able to justify the expense. The average stay of a CISO is under 1.5 years, as it is difficult to be successful in the role in the current environment.
Executive board awareness	Business executives still think of the most important business risks as technology risk, human capital risk, interest rate risk, political risk, competition risk, and regulatory risk. In the next few years, cybersecurity risk should rise to number one or two. As such, cybersecurity expenditure could rise across several industries in the near future.

Source: GlobalData

Cybersecurity Trends in Healthcare

Trend	What's happening?
Prevention begins with endpoint education	Employees are on the front line of defense against cyberattacks, since endpoint security systems can fail to capture all threats. This means that cyber risk education is vital. Employees should be educated about how their day-to-day activities interact with the organization's security defenses. They need to be informed about the ramifications of sharing sensitive account credentials or installing unsanctioned applications, and the dangers of opening unknown email attachments. Healthcare organizations continue to fall short on educating their staff about cyber threats due to the fragmented nature of healthcare, and few employees are aware of potential gateways for cyber threats into the enterprise network. Endpoints are the weakest link in a clinical setting. Given the increasing use of devices such as mobile phones, personal computers (PCs), and desktops, it remains a key challenge for IT departments to secure the enterprise network from ransomware attacks and malicious access without interrupting daily operations. Healthcare organizations would reap the benefits of having rigorous and effective endpoint security measures to reinforce their security—particularly, by having a centralized management portal to control and manage the enterprise's endpoints and network. All healthcare organizations should seek ongoing training programs for data privacy, protection, and cybersecurity. Such showcase sessions will raise the profile of the cybersecurity challenge from just another IT issue to that of a collective business responsibility. Vendors should shore up these efforts by simplifying cybersecurity language. Vendors should also position themselves to support carriers by creating and implementing guidelines (such as housekeeping and best practice) for employees' access to IT systems and networks. In addition, there should be stricter off-boarding practices to ensure that network permission is stripped from employees who leave the firm.
Multi-factor authentication uptake is on the rise, albeit slowly	Multi-factor authentication is widely valued in healthcare settings and its adoption continues to rise. Passwords are the most common authentication tools in healthcare, yet they are easy to hack, particularly when employees are careless about sharing them and changing them. While multi-factor authentication is not new, its uptake among healthcare is increasing slowly as companies realize the importance of two-factor authentication for data sharing among employees, patients, and supporting clinical staff. On all counts, securing the patient database and electronic patient record (EPR) is crucial for healthcare. By working with security vendors, healthcare organizations can facilitate the implementation of two-factor authentication at a low cost—using various platforms such as physical tokens, soft tokens, and smartphones—as well as its integration with internal systems. Enabling two-factor authentication has become key for healthcare providers as they look to protect patient data from unauthorized access and tampering.
Biometrics	Biometric identity management is currently being explored by more advanced healthcare organizations and pharma companies. GlobalData expects the use of biometrics in healthcare organizations to grow over the next three to five years, particularly as a way to offer extra cybersecurity layers, control identity management and access, and offer a smoother clinical experience. The main barrier to implementing biometric measures for patients remains privacy and security. Thus, biometric measures are currently limited to clinical staff as opposed to a larger personalization agenda in healthcare for patients.
Network segmentation reinforces providers' security	Network segmentation, which involves separating each network and making it visible only to those who have the right to access it, is not a new practice. It is gaining popularity as a way for carriers to control levels of access to sensitive data in the context of data sharing between patients and healthcare networks. The greatest benefit of network segmentation for healthcare organizations and the wider healthcare ecosystem is that it can limit access to medical data and ensure compliance with regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Network segmentation can limit the vulnerability of legacy systems that are currently impractical to upgrade or are in the process of being upgraded. Many attacks start with phishing emails to gain access to the organization's network, then make their way through back-office systems and into critical infrastructure. Network segmentation can help restrict the movement of the threat across the networks.

Trend	What's happening?
Real-time analytics detect advanced threats	Healthcare organizations are working towards breaking down data silos for more effective sharing across healthcare networks. Simultaneously, vendors are continuously striving to add new channels and devices that plug into the enterprise network, which results in more data flows. Analytics is positioned as a core enabler to help vendors achieve superior customer service. While healthcare providers already apply analytics to some extent to improve population health management and clinical efficiency, it has not yet been used to ramp up an enterprise's security position. Behavioral analysis is a particularly niche technique within the healthcare sector; in other industries, it has already proven to be effective against outsider and insider threats by detecting abnormal activities. Real-time analytics are considered more powerful, as legacy SIEMs can meet compliance requirements but are no longer well-placed to detect advanced threats. Vendors will want to consider responding to the perceived shortcomings of SIEM—namely, that the systems can be expensive to deploy and complex to operate and manage. Some vendors advise that SIEM is no longer sufficient in its own right, given that malware can already penetrate anti-virus software.
Push for increasing medical device cybersecurity regulations	In the age of big data, novel medical devices are increasing in connectedness to the Internet, other medical devices, and healthcare networks. Examples of connected medical devices include infusion pumps, implanted pacemakers, and insulin pumps. Connected devices can receive data, send data, or both. The use of connected devices brings the risk for hacking directly to patients. As such, considerations need to be made to secure not only the device itself, but also the device's stored data and information. Federal governments around the world did not have many ways to regulate the levels of cybersecurity for medical devices 10 years ago. The EU has recently initiated the GDPR, which mandates that any organization wishing to conduct business in Europe must follow five key GDPR requirements, and European regulators have published cybersecurity recommendations for many industries including medical devices. Similarly, over the last five years, the FDA has issued two guidance documents for medical device manufacturers: "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" in 2014, and "Postmarket Management of Cybersecurity in Medical Devices" in 2016. These documents are not enforceable regulations, but rather tips and suggestions for manufacturers that are incorporating wireless capabilities into medical devices. In July 2017, a bill called the "Medical Device Cybersecurity Act of 2017" was proposed in the US Senate. This bill aims to amend the Federal Food, Drug, and Cosmetic Act to require the FDA to create a cybersecurity report card for connected medical devices, which manufacturers must then include in a premarket approval application. More recently, the FDA released the Medical Device Safety Action Plan in April 2018, which includes notes on advancing medical device cybersecurity through updated premarket guidance and requirements, as well as the establishment of a CyberMed Safety Analysis Board (CYMSAB). Although governing bodies largely leave cybersecurity responsibilities to device manufacturers, more stringent regulations and guidelines will encourage manufacturers to incorporate cybersecurity as a core component of device development rather than as a later addition, which will strengthen medical devices against cyber hacks.

Source: GlobalData

Industry analysis

The third wave of cybersecurity

We are currently in the third wave of the cybersecurity industry, and it is the most challenging in terms of technology and scale.

The initial wave comprised the earliest days of the internet until 2005, when the internet's spread was small and what useful information there was on it was largely research papers. Threats against the computer network were primarily hackers trying to get access to US military systems.

From 2005, the rise of mobile and the cloud saw attackers develop increasingly sophisticated techniques to bypass cyber defenses. The HTTP web protocol, whitelisted by firewalls, became the method of choice to deliver malware. The fledgling cybersecurity industry struggled to deliver sufficient anti-virus signatures to combat the 500,000 new pieces of malware being created monthly, while mobile and cloud technology created hundreds of new entry points for organizations to worry about. Attacks on organizations were designed to avoid detection, with the term advanced persistent threat coined to describe cyberattacks in which intruders gained access to a network and remained undetected.

In response, next-generation firewalls (which attempt to block undesirable HTTP content) were created, and defensive measures were employed that relied on spotting malicious behavior rather than producing anti-virus signatures. The move towards centralizing visibility of assets first led to the creation of security information and event management systems (SIEMs), while cloud and mobile security defensive postures were improved with the development of cloud access security brokers (CASBs) and mobile security platforms.

A need for vigilance and resilience

The third wave of cybersecurity is epitomized by a spaghetti-like array of assets that include traditional infrastructure, applications, managed and unmanaged endpoints, the IoT, and cloud services, with each targetable by several attack methods. Phishing targets users and eats away at any security weaknesses in the relationship between an organization and its supply chain. Typically the security standards in organizations' supply chains are lower than in the organization itself. Another concern is how corporate supply chain trust relationships – and indeed corporate technologies such as VPNs, which were once considered secure - can be used to launch attacks, if the credentials of trusted individuals become compromised. The enterprise attack surface, already massive, is growing rapidly with the forced move to greater remote working in 2020.

To counter this, cyber-aware organizations must adopt cybersecurity measures that allow them to be resilient, vigilant, and secure, that keep their employees and partners identified and trusted, and allow the organization to remain risk-aware. In general, organizations fail to understand the landscape they are trying to defend. Consequently, defensive decisions aren't taken, and actions are not prioritized, leaving enterprises open to compromise.

Predictive risk assessments

The latest wave of innovation involves the adoption of a more proactive defensive approach, using machine learning and AI to discover and analyze the growing landscape for attacks. The target is to have more comprehensive, predictive assessments of breach risk that recognize and prioritize the necessary steps to avoid breaches.

The reality is that all software is at risk through human error and inadvertent security holes, which are there to be exploited. Other defensive measures being introduced to improve organizational resilience are zero trust techniques and the use of DevSecOps, where engineers continuously monitor, attack, and determine defects.

Chief executives and chief financial officers want to ensure they get value for money from their cybersecurity investments, which means cybersecurity spending is moving from being project-oriented to becoming outcome-oriented. What that means is investments made to keep the organization secure must demonstrate a measurable reduction in breach risk, particularly with spending under scrutiny post-COVID-19.

Market size and growth forecasts

Security products are typically delivered through software and services, rather than hardware.

The explosion of available bandwidth, the emergence of cloud computing, and year-on-year improvements in the price-to-performance ratios for commodity hardware have all combined to ensure that technology functionality previously only achievable using specialist hardware can now be delivered using a combination of general-purpose computing hardware and software.

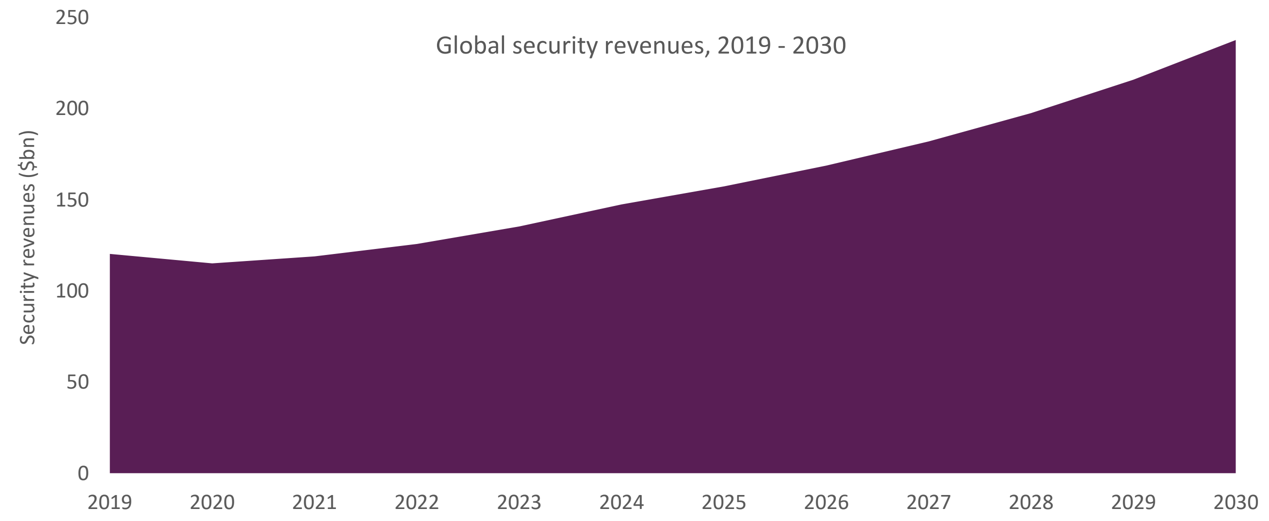
In the world of software defined everything (SDE), the details of the underlying hardware become irrelevant, and the focus shifts to a virtualized software layer instead. In this world, it no longer makes sense to think of servers, or even central processing units (CPUs), with the focus now on the resources that an application requires. The environment manages the rest. Software defined networking (SDN) is a part of this new world, driving change in the network security landscape.

Network security company Palo Alto is a hardware company that is diversifying into software and services because the future of network security is now widely considered to be in the cloud. Other vendors are typically mixing software and services in their client offerings. For example, Dell Secureworks' managed security service is paired with Red Cloak, a cloud-based suite of software for threat detection and response.

Companies worldwide are expected to spend $115.1bn on cybersecurity in 2020, with $45bn (39%) coming from managed security services, according to figures produced by GlobalData. GlobalData expects the global cybersecurity industry will see a drop in security spending in 2020 as a result of the COVID-19 pandemic. By 2030, global security revenues will have recovered and are expected to have climbed to $237.7bn, growing at a CAGR of 6.4% between 2019 and 2030. Managed security services will continue to account for around 38% of total cybersecurity revenues.

By 2030, global security revenues will have reached nearly $238bn

Revenues are expected to grow at a CAGR of 6.4% between 2019 and 2030



Source: GlobalData.

Note: Our security revenues forecast covers hardware, software and services. Hardware such as content-filtering and anti-spam appliances, firewalls and VPN appliances, intrusion prevention systems, multi-factor authentication, network access control, and unified threat management appliances. Software includes application security, data protection, endpoint security platforms, fraud prevention and transactional security, identity & access management, messaging security, network security, security intelligence and event management, server security, and web security. Managed security services include business continuity, DDoS mitigation, emergency incidence response, governance, risk and compliance, identity management, patch management, managed authentication, and managed detection and response services.

AI technologies are changing cybersecurity

The old approach of running a human-led security operations center (SOC), using SIEM or log management tools to correlate and highlight alerts for manual follow-up and investigation, is outdated.

A more effective approach is to use intelligent automation to alleviate the data burden facing today's analysts. AI and ML technologies improve threat intelligence, prediction, and protection. They also enable faster attack detection and response, while reducing the need for human cybersecurity specialists (which are in desperately short supply).

AI and ML's most significant use is in helping security operations understand what to do with security threats when they meet the enterprise. That is because the increasing complexity, sophistication, and persistence of cybercriminal activity requires already under-pressure security operations teams to rethink how best to use people, processes, and technology.

Two examples of ML in cybersecurity are malware classification and network traffic analysis.

In malware classification, evolving and self-changing signature-based malware detection has a catch-rate below 50%. Modern anti-malware solutions usually combine behavior analysis and advanced static analysis to keep catch-rates high. Behavior analysis can use ML and non-ML algorithms to identify whether running malware at execution shows suspicious activity, such as trying to access the registry or snooping in the memory.

Although behavior is usually a good indicator of malicious intent, it can only be observed and detected during run-time (using dynamic analysis). Ideally, organizations would prefer to prevent malware from executing at all. So several endpoint and breach detection products are using ML models to classify malware before it executes (static analysis). In contrast to hard-matching a malware hash signature, ML models rely on thousands of features of a malware sample to make a statistical verdict. An ML algorithm can learn and weigh features itself and discover relevant properties of malware samples that even the best malware experts cannot find. Once a model has been trained on malware samples it can be kept fresh through continuous feeding of new samples.

ML is used in network traffic analysis to detect attackers that have breached the perimeter and are now active in the network. Based on packet header and flow data information (such as protocol, number of bytes, rates, counters) ML-based traffic analysis systems can employ both supervised and unsupervised learning algorithms to classify and cluster attacks. Anomaly detection algorithms are used in network traffic analysis to establish a baseline of normal behavior and then detect deviations from it. Network detection needs to have some form of memory built in to retain the context of activities over time, which is crucial to identify slow-moving attacks.

Research in 2018 by the Ponemon Institute on the value of AI in cybersecurity discussed the extent to which AI can save time and reduce pressure on corporate cyber teams. Ponemon found that AI has reduced application security risk in organizations that have achieved greater deployment of these technologies, helped decrease the complexity of organizations' security architecture, and improved the ability to detect previously undetectable zero-day exploits.

Most significantly, AI has reduced the time taken to deal with cyber exploits. The average cost of not using AI to address cyber exploits is more than $3m versus just over $800,000 if AI is used. Thus, a company can potentially save an average of about $2.5m in operating costs.

Labor hours spent containing cyber exploits each week	Not facilitated by AI	Facilitated by AI	AI advantage
Organizing and planning approaches to cyber defense	25.32 hours	16.05 hours	9.27 hours
Capturing actionable intelligence about cyber exploits and malware infections	80.20 hours	41.11 hours	39.09 hour
Investigating and detecting application vulnerabilities	195.88 hours	70.48 hours	125.40 hours
Investigating actionable intelligence about cyber exploits or malware	66.28 hours	24.23 hours	42.05 hours
Cleaning, fixing, and/or patching networks, applications and devices (i.e. endpoints) damaged/infected by exploits or malware	212.89 hours	39.63 hours	173.26 hours

Labor hours spent containing cyber exploits each week	**Not facilitated by AI**	**Facilitated by AI**	**AI advantage**
Documenting and/or reporting on the cyber event.	25.07 hours	15.91 hours	9.16 hours
Time wasted by security staff members chasing erroneous or false positives	400.83 hours	41.42 hours	359.41 hours
Unplanned downtime due to cleaning, fixing or patching of malware-infected networks, applications and devices.	3.95 hours	1.90 hours	2.05 hours
Total hours per week	1,010.42 hours	250.73 hours	759.69 hours
Total hours per year	52, 541.84 hours	13,037.96 hours	39,503.88 hours
Estimated total cost per year	$3,283,865	$814,873	$2,468,992

Source: Ponemon Institute 'The Value of Artificial Intelligence in Cybersecurity' report

Despite the positives of implementing AI, there are significant obstacles to its widespread use, of which staffing and internal expertise are the most significant. Half of the respondents in the Ponemon study said too many staff were required to implement and maintain AI-based technologies, while 45% said they lacked the internal expertise to validate vendors' claims.

A further problem is cybercriminals themselves using AI and ML to create distributed, targeted malware and attacks. The fear is that attackers' use of data from both successful and unsuccessful breaches and vulnerabilities will lead to a new generation of super-malware. In the future, there may be fewer, more successful attacks that result in more significant damage.

Moving towards the edge

To counter the cyber threat, the cybersecurity industry and the businesses it is trying to protect are re-orienting their security programs by distributing controls towards the edge, driven by the technology shift to cloud computing and edge computing. Organizations are also trying to adopt a zero trust model, treating the individual user or entity separately in terms of their security score.

With the increase in popularity of edge devices - smartphones, tablets, smartwatches, etc. - organizations are now considering an additional tenet of identity. This not only looks at the device itself but also the identity of the person using it, plus short-lived data about what is going on in the user's IT session. For example, what time zone is it taking place in, and in which geography?

The reason for this approach is to understand the individual and their identity and know what is normal behavior for that individual. It may be normal for an individual to access his email from London at 9am each day but abnormal for them to log-in from Minsk at 1am. Equally, someone who normally logs into Salesforce during working hours every day trying to export an entire database at 3am should set off alarm bells.

The need to help customers gain access to and understand this information has led to competition among vendors such as VMware, BlackBerry, Proofpoint, and FireEye to become organizations' single security platform of choice because companies don't want numerous security agents and tools.

Understanding the malware threat

Without cybercriminals, there would be no need for a cybersecurity industry. The malware industry has evolved from something that was originally supposed to be fun, with hackers creating programs to gain access to unauthorized places, to an industry that is technically advanced, ruthless, and operates as a business.

Malware organizations are now starting to stratify themselves and their attacks, involving low-level operators using commodity tools or even commercial off-the-shelf software for their campaigns. They will include tools used in penetration testing, such as PowerSploit, PowerShell Empire, and Cobalt Strike, to carry out campaigns at a lower level.

The same hacking organizations will then save their more sophisticated toolchains – their A-teams – for more targeted operations. Sometimes they will use both approaches, adopting an initial 'spray and pray' technique with the commodity tools, and then using the more targeted operations once they have established beachheads in various networks as part of a broader operation.

In that respect, the organizations – examples would include Lazarus Group, Fancy Bear, and Carbanak (also known as Fin7) - are operating as a company, distributing the commodity tasks to lower levels and saving the higher brain functions for other, more valuable targets.

The rise and rise of ransomware

The most successful – and most lucrative – current means of attack is ransomware, a type of malware that prevents access to a computer system or data until a ransom is paid to the attacker. It is used in various forms, including as a service and as a weapon on behalf of nation-states.

In ransomware as a service, someone with limited technology skills can either buy an exploit kit to help them create software, or they can approach ransomware authors who will take a percentage of a ransomware payment. This method is typically used to commit financially motivated, low-level cybercrime. There were several examples of this in 2019 with extensive ransomware attacks against state and local governments, particularly in the US. Cities attacked included Baltimore, Albany, and Lake City. Baltimore has said the ransomware attack it suffered will cost it at least $18m.

Ransomware as a weapon is typically used to attack public services. It is primarily motivated by geopolitical rather than financial goals. Examples include the Russian state deploying NotPetya against Ukraine, and WannaCry, a ransomware kit created by North Korea, which hit around 230,000 computers globally, including a third of National Health Service trusts in the UK.

The costs to organizations from ransomware are staggering. Research by Cybersecurity Ventures estimated that global ransomware damage costs will reach $20bn by 2021, 57 times more than in 2015.

The organizational cost of an insider threat

Insider threats to organizations are increasing. According to the Ponemon Institute, between 2018 and 2020, the average number of incidents involving employee or contractor negligence has increased from 13.2 to 14.5 incidents per organization. The average number of credential theft incidents has almost tripled over the past two years, from 1.0 to 2.7 per organization. Some 60% of organizations have more than 30 incidents each year.

Breaches caused by negligent insiders represent the bulk of internal incidents, but a determined insider attack is both difficult to spot and expensive to solve. According to Ponemon, it takes an average of 77 days to contain each insider threat incident. Only 13% of incidents are contained in less than 30 days.

Most intentional internal breaches are caused by employees sharing work data to personal systems, often because they are trying to get a job done. However, this can still breach company policy and put data at risk. An Egress Insider Data Breach survey in 2020 found that 32% of incidents were caused in this way, with employees leaking data to a competitor resulting in 22% of incidents, and employees leaking data to cybercriminals 21%. In 18% of cases, the reason was employees taking data to a new job.

The Egress survey found that despite years of warnings about the risk of insider cyber threats, the number of incidents and the associated costs continues to rise. The burden of responsibility for data protection is also not being shared across organizations, with senior employees often found to be the most irresponsible.

Employees tend to exhibit different breach personas informed by their roles and seniority in the organization. The personas range from careless clerical staff sending accidental emails to devious directors whose proprietary view of data cultivates a cavalier approach. A cultural shift is required if companies are to get on top of the insider threat.

Operational technology and critical national infrastructure attacks

There have been several warnings of the potential impact of cyberattacks on the Industrial Internet and critical national infrastructure (CNI), but a February 2020 attack on a gas compression plant in the US will concentrate minds as to the extent of the disruption cyberattacks can cause.

The cyber incident, which shut down the plant for two days, was a ransomware attack on a natural gas facility and progressed because the perpetrator was able to jump from the facility's IT network onto the operational network when an employee mistakenly clicked on an email link.

According to an alert issued by the Cybersecurity and Infrastructure Security Agency (CISA), loss of availability occurred on human-machine interfaces, data historians, and polling servers. The attack was limited to Windows-based systems and did not impact any programmable logic controllers responsible for directly reading and manipulating physical processes. Surprisingly, the victim organization's emergency response plan did not specifically refer to how it would cope with cyberattacks, but only threats to physical safety.

The failure to segment OT and IT networks was a critical factor in the attack. Organizations would normally ensure that access to the OT network is sufficiently protected to prevent an attack from being successful.

The ease with which the gas compression plant was attacked highlights the damage that can be caused by a successful attack on industrial control systems (ICS) and SCADA within CNI. The attack is more likely to come from state-sponsored groups, which might target such systems as part of international conflicts. The most famous attack on a SCADA facility was the Stuxnet worm, which attacked an Iranian nuclear facility in 2010.

The threat to infrastructure systems has prompted industrial and cybersecurity vendors to work more closely to create cybersecurity defenses for power plant operators. Thales and GE Steam Power are to perform joint training for customers that operate power plants.

Cybercrime is a global affair

In the West, the countries most commonly associated with cybercrime include Russia, China, and Iran, but analysis of the top 10 attack originators over the last five years shows a much broader global picture.

LexisNexis Risk Solutions, in its July-December 2019 cybercrime report, found that the top 10 attack originators are spread across five continents, with the US, Canada, and the UK joined by growth economies Mexico, India, and Bangladesh. This research highlights how truly global cybercrime has become. Nation-state attacks continue, usually for geopolitical reasons, with Australia warning in June 2020 that its organizations were being targeted by a "state-based cyber actor."

Top 10 global attackers by country of origin

2019 ranking	Country	2018 ranking
1	US	1
2	Canada	2
3	UK	5
4	Brazil	4
5	Germany	3
6	Mexico	12
7	France	7
8	India	6
9	Italy	10
10	Bangladesh	17

Source: LexisNexis Risk Solutions, GlobalData

Solving the cyber skills shortage

One of the biggest challenges facing the cybersecurity industry is a worldwide skills shortage, which makes recruiting cybersecurity experts extremely difficult.

The scale of the global IT security skills shortage was revealed in a report by the International Information System Security Certification Consortium, or (ISC)². The organization compiled its Cybersecurity Workforce Study from interviews with over 3,200 security professionals around the world. In November 2019, the total number of unfilled positions stood at 4.1 million, up from 2.9 million in November 2018.

The report suggested four key strategies to help organizations tackle such shortages, including in-house training and development, and setting applicant qualification requirements at the right level to attract the widest response.

Among the jobs most in demand are

- cybersecurity managers and administrators, who are typically responsible for implementing and overseeing the cybersecurity program for a given system or network;
- cybersecurity consultants, who play the role of both an attacker and a defender to exploit vulnerabilities and detect weaknesses in an organization's computer network, systems, and applications; and
- cybersecurity analysts, who keep tabs on threats and monitor their organization's network for any potential security vulnerabilities. Using information collected from threat monitoring tools and other sources, they identify, analyze, and report on events that have occurred or may occur on the network.

Use cases

The case studies listed below demonstrate how healthcare companies are using cybersecurity for improved outcomes.

UK's NHS: The Security Operations Centre

- In November 2017, NHS Digital announced a £20M ($26M) project to boost its ability to support the NHS with its data security. The newly formed Security Operations Centre (SOC) provided enhanced monitoring of national services across health and care, and also enabled NHS Digital to offer specific advice and guidance to local NHS organizations. This investment included a monitoring service that analyzes intelligence and shares guidance, advice, threat intelligence, and remediation to relevant contacts in healthcare, on-site data security assessments for NHS organizations to identify any potential weaknesses, specialist support for any NHS organization that may have been affected by a cybersecurity incident, and ongoing monitoring of NHS Digital national systems and services.

- The founding of the SOC is one of NHS Digital's moves to ramp up its cybersecurity efforts in the wake of the WannaCry attack, which caused widespread disruption to global IT systems and affected at least 81 of 236 NHS trusts in England.

- In February 2018, NHS Digital added £10M ($13M) to its prospective cybersecurity contract in hopes of procuring the services of an external cybersecurity partner for its SOC. The partner would be charged with providing additional support to NHS Digital's in-house security team, including cyber penetration testing and real-time monitoring of NHS networks.

- In October 2018, NHS Digital appointed IBM as its cybersecurity partner, under a three-year contract. As part of this partnership, IBM security analysts have worked closely with NHS Data Security Centre analysts to map out the cyber threat landscape and develop a plan to address these threats. Since the partnership started, IBM has helped NHS Digital block tens of millions of suspicious transactions and has significantly improved response times when cyber attacks do occur.

ICU Medical: the First Medical Device Manufacturer to Obtain Certification Under the UL CAP

- ICU Medical is a medical device manufacturer based in San Clemente, California, US, which is in the business of designing and creating a complete line of safe and reliable intravenous (IV) therapy products for use across the continuum of care. Their products include needle-free IV connectors and sets, IV pumps, IV catheters, and monitoring systems.

- In June 2018, ICU Medical became the first medical device manufacturer to obtain certification under the Underwriters Laboratories Cybersecurity Assurance Program (UL CAP), a new cybersecurity management program from UL designed to minimize risks by creating standardized, testable criteria for assessing software vulnerabilities and weaknesses in order to help reduce exploitation, address known malware, enhance security controls, and expand security awareness. The certification was for its Plum 360 drug infusion system that provides full interoperability with patient electronic health records (EHR), reducing the need for manual input and transcription of infusion data to better manage patient safety and clinician workflows. In addition, Plum 360 features closed-system air management to minimize patient therapy interruptions, contamination risk, and exposure to hazardous medications.

- The UL assessment uses ANSI UL 2900 medical device cybersecurity standards to assess key categories including quality management documentation, product design and use, security risk management (including safety-related controls), managing known vulnerabilities with exposures, and managing software weaknesses, as well as measures to address potential zero-day vulnerabilities.

- Since ICU Medical, many other medical device manufacturers have also worked to obtain UL CAP certification. In December, 2018, Becton, Dickinson and Company announced that they had completed an enterprise level cybersecurity assessment from UL. In March, 2020, Royal Philips announced that they were the first medical device manufacturer to receive a new UL certification (UL IEC 62304).

Abbott: Cybersecurity Patches for Pacemakers

- In 2017, Abbott began updating its firmware for pacemakers, programmers, and remote monitoring systems to fix severe cybersecurity flaws in the devices. The latest update, approved by the FDA in April 2018, applies to about 350,000 of Abbott's implantable cardioverter defibrillators and implantable cardiac resynchronization therapy defibrillators.

- The devices were originally manufactured by St. Jude Medical, which Abbott acquired in January 2017. St. Jude went under fire for failing to reveal a deadly defect with their defibrillators and continuing to ship the devices despite knowing the issues with rapid battery depletion. St. Jude also failed to inform management and a medical advisory board about the battery issues, which led to the death of a patient. Additionally, their MerlinHome Monitoring System platform, which registers their defibrillators, was riddled with cybersecurity flaws that could end up draining battery life or manipulating a pacemaker's beat rates. Because of the cybersecurity concerns, the FDA issued its first cybersecurity recall for a medical device.

- Since acquiring St. Jude Medical, Abbott has received an FDA warning letter charging with failing to reveal the deadly defect.

Animas Corporation, a Johnson & Johnson Company, and Medtronic: the Announcement of Cybersecurity Vulnerabilities with Insulin Pumps

- In October 2016, Animas Corporation disclosed to users of the Animas OneTouch Ping insulin pump that unauthorized users could potentially gain access to the pump through its unencrypted radio frequency communication system.

- Animas, in the letter that was sent to its customers, said that they investigated the issues and worked with the appropriate regulatory authorities and security experts to remedy the situation. They also informed customers that they could turn off the radio frequency feature of the pump, but by doing this, the pump and meter will no longer communicate, and the blood glucose readings would need to be entered manually on the pump.

- In 2019, the FDA issued a warning regarding Medtronic MiniMed insulin pumps, due to cybersecurity vulnerabilities that could allow someone other than the patient to access a pump and change its settings. Later in 2019, the FDA issued a Class I recall on the remote controllers for Medtronic MiniMed insulin pumps, citing security risks. As of September, 2020, Medtronic still markets certain brands of MiniMed insulin pumps which were unaffected by this recall and presumably have better cyber protection.

Medtronic: Vulnerabilities Detected in Implantable Cardiac Devices, Programmers, and Home Monitors

- In March, 2019, the FDA issued a safety communication citing cybersecurity vulnerabilities within Medtronic's wireless system that connects its implantable cardiac devices with their programmers and home monitors. The reason for these cybersecurity vulnerabilities was that the Medtronic did not use encryption, authentication or authorization within its wireless telemetry system. As a result, the system was exposed to external access, meaning that someone other than the patient or the patient's physician could theoretically access the devices, programmers or monitors and change their settings.

- Medtronic, in efforts to mitigate the issue, released a first round of software updates for these devices in January, 2020. Medtronic also released a second round of software updates in June, 2020, increasing their device coverage. In addition, Medtronic issued several recommendations to users with the affected devices in order to minimize the risk of exploitation of these vulnerabilities.

TRIMEDX and Medigate: Strategic Partnerships Strengthen Cybersecurity in Medical Devices

- More and more medical devices are being designed with integration into cloud networks for the purposes of data collection and sharing. According to Deloitte Development LLC in July 2018, 68% of medical devices are projected to be connected devices by the year 2025. As the number of connected devices grows, the need to ensure data protection and cybersecurity grows as well. Medical device manufacturers have sometimes been slow to adopt solid cybersecurity practices, leaving their devices exposed to cyber attack. Health systems are often even further behind, since they have so many ways in which they need to prioritise their resources.

- In response to the growing need for cybersecurity of medical devices, some companies are entering into strategic partnerships to improve their offerings. In July, 2020, Healthcare technology company TRIMEDX announced a strategic partnership with Medigate, with the goal of meeting the unique demands of clinical asset management and medical device safety and security for healthcare systems. TRIMEDX is a leader in clinical asset management and brought its new CAM Advanced and CYBER Advanced product offerings to the partnership. Medicate is a dedicated medical device security and asset management solution firm.

- Through their partnership, TRIMEDX and Medigate deliver an integrated solution that merges the TRIMEDX CAM Advanced and CYBER Advanced solutions with Medigate's real-time visibility, utilization data and threat/vulnerability detection. This type of partnership sets the stage for other companies who specialize in specific aspects of cybersecurity to partner with each other and make their combined offerings more marketable to medical device manufacturers and health systems who are requiring more and more cybersecurity solutions.

Mergers and acquisitions

The key M&A transactions associated with cybersecurity in the last three years are listed in the table below.

Date announced	Acquirer	Target	Value ($m)	Target company description
Sept 2020	Motorola Solutions Inc	Delta Risk LLC	Not disclosed	Provider of cyber security and risk management services
Sept 2020	Check Point Software Technologies Ltd	Odo Security	$30M	Network organization provider
Sept 2020	ThreatConnect Inc	Nehemiah Security LLP	Not disclosed	Cybersecurity platform provider
Aug 2020	Tesserent Ltd	Airloom	$10.62M	Software platform for enterprise security management
Aug 2020	Motorola Solutions Inc	Pelco Inc	$110M	Video security solutions provider
Aug 2020	Apple Inc	Mobeewave	$100M	Secure mobile payments solutions
Aug 2020	Palo Alto Networks Inc	The Crypsis Group	Not disclosed	Cybersecurity and IT service management company
Aug 2020	Konica Minolta Business Solutions USA Inc	Depth Security LLC	Not disclosed	Security service provider
July 2020	Fortinet Inc	OPAQ Networks Inc	Not disclosed	Provider of network security software products
July 2020	Tesserent Ltd	Seer Security	$7.14M	Cybersecurity consultancy firm
July 2020	Welltel (Ireland) Ltd	Novi	$3.37M	Provider of cybersecurity infrastructure, professional services and support
Jun 2020	VMware	Lastline	Not disclosed	Malware protection software
Jun 2020	IBM	Spanugo	Not disclosed	Cloud security posture management
Jun 2020	Microsoft	CyberX	$165M	IoT security
June 2020	BIO-key International Inc	PistolStar Inc	$2.5M	Identity and access management solutions
June 2020	Agora Telecom Inc	FIT Network	$1M	Integrator of electronic security, connectivity and unified communications
June 2020	OneTrust LLC	Integris Software Inc	Not disclosed	Provider of data risk intelligence solution
May 2020	Zscaler	Edgewise Networks	Not disclosed	Secure application-to-application communications for public clouds
May 2020	Cisco	ThousandEyes	$1B	Network monitoring
May 2020	Hebei Baoding Dongfang Paper Milling Company Limited	Baoding Huizhi Ruixing Information Technology Co., Ltd	$3.04M	Provider of healthcare IT solutions

Date announced	Acquirer	Target	Value ($m)	Target company description
Apr 2020	Accenture plc	Revolutionary Security LLC	Not disclosed	Enterprise security for operational technology (OT) and IT systems
Apr 2020	Zscaler	Cloudneeti	Not disclosed	Cloud security posture management
Apr 2020	Rapid7	DivvyCloud	$145M	Cloud management and automation
Mar 2020	Accenture	Context Information Security	Not disclosed	Cyber defense consultancy, including experience in financial services
Mar 2020	Hellman and Friedman	Checkmarx	$1.15B	Security for application development and DevOps.
Mar 2020	Palo Alto Networks	CloudGenix	$420M	Cloud-delivered SD-WAN
Mar 2020	Watchguard Technologies	Panda Security	Not disclosed	Endpoint security
Mar 2020	Motorola Solutions Inc	IndigoVision Group plc	$37.37M	End-to-end IP security management systems
Feb 2020	HP Enterprise	Scytale	Not disclosed	Cloud-native security and zero trust networking
Feb 2020	Symphony Technology Group	RSA (acquired from Dell)	$2.075B	Threat detection and response, and identity and access management
Feb 2020	Aon	Cytelligence	Not disclosed	Incident response and digital forensics
Feb 2020	Advent International	Forescout	$1.9B	Device visibility and control
Feb 2020	McAfee, Inc	Light Point Security LLC	Not disclosed	Browser isolation software provider
Feb 2020	Everbridge Inc	CNL Software Ltd	$35.7M	Provider of Physical Security Information Management (PSIM) software
Jan 2020	LexisNexis Risk Solutions	Norton LifeLock ID Analytics business	$375M	Credit and fraud risk solutions for enterprises
Jan 2020	Mimecast	Segasec	Not disclosed	Protection against fake websites, phishing scams and credential harvesting
Jan 2020	Accenture	Symantec Cyber Security Services	Not disclosed	Global threat monitoring and analysis
Jan 2020	WESCO International Inc	Anixter International Inc	$4.52B	Distributor of network and security solutions and more
Dec 2019	F5 Networks Inc	Shape Security, Inc	$1B	Website defense against attacks from malware, botnets, and scripts
Dec 2019	Palo Alto Networks Inc	Aporeto Inc	Not disclosed	Machine identity-based micro-segmentation
Dec 2019	Leidos	Dynetics	$1.65B	Defense specialist with clients in the US intelligence community and NASA
Dec 2019	Fortinet	CyberSponse	Not disclosed	Security orchestration, automation and response

Date announced	Acquirer	Target	Value ($m)	Target company description
Nov 2019	Sumo Logic	JASK Labs	Not disclosed	Cloud-native autonomous SOC software
Nov 2019	Aqua Security	CloudSploit	Not disclosed	Cloud security posture management
Nov 2019	OpenText	Carbonite	$1.42B	Data protection, backup, and endpoint security
Nov 2019	Check Point Software	Cymplify	Not disclosed	IoT cybersecurity
Nov 2019	Proofpoint	Observe IT	$225M	Monitoring and auditing technology solutions
Oct 2019	Fortinet	EnSilo	Not disclosed	Endpoint security tools
Oct 2019	Thoma Bravo	Sophos	$3.9B	UK cybersecurity company offering range of services
Oct 2019	Elastic	Endgame	$234M	Endpoint protection, detection, and response technology
Oct 2019	NetNordic Holding AS	RanTek A/S	Not disclosed	Optimization of networks, security, data center and back-up
Sept 2019	Swiss IT Security AG	Intellec AG	Not disclosed	Provider of IT security through mobile device management
Aug 2019	Broadcom	Symantec	$10.7B	Enterprise security
Aug 2019	VMware	Carbon Black	$2.1B	Cloud-native endpoint protection specialist
July 2019	Wallix Group SA	Simarks Software S.L.U.	$1.46M	Developer of cyber security software
Jun 2019	Cisco	Sentryo	Not disclosed	Industrial IoT platform
May 2019	FireEye	Verodin	$254M	Solution to check effectiveness of cybersecurity controls
May 2019	Insight Venture	Recorded Future (minority stake)	$780M	Real-time threat intelligence
May 2019	Palo Alto Networks	PureSec	Not disclosed	End-to-end security for serverless functions
May 2019	Palo Alto Networks	Twistlock	$410M	Container security for cloud-native applications and workloads
May 2019	Orange	SecureLink	$577M	European cybersecurity services
April 2019	Zacco	Lakhshya Cyber Security Labs Pvt Ltd	Not disclosed	Provider of research and development in cyber security solutions
Mar 2019	NTT Security	WhiteHat Security	Not disclosed	Application security
Mar 2019	Verizon	ProtectWise	Not disclosed	Cloud-based network detection and response services
Feb 2019	Palo Alto Networks	Demisto	$560M	Security orchestration, automation and response

Date announced	Acquirer	Target	Value ($m)	Target company description
Feb 2019	Symantec	Luminate Security	Not disclosed	Secure access cloud technology as a VPN replacement
Feb 2019	Carbonite	Webroot	$618M	Endpoint detection and response security
Feb 2019	Epik LLC	BitMitigate	Not disclosed	Cybersecurity software developer
Jan 2019	Akamai	Janrain	Not disclosed	Customer identity access management
Nov 2018	BlackBerry	Cylance	$1.4B	AI to predict and prevent known cyber threats to fixed endpoints
Oct 2018	Palo Alto Networks	Redlock	$173M	Cloud threat defense
Jul 2018	AT&T	AlienVault	Not disclosed	Threat intelligence and unified security management platform
Jun 2018	Fortinet	Bradford Networks	Not disclosed	Network access control
Apr 2018	Palo Alto Networks	Secdo	Not disclosed	Endpoint detection and response
Apr 2018	RSA	Fortscale	Not disclosed	Embedded behavioral analytics
Apr 2018	Critical Start	Advanced Threat Analytics	Not disclosed	Security analytics platform
Mar 2018	VMware	E8 Security	Not disclosed	Behavioral analytics
Mar 2018	Palo Alto Networks	Evident.io	$300M	Cloud services infrastructure protection
Mar 2018	Akamai Technologies	Soasta	Not disclosed	Digital performance management
Feb 2018	Splunk	Phantom Cyber	$350M	Security automation technology developer
Feb 2018	Thoma Bravo	Barracuda Networks	$1.6B	Security for cloud-connected networks and applications
Feb 2018	Carbonite	Mozy	$146M	Cloud-based secure backup to automatically sync and recover data
Feb 2018	General Dynamics	CSRA	$9.6B	Technology services provider to US government clients
Feb 2018	RSE Venture	Oxford Solutions	$30M	Provides global managed security services
Feb 2018	Proofpoint	Wombat Security	$225M	Security awareness training software
Feb 2018	On Assignment	ECS Federal	$750M	Cybersecurity services for US federal government
Jan 2018	Relx Group	ThreatMetrix	$817M	Context-based business security and fraud prevention solutions
Jan 2018	KPMG	Cyberinc	$33M	Identity and access management

Source: GlobalData

Timeline

Almost every day, new cybersecurity breaches are reported across the world. General cybersecurity as well as medical-specific cybersecurity milestones are set out in the table below, which shows how the cybersecurity theme has developed over the last 50 years.

The Cybersecurity Story

Key Milestones in the Global Cybersecurity Landscape

1971	The first computer virus, known as "The Creeper," was purposely designed and released on ARPANET and copied itself to the remote system, displaying the words: "I am the Creeper: Catch me if you can."
1982	The first large-scale computer virus outbreak was caused by "Elk Cloner," a virus developed by a 15-year-old high school student as a practical joke. Elk Cloner was spread by floppy disks and affected the Apple II operating system.
1986	The first Computer Fraud and Abuse Act was passed, defining Federal computer-related crimes and associated penalties.
1988	Cornell graduate Robert Morris created and deployed the first worm. It was an aggressive, self-propagating virus that crippled 10% of the 88,000 computers on the ARPANET, which by 1990 became the internet.
1999	The Melissa and ILOVEYOU worms infected tens of millions of PCs across the world, causing email systems to fail.
2000	The council of Europe drafted a Cybercrime Treaty to promote the international harmonization of laws against computer crimes.
2002	A DDoS attack struck the 13 DNS root servers, knocking out all but five. This was the first attempt to disable the internet itself rather than individual hosts or enclaves.
2008	An employee at the US Central Command put a “candy drop” flash drive he found in the HQ car park into his laptop and exposed data on classified and unclassified systems.
2008	The National Cybersecurity Division of the US Department of Homeland Security released the Common Attack Pattern Enumeration and Classification resource, a publicly accessible taxonomy of attack patterns.
2008	National Security Presidential Directive 54/Homeland Security Presidential Directive 23 formalized the Comprehensive National Cyber-Security Initiative, which was intended to establish a frontline defense against a full spectrum of cyber threats.
2011	Sensitive personal information for over 4.9 million patients was stolen from the car of an employee of Science Applications International Corporation (SAIC).
2012	General Keith Alexander, the US Cybersecurity Chief, said that the loss of industrial information and intellectual property through cyber espionage constituted the "greatest transfer of wealth in history," referring to Chinese statesponsored hackers.
2013	US retailer Target suffered a data breach whereby the personal data of 40 million credit card customers was compromised. Access was gained via a third-party air conditioning supplier’s control systems and was exacerbated by Target’s weak internal segregation of network systems.
2013	Advocate Health Care reported a data breach involving personal information and unencrypted medical records of 4.03 million patients. In 2016, Advocate settled a lawsuit regarding the breach by paying $5.55M.
2014	Serious data breaches were suffered by Sony Pictures, JP Morgan, and Apple’s iCloud servers in China.
2014	Hackers exploited a software vulnerability to access sensitive personal information of 4.5 million patients of Community Health Systems, which operated over 200 hospitals in the US.
2015	Serious data breaches were suffered by the US Office of Personnel Management, TalkTalk, and Ashley Madison.
2015	US officials announced that Russian hackers gained access to White House and State Department emails in 2014.
2015	The deadline passed for Europay, MasterCard, Visa (EMV) chip card acceptance at the point of sale (POS), prompting many warnings to e-commerce merchants that fraudsters would likely step up their attacks against cardnot-present transactions.
2015	The major card networks continued their push of tokenization for securing mobile and online transactions, including efforts to embed the technology in their own payment products, such as Mastercard’s Masterpass.
2015	Nearly 100 million patient records were stolen from Anthem Blue Cross, Premera Blue Cross, and Excellus Blue Cross Blue Shield combined. These breaches included highly sensitive personal data.
2015	Hackers accessed the University of California, Los Angeles (UCLA) health system and stole over 4.5 million patient records. It was later discovered that UCLA had not encrypted its patient data.
2016	Yahoo revealed a 2014 breach of 500 million users’ personal details—the largest such breach in history.

2016	The EU NIS Directive came into force.
2018	Intel reports Meltdown and Spectre vulnerabilities in its chips, which allows a rogue developer to read a chip’s memory.
2018	The EU NIS Directive may be transposed into national laws in each EU member state.
2018	The EU’s GDPR will enter into force.
2018	Over 16,000 patients of Philadelphia-based Independence Blue Cross had their data exposed online. This data breach was the result of an employee uploading a file to a public-facing website online.
2019	Large breaches occured in Singapore's health sector. Personal information for 808,000 blood donors was mishandled and leaked online, and later in the same month, the HIV status of 14,200 individuals was leaked online.
2019	A large data breach occurred at the American Medical Collection Agency (AMCA), exposing information on at least 20 million patients. AMCA filed for bankruptcy as a result of costs associated with the breach.

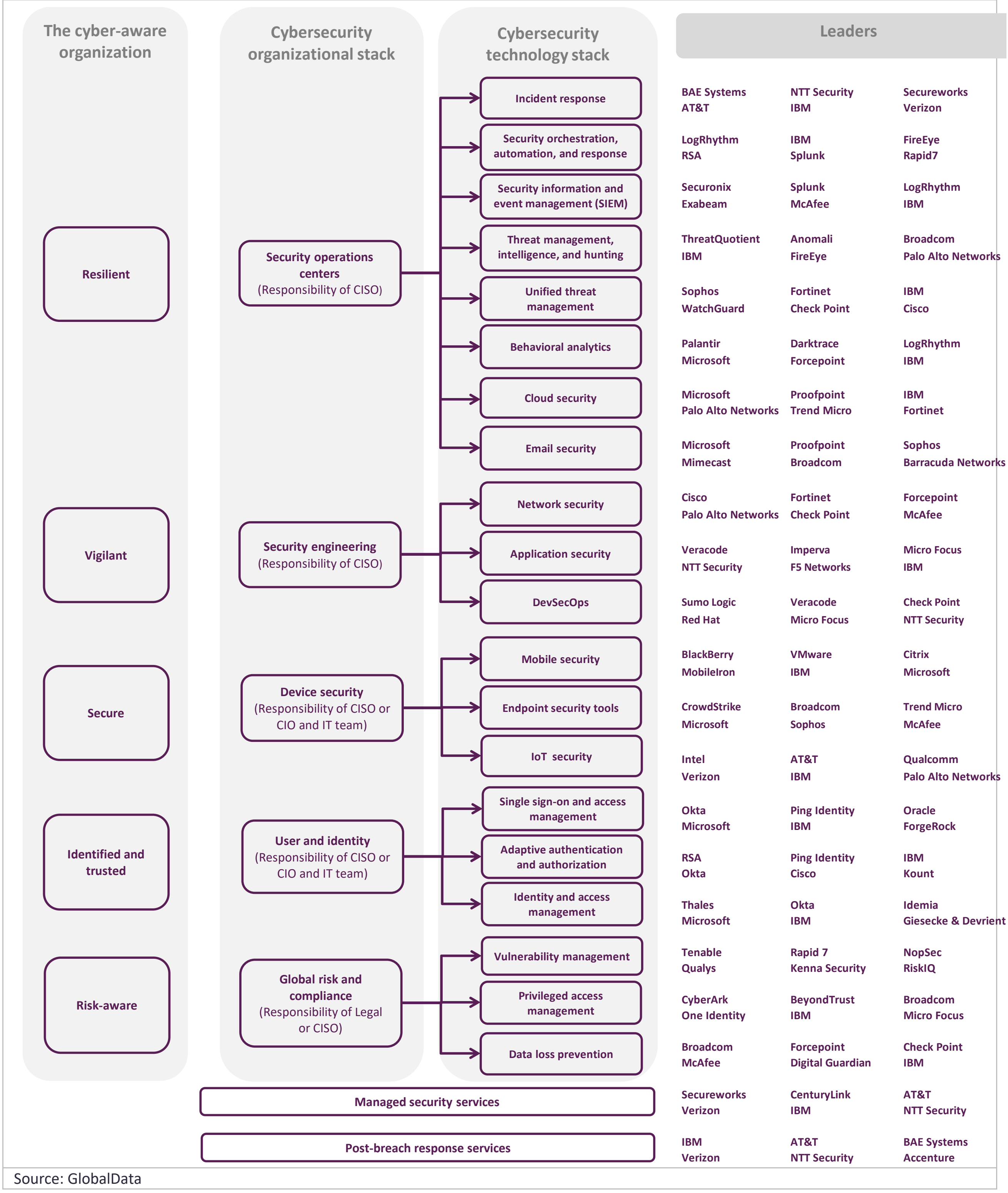
Source: GlobalData

Value chain

The cybersecurity value chain is made up of three main areas: the cyber-aware organization, the cybersecurity organizational stack, and the cybersecurity technology stack. The graphic below describes each of these three elements and identifies the leading vendors across 22 segments of the technology stack.

The cybersecurity value chain

This value chain reflects how organizations tackle cybersecurity



The cyber-aware organization	Cybersecurity organizational stack	Cybersecurity technology stack	Leaders		
Resilient	Security operations centers (Responsibility of CISO)	Incident response	BAE Systems AT&T	NTT Security IBM	Secureworks Verizon
		Security orchestration, automation, and response	LogRhythm RSA	IBM Splunk	FireEye Rapid7
		Security information and event management (SIEM)	Securonix Exabeam	Splunk McAfee	LogRhythm IBM
		Threat management, intelligence, and hunting	ThreatQuotient IBM	Anomali FireEye	Broadcom Palo Alto Networks
		Unified threat management	Sophos WatchGuard	Fortinet Check Point	IBM Cisco
		Behavioral analytics	Palantir Microsoft	Darktrace Forcepoint	LogRhythm IBM
		Cloud security	Microsoft Palo Alto Networks	Proofpoint Trend Micro	IBM Fortinet
		Email security	Microsoft Mimecast	Proofpoint Broadcom	Sophos Barracuda Networks
Vigilant	Security engineering (Responsibility of CISO)	Network security	Cisco Palo Alto Networks	Fortinet Check Point	Forcepoint McAfee
		Application security	Veracode NTT Security	Imperva F5 Networks	Micro Focus IBM
		DevSecOps	Sumo Logic Red Hat	Veracode Micro Focus	Check Point NTT Security
Secure	Device security (Responsibility of CISO or CIO and IT team)	Mobile security	BlackBerry MobileIron	VMware IBM	Citrix Microsoft
		Endpoint security tools	CrowdStrike Microsoft	Broadcom Sophos	Trend Micro McAfee
		IoT security	Intel Verizon	AT&T IBM	Qualcomm Palo Alto Networks
Identified and trusted	User and identity (Responsibility of CISO or CIO and IT team)	Single sign-on and access management	Okta Microsoft	Ping Identity IBM	Oracle ForgeRock
		Adaptive authentication and authorization	RSA Okta	Ping Identity Cisco	IBM Kount
		Identity and access management	Thales Microsoft	Okta IBM	Idemia Giesecke & Devrient
Risk-aware	Global risk and compliance (Responsibility of Legal or CISO)	Vulnerability management	Tenable Qualys	Rapid 7 Kenna Security	NopSec RiskIQ
		Privileged access management	CyberArk One Identity	BeyondTrust IBM	Broadcom Micro Focus
		Data loss prevention	Broadcom McAfee	Forcepoint Digital Guardian	Check Point IBM
	Managed security services		Secureworks Verizon	CenturyLink IBM	AT&T NTT Security
	Post-breach response services		IBM Verizon	AT&T NTT Security	BAE Systems Accenture

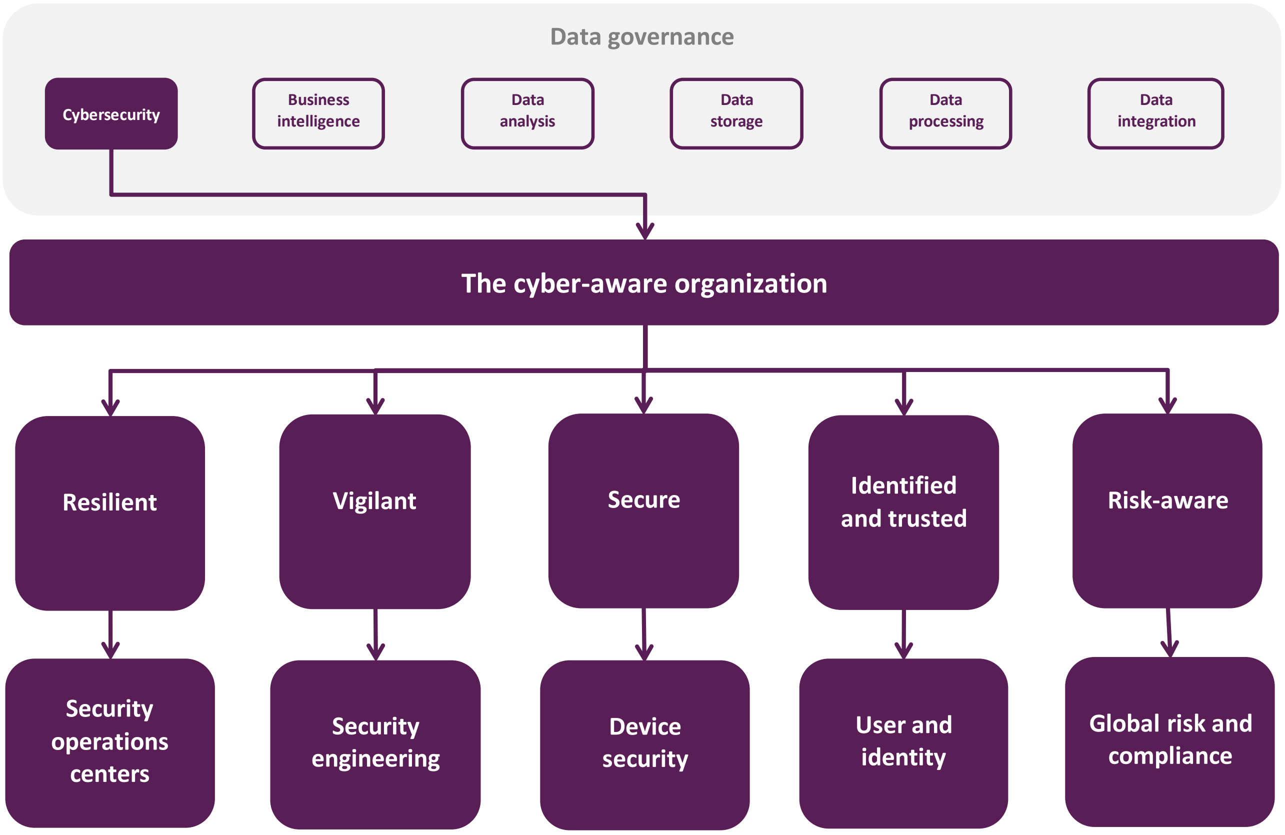
Source: GlobalData

The cyber-aware organization

The cyber-aware organization is able to define its defensive position in five key areas. It must be:

- **Resilient**. Able to respond to security incidents when they happen, whether through email, the cloud, or mobile devices.
- **Vigilant**. Able to detect threats, hunt them down, and see where future threats are coming from.
- **Secure**. Able to deliver security for networks (including both firewalls and intrusion detection systems), endpoints, and applications.
- **Identified and trusted**. Able to identify and trust its employees and partners as they interact with the organization.
- **Risk-aware**. Able to fully understand its governance, risk, and compliance stance.

The cyber-aware organization



Source: GlobalData

The cybersecurity organizational stack

A specific part of the organization should be responsible for each of these five key elements.

To ensure resilience, the security operations center (SOC) takes responsibility for incident response, for areas such as email and cloud security, and for threat management, threat intelligence, and forensics. A key part of the incident response capability is understanding what is going on.

The need for vigilance defines the role of an organization's security engineering, covering areas such as application security, ensuring that the organization's products and applications have effective security built into them. Security engineering is also responsible for on-premise hardware and software, including firewalls and intrusion detection systems.

Making the organization secure is the goal of device security, which includes mobile security, endpoint security tools, IoT security, and network security.

The organization's user and identity policy should ensure that all users are identified and trusted. It comprises all areas where it is important to be able to vouch for who is logging on and using company systems. It includes areas such as single sign-on and access management as well as adaptive authentication and identity and access management.

Vulnerability management, asset management, privileged asset management, and data loss prevention typically come under the risk-awareness management banner.

These five areas – SOCs, security engineering, device security, user and identity, and global risk and compliance – make up the cybersecurity organizational stack. A different corporate officer or team is responsible for each area.

Both SOCs and security engineering are the responsibility of the CISO. Device security is led by the CIO and the IT team. User and identity is the remit of either the CISO or the IT team, and risk awareness usually falls to an organization's legal team or the CISO.

The cybersecurity technology stack

The cybersecurity technology stack is made up of 22 segments. In the following section, we will provide an overview of each segment, including analysis of the leading and challenging vendors.

Incident response

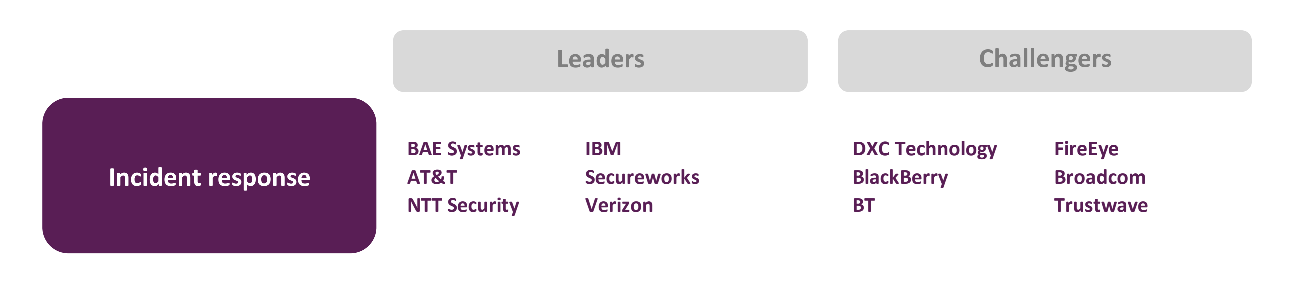
Incident response is the methodology an organization uses to respond to and manage a cyberattack.

An attack or data breach can create havoc, potentially affecting customers, intellectual property, company time and resources, and reputation and brand value. An effective incident response, led by the CISO, aims to reduce this damage and recover as quickly as possible.

The incident response may include the use of specialist external cybersecurity vendors with the experience and technical knowledge to help. Leaders include BAE Systems, AT&T, NTT Security, IBM, Secureworks, and Verizon.

The Cybersecurity value chain

Leaders and challengers in incident response



Incident response

Leaders

BAE Systems
AT&T
NTT Security
IBM
Secureworks
Verizon

Challengers

DXC Technology
BlackBerry
BT
FireEye
Broadcom
Trustwave

Source: GlobalData

Security orchestration, automation, and response (SOAR)

SOCs use SOAR’s automated functions to deal with threats faster and more efficiently, while also reducing workloads and standardizing security incident response processes.

Each of the three SOAR components performs a different SOC function. Orchestration integrates different technologies and connects between security tools to improve incident response capabilities. Automation provides automated detection and response tools to decrease the time it takes security teams to identify and deal with security incidents and reduce their workload. Response allows security teams to run automated workflows that perform actions such as launching investigations and containing and mitigating threats.

Leaders in the provision of SOAR solutions include LogRhythm, RSA, IBM, Splunk, FireEye, and Rapid7.

The Cybersecurity value chain

Leaders and challengers in security orchestration, automation, and response

	Leaders		Challengers	
Security orchestration, automation, and response	LogRhythm	Splunk	Ayehu	Palo Alto Networks
	RSA	FireEye	Fortinet	Cyberbit
	IBM	Rapid7	Raytheon	DFLabs

Source: GlobalData

Security information and event management (SIEM)

SOAR is supported by, and works hand-in-hand with, SIEM, which offers a combined process of incident detection and incident response. Typically, it includes features such as alerts, analytics, dashboards, and forensic analysis.

SIEM and SOAR share several components, and security operations teams may use the terms interchangeably. However, SIEM and SOAR are two different security solutions. The SIEM process can be summed up as: collect data from internal sources; aggregate the data; analyze the data to detect possible cybersecurity breaches; and alert the team so they can verify the presence of threats. This last step can cause a problem in that it is human resource-intensive, requiring numerous hours of repetitive tasks.

Leading vendors in SIEM include Securonix, Exabeam, Splunk, McAfee, LogRhythm, and IBM.

The Cybersecurity value chain

Leaders and challengers in security information and event management

	Leaders		Challengers	
Security information and event management	Securonix	McAfee	Micro Focus	Sumo Logic
	Exabeam	LogRhythm	AT&T	Trustwave
	Splunk	IBM	RSA	FireEye

Source: GlobalData

Threat management, intelligence, and hunting

Threat management, threat intelligence, and threat hunting describe the use of detection and mitigation techniques to protect against IT security threats.

Threat management includes real-time monitoring, proactive reporting, data analytics, breach alerts, and ML.

Threat intelligence comprises the data collected and analyzed by an organization to understand a cyber threat's motives and its attack behaviors.

Threat hunting is the process of seeking out adversaries before they can successfully execute an attack. Many organizations are putting an increased emphasis on programmatic threat hunting because of the increasing ability of malicious actors to evade traditional detection methods.

Most cybersecurity vendors have expertise in this area, but leaders would include ThreatQuotient, IBM, Anomali, FireEye, Broadcom, and Palo Alto Networks.

The Cybersecurity value chain

Leaders and challengers in threat management, intelligence, and hunting

	Leaders		Challengers	
Threat management, intelligence, and hunting	ThreatQuotient IBM Anomali	FireEye Broadcom Palo Alto Networks	McAfee LogRhythm RSA	AT&T ThreatConnect Proofpoint

Source: GlobalData

Unified threat management

The number of threats and their complexity is too much for most organizations to handle. At the same time, CISOs have an increasing number of security vendors to manage, with each one generating alerts that must be investigated.

Unified threat management (UTM) brings some degree of simplification, as a single piece of software or hardware performs multiple security functions simultaneously. Instead of having multiple firewalls, antivirus, intrusion detection, and intrusion prevention systems all running separately, UTM brings all these defenses into a single, centrally-controlled system, which provides more of an integrated model and, importantly, brings a reduction in administration for those responsible for network security.

Leaders in UTM include Fortinet, WatchGuard, Sophos, Check Point, IBM, and Cisco.

The Cybersecurity value chain

Leaders and challengers in unified threat management

	Leaders		Challengers	
Unified threat management	Sophos WatchGuard Fortinet	Check Point IBM Cisco	SonicWall Juniper Networks Hillstone Networks	Stormshield Rohde & Schwarz Barracuda Networks

Source: GlobalData

Behavioral analytics

Behavioral analytics, sometimes described as user and entity behavior analytics (UEBA), is a cybersecurity process that takes note of the normal conduct of users and applications within the organization. What sets alarm bells ringing is when a supposedly normal user exhibits anomalous behavior.

For example, if a user typically downloads around 10MB of files every day and then downloads gigabytes of data in the early hours of the morning, this change in behavior pattern should be picked up.

Following the acquisitions of leading vendors Fortscale and E8 Security in 2018 (by RSA and VMware, respectively), the consolidation trend in behavioral analytics continued in 2019 with Micro Focus acquiring Interset, Broadcom buying Bay Dynamics and Exabeam buying SkyFormation.

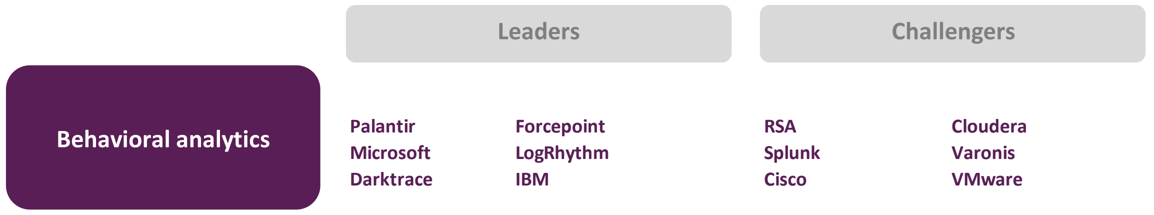
An ongoing area of development will be AI analysis of behavioral biometric data. Sophisticated ML algorithms can build up a profile of a user's typical behavior, identify unusual patterns of activity, and highlight potential threats in real-time before they have a chance to materialize.

By automatically detecting suspicious data, the whole security process becomes more efficient, preventing the need for a painstaking manual review of log data.

Leaders in behavioral analytics include Palantir, Microsoft, Darktrace, Forcepoint, LogRhythm, and IBM.

The Cybersecurity value chain

Leaders and challengers in behavioral analytics



	Leaders	Challengers
Behavioral analytics	Palantir Microsoft Darktrace Forcepoint LogRhythm IBM	RSA Splunk Cisco Cloudera Varonis VMware

Source: GlobalData

Cloud security

Two key developments in cloud security as cloud delivery models become more complex are the emergence of cloud access security brokers (CASB) and cloud security posture management (CSPM).

CASB is on-premise or cloud-hosted software that sits between cloud service consumers and cloud service providers to enforce security, compliance, and governance policies for cloud applications.

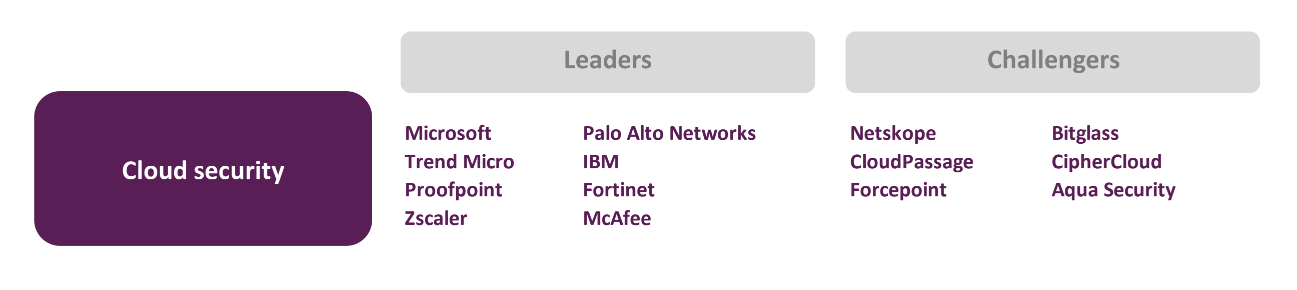
CSPM tools will be used in 2020 to identify and resolve cloud risks across public cloud environments, and to provide security, compliance, and risk capabilities. Companies strong in these new cloud developments include Microsoft, McAfee, Zscaler – which bought CSPM specialist Cloudneeti in April 2020 - Forcepoint, Bitglass, Netskope, CloudPassage, and CipherCloud.

A large number of cyberattacks on organizations' public cloud environments are the direct result of customer misconfiguration and mismanagement. A 2020 survey by DivvyCloud research found that nearly 33.4 billion records were exposed in breaches due to cloud misconfigurations in 2018 and 2019, costing enterprises nearly $5 trillion in costs. Getting cloud configuration and compliance right must be a priority for organizations.

The cloud security arena is competitive with leaders including Microsoft, Proofpoint, Palo Alto Networks, Trend Micro, IBM, Fortinet, Zscaler, and McAfee.

The Cybersecurity value chain

Leaders and challengers in cloud security



Cloud security

Leaders

Microsoft
Trend Micro
Proofpoint
Zscaler

Palo Alto Networks
IBM
Fortinet
McAfee

Challengers

Netskope
CloudPassage
Forcepoint

Bitglass
CipherCloud
Aqua Security

Source: GlobalData

Email security

Despite continuing efforts at security awareness that implore employees to be safe in the way they manage their messages, most cyberattacks are initiated by email, with a user tricked into opening a malicious attachment, clicking a malicious link, or responding with confidential data.

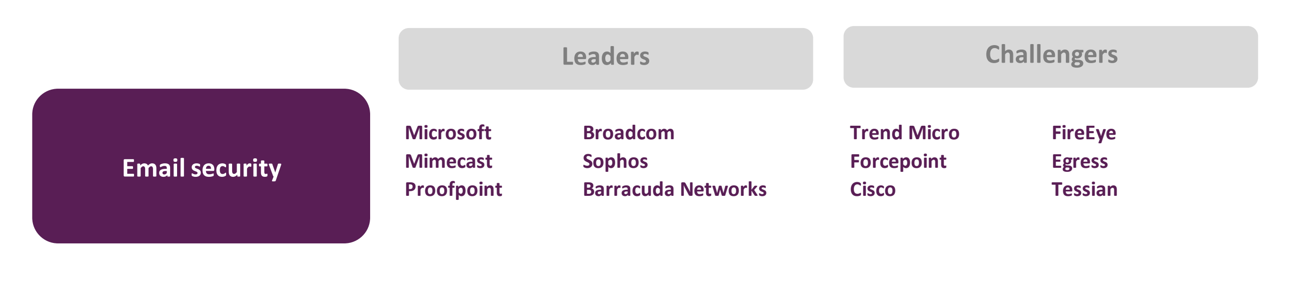
The FBI's 2019 Internet Crime report found that, of the total reported losses from cyber-crime of $3.5bn, more than half ($1.8bn) came from business email or email account compromise.

One of the most frequent sources of data breaches is in email addressing mistakes, where the email is sent to an inadvertent recipient. ML is used by some vendors to monitor employees' mistakes in this area, with previous patterns of sending used to check on the user's planned recipient and highlight any discrepancies.

Email security leaders include Microsoft, Mimecast, and Proofpoint, with other vendors including Broadcom, Sophos, and Barracuda Networks.

The Cybersecurity value chain

Leaders and challengers in email security



Email security

Leaders

Microsoft
Mimecast
Proofpoint

Broadcom
Sophos
Barracuda Networks

Challengers

Trend Micro
Forcepoint
Cisco

FireEye
Egress
Tessian

Source: GlobalData

Network security

Effective network security is needed because the connections between an organization's networks and the internet, as well as other partner networks, expose its systems and technologies to attack. Today's network landscape spans many sites, and the use of mobile and remote working and cloud services makes defining a fixed network boundary difficult.

Types of network security include: network access control, which can be set to grant users access to a network but not to specific confidential folders; firewalls, which act as a barrier between untrusted external networks and the trusted internal network; and VPNs, which create a connection to the network from another endpoint or site. VPNs are particularly at risk because of trust concerns. An organization could grant access to someone it thinks is a trusted user, only to find that someone has stolen that trusted user's credentials. This type of scenario is a major reason why the concept of zero trust is taking off.

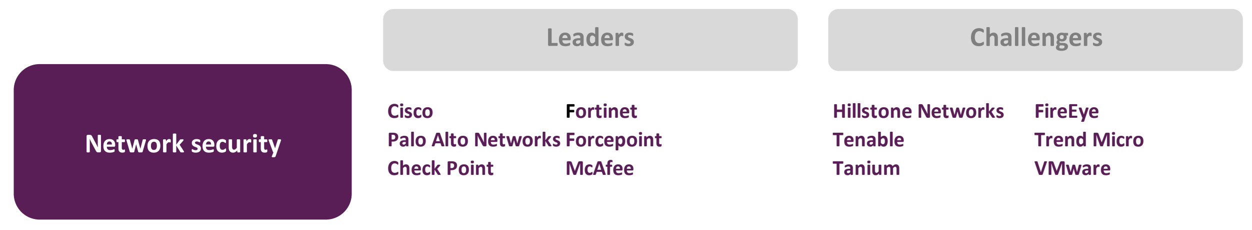
A bigger change is already underway in network security, with a move to the cloud that companies like Cisco and Palo Alto Networks must manage.

Nearly 70% of enterprise organizations are currently migrating data for enterprise resource planning (ERP) applications to the cloud, according to a 2019 report from the Cloud Security Alliance. Palo Alto Networks bought Evident.io and Redlock in 2018 to beef up its positioning in the cloud-based network security area, which has been dubbed secure access service edge (SASE).

Leaders in network security include Cisco, Palo Alto Networks, Check Point, Fortinet, Forcepoint, and McAfee.

The Cybersecurity value chain

Leaders and challengers in network security



	Leaders		Challengers	
Network security	Cisco	Fortinet	Hillstone Networks	FireEye
	Palo Alto Networks	Forcepoint	Tenable	Trend Micro
	Check Point	McAfee	Tanium	VMware

Source: GlobalData

Application security

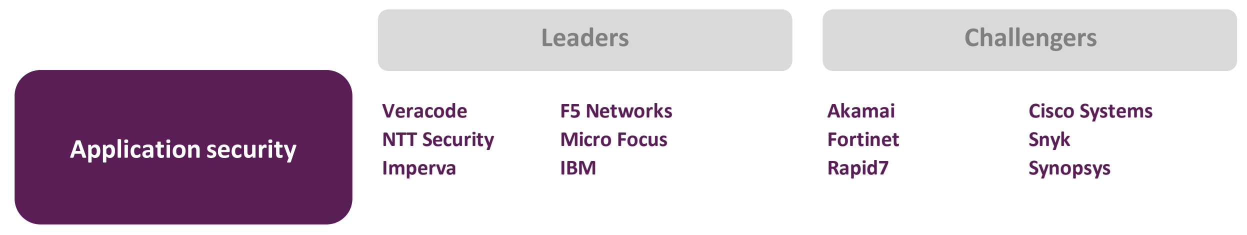
Application security aims to protect software applications from cyberattacks. The most effective way of achieving this is by preventing security vulnerabilities, which could allow the app to be compromised, from being introduced into the app's code.

Vulnerabilities are introduced typically because app development has to be fast, which means that security is often bolted on to the application as an afterthought rather than being built in from the beginning. It is this concern that has driven the rise of DevSecOps.

Application security leaders include Veracode, NTT Security, Imperva, F5 Networks, Micro Focus, and IBM.

The Cybersecurity value chain

Leaders and challengers in application security



	Leaders		Challengers	
Application security	Veracode	F5 Networks	Akamai	Cisco Systems
	NTT Security	Micro Focus	Fortinet	Snyk
	Imperva	IBM	Rapid7	Synopsys

Source: GlobalData

DevSecOps

One means of ensuring that applications are built with fewer security vulnerabilities is DevSecOps, in which development, operations, and security teams collaborate in application rollouts.

The complexity of today's systems demands greater collaboration between application developers and security teams, to ensure that security is built into daily processes. Applications continue to be vulnerable to attack because they are not coded with security in mind. Bypassing security, or building overly complex applications, only makes it easier for attackers to find ways to compromise them and gain access to data or systems.

The goal of DevSecOps is to get security back into the lifecycle. According to WhiteHat Security, now part of NTT Security, companies take an average of 174 days to fix a vulnerability found when using dynamic analysis in production. However, companies that have implemented DevSecOps do it in just 92 days. For vulnerabilities found in development using static analysis, carried out when a program is not running, an average company takes 113 days, while DevSecOps companies take 51 days.

Vendors leading in DevSecOps are Sumo Logic, Red Hat, Veracode, Micro Focus, Check Point, and NTT Security. This is likely to be an area of M&A interest.

The Cybersecurity value chain

Leaders and challengers in DevSecOps

	Leaders		Challengers	
DevSecOps	Sumo Logic	Micro Focus	Synopsys	Aqua Security
	Red Hat	Check Point	Contrast Security	Continuum Security
	Veracode	NTT Security	ThreatModeler	Checkmarx

Source: GlobalData

Mobile security

Mobile security refers to the measures taken by enterprises to protect sensitive data stored on corporate portable devices, as well as to prevent unauthorized mobile devices from accessing the enterprise network.

Mobile security addresses the specific threats to the corporate network from wireless connections, whether they are internal (through Wi-Fi) or external (through an employee working from home or from another location, such as a coffee shop). Enterprises now expect their mobility solutions to provide access to corporate applications, data, and services seamlessly, regardless of device type, network, or location. Painful experiences with employees wanting to use their own devices to connect to the corporate network have demonstrated to organizations just how complex mobility can get. Leaders in mobile security include BlackBerry, MobileIron, VMware, IBM, Citrix, and Microsoft.

The Cybersecurity value chain

Leaders and challengers in mobile security

	Leaders		Challengers	
Mobile security	BlackBerry	IBM	McAfee	Micro Focus
	MobileIron	Citrix	Check Point	Thales
	VMware	Microsoft	Fortinet	Zimperium

Source: GlobalData

Endpoint security tools

Endpoint security refers to the method used for protecting the network when it is accessed via an endpoint device, such as a laptop or smartphone. Endpoint security software protects these points of entry from risky activity carried out by employees or from a malicious attack.

Organizations no longer have such an easily defined security perimeter, and new layers of security are needed. Security must maintain control over access points to prevent the vulnerabilities that can arise through the use of remote devices.

Leaders in the competitive endpoint security market include CrowdStrike, Microsoft, Broadcom, Sophos, Trend Micro, and McAfee. Two hot, well-funded players to watch are SentinelOne and Tanium.

The Cybersecurity value chain

Leaders and challengers in endpoint security tools

	Leaders		Challengers	
Endpoint security tools	CrowdStrike	Sophos	BlackBerry	Kaspersky Lab
	Microsoft	Trend Micro	VMware	Tanium
	Broadcom	McAfee	F-Secure	SentinelOne

Source: GlobalData

IoT security

The explosion in the number of connected devices has significantly increased potential points for cyberattacks and created a massive security gap that the cybersecurity industry is starting to address.

The big challenge for organizations trying to address IoT security is that most of the devices have weak or no security controls. Security cameras are an example of the sort of device at risk. The Mirai botnet, composed primarily of embedded and IoT devices, overwhelmed several high-profile targets in late 2016 with massive distributed denial-of-service (DDoS) attacks. The botnet infected nearly 65,000 IoT devices in its first 20 hours before reaching a steady-state population of between 200,000 and 300,000 infections. Mirai targeted a variety of IoT and embedded devices including IP cameras, routers, and printers. Its bots scanned the IPv4 address space for devices that ran telnet or SSH and attempted to log in using a hardcoded dictionary of IoT credentials. Once successful, the bot sent the victim’s IP address and associated credentials to a report server, which asynchronously triggered a loader to infect the device.

IoT at-risk devices include anything with an internet connection, from a refrigerator to smart locks, thermostats, lightbulbs, and vehicles. A notable threat is the prospect of attacks on sensors and devices used within the Industrial Internet or in smart cities.

Leaders in IoT security are Intel, IBM, AT&T, Verizon, Qualcomm, and Palo Alto Networks.

The Cybersecurity value chain

Leaders and challengers in IoT security

	Leaders		Challengers	
IoT Security	Intel	IBM	Cisco	Broadcom
	Verizon	Qualcomm	Check Point	Armis
	AT&T	Palo Alto Networks	McAfee	Vdoo

Source: GlobalData

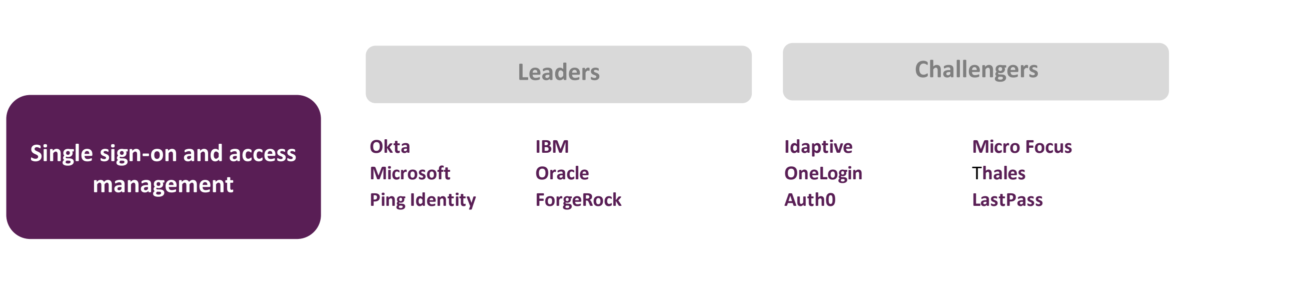
Single sign-on and access management

Single sign-on is typically used in enterprises to reduce (and make a better job of managing) the number of credentials an employee requires to access enterprise applications. A key benefit is that users are likely to create a stronger, unique password if they only need to create one, or opt for multi-factor authentication (MFA) if they only need to do it once. Single sign-on allows organizations to improve their security posture by reducing the number of identity credentials users have to manage by consolidating multiple identities into a single identity.

Leading vendors in single sign-on and access management include Okta, Microsoft, Ping Identity, IBM, Oracle, and ForgeRock.

The Cybersecurity value chain

Leaders and challengers in single sign-on and access management



Single sign-on and access management

Leaders

Okta
Microsoft
Ping Identity
IBM
Oracle
ForgeRock

Challengers

Idaptive
OneLogin
Auth0
Micro Focus
Thales
LastPass

Source: GlobalData

Adaptive authentication and authorization

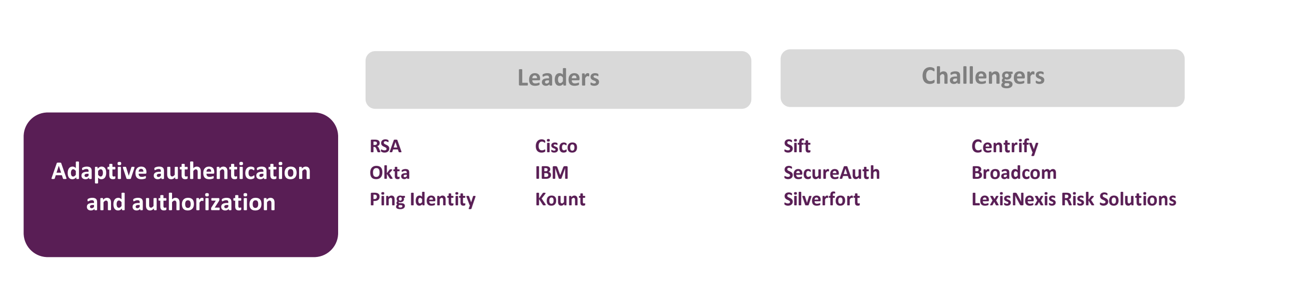
Standard authentication methods, including MFA, ask users for specific credentials whenever they try to log in or access corporate resources. If users always log in with standard credentials, such as username and password, it makes them vulnerable to cyberattacks. Adaptive authentication asks for different credentials depending upon the situation, thereby tightening security.

Adaptive authentication works by creating a profile for each user, which includes information such as the user's geographical location, registered devices, and job role. Each time someone tries to authenticate, the request is evaluated and assigned a risk score. Depending on the risk score, the user may be required to provide additional credentials or, conversely, allowed to use fewer credentials.

Leaders in adaptive authentication include RSA, Okta, Ping Identity, Cisco, IBM, and Kount.

The Cybersecurity value chain

Leaders and challengers in adaptive authentication and authorization



Adaptive authentication and authorization

Leaders

RSA
Okta
Ping Identity
Cisco
IBM
Kount

Challengers

Sift
SecureAuth
Silverfort
Centrify
Broadcom
LexisNexis Risk Solutions

Source: GlobalData

Identity and access management

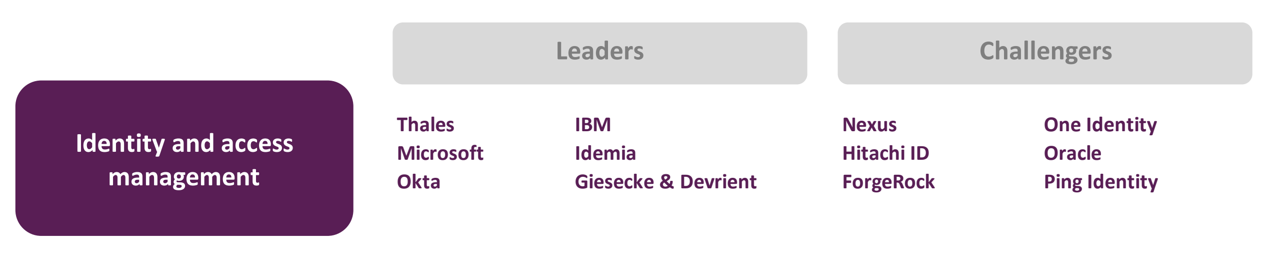
Identity and access management (IAM) refers to the collection of policies, processes, and systems that bind an individual to a set of permissions within a system. Such permissions may allow an individual to perform functions, such as altering an industrial control process, accessing data, or administering a system.

Access management is the process of identifying, tracking, controlling, and managing authorized or specified users' access to a system, application, or any IT instance. IAM can be broken down into several broad areas, including policy (who is authorized to access systems, data, or functionality, and how can they request access?), and identity management (how an organization establishes the identity of a person, both at the first point of contact and during subsequent interactions with systems or processes).

Leaders in identity and access management include Thales, Microsoft, Okta, IBM, Idemia, and Giesecke & Devrient.

The Cybersecurity value chain

Leaders and challengers in identity and access management



Identity and access management

Leaders		Challengers	
Thales	IBM	Nexus	One Identity
Microsoft	Idemia	Hitachi ID	Oracle
Okta	Giesecke & Devrient	ForgeRock	Ping Identity

Source: GlobalData

Vulnerability management

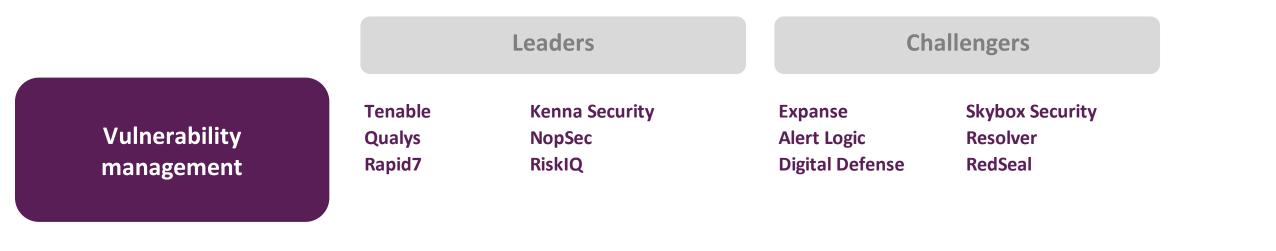
Vulnerability management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities, both in systems and the software that runs on those systems. Organizations typically have a vulnerability management process, which allows them to understand what vulnerabilities are present within their IT estate. The UK National Cyber Security Centre believes that executive staff should ideally be as aware of the major vulnerabilities in their IT estate as they are of their financial status.

Having a vulnerability management framework in place that regularly checks for new vulnerabilities is crucial for preventing cybersecurity breaches. Without a vulnerability testing and patch management system, old security gaps may be left on the network for extended periods. This gives attackers more of an opportunity to exploit vulnerabilities and carry out their attacks.

Leaders in vulnerability management include Tenable, Qualys, Rapid7, Kenna Security, NopSec, and RiskIQ.

The Cybersecurity value chain

Leaders and challengers in vulnerability management



Vulnerability management

Leaders		Challengers	
Tenable	Kenna Security	Expanse	Skybox Security
Qualys	NopSec	Alert Logic	Resolver
Rapid7	RiskIQ	Digital Defense	RedSeal

Source: GlobalData

Privileged access management

Privileged access management (PAM) comprises the cybersecurity strategies and technologies needed to exert control over the privileged access and permissions for users, accounts, processes, and systems.

By referencing the appropriate level of privileged access controls, PAM helps organizations condense the parts of the organization that can be attacked and prevent, or at least mitigate, the damage caused by either external attacks, insider malfeasance, or negligence.

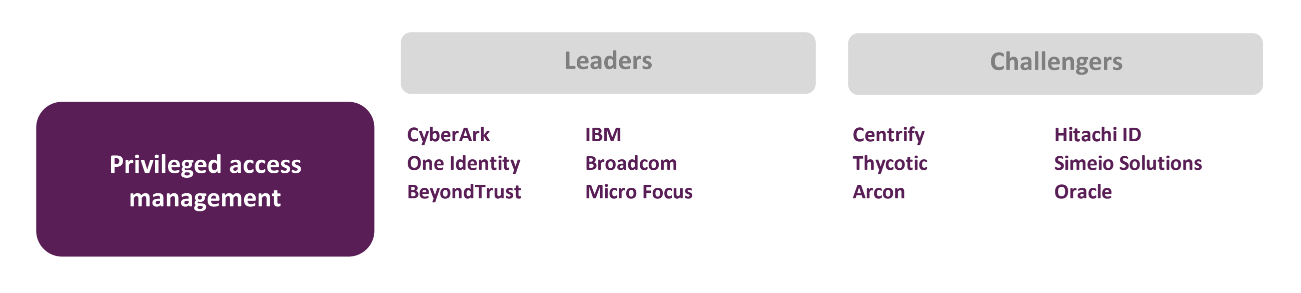
The central goal of PAM is the enforcement of least privilege, defined as the restriction of access rights and permissions for users, accounts, applications, systems, devices, and computing processes to the absolute minimum necessary to perform routine, authorized activities.

PAM is considered by many technologists as one of the most important security projects for reducing cyber risk and achieving a significant return on investment (ROI).

Leaders include CyberArk, One Identity, BeyondTrust, IBM, Micro Focus, and Broadcom.

The Cybersecurity value chain

Leaders and challengers in privileged access management



Privileged access management

Leaders

CyberArk
One Identity
BeyondTrust

IBM
Broadcom
Micro Focus

Challengers

Centrify
Thycotic
Arcon

Hitachi ID
Simeio Solutions
Oracle

Source: GlobalData

Data loss prevention

Organizations must take all necessary steps to maximize the security of their data. Data loss prevention (DLP) describes a set of tools and processes used to achieve this and ensure that sensitive data is not lost, misused, or accessed by unauthorized users.

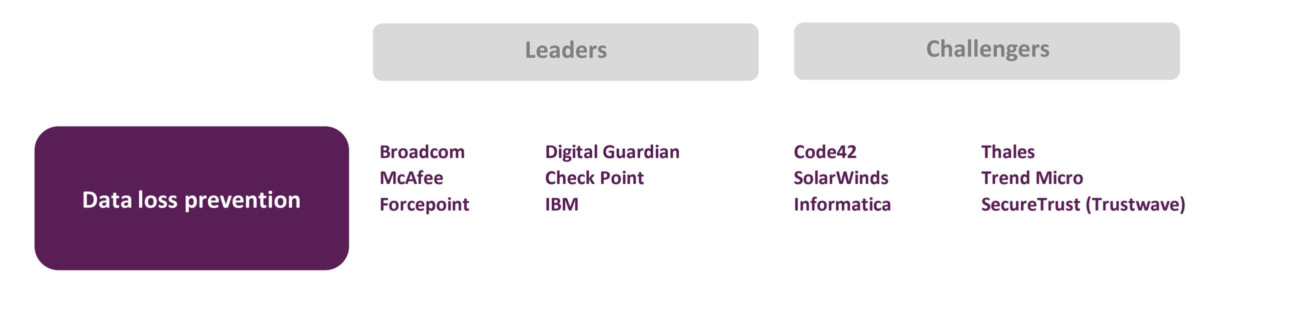
DLP software classifies regulated, confidential, and business-critical data and identifies any violations of policies both defined by organizations or driven by regulatory compliance, such as GDPR. If any violations are identified, DLP enforces remediation with alerts, encryption, and other protective actions to prevent end-users from accidentally or maliciously sharing data that could put the organization at risk.

DLP software and tools monitor and control endpoint activities, filter data streams on corporate networks, and monitor data in the cloud to protect data at rest, in motion, and in use. The development of the CISO role has driven the wider adoption of DLP. CISOs often report to the chief executive, who should want to know the game- plan for preventing data leaks. DLP gives CISOs the necessary reporting capabilities and ammunition to provide regular updates to the CEO.

Leaders in DLP include Broadcom, McAfee, Digital Guardian, Forcepoint, Check Point, and IBM.

The Cybersecurity value chain

Leaders and challengers in data loss prevention



Data loss prevention

Leaders

Broadcom
McAfee
Forcepoint

Digital Guardian
Check Point
IBM

Challengers

Code42
SolarWinds
Informatica

Thales
Trend Micro
SecureTrust (Trustwave)

Source: GlobalData

Managed security services

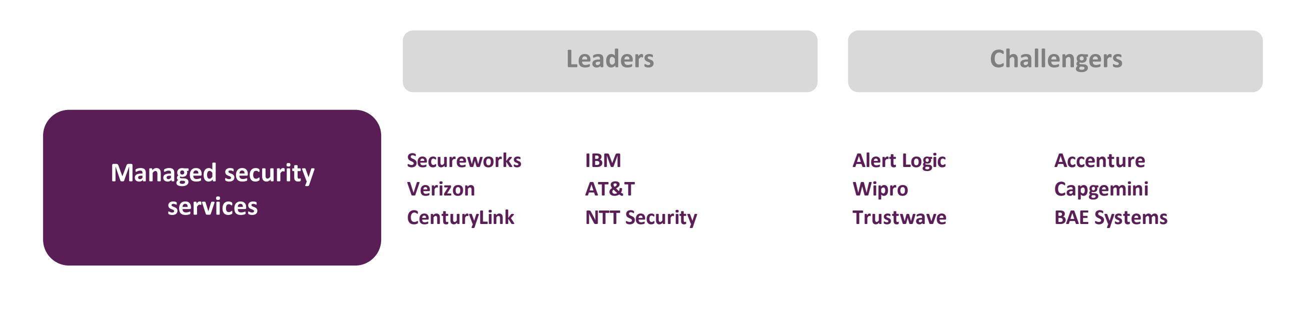
Managed security services typically include the provision of remote, round-the-clock monitoring of security events and response for threat detection, as well as the administration and management of IT security technologies. Typically the services are provided by remote SOCs.

Other services provided include administering and managing firewalls, UTM, incident response services, vulnerability assessment, and threat intelligence. Increasingly, managed security service providers (MSSPs) are providing monitoring of operational technology, including ICS and SCADA systems and IoT devices.

Leaders in managed security services include Secureworks, IBM, Verizon, AT&T, CenturyLink, and NTT Security.

The Cybersecurity value chain

Leaders and challengers in managed security services



	Leaders		Challengers	
Managed security services	Secureworks Verizon CenturyLink	IBM AT&T NTT Security	Alert Logic Wipro Trustwave	Accenture Capgemini BAE Systems

Source: GlobalData

Post-breach response services

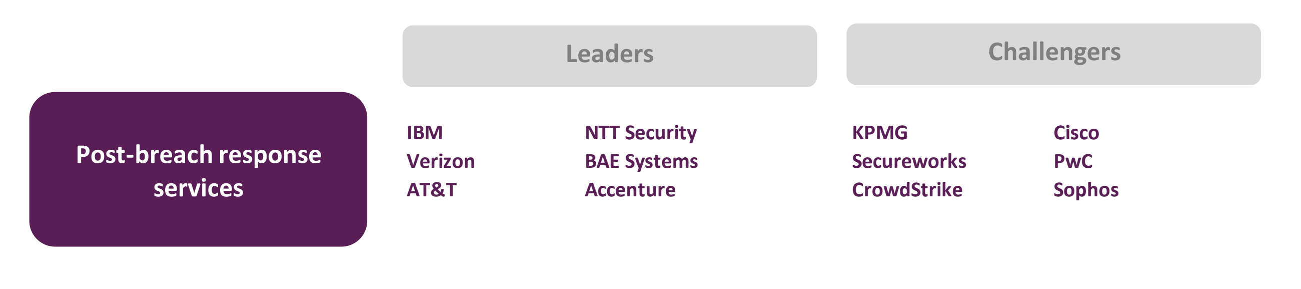
Post-breach response services provide support to organizations that have been on the receiving end of a data breach. When such a breach happens, it can threaten the organization's customer base, revenue, and reputation.

Post-breach response services typically also include pre-breach planning, such as the creation of an incident response plan and a risk assessment to identify gaps in security posture, as well as preparing and supporting necessary communications regarding the breach. Post-breach services will include attack detection and threat hunting, and stopping the continuing spread of advanced malware and ransomware encryption in an on-going attack.

Leaders in post-breach response services include IBM, Verizon, AT&T, NTT Security, BAE Systems, and Accenture.

The Cybersecurity value chain

Leaders and challengers in post-breach response services



	Leaders		Challengers	
Post-breach response services	IBM Verizon AT&T	NTT Security BAE Systems Accenture	KPMG Secureworks CrowdStrike	Cisco PwC Sophos

Source: GlobalData

Impact of COVID-19 on Cybersecurity in Medical

The COVID-19 pandemic has had unanticipated and significant impacts on all industries around the globe. This report will summarize the pandemic's impact on Cybersecurity, specifically within the Healthcare space.

Today, organizations are plagued by cyberattacks that are advanced, persistent, and which can wreck both operations and reputation. Companies manage an array of assets, including infrastructure, applications, managed and unmanaged endpoints, mobile devices, and cloud services, all of which can be attacked. Attack types include phishing (the most popular) and ransomware (becoming the most lucrative).

The COVID-19 pandemic has only heightened the pre-existing need for cybersecurity in the healthcare sector. As physical lockdowns and social distancing measures are increasingly mandated around the globe in an effort to curb the transmission of the virus, workplaces and healthcare providers are turning to digital means to stay connected and keep business afloat. As the importance of cybersecurity becomes increasingly apparent throughout the pandemic, spending on cybersecurity will show itself to be immune to any pandemic-induced reduction. Companies worldwide are expected to spend $115bn on security in 2020, according to GlobalData figures. The global security industry will be worth nearly $238bn by 2030, having grown at a compound annual growth rate (CAGR) of 6.4% between 2019 and 2030.

Trends in Cybersecurity in Healthcare – Impact of COVID-19

Work from home mandates force cybersecurity initiatives to move quickly

The rush to remote working in many places around the world in mid-March 2020 meant that many corporate IT security teams did not have enough time to put security defenses in place to protect cyber-naïve home workers. The proportion of attacks targeting home workers increased from 12% of malicious email traffic before the UK's lockdown began in March to more than 60% six weeks later, according to cybersecurity company Darktrace.

Soon after lockdown, law enforcement agencies warned of a large increase in pandemic-related fraud, using tactics designed to piggyback on COVID-19-related issues. Examples included phishing emails relating to sales of phony coronavirus test kits and fake personal protective equipment (PPE). Hackers also targeted hospitals with ransomware and used a popular university dashboard showing COVID-19 cases as a vehicle to deliver Android spyware.

While some companies have had a remote working structure in place for several years, many preferred their staff to work from offices. Suddenly, the entire organization had to be allowed to work remotely, so the breadth and depth of remote working - and the risk - dramatically increased.

There will be financial fallout from COVID-19, which may mean that companies reduce their security costs. Firms already looking for cost reductions across functions will ask themselves if they have the right model for security and whether they should look at cybersecurity differently as part of any post-COVID-19 corporate transformation.

Companies explore new avenues to establish solid cybersecurity in response to heightened risk during COVID-19 pandemic

Companies in the healthcare field, from medical device manufacturers to healthcare service providers and more, are like any other company in their increased vulnerability to cyberattacks during the COVID-19 pandemic. Companies have been forced to establish what their strategic operational initiatives will be to address the effects of COVID-19 and the role cybersecurity plays. Some of the initiatives that organizations have deployed include:

- Realignment and prioritization of IT programs, with a particular focus on more tactical short term solutions
- Provision of adequate security measures for remote workers
- Assurance of credible cloud security measures as greater pressure is placed on accessing data outside the enterprise network

Hospitals must balance the need for remote sharing of clinical results with the need to protect personal patient information from cyberattack

As the need to maintain social distance remains paramount throughout the pandemic, healthcare providers must find ways to share important clinical data with each other while remaining physically distanced. In order to share information remotely, many hospitals and clinics are turning to cloud-based sharing software, which comes with an inherent elevated level of risk to cyberattack. One solution to this problem is for healthcare providers to partner with technology firms that specialize in both IT and cybersecurity. As one example, SWASH, a British consortium of National Health Service (NHS) trusts, recently partnered with Sectra, an international medical imaging IT and cybersecurity company. With this partnership, Sectra will manage all of SWASH's medical imaging as well as software used to interpret the images, using their own secure cloud. This solution actually lowered the operational costs for SWASH while providing the consortium with a unified, protected solution for data storage and sharing. Further partnerships such as this are likely to be observed as more and more healthcare providers transition to cloud-based data sharing with heightened need for data protection.

Training on cybersecurity for remote workers is in high demand

With so many employees across almost every industry working remotely during the pandemic, the need to provide these employees with adequate cybersecurity awareness training has skyrocketed. The healthcare field is not exempt to this trend, with remote workers often having access to sensitive patient information. Even government organizations are doing their part to raise awareness; for instance, the Government of Canada produced a website complete with multiple resources and guidance for how to "stay cyber-healthy" during COVID-19, including tips on how to protect against cyberattack while working from home. Private companies have also taken advantage of the need for cybersecurity training; in May 2020, Microsoft announced availability of the Microsoft Cybersecurity Awareness Kit. The kit contains videos, interactive courses, posters, and infographics all designed to raise employee awareness of the dangers of cyberattack during COVID-19. As the pandemic continues, the demand for this type of training will continue to increase.

COVID-19 contact tracing apps raise cybersecurity concerns

Many countries around the world have developed and started launching digital contact tracing apps, with the ultimate goal of reducing future COVID-19 outbreaks. The idea behind these apps is to trace the location of anybody who tests positive for COVID-19 infection, thereby identifying others who may have come into contact with them; this way, others can be notified of their proximity to a positive case and can be tested themselves. Since these apps would collect sensitive, private health and location information from potentially millions of people worldwide, the need for cybersecurity within these apps is paramount. Many organizations have published reports delineating exactly what would be needed to maintain adequate cybersecurity with contact tracing apps, and app developers such as Google and Apple have responded to these concerns by listing their current practices in place to ensure cybersecurity and user privacy. Even so, many are still worried about inherent cybersecurity flaws in Bluetooth technology, upon which most contact tracing apps will be based. The most likely scenario is that app developers will have to work with cybersecurity specialists and government bodies to ensure cybersecurity needs are met within these apps.

Winners from COVID-19

Winners include cybersecurity software providers and cybersecurity training providers:

- **Providers of cybersecurity software:** CrowdStrike, Palo Alto Networks, Check Point, McAfee, Sectra
- **Providers of cybersecurity training:** KnowBe4, Microsoft

Losers from COVID-19

Losers include any company that is not enhancing its cybersecurity platform in response to heightened vulnerability during the COVID-19 pandemic.

Companies

In this section, GlobalData highlights the listed, private and healthcare companies that are making their mark within the cybersecurity theme.

Public companies

The table below lists some of the leading public companies impacted by this theme and summaries their competitive position.

Company	Country	Competitive position in the Cybersecurity theme
BlackBerry	Canada	BlackBerry's $1.4bn acquisition of Cylance in 2019 pitched a company that made its name with smartphones into the center of the cybersecurity market. BlackBerry's heritage in enterprise messaging gives it a strong play in the mobile security space, and Cylance's ML technology fills a security gap in BlackBerry's Spark IoT communications platform. Cylance's endpoint detection and response technology also beefs up BlackBerry's product catalog. Like many next-generation endpoint providers, BlackBerry now finds itself in the managed services business because cybersecurity's complexity makes it too difficult for companies to run independently.
Broadcom	US	Having initially considered buying all of Symantec, Broadcom eventually acquired just the enterprise security business and then sold the managed services operation to Accenture. After previously buying Brocade, which made data center and enterprise storage networking equipment, and mainframe software company CA Technologies, Broadcom increased its infrastructure software position through the Symantec purchase. The last major chip company to buy a cybersecurity company was Intel, which bought McAfee in 2010 and sold it to private equity seven years later.
Check Point Software	Israel	Check Point has come under pressure from competitors such as Palo Alto Networks and faced criticism over its pricing policies. Although Check Point once had almost 180,000 security appliance customers, it is believed to have lost several thousand over perceived issues with pricing and ease of use. Check Point previously lacked network intelligence and wireless network security offerings, but its purchase of Dome9 in 2018 enabled a move into network security intelligence for AWS, Azure, and Google, delivering cloud intrusion detection, network traffic visualization, and user activity analytics.
Cisco Systems	US	At the end of May 2020, Cisco announced plans to acquire ThousandEyes, an internet intelligence firm whose network intelligence platform focuses on the user experience and network performance. The platform gathers data from various points throughout the public internet to identify dependencies that impact service delivery. Three months earlier, in February 2020, Cisco launched Securex, a security portfolio offering endpoint, network, and cloud-level security focused on incident response, managed detection and response, and zero trust advisory. Cisco's security business is dwarfed by its revenue from networking, and recent initiatives only reinforce the impression that Cisco primarily regards security as a means to increase the size of its networking deals.
FireEye	US	FireEye is a strong player in external threat intelligence services. However, its offering lacks the breadth of its rivals. This has resulted in customer churn and lower margins which, coupled with a recent restructuring, fueled rumors that FireEye could be acquired, either by a rival or by a private equity company. The speculation grew when it emerged that the company had spoken with advisors to explore a potential sale. Cisco has frequently been mooted as a possible buyer but has so far ruled out an acquisition.

Company	Country	Competitive position in the Cybersecurity theme
Fortinet	US	Fortinet is mounting a challenge to Cisco in several security areas, including next-generation firewall (NGFW), intrusion prevention systems (IPS), wireless, sandboxing, and cloud. It has also been making acquisitions, buying CyberSponse, a SOAR platform provider, and EnSilo, a privately-held advanced endpoint security company. Areas that Fortinet is perceived to be behind on are ML and behavioral analytics. This is also where Cisco and Palo Alto Networks, its key competitors, are making big bets. Cloud service providers are the backbone of global internet trade, and that is where Fortinet is strong.
IBM	US	IBM has arguably the industry's most extensive managed security portfolio, covering all the critical IT security domains, including governance, risk and compliance, identity management, and data applications and infrastructure security. It has also done significant work in key areas such as cloud security and mobile security. Its managed security offering, while comprehensive, is also complex, making it hard for mid-sized organizations to navigate the catalog and find solutions that are appropriate for their organization. IBM's offerings can be bought as discrete solutions, packaged together, or bundled with other managed services.
Microsoft	US	Microsoft has strong capabilities in AI and is putting this to work within Microsoft 365 Enterprise, automatically remediating endpoint cyberattacks. Late in 2019, it launched a production version of its Sentinel on-demand SIEM service. Azure Sentinel promises a complete view of the full threat landscape, applies ML and other AI technologies to assess security data and investigate threats, and incorporates automation to expedite both deployment and incident response times. In mid-May 2020, Microsoft introduced new COVID-19 threat intelligence sharing feeds for Azure Sentinel customers and also made them available for non-Azure users on GitHub. The move means that even those who are not Microsoft customers can improve their protection against COVID-19-themed cyberattacks.
Palo Alto Networks	US	Palo Alto Networks went on a spending spree in 2019, acquiring five companies: Aporeto, Zingbox, Twistlock, PureSec, and Demisto. From a beginning in firewalls, Palo Alto has become one of the largest cybersecurity companies in the world, securing endpoints, networks, and the cloud with products including NGFW, endpoint, and cloud-based security products including CASBs, sandboxing, threat intelligence, and virtual firewalls. In March 2020, its spending spree continued with the acquisition of SD-WAN provider CloudGenix.
Secureworks	US	Secureworks offers a range of managed and consultative security services centered on its Counter Threat Platform (CTP), emphasizing accelerated threat detection to limit the effects of a breach. In March 2020, it launched a new SOAR solution that merges technology, managed services, and incident response capabilities while providing context for incidents based on other elements in the customer's environment. Secureworks also offers a well-regarded incident response retainer that provides proactive as well as reactive response services. Secureworks generally has lower visibility in Europe and Asia-Pacific for managed security services compared with its position in the US market.
Verizon	US	Verizon provides managed security services with a particular focus on advancing threat intelligence. In March 2019, it acquired network detection and response vendor ProtectWise. Verizon's managed security services portfolio is strong because it offers a broad set of intelligence-based security protections that, along with its integrated network security capabilities and emphasis on effective governance, risk, and compliance management, appeal to a broad cross-section of multinational customers.

Source: GlobalData

Private companies

The table below lists some of the interesting private companies associated with this theme and summarizes their competitive position.

Company	Country	Competitive position in the Cybersecurity theme
Balbix	US	Balbix is a startup with the right specialism at the right time: AI in cybersecurity. Balbix uses AI to assess various platforms on the web for breach risk, focusing on providing solutions for apps and other assets in a network. The Balbix Brain also prescribes a prioritized set of necessary actions to improve a user's cybersecurity posture. One of its backers is former Cisco chief executive John Chambers' JC2 Ventures fund.
Beyond Identity	US	Beyond Identity wants to replace passwords with an approach that employs self-signed X.509 digital certificates on endpoint devices to change the way users log in to the network. The company launched publicly in April 2020 with $30m in Series A funding, having operated in stealth mode for a year under the name ZeroPW. The company's two co-founders have a long Silicon Valley history. Jim Clark founded pioneering web browser Netscape and Silicon Graphics while Thomas Jermoluk was president and chief operating officer of Silicon Graphics.
Bitglass	US	With businesses now moving operationally important workloads to the cloud, securing those environments is top of mind. Bitglass is one of a growing number of cloud access security brokers, which protect critical corporate resources delivered via an on-demand model. The company aims to secure any software as a service (SaaS) app, custom app, or infrastructure as a service (IaaS) platform, offering data protection, zero-day threat protection, monitoring, and identity and access management. Bitglass incorporates file and field-level encryption that preserves search and sort, regional data sequestration, unmanaged app control, and agentless mobile security for organizations operating a bring-your-own-device (BYOD) policy.
Cybereason	US	Boston-based Cybereason provides endpoint detection software. Its automated hunting engine looks for unusual behavioral patterns, blocks known attacks, and aggregates good and bad behavioral data to simplify investigation. It received $200m in funding in 2019, bringing its investment total to almost $400m. In February 2020, the company disclosed that it had uncovered a malware campaign using Bitbucket repositories to launch cyberattacks.
Darktrace	UK	Darktrace was founded by Cambridge University mathematicians and government cyber intelligence experts in the US and UK. Its original AI technology, the Enterprise Immune System, was supplemented by the company's Antigena autonomous response technology, which allowed the Enterprise Immune System to react to in-progress cyberattacks, giving hard-pressed security teams the time they need to catch up. In November 2017, Darktrace launched a new business unit, Darktrace Industrial, to fight threats in industrial and SCADA networks.
ForgeRock	US	ForgeRock specializes in digital identity, providing a platform that consists of identity management, access management, user-managed access, directory services, edge security, and an identity gateway. In April 2020, it raised $93.5m in Series E funding and has now raised more than $230m since its foundation. The company's Identity Cloud, Identity Governance, and Autonomous Identity products use AI and ML to manage areas such as overprovisioned user access rights more effectively.

Company	Country	Competitive position in the Cybersecurity theme
Palantir Technologies	US	Palantir was created by Silicon Valley billionaire investor Peter Thiel in 2004. In 2020, it is heading for revenues of $1bn and possibly an IPO. The Palo Alto company specializes in data analytics and has close links to the US government, particularly the Department of Defense. A Palantir web app is being used by staff at the US Centers for Disease Control and Prevention to help it see where COVID-19 is spreading. The company has also helped the UK's National Health Service deal with the pandemic.
Recorded Future	US	Recorded Future is another threat intelligence company using ML to detect new malware entities. In May 2019, Insight Partners took a controlling interest in the company valuing it at more than $780m. Recorded Future is, at the time of writing, the world's largest privately-held threat intelligence software company, with more than 400 clients. One of its latest is the US Cyber Command, one of 11 unified commands of the US Department of Defense (DoD). Under the $50m contract, Recorded Future will provide commercial threat reporting to support US CyberCom's ability to direct the operation and defense of specified DoD information networks.
Secret Double Octopus	Israel	Secret Double Octopus (SDO) is an Israeli software company which replaces vulnerable passwords with password-less MFA. Its proprietary phone-as-a-token tech sets out to prevent unauthorized use of a system and identity theft. Its Octopus Authentication Server lets employees forego a password when logging into workstations, cloud services, legacy applications, and other common workplace tools.
SentinelOne	US	SentinelOne, which provides an ML-based solution for monitoring and securing laptops, phones, and containerized applications, gained Series E funding of $200m in February 2020 that took its market valuation to $1.1bn. The company has Israeli cyber-intelligence roots but is based in Silicon Valley.
Sophos	UK	Sophos is a UK cybersecurity company that was acquired by Thoma Bravo in March 2020. A key part of Sophos's product set is its Cloud Optix tool, which aims to automate and simplify the detection and response of cloud security vulnerabilities and misconfigurations to reduce risk exposure. The tool uses AI to reduce alert fatigue and shrink incident response and resolution times by identifying the risk, profiling the security and compliance risks, and providing contextual alerts that group affected resources, while also adding detailed remediation steps. In early June, Thoma Bravo said that it plans to reduce headcount at Sophos by up to 16% and close some facilities due to the coronavirus pandemic. Thoma Bravo wants to accelerate development of Sophos's new product portfolio, including its cloud-managed protection capabilities, the fastest growing part of its business.

Source: GlobalData

Healthcare companies

The table below lists some of the interesting healthcare companies associated with this theme and summarizes their competitive position.

Company	Country	Competitive position in the Cybersecurity theme
Clearwater Compliance (Private)	US	Clearwater Compliance is a leading provider of healthcare compliance and cyber risk management solutions. Its mission is to empower hospitals and health systems to successfully manage healthcare's evolving cybersecurity risks and ensure patient safety.
CynergisTek (Public)	US	CynergisTek is a cybersecurity and information management consulting firm dedicated to serving the healthcare industry. Since 2004, CynergisTek has offered specialized services and solutions to help organizations achieve privacy, security, and compliance, as well as to document output goals. The company has partnered with hundreds of healthcare organizations and has been named in numerous research reports as one of the top firms that provider organizations turn to for privacy and security. Additionally, CynergisTek won the 2017 Best in KLAS award for Cyber Security Advisory Services.
Fortified Health Security (Private)	US	Fortified Health Security is a cybersecurity firm that focuses solely on serving the healthcare market. Fortified focuses on strengthening client security posture over time by working closely with organizations to assess risk, implement safeguards to protect sensitive information, and assist with compliance to state, HIPAA, and other federal regulations. The company was named the 2018 North American IoT Company of the Year by Frost & Sullivan for its strong overall performance and impressive portfolio of healthcare cybersecurity solutions.
MedCrypt (Private)	US	MedCrypt's APIs are used to encrypt data sent to and from devices. Commands sent to a device are all cryptographically signed. The device communicates with a locally installed MedCrypt Node, which manages users' public keys and user permissions, as well as validates data signatures. MedCrypt specifically works for medical devices, but does not also work for PCs.
Medigate (Private)	Israel	Medigate is a dedicated medical device security platform that protects all of the connected medical devices on healthcare provider networks by delivering complete visibility into devices and risk, detecting anomalies, and actively blocking malicious activities. Medigate identifies and classifies the specific type of device including its make and model, understands its normal communications and operations, and provides full visibility into their risk and security status.
Protenus (Private)	US	Protenus protects patient data security with timely alerts to suspicious activity in the electronic health record (EHR). It also mitigates both risk and public exposure, reinforces trust across the enterprise, and enhances patient privacy.
Vizient, Inc. (Private)	US	Vizient is a healthcare performance improvement company that empowers members to deliver exceptional, cost-effective care. Vizient formed the Medical Device Cybersecurity Task Force in June 2017 in order to provide leadership and facilitate collaboration to minimize the risk and cost of medical device cybersecurity, as well as to foster standardized practices for the benefit of the healthcare industry.

Source: GlobalData

Glossary

Term	Definition
5G	5G refers to the fifth generation of cellular technology standards that will be based on IMT2020 standards, under development by the 3GPP. The term '5G' does not explicitly refer to any particular technology or standard and is therefore a loose term that can be used and interpreted in multiple different ways, typically for marketing purposes.
Advanced persistent threat	A sophisticated, systematic cyberattack program that continues for an extended period of time, often orchestrated by a group of skilled hackers
Antivirus	Software designed to identify and remove computer viruses or other malware on an organization's devices or IT systems.
Artificial intelligence (AI)	Refers to software-based systems that use data inputs to make decisions on their own.
Attack surface	The totality of different points where hackers could enter or extract data from an environment. Applies to software, networks, and humans, and represents the sum of an organization's security risk exposure.
Authentication	Process in which a user's credentials are compared to what is listed in a database of authorized users' information. Two-factor authentication involves signing in with known login information plus a second "factor," such as a physical token.
Botnet	A robot network of private computers infected with malicious software and controlled as a group without the owner's knowledge
Chief information security officer (CISO)	The role of the CISO is to protect a company's assets (both physical and digital) from cyberattack.
Cloud access security broker	On premise or cloud based software that sits between cloud service users and cloud applications to monitor all activity and enforce security policies
Cloud computing	Computing delivered as an online service. It encompasses the provision of IT infrastructure, operating software, middleware and applications hosted within a data center and accessed by the end user via the internet.
Cloud security posture management (CSPM)	A collection of tools used to reduce customer configuration and setup errors in cloud environments which are behind most cloud security mishaps.
Cross-site scripting (XSS)	A common type of cyberattack in which malicious scripts are injected into websites and web applications and run on an end user's platform,
Cybercrime	Any crime that involves a computer and a network.
Cybersecurity	The practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.
Deepfakes	Visual or audio content that has been manipulated or generated using artificial intelligence, with the intention of deceiving the audience.
DevOps	A set of practices automating the processes between software development and IT teams, so they can build, test, and release software faster and more reliably.
DevSecOps	DevSecOps is the philosophy of integrating security practices within the DevOps process. It involves creating a 'security as code' culture with ongoing, flexible collaboration between release engineers and security teams.
Distributed denial-of-service (DDOS)	A coordinated attack in which multiple connected machines in a botnet, usually infected with malware or otherwise compromised to co-opt them into the attack, flood a network, server, or website with so much data as to make it unusable.
Encryption	A method for scrambling a message, file, or other data and turning it into a secret code. The code can only be read using a "key" or other piece of information (such as a long string of numbers), usually created with an algorithm
Edge computing	Refers to a network architecture concept that enables cloud computing capabilities and an IT service environment at the edge of the network. By running applications and performing

Term	Definition
	processing tasks closer to the customer, edge computing delivers superior performance with reduced latency.
Endpoint	An internet-capable computer hardware device on a TCP/IP network. Typically includes desktop computers, laptops, smartphones, tablets, thin clients, printers, or other specialized hardware such as POS terminals and smart meters.
Endpoint security	A method for protecting the corporate network when accessed via remote devices such as laptops or other wireless and mobile devices. Each device with a remote connection to the network creates a potential entry point for security threats.
Firewall	A security system that blocks unauthorized access to a network. Firewalls typically monitor and control traffic between an internal network (trusted to be secure) and an external network (not trusted).
General Data Protection Regulation (GDPR)	A regulation that came into force across the EU in May 2018, giving consumers certain rights and protections over the data that organizations hold on them, including the right to data portability.
Hacker	A person who uses computers to gain unauthorized access to data.
Hacktivism	Computer or internet hacking activities motivated by social or political causes.
Identity management	A method to identify individuals or machines in an IT system and control their access to resources within that system by associating user rights and restrictions with each established identity.
Incident response	An organization’s structure for managing, mitigating and resolving cybersecurity events, such as breaches.
Industrial control system (ICS)	Systems and associated instrumentation, including devices, systems, networks, and controls, used to operate or automate industrial processes.
Internet of Things (IoT)	An umbrella term used to describe the use of connected sensors and actuators to control and monitor the environment, the things that move within it, and the people that act within it.
Machine learning	An application of AI that gives computer systems the ability to learn and improve from data without being explicitly programmed.
Malware	Malicious or hostile software used to attack or infiltrate a computer system or network. Often embedded in non-malicious files or programs, malware includes computer viruses, worms, ransomware and spyware.
Managed security services	Network security or cybersecurity monitoring services outsourced to a service provider. Services may which may include virus and spam blocking, intrusion detection, firewalls and virtual private network (VPN) management.
Multi-factor authentication (MFA)	Sometimes referred to as two-factor authentication or 2FA, multi-factor authentication is a security enhancement that allows someone to present two pieces of evidence – their credential – when logging in to their account.
Network security	The process of using specialized hardware and software to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction or improper disclosure, thereby creating a secure platform for computers, users, programs and tools.
Next-generation firewall (NGFW)	A network security device that provides capabilities beyond a traditional firewall. While a traditional firewall typically provides inspection of incoming and outgoing network traffic, a next-generation firewall includes additional features like application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence.
Orchestration	Establishing, centralizing, and standardizing threat detection and incident response procedures. Includes automation and integration of different security workflows, technologies and tools.

Term	Definition
Penetration testing	This refers to techniques for actively testing an organization's computer or network security, usually by identifying potential vulnerabilities and weak spots and trying to exploit them.
Phishing	A practice in which an attacker pretends to be a trusted entity by using fake emails and websites in order to steal sensitive data such as passwords or credit card details.
Privileged access management (PAM)	Cybersecurity strategies and technologies used to exert control over the privileged access and permissions for users, accounts, processes, and systems.
Ransomware	A type of malware that prevents access to the target's computer system or data until a ransom is paid to the attacker. Often uses encryption to lock up files or IT systems, holding them hostage until money is paid for a decryption key.
Remediation	What an organization does to limit or stop an attack once it is detected, as part of incident response. Includes things like blocking IP addresses, removing infected files or devices, and restoring affected systems to a known good state.
Sandbox	A security mechanism for separating running programs. It is often used to execute untested or untrusted programs, or code from untrusted sources, without risking harm to the host machine or operating system.
Security information and event management (SIEM)	The combined process of incident detection and incident response. Includes features such as alerts, analytics, dashboards and forensic analysis.
Security orchestration, automation and response (SOAR)	Refers to a collection of software solutions and tools that allow organizations to streamline security operations in three key areas: threat and vulnerability management, incident response, and security operations automation.
Smart city	A city that uses connected sensors to enhance the quality and performance of urban services such as energy, transport and utilities to make the city function more efficiently.
Software as a service (SaaS)	SaaS is IaaS plus PaaS and the application that runs on them. The software is usually invoiced on a per user subscription basis or on a transactional basis. SaaS allows users to access applications over the internet that are managed by a third-party vendor without having to download the software locally (e.g. Salesforce).
Software defined everything (SDE)	An environment in which all aspects of an application and the infrastructure it needs to operate are defined, configured, and managed at runtime in software.
Software defined networks (SDN)	An emerging architecture for data networks. It allows software – rather than hardware – to control the network path along which data packets flow. It is still under development but, ultimately, it may replace IP networking, a hardware standard, as the main standard governing the transmission mechanisms of the internet.
Software defined wide-area networks (SD-WAN)	The application of the core principles of SDN to wide-area networking technology.
Supervisory control and data acquisition (SCADA)	A system comprised of software and hardware used to control and monitor a process or application. A typical application for SCADA would be monitoring or controlling an industrial process, or collecting, processing and analyzing real-time data.
Threat detection	Methods for identifying system vulnerabilities and hacking behaviors. Can include any number of technologies, including ML, statistical modeling, and network traffic monitoring.
Threat intelligence	Refers to data collected and analyzed by an organization in order to understand a cyber threat's motives and attack behaviors
Unified threat management (UTM)	A cybersecurity solution that combines multiple security functions – network firewalling, intrusion detection and prevention, anti-virus, anti-spam, content-filtering and leak prevention etc. – within a single security system.
Virtual private network (VPN)	A private network (e.g. a corporate network) that extends across a public network (e.g. the internet). VPNs are used to allow secure remote access to documents across unsecured public networks.

Term	Definition
Virus	A type of malware that, when executed, copies itself and infects other computer programs by modifying them.
Vulnerability	A weakness that allows an attacker to compromise an application, device, or network.
Worm	A type of malware that is standalone (unlike a virus, which is attached to another program) and spreads to other machines by replicating itself. Worms are capable of highly targeted attacks, such as the Stuxnet worm allegedly used to disrupt Iran's nuclear program in 2009-10.
Zero-day attack	A hack that exploits a vulnerability in software that is unknown to the security vendor at the time of exploit. The security vendor therefore has "zero days" to fix it.
Zero trust	A security model that uses strict identity verification for every person or entity attempting to access an organization's network resources, regardless of whether the person or entity is in the office bound by the network perimeter or accessing the network remotely.

Source: GlobalData

Further reading

GlobalData reports

Publication date	Report title
24 June 2020	Thematic Research: Cybersecurity (2020)
10 April 2020	Analyst Briefing: Considerations for Cybersecurity in Healthcare
31 Mar 2020	Analyst Briefing: Cybersecurity poses increased concern amid COVID-19 outbreak
31 Mar 2020	Analyst Briefing: COVID-19: Impact on Cybersecurity
01 Oct 2019	Emerging Technology Trends Survey - Cybersecurity
11 Sept 2019	Digital Innovation Case Studies – Cybersecurity
31 Oct 2018	FDA Releases New Guidance on Medical Device Cybersecurity

Source: GlobalData

Our thematic research methodology

Companies that invest in the right themes become success stories. Those that miss the important themes in their industry end up as failures.

Viewing the world's data by themes makes it easier to make important decisions

We define a theme as any issue that keeps a CEO awake at night. GlobalData's thematic research ecosystem is a single, integrated global research platform that provides an easy-to-use framework for tracking all themes across all companies in all sectors. It has a proven track record of identifying the important themes early, enabling companies to make the right investments ahead of the competition, and secure that all-important competitive advantage.

Traditional research does a poor job of picking winners and losers

The difficulty in picking tomorrow's winners and losers in any industry arises from the sheer number of technology cycles – and other themes – that are in full swing right now. Companies are impacted by multiple themes that frequently conflict with one another. What is needed is an effective methodology that reflects, understands, and reconciles these conflicts.

That is why we developed our "thematic engine"

At GlobalData, we have developed a unique thematic methodology for ranking all companies in all sectors based on their relative strength in the big investment themes that are impacting their industries. Our thematic engine identifies which companies are best placed to succeed in a future filled with multiple disruptive threats.

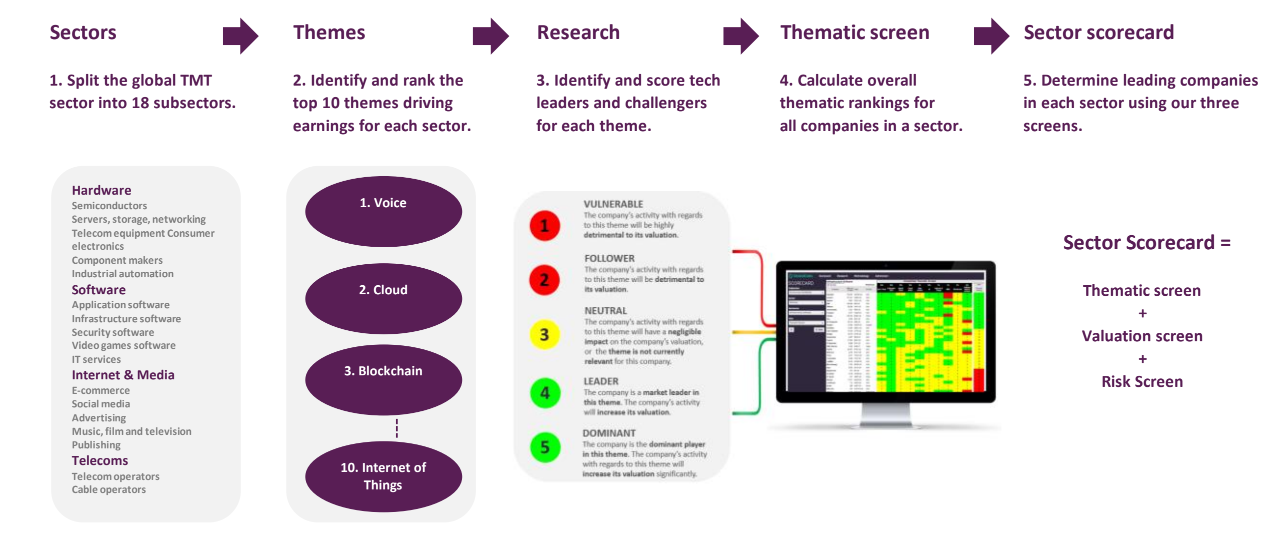
To do this, we rate the performance of the top 1,000 companies against the 50 most important themes impacting those companies, generating 50,000 thematic scores. The algorithms in GlobalData's thematic engine help to identify the long-term winners and losers within each sector.

How do we create our sector scorecards?

First, we split each industry into its component sectors, because each sector is driven by a different set of themes. Taking the TMT (technology, media and telecom) industry as an example, we split this industry into the 18 sectors shown in the graphic below.

Our five-step approach for generating a sector scorecard

Here we use the tech, media and telecom sector as an example sector, for illustration purposes



Sectors

1. Split the global TMT sector into 18 subsectors.

Hardware
Semiconductors
Servers, storage, networking
Telecom equipment Consumer electronics
Component makers
Industrial automation
Software
Application software
Infrastructure software
Security software
Video games software
IT services
Internet & Media
E-commerce
Social media
Advertising
Music, film and television
Publishing
Telecoms
Telecom operators
Cable operators

Themes

2. Identify and rank the top 10 themes driving earnings for each sector.

1. Voice
2. Cloud
3. Blockchain
10. Internet of Things

Research

3. Identify and score tech leaders and challengers for each theme.

1 VULNERABLE
The company's activity with regards to this theme will be highly **detrimental to its valuation.**

2 FOLLOWER
The company's activity with regards to this theme will be **detrimental to its valuation.**

3 NEUTRAL
The company's activity with regards to this theme will have a **negligible impact** on the company's valuation, or the **theme is not currently relevant** for this company.

4 LEADER
The company is a **market leader in this theme.** The company's activity will **increase its valuation.**

5 DOMINANT
The company is the **dominant player in this theme.** The company's activity with regards to this theme will **increase its valuation** significantly.

Thematic screen

4. Calculate overall thematic rankings for all companies in a sector.

Sector scorecard

5. Determine leading companies in each sector using our three screens.

Sector Scorecard =
Thematic screen
+
Valuation screen
+
Risk Screen

Source: GlobalData

Second, we identify and rank the top 10 themes for each sector (these can be technology themes, macroeconomic themes, or industry-specific themes). Third, we publish in-depth research on specific themes, identifying the winners and losers within each theme. The problem is that companies are exposed to multiple investment themes and the relative importance of specific themes can fluctuate. So, our fourth step is to create a thematic screen for each sector to calculate overall thematic leadership rankings after taking account of all themes impacting that sector. Finally, to give a crystal-clear picture, we combine this thematic screen with our valuation and risk screens to generate a sector scorecard used to help assess overall winners and losers.

What is in our sector scorecards?

Our sector scorecards help us determine which companies are best positioned for a future filled with disruptive threats. Each sector scorecard has three screens:

- **The thematic screen** tells us who are the overall technology leaders in the 10 themes that matter most, based on our thematic engine;
- **The valuation screen** tells us whether publicly listed players appear cheap or expensive relative to their peers, based on consensus forecasts from investment analysts; and
- **The risk screen** tells us who the riskiest players in each industry are, based on our assessment of four risk categories: corporate governance risk, accounting risk, technology risk, and political risk.

How do we score companies in our thematic screen?

Our thematic screen ranks companies within a sector based on overall technology leadership in the 10 themes that matter most to their industry, generating a leading indicator of future earnings growth.

Thematic scores predict the future, not the past.

Our thematic scores are based on our analysts' assessment of their competitive position in relation to a theme, on a scale of 1 to 5:

1	**Vulnerable**	The company's activity with regards to this theme will be highly detrimental to its future performance.
2	**Follower**	The company's activity with regards to this theme will be detrimental to its future performance.
3	**Neutral**	The company's activity with regards to this theme will have a negligible impact on the company's future performance, or this theme is not currently relevant for this company.
4	**Leader**	The company is a market leader in this theme. The company's activity with regards to this theme will improve its future performance.
5	**Dominant**	The company is a dominant player in this theme. The company's activity with regards to this theme will significantly improve its future performance.

How our research reports fit into our overall thematic research ecosystem?

Our thematic research ecosystem is designed to assess the impact of all major themes on the leading companies in a sector. To do this, we produce three tiers of thematic reports:

- **Single Theme:** These reports offer in-depth research into a specific theme (e.g. artificial intelligence). They identify winners and losers based on technology leadership, market position, and other factors.
- **Multi-Theme:** These reports cover all themes impacting a sector and the implications for the key players in that sector.
- **Sector Scorecard:** These reports identify those companies most likely to succeed in a world filled with disruptive threats. They incorporate our thematic screen to show how conflicting themes interact with one another, as well as our valuation and risk screens.

About GlobalData

GlobalData is a leading provider of data, analytics, and insights on the world's largest industries.

In an increasingly fast-moving, complex, and uncertain world, it has never been harder for organizations and decision makers to predict and navigate the future. This is why GlobalData's mission is to help our clients to decode the future and profit from faster, more informed decisions. As a leading information services company, thousands of clients rely on GlobalData for trusted, timely, and actionable intelligence. Our solutions are designed to provide a daily edge to professionals within corporations, financial institutions, professional services, and government agencies.

Unique Data

We continuously update and enrich 50+ terabytes of unique data to provide an unbiased, authoritative view of the sectors, markets, and companies offering growth opportunities across the world's largest industries.

Expert Analysis

We leverage the collective expertise of over 2,000 in-house industry analysts, data scientists, and journalists, as well as a global community of industry professionals, to provide decision-makers with timely, actionable insight.

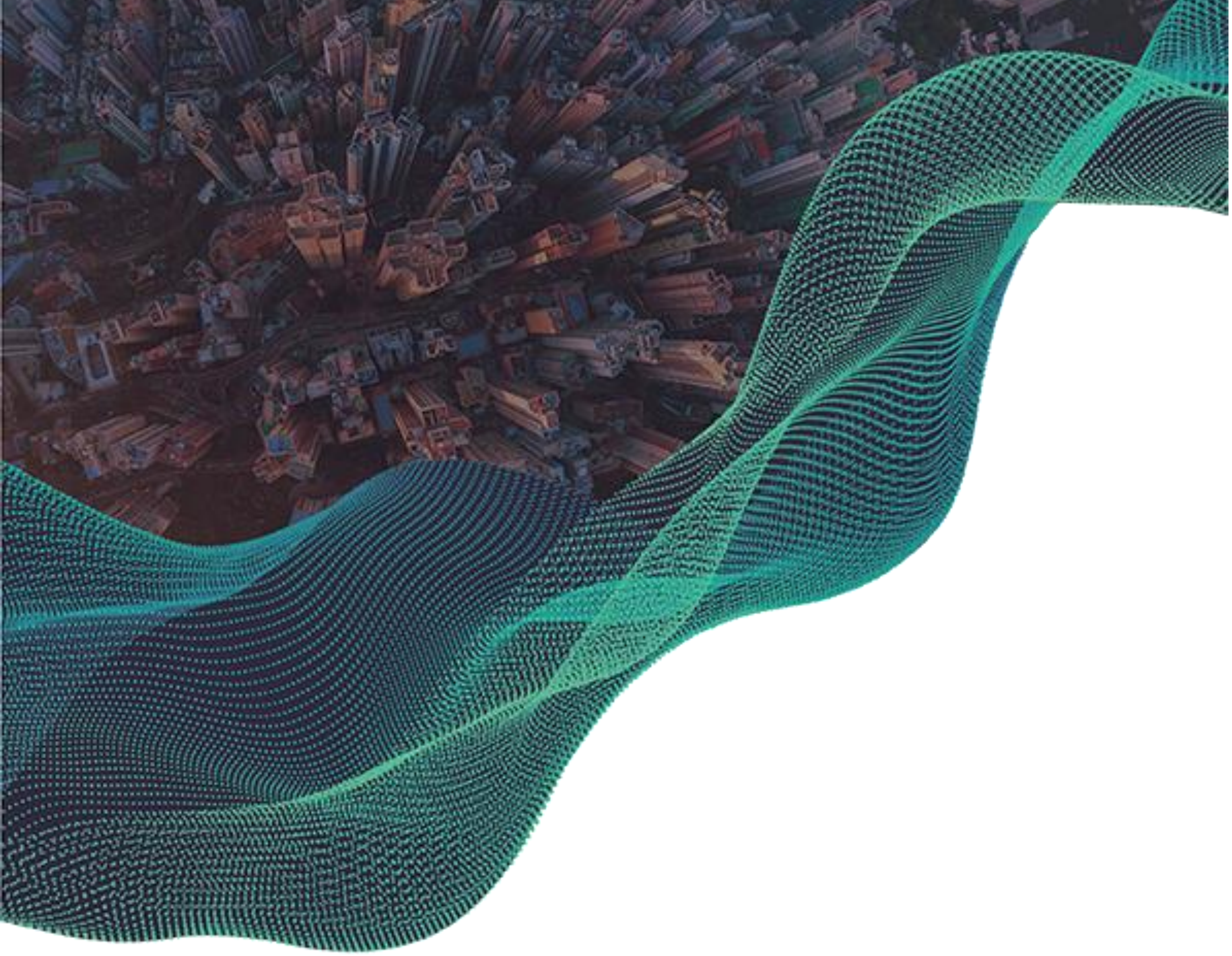
Innovative Solutions

We help you work smarter and faster by giving you access to powerful analytics and customizable workflow tools tailored to your role, alongside direct access to our expert community of analysts.

One Platform

We have a single taxonomy across all of our data assets and integrate our capabilities into a single platform – giving you easy access to a complete, dynamic, and comparable view of the world's largest industries.

Disclaimer: All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher, GlobalData. The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions and recommendations that GlobalData delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such, GlobalData can accept no liability whatsoever for actions taken based on any information that may subsequently prove to be incorrect.



Contact Us

If you have any more questions regarding our thematic research services, please get in touch.

Head of Thematic Research
Cyrus Mewawalla
cyrus.mewawalla@globaldata.com
+44 (0) 207 936 6522

Customer Success
Understand how to use our Themes product
customersuccess.thematic@globaldata.com
+44 (0) 207 406 6764