TEAM8™

2022 Cybersecurity Themes Report

February 2022

Table of Contents

Introduction

In 2021, we continued to see huge changes in IT and cybersecurity, partly as a result of the COVID-19 pandemic. These changes included a continued expansion in remote work, accelerated digital transformation, an increase in cloud adoption, transformations in healthcare, and more. It's incredible just how much of the world became more digital and more connected in such a short timespan. It has been, without a doubt, a year of disruption.

Cyber attackers see disruption as an opportunity. Not only are there more vulnerabilities in our existing infrastructure, but the more humanity moves online and to a more connected reality, the more we also become vulnerable to cyber attacks. In 2021, cybercriminals continued to take advantage of existing and new vulnerabilities, and doubled-down on their exploitation efforts with anything from financial fraud to phishing campaigns to botnets. And on top of this, there was also a tsunami of ransomware, software supply chain attacks, and social media attacks, many of which made major headlines in 2021.

With faster digitization and increased vulnerabilities, there's now a growing resiliency gap that's creating a surge in demand for cybersecurity, specifically the need for Smarter Security and increased resilience in order to both protect and mitigate against cyber attacks. If this gap grows too large or too quickly, it could completely erode public trust in our systems. Trust is the cornerstone of digital civilization, and its deterioration could have dramatic consequences on our society and techno-future.

The impact of the pandemic and the increase in remote work

The increased cybersecurity risk of remote work is clear. Research shows that remote work and digital transformation are responsible for a substantial proportion of data breaches. Remote work has also increased the frequency and cost of these breaches. According to IBM's 2021 Cost of A Data Breach Report, 17.5% of breaches included remote work as a factor, with the cost of a breach increasing by an average of $1.07 million per breach if remote work was a factor. Furthermore, companies with a majority of their workforce working remotely took 58 days longer to detect and contain breaches than those for whom the majority were onsite.[1]

As the pandemic has driven an increase in remote work and accelerated the use of cloud technologies, opportunities for attackers have also expanded, pushing cybersecurity risk far higher up the corporate agenda. The impact from these major events are being felt in every one of our key cybersecurity trends, and will continue to have a significant effect over the next few years as the emergency, short-term measures put in place in 2020 and 2021 become more embedded, and transform into long-term strategic priorities.

Shift in focus for ransomware

Ransomware is not new – IT and cybersecurity professionals have been talking about it and managing it for over a decade. The big difference today is that these attacks can put whole enterprises, as well as critical infrastructure, at risk. In the past, when ransomware was targeting single computers, it was primarily an issue around data – with attackers threatening to limit access. Then, the move to enterprise-wide ransomware changed the goal of the attacker to be around disruption of operations. This has now created an operational resilience risk that can turn whole companies dark, making it both more high profile and more dangerous.

The Colonial Pipeline attack, in which hackers demanding ransom led the company to shut down its entire oil pipeline, brought the issue into sharp relief. Today, ransomware is a genuine existential risk to the survivability of an enterprise.

High profile attacks are leading to increased government response

In 2021, we saw an increased willingness by governments worldwide to step into cybersecurity in the context of commercial enterprises. The Biden administration highlighted cybersecurity as one of its highest priorities, calling it "a national security and economic security imperative." President Biden's Executive Order 14028 on Improving the Nation's Cybersecurity and other recent moves and announcements by the Administration address a range of issues, including that the U.S. government will consider ransomware, even against private companies, as a hostile act against the U.S. government.[2] It also announced that attacks against critical infrastructure would be treated as nation-state attacks, and that it can, and will, use government powers to retaliate.

Other countries are also taking this seriously, seen for example in the European Union's (EU) recent introduction of the Digital Operations Resilience Act (DORA). DORA represents the EU's efforts to unify third-party risk management among financial institutions.[3] Moreover, in November 2021, the UK introduced the Product Security and Telecommunications Infrastructure Bill, which established new cybersecurity requirements for manufacturers and distributors of IoT devices.[4]

What's next for cyber

If change continues at the rate it did in 2021, with a corresponding increase in cyberattacks, enterprises and governments could be in trouble. Now is the time to make the world's technology infrastructure more resilient, including through better automation and improved cybersecurity at the design phase.

As cybersecurity risk continues to move higher up the priority list, inevitably private sector investment has and will continue to increase. This is already evident from recent cyber investment activity in the first half of 2021, which, according to Momentum Partners, shattered all past records, and included 593 M&A and financing transactions equaling $51 billion in deal value. This represents more than a 100% increase from the 293 transactions, and a 250% increase from the $14.5 billion in deal value that was recorded during the first half of 2020.[5]

Much of this private investment is expected to go into areas influenced by recent events, i.e. areas that digital transformation and remote work have impacted. This includes cloud adoption and digital services, both of which will be important drivers of cybersecurity spending.

Finally, identity is at the heart of digital transformation, and abuse of access is viewed as a common factor in breaches, spurring interest in all areas within identity and access management (IAM).

All of these trends inform our seven cybersecurity themes for 2022

7 Themes Driving the Future of Cybersecurity

The following represent Team8's seven cybersecurity themes. Each theme includes the threats and technology trends driving it, as well as the impact of the theme and the key takeaways.

To offer a rounded discussion, we include the views of both defenders and attackers by incorporating perspectives and examples from CISOs in our Village, alongside Team8's Attacker Perspective. We have also offered suggestions on the types of products and services that may serve as solutions, as well as selected providers in each category.

How We Identified Our Themes

To highlight areas of immense future business growth and product development from a technology, market trends, regulatory, and venture funding standpoint, we engaged with experts and specialists across our Village (350+ C-level executives, many from Fortune 500 or Forbes Global 2000 organizations), the Team8 cybersecurity team, and our range of global advisors.

We also considered Team8's "Attacker Perspective" (our unique insights into how attackers think and operate), in addition to publicly-available information and research from a range of well-regarded sources. We then cross-referenced our findings with one-on-one interviews with CISOs & cyber defenders, confirming the top areas of acceleration in cybersecurity from the perspective of security leaders.

We considered both mature and nascent markets to gather a broad perspective and track early, emerging technologies that will influence the future and lead to high-growth opportunities in the next few years.

2022 Cybersecurity Themes by Rate of Acceleration

01

Cloud Security

A massive shift to hybrid and multi-cloud will drive a focus on configuration management and SaaS Security.

02

Smarter Security

More attacks and alerts with less staff to handle the volume, means security must get smarter by using AI and automation.

03

Resilience & Recovery

As ransomware increases and digital infrastructure becomes "business-critical", it's more important than ever to manage cybersecurity resilience proactively, and to be ready to rapidly recovery from attacks at any time.

04

Security of Things

More internet-connected devices creates more vulnerabilities, each which represent a potential breach-point into an organization or to private data.

05

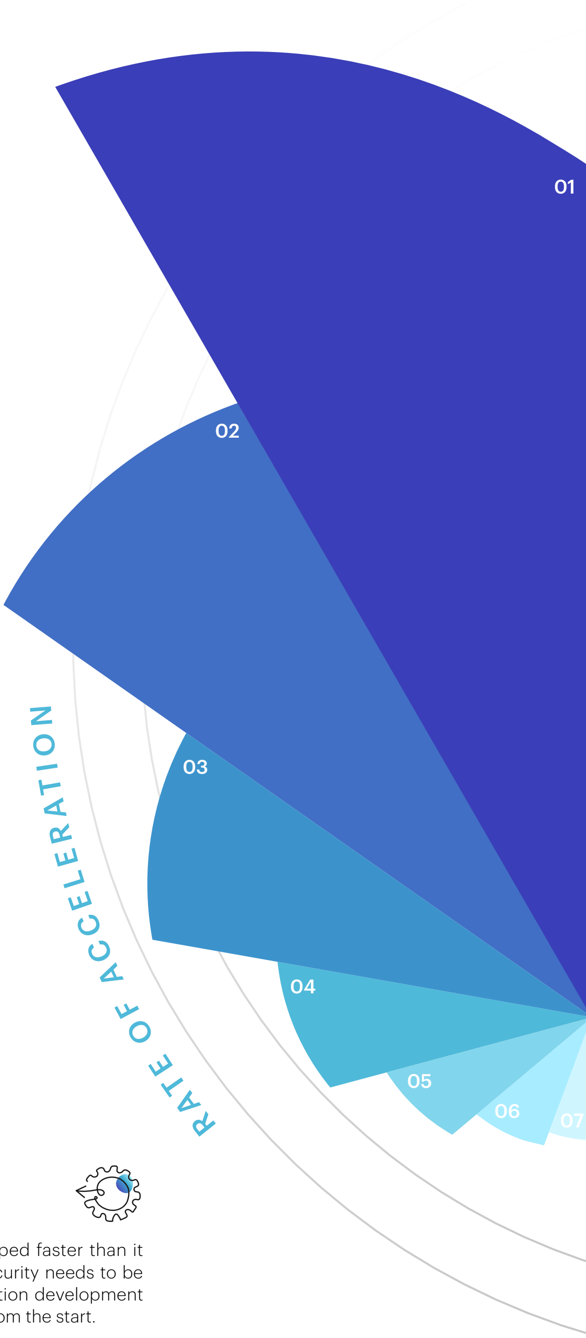
Perimeterless World

The enterprise perimeter is nearly obsolete thanks to accelerated digital transformation and the shift to remote work. The future will require a renewed focus on identity and zero trust solutions.

06

Data Security

As businesses and consumers create richer digital footprints, stronger regulation and consumer preferences will drive investment in data protection and data privacy solutions.



07

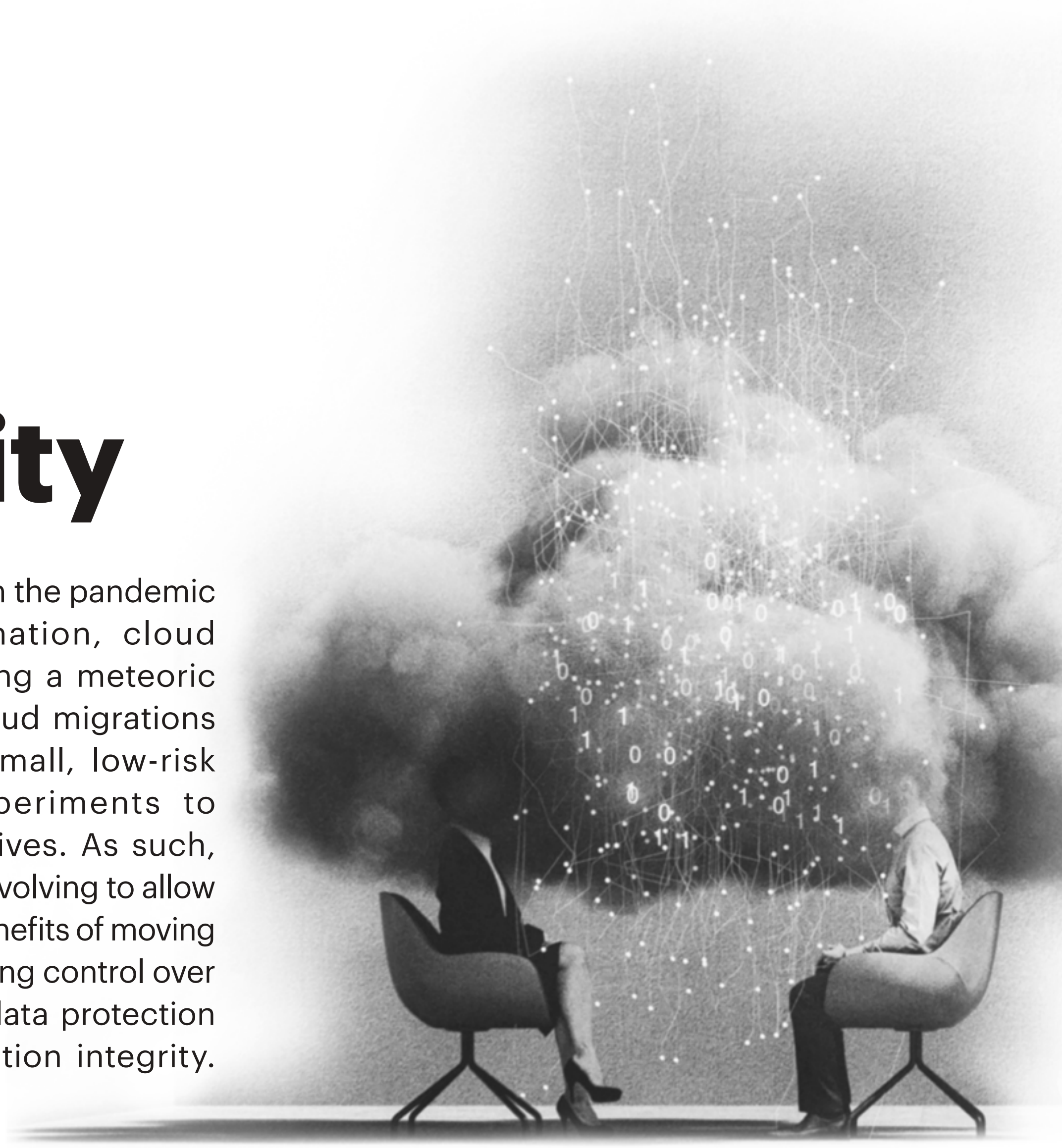
Shift-Left

Software is being developed faster than it can be secured. Cybersecurity needs to be shifted-left in the application development process and embedded from the start.

01

Cloud Security

Buoyed by tailwinds from the pandemic and digital transformation, cloud adoption is experiencing a meteoric rise, and enterprise cloud migrations are expanding from small, low-risk applications and experiments to business-critical initiatives. As such, security capabilities are evolving to allow enterprises to reap the benefits of moving to the cloud, while retaining control over their security posture, data protection programs, and application integrity.



Drivers & Developments:

Cloud Security is easily the number one theme for 2022, as cloud adoption, spurred by pandemic work realities and changes in business models, continues to accelerate. The pandemic forced entire industries to modify and transform operations, with close to one-third of companies viewing cloud adoption as "significantly more important" than prior to the pandemic.[6] As companies work to secure these new and existing cloud deployments, budget allocations to Cloud Security will grow substantially.

Growth of IaaS/PaaS and SaaS driving security needs

The COVID-19 pandemic has accelerated the adoption of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) environments. Organizations are expediting cloud migrations for scale, with most (71%) pursuing a hybrid or multi-cloud strategy, while few (27%) depend on a single cloud for their business requirements.[7] This allows them to integrate multiple services, improve scalability, and manage business continuity, while mitigating the risks that come with using a single vendor.

IaaS/PaaS vendors provide a variety of their own native security controls and configurations, however, these capabilities can be difficult to manage and configure properly in order to provide full Cloud Security to secure multi-cloud environments. As a result, end-users are still having a difficult time holding up their end of the shared responsibility model.

In contrast to IaaS/PaaS, SaaS comprises thousands of offerings, many of which offer limited out-of-the-box security controls. A distributed workforce with unrestricted access to such a large number of apps has caused businesses to see an increase in solutions not managed by the IT team ("shadow IT"). Data indicates that shadow IT increased by nearly 8% between 2020 and 2021, with the average company using a massive 254 apps (and large enterprises of 10k+ employees averaging 364 apps). In 2021, 56% of the apps in use across businesses of all sizes were shadow IT. Having said that, the magnitude of shadow IT also corresponded to the size of the business, with medium and large organizations using a lower percentage of shadow IT apps than small businesses.[8]

Since many of these tools have not been reviewed by IT, their adoption often leads to misconfigurations and unmonitored usage. Some exceptions include Microsoft Office 365, Google Workspace, and Salesforce, which offer customers a broad spectrum of security controls. Nonetheless, similar to IaaS/PaaS, setting up these controls properly can be difficult, and the more platforms in use, the more of a challenge it becomes to manage and integrate them.

Key Cloud Security considerations

According to the findings in a recent Fortinet survey, 67% of cybersecurity professionals believe that the cloud environment and the shared responsibility model make misconfigurations the biggest Cloud Security risk, with multi-cloud and multi-vendor environments compounding this risk significantly.[7] Moreover, Gartner claims that until the end of 2025, avoidable misconfigurations or user error will be the root cause of more than 99% of cloud breaches.[9]

DEFENDER'S PERSPECTIVE

One of the next major defense frontiers in the world of Cloud Security will be SaaS. The first generation of this problem has been addressed by CASB solutions because they help provide basic monitoring and oversight. However, there is still a significant gap between the capabilities offered and the capabilities an enterprise used to have when these were on-premise applications. There are basic SaaS management tools that help companies track things like billing, permissions, and configurations, but you're not getting into the granularity of all of the underlying data elements, what they were accessing, etc. The other piece that's missing is transparency about the security health of the infrastructure in which these SaaS applications are running. And any solution there is going to be API-driven.

Omkhar Arasaratnam
Engineering Director, Google
Google

This makes Cloud Security Posture Management (CSPM) a key focus area for 2022. CSPM functionality includes automatic misconfiguration detection and remediation, data risk evaluation, detection of excessive permissions, cloud policy violation monitoring, and regulatory compliance with HIPAA, GDPR, and CCPA.

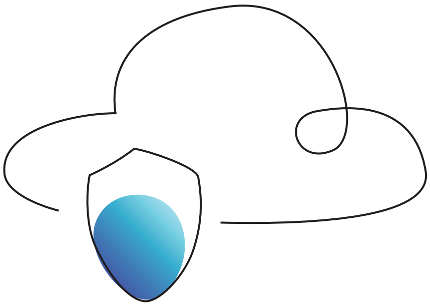
Similarly, in order to manage for shadow IT or misconfigurations in approved SaaS applications, investment will be needed in SaaS Security Posture Management (SSPM) and SaaS Management Platforms (SMP).

Shifting to cloud-native applications

It is already well understood that the cloud is extremely complex, so most individuals and companies would rather consume tools as a suite rather than a complicated combination of niche products. As a result, Cloud Native Application Protection Platforms (CNAPP) have recently come into focus. CNAPPs help secure cloud-native applications by consolidating multiple cloud-native tools and data sources.

Unlike legacy monolithic applications, cloud-native applications are built using numerous individual microservices, which are deployed in cloud environments and together create the application. Developers can work on each microservice separately, and do not have to wait for all components to be ready before deploying to production. This is entirely different from major legacy software builds, which take place slowly and only occasionally, meaning that for cloud-native applications, security must start proactively during development.

In order to satisfy the full set of requirements for cloud-native application protection, the Cloud Workload Protection Platform (CWPP) market is shifting-left and further converging with the CSPM market. This will also drive investment in Cloud Infrastructure Entitlement Management (CIEM), which is the next evolution of tools for managing permissions and enforcing least privilege in the cloud.



Solutions

Cloud Workload Protection Platform (CWPP)	Cloud Infrastructure Entitlement Management (CIEM)	Cloud Security Posture Management (CSPM)
SaaS Security Posture Management (SSPM)	Cloud Native Application Protection Platform (CNAPP)	SaaS Management Platform (SMP)
Container Security	Cloud Access Security Broker (CASB)	Serverless Security

Select Providers

paloalto NETWORKS

WIZ

Check Point SOFTWARE TECHNOLOGIES LTD.

Lacework

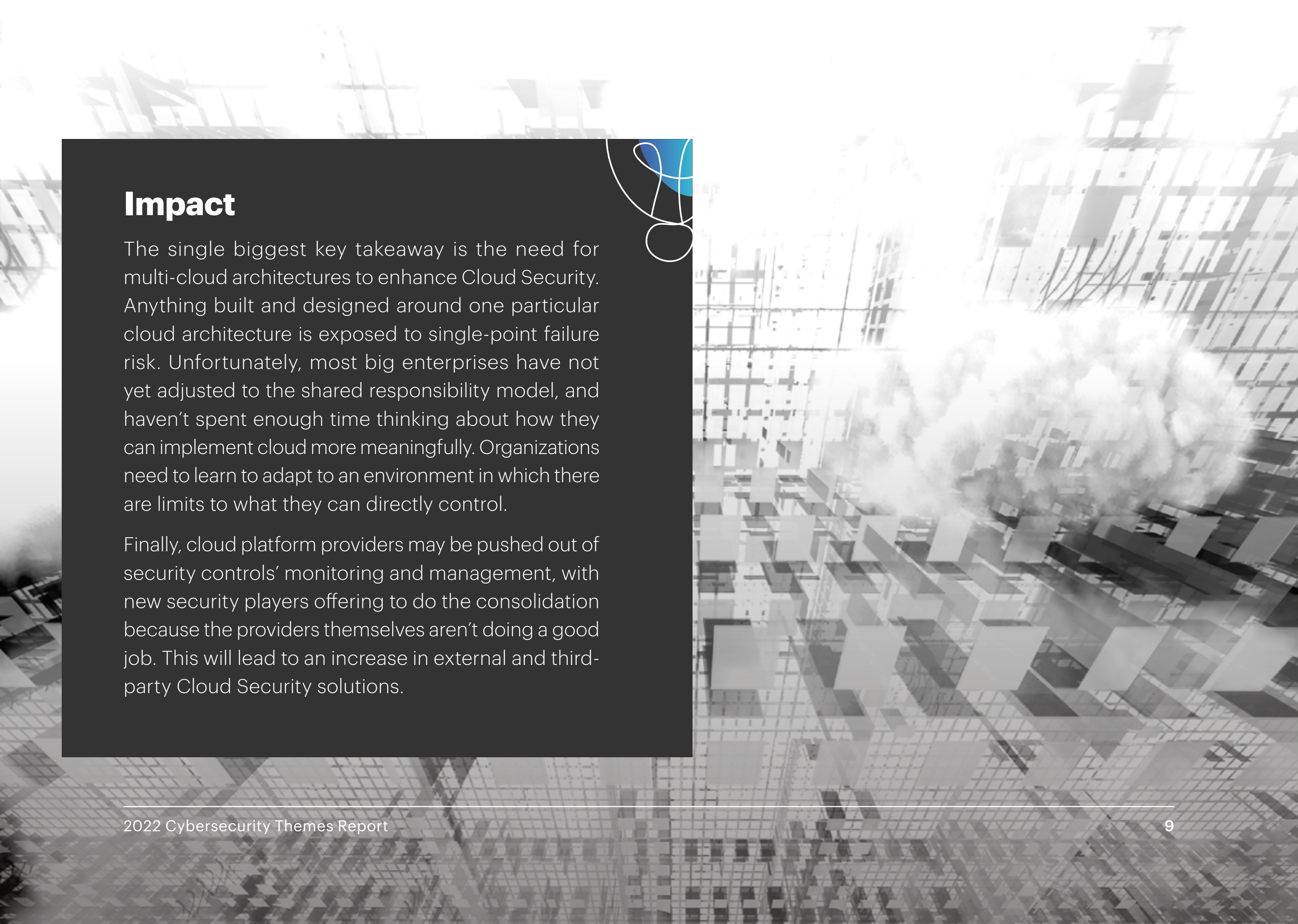
aqua

netskope

orca security

TEAM8'S ATTACKER PERSPECTIVE

Beyond simple misconfiguration, any service or application in the cloud has a complex supply chain, which increases the attack surface significantly. This was evident in the Log4j vulnerability, which was an open-source supply chain issue within Apache. With on-premise solutions, if you have a supply chain problem, you have "walls" - the attackers have to find their way, layer by layer, to the target. In the cloud (where everything is exposed), attackers can see the entire attack chain and hit the weakest link, without having to work their way through it. As companies are moving to the public cloud, and specifically to SaaS, by definition they also have a supply chain in the cloud. And as more critical business functionality depends on vendor-supplied software, attackers are evolving their modus operandi to focus more on the vendors, and on poisoning the cloud supply chain.

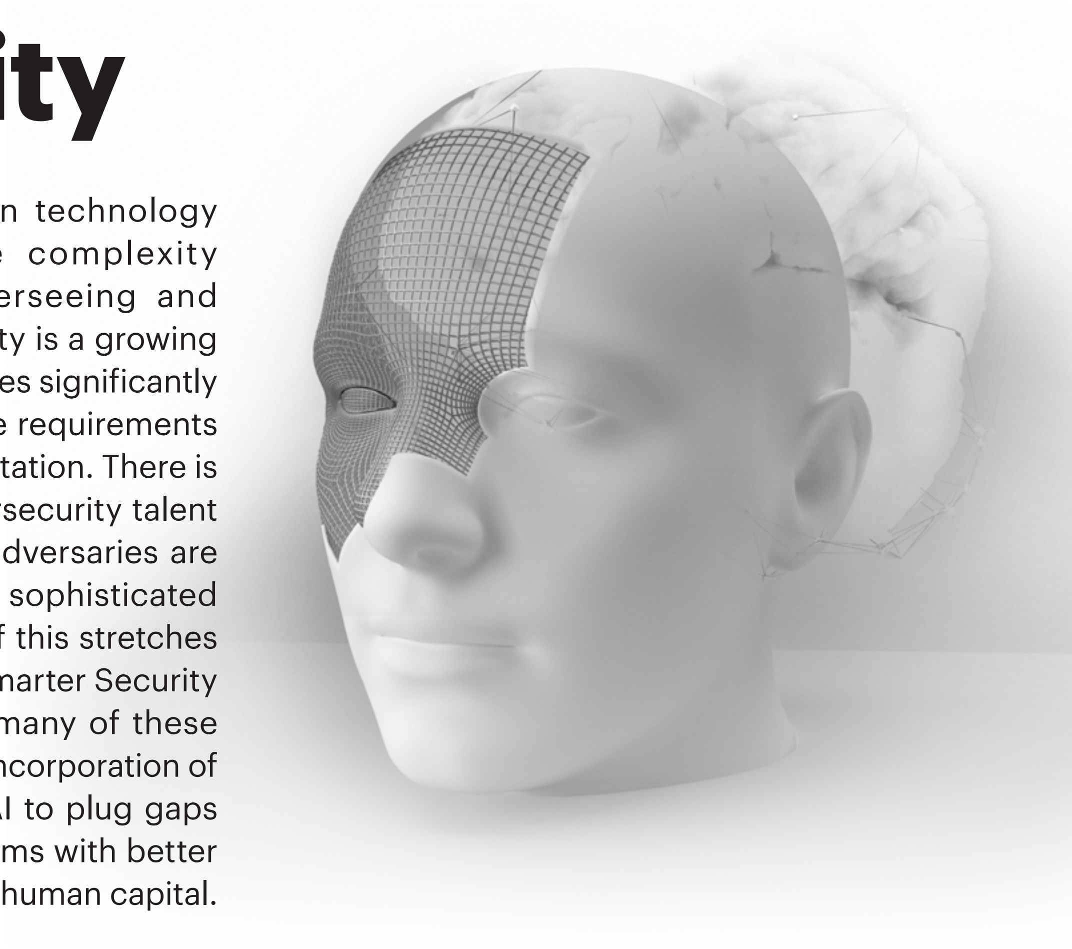


Impact

The single biggest key takeaway is the need for multi-cloud architectures to enhance Cloud Security. Anything built and designed around one particular cloud architecture is exposed to single-point failure risk. Unfortunately, most big enterprises have not yet adjusted to the shared responsibility model, and haven't spent enough time thinking about how they can implement cloud more meaningfully. Organizations need to learn to adapt to an environment in which there are limits to what they can directly control.

Finally, cloud platform providers may be pushed out of security controls' monitoring and management, with new security players offering to do the consolidation because the providers themselves aren't doing a good job. This will lead to an increase in external and third-party Cloud Security solutions.

Smarter Security

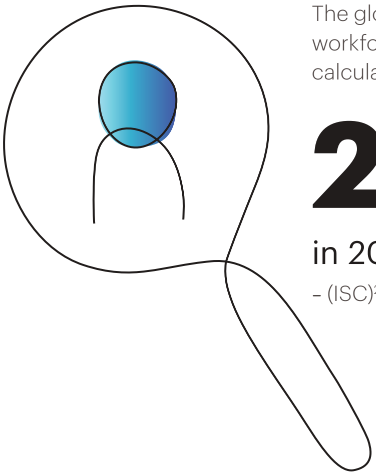


The pace of change in technology has added immense complexity to cybersecurity. Overseeing and managing this complexity is a growing challenge, and contributes significantly to the cost and resource requirements of technology implementation. There is also a shortage of cybersecurity talent while, simultaneously, adversaries are increasingly leveraging sophisticated attack capabilities. All of this stretches response capabilities. Smarter Security solutions will mitigate many of these challenges through the incorporation of automation, data, and AI to plug gaps and provide security teams with better options to best-use their human capital.

Drivers & Developments:

While the pandemic has impacted staffing in multiple areas, cybersecurity labor shortages have long been a problem, and have only worsened as a result of recent market changes. The global cybersecurity workforce shortage was calculated to be a stunning 2.7 million in 2021.[10] Additionally, research by Microsoft indicates that there is one open cybersecurity position for approximately every two that are filled in the U.S.[11] Some of these are critical roles, and organizations have identified cybersecurity staff shortages as a notable risk.

Increasing the pressure, attacks and alerts are also up, and have been accelerating since the pandemic. In part, this is due to an increase in autonomous and/or AI-driven attacks, in which attackers leverage automation and AI for offensive capabilities. In fact, 96% of executives have started preparing to defend their organizations against such offensive AI attacks.[12]



The global cybersecurity workforce shortage was calculated to be a stunning

2.7M

in 2021

- (ISC)²

Automation and AI are the future of cybersecurity

This volume of attacks, particularly in the context of insufficient staff to face them and the complexity of the IT environments in which organizations are operating, means more security automation is needed.

AI and automation are key components for solving many challenges related to attacks, alerts, and visibility/monitoring. These components can augment security analyst capabilities, and reduce the cost and time needed by security operations teams undertaking threat hunting, incident response, vulnerability management activities, and day-to-day security management. According to Oracle, 40-45% of cyber and IT professionals believe that AI can outperform security analysts in detecting fraud, recognizing anomalous behavior, monitoring configuration controls, and triaging security alerts.[6]

AI and machine learning (ML) have frequently been used to identify and protect against threats such as new malware, exploits, or phishing. The proportion of companies who have deployed security AI and automation increased by 6% in 2021 to 65%.[1] As a matter of fact, 9 out of 10 security professionals consider Smarter Security technologies to be foundational to their Cloud Security strategy, and 32% of companies are prioritizing security AI as a key investment area in 2022.[6] Although broad, impactful use of AI is still far away, AI and ML security solutions are expected to grow in technical proficiency in terms of both identifying suspicious behavior and automating a successful response.

DEFENDER'S PERSPECTIVE

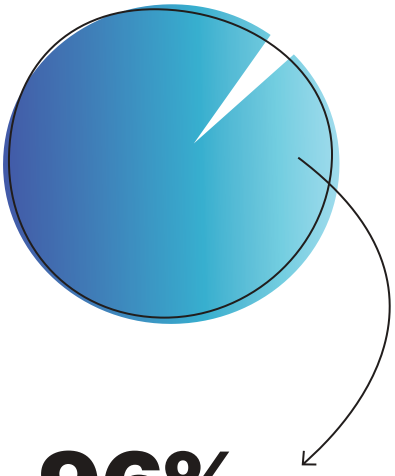
Smarter Security is about empowering teams by using automation, data, and AI to identify and remediate threats faster. These enhanced tools allow us to more effectively prioritize high-impact investigations, and threat hunting, however are not limited to 'detection' only activities. On a whole, Smarter Security becomes an added 'layer' on top of existing infrastructure to seamlessly integrate more sophisticated tools, allowing organizations to proactively reduce risk and offer safer banking experiences to customers.

Stephen Sparkes
CISO, Scotiabank
Scotiabank

The positive cost impact is significant. For example, security AI and automation can improve the speed and quality of detection, thus reducing the likelihood of breaches. Additionally, Smarter Security can also drive cost reduction. When breaches do occur, companies with fully-deployed security AI and automation are known to spend less time identifying and containing the breach. Organizations that leveraged Smarter Security saw significantly lower costs related to security breaches at an average of $2.90 million, compared to $6.71 million at organizations without security AI and automation.[1]

In fact, Smarter Security is one of the few security actions organizations can take that not only improves security, but also has a positive ROI for the business. Thus, while companies are reducing their budgets in some areas in response to the pandemic, they are still willing to invest in AI and ML as integral parts of their security program – especially where there is a positive ROI as a result of better outcomes and lower costs.

Consequently, demand for security orchestration, automation and response (SOAR) is growing. SOAR solutions lie at the intersection of security orchestration and automation tools, incident response tools, and threat intelligence platforms (TIPs). These formerly independent tools have converged to help organizations defend against sophisticated threats with constrained resources, as well as to integrate and automate workflows, playbooks, and processes.



96%

of executives have started preparing to defend against offensive AI attacks

– MIT

TEAM8'S ATTACKER PERSPECTIVE

The common notion in many security teams is that collecting more data will solve their problems; however, this is not necessarily the case. As with many big data problems, arguably we're not smart enough with the data we already have. Organizations need to be smarter at the security engineering level, and connect individual security tools. For example, if the endpoint sees something strange, the firewall should limit access, and other tools should modify user permissions associated with the crown jewels. At this point, we don't have Smarter Security, we only have smarter detection, and a sprinkle of automation. For attackers, as long as Smarter Security is not enabled, security measures will be seen as independent tools they need to circumvent one-by-one. Smarter Security will genuinely work when the attacker sees the security tools as an integrated system that interacts with itself.

Select Providers

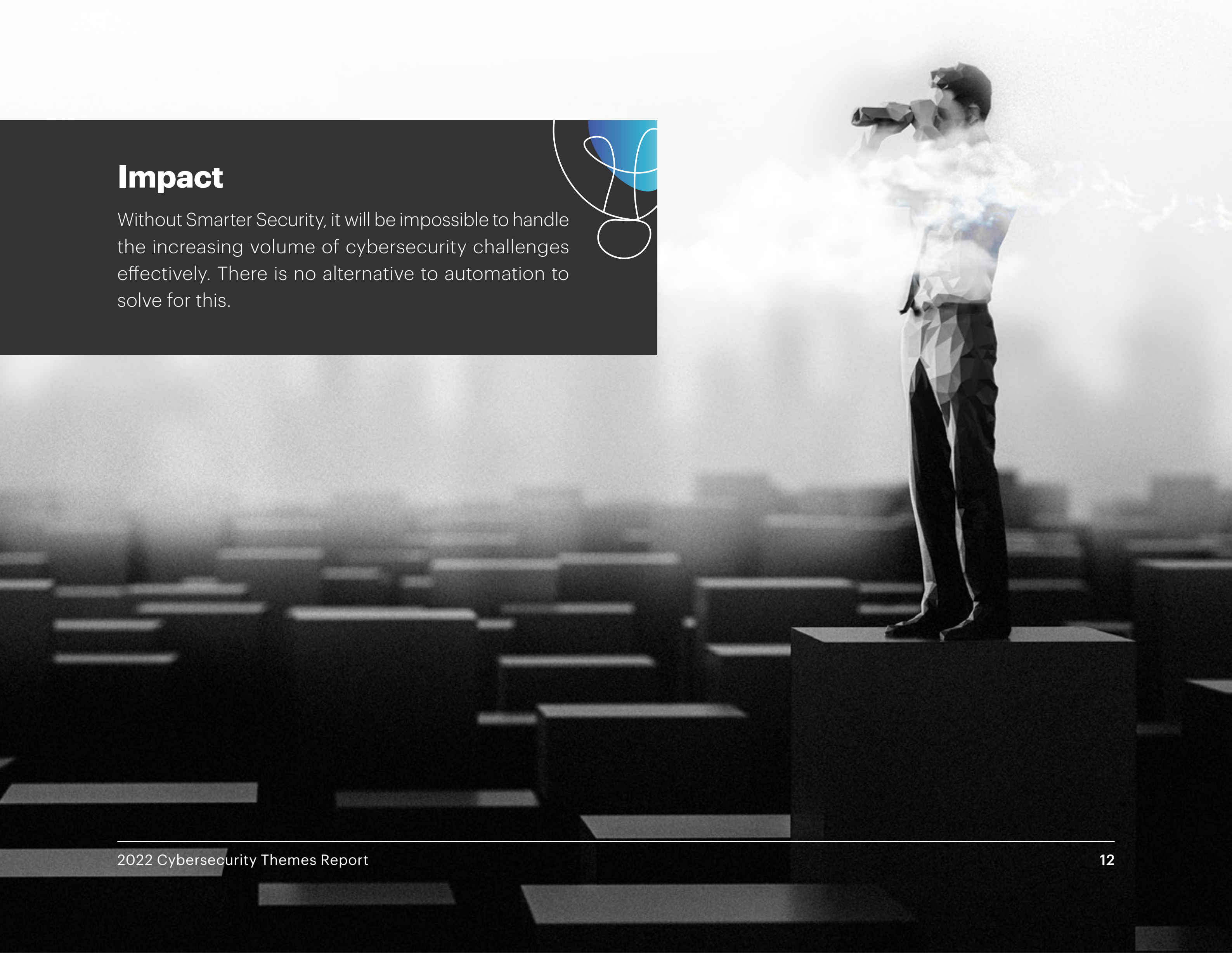
paloalto NETWORKS
tufin
exabeam
VULCAN.
DATADOG
Cynet
splunk>

Solutions

Security Information & Event Management (SIEM)	Logging & Analytics	Vulnerability Management
Security Orchestration, Automation & Response (SOAR)	Security Policy Automation	Security Visibility & Monitoring
Robotic Process Automation (RPA)		

Impact

Without Smarter Security, it will be impossible to handle the increasing volume of cybersecurity challenges effectively. There is no alternative to automation to solve for this.



03

Resilience & Recovery

In a world in which digital infrastructure is now business-critical infrastructure, cybersecurity cannot afford to stop at "identify, protect, detect, and respond." Any sound security strategy must also include the capability for rapid recovery from degradation, disruption, or denial of access to enterprise systems or data, and swift reconstitution of assets and capabilities. Our understanding of resiliency has expanded to include this.

Drivers and Developments:

Ransomware threatens resilience

Ransomware, which continues to expand, is one of the most important drivers of the need for Resilience and Recovery. As the nature of these attacks develops, preparing for and responding to them is becoming a priority for many boards. While originally ransomware was designed to grab data then threaten to sell or release it, it evolved to attackers locking up an organization's data, only to restore it once the ransom was paid. The most recent evolution has hackers making an enterprise's entire system unavailable – in effect taking the entire business hostage. Ransomware is also continually getting more sophisticated, targeting specific data points as opposed to general attacks.

DEFENDER'S PERSPECTIVE

The company's executive leadership or board of directors are usually the ones who decide whether to pay the ransom or not, and sometimes, not paying may cripple the business, damage its customers, or worse, risk critical infrastructure. Moreover, cryptocurrency is ubiquitous, and sometimes untraceable, so the reality is that companies who wish to pay the ransom may find ways to do so despite regulatory restrictions. In any case, organizations should almost always negotiate with the threat actor, even if they have no intention of paying. Negotiating buys critical time that allows the incident response team, together with the IT and security team, to effectively remediate and recover affected systems, while implementing the necessary countermeasures to significantly reduce the likelihood of another ransomware attack or retaliation attempts by the threat actor.

David Warshavski
VP, Enterprise Security, Sygnia
SYGNIA

In 2021, 37% of enterprises suffered a ransomware attack.[13] And ransomware was present in 10% of breaches, double the frequency seen in 2020, to the point where ransomware is now in third place for actions that cause breaches.[14] The banking sector was inordinately impacted, showing a 1,318% rise in ransomware attacks in the first half of 2021.[15] Ransomware-related breaches are also more expensive than other breaches, with an average ransomware attack costing $4.62 million vs. $4.24 million for an average breach – and that's not including the cost of the ransom itself.[1]

Of course, whether or not to pay the ransom is an important question. Anti-money laundering and terrorist financing laws around the globe help to prevent payment. For example, the United States Office of Foreign Assets Control's (OFAC) recent restrictions make paying a ransom potentially a criminal offense.[16] Research also indicates that it's more costly to pay the ransom, not least because paying has limited impact on the recovery efforts. In fact, the total cost of ransomware more than doubles if the ransom is paid.[17] Even worse, 80% of ransomware victims are hit at least twice, often on an escalating basis.[18] It will be interesting to see whether recent enforcement actions, such as the unprecedented January 2022 arrest by Russia of 14 alleged members of the REvil ransomware group, will contribute to a decline in ransomware going forward, at least in the short-term.[19]

As part of the response, some victims may choose to file a cyber insurance claim, and hire an outside incident response team to evaluate the damage and help with recovery efforts. Cybersecurity insurance companies can also provide upfront services to improve the security posture before an attack, thereby reducing the likelihood of an incident. However, insurance companies are starting to require advanced security in order to even issue a policy, and some are cutting ransomware coverage entirely or offering policies that only provide incident response, without damages.

Don't forget the users

It's important to note that while ransomware is a key driver for the need for resilience, it's not the only driver. User or administrator error can also be a challenge – such as in the Facebook outage in October 2021 that took down Facebook, Messenger, Whatsapp, and Oculus all at the same time.[20] Similarly, Amazon Web Services experienced a significant outage in December 2021, which affected a number of websites, services, and vital internal tools.[21] Such examples of lost business represented the largest share of breach costs, and included costs resulting from higher customer churn, lost revenue from outages, or increasing customer acquisition costs due to new reputational issues.[1]

The importance of recovery

The cost and recovery effort is no less of a consideration. Recovery of both data and systems (which can be much more complicated) becomes the core issue, even after the initial response to an attack has been navigated. According to industry surveys, companies recover the entirety of their data in only 8% of ransomware attacks.[13] Recovery is also impacted by the time it takes to identify and contain any sort of breach, with the cost increasing significantly the longer it takes.[1]

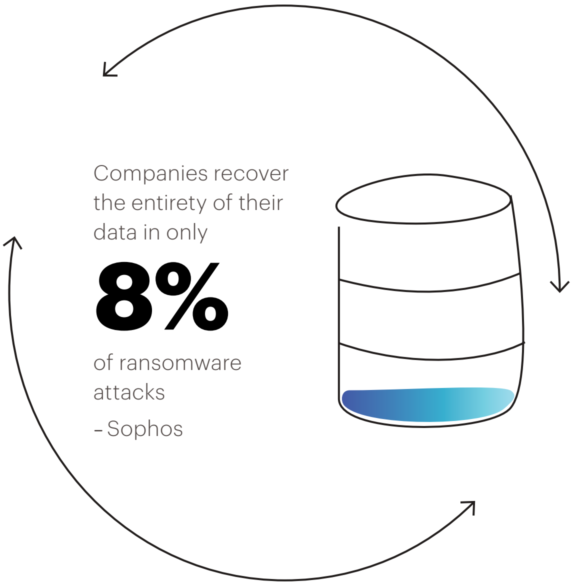
Backup and Disaster Recovery (BDR) techniques such as SaaS application backup, backup-as-a-service, ransomware protection, and cloud backup are all accelerating backup infrastructure modernization as disaster recovery budgets increase. For heavy-duty enterprise backup, isolated recovery environments with immutable data vaults offer the strongest degree of security and recovery.[22] And for SaaS, there are many third-party backup-as-a-service solutions that have more features, are easier to set up, and are compatible with more SaaS applications than solutions from most classic enterprise backup providers. As a recent Gartner survey indicates, overall, organizations with a robust disaster recovery program are 40% more likely to have a better general resilience posture.[23]

But the reality is that this set of "backup and recovery" tools really are just backup tools – the recovery piece is almost exclusively manual, and the lack of automation in recovery is a problem that can't be emphasized enough. Additionally, BDR is only a solution if the backups are actually performed. There are now some businesses designed to help companies exercise this "resiliency muscle", and to ensure that Business Continuity Planning (BCP) is in place and acted upon. For instance, annual "drills" and practice scenarios, where backups must actually be tested and used, can ensure that companies are truly prepared in the event of a crisis.

Ultimately, while the demand for Resilience and Recovery solutions is way up, supply is not. The reality is that there is still a lack of great tools, and this represents both a threat and an opportunity for attackers and defenders alike.

TEAM8'S ATTACKER PERSPECTIVE

Ransomware has evolved from stealing data for the purpose of extortion, to locking local data, to locking entire systems, since it is much easier to monetize control over a target than to monetize stolen data. But the ROI for attackers is worsening as companies are getting better at backups. And as companies become more resilient, the attacker's ability to lock data becomes materially reduced. Thus, from a profit perspective, attackers have no choice but to go back to the data extortion aspect of it. For example, even if you can restore from backups, attackers will threaten to damage your brand/reputation by releasing your emails.



Companies recover the entirety of their data in only

8%

of ransomware attacks

- Sophos

Solutions

Cyber Exercise Facilitation	Cyber Ranges	Incident Response
Application Performance Monitoring (APM)	Business Continuity Planning (BCP)	Ransomware Protection
Backup and Disaster Recovery (BDR)	Self-Healing Systems	

Select Providers

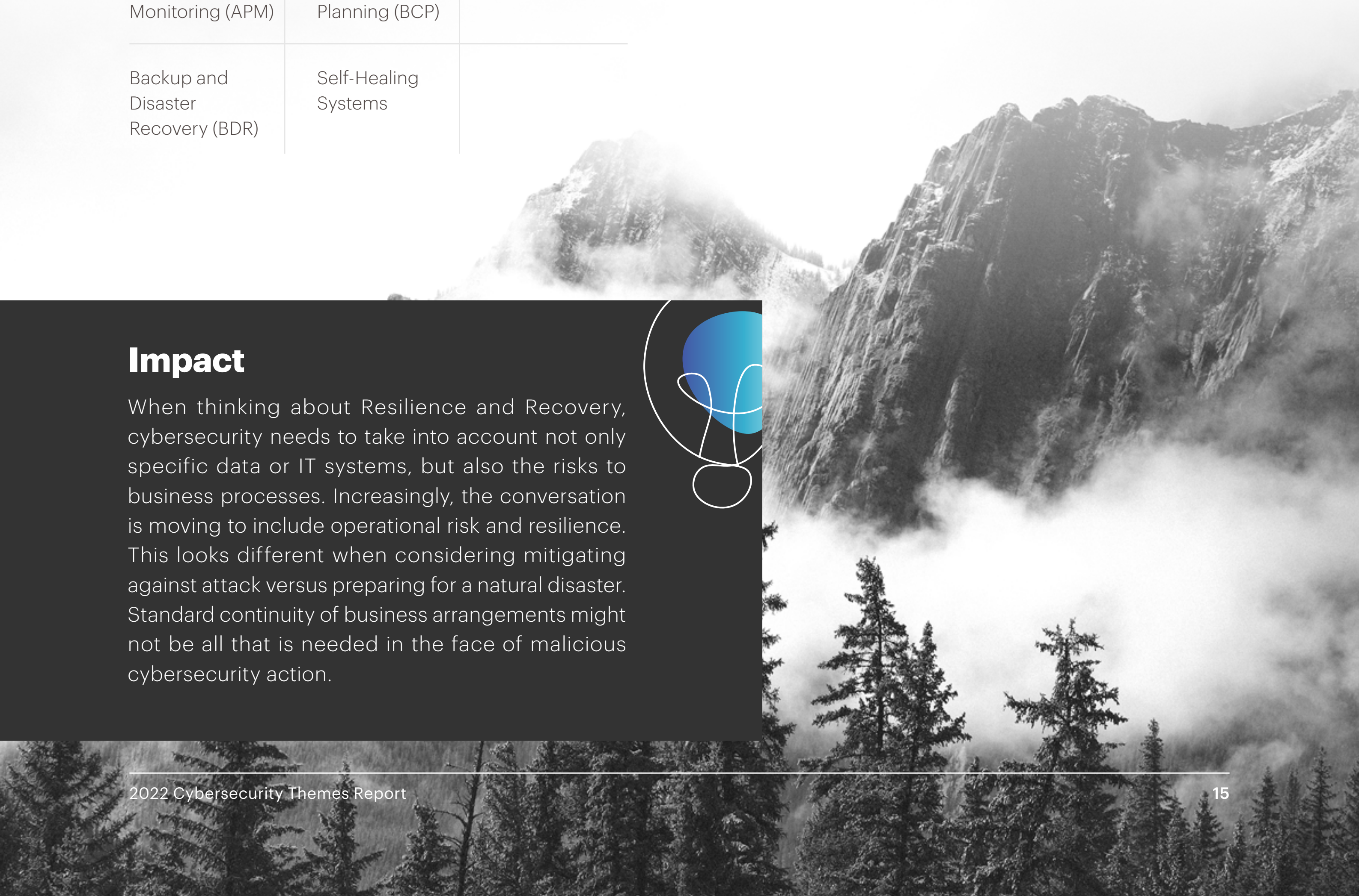
SEMPERIS

IMMERSIVELABS

Own{backup}

rubrik

COMMVAULT



Impact

When thinking about Resilience and Recovery, cybersecurity needs to take into account not only specific data or IT systems, but also the risks to business processes. Increasingly, the conversation is moving to include operational risk and resilience. This looks different when considering mitigating against attack versus preparing for a natural disaster. Standard continuity of business arrangements might not be all that is needed in the face of malicious cybersecurity action.

Security of Things

The growth of the Internet of Things (IoT) is driving digitization and unlocking business value. But Security of Things requires that every connected device or network – each with its own identifier and ability to transfer or process data – must be protected. Traditional endpoints such as servers, desktops, or laptops are now joined by a multitude of new ones such as smart devices, sensors, and motor vehicles. The number of total endpoints is growing, and many are largely autonomous without much onboard security functionality or strong APIs for security management. Importantly, each of these devices acts as a potential breach-point into an organization or to private data, which increases overall risk exponentially.

Drivers & Developments:

One of the complexities of the Security of Things is that it encompasses various security environments, such as traditional IT endpoint security, Operational Technology (OT), IoT Security, and mobile security, as well as different threat types depending on the digital environment.

Traditional (IT) endpoint security issues represent some of the most challenging security problems of not only the past, but also of today and tomorrow. Up to 70% of companies are experiencing difficulties with endpoint security, and are suffering from a 47% rise in cybersecurity attacks, including phishing attempts.[6] It's a game of cat and mouse in which the bad actors constantly seek and find new approaches.

As a result, Endpoint Detection and Response (EDR) solutions are growing in adoption, while Endpoint Protection Platform (EPP) solutions are reaching full maturity. The more recent concept of Unified Endpoint Security (UES) attempts to combine elements of EDR, EPP, and Mobile Threat Defense (MTD). However, there can be a tradeoff to this approach – that is, a set of tools that theoretically work better together, but do not necessarily provide best-of-breed solutions for each piece.

The question is, is the improvement from advanced configurations worth the trouble? Certainly, the most sophisticated enterprises are saying the extra complexity is worth it. However, these tools can only be installed on sophisticated endpoints, leaving much to be desired when it comes to the protection of simpler endpoints, such as smart devices and other consumer IoT.

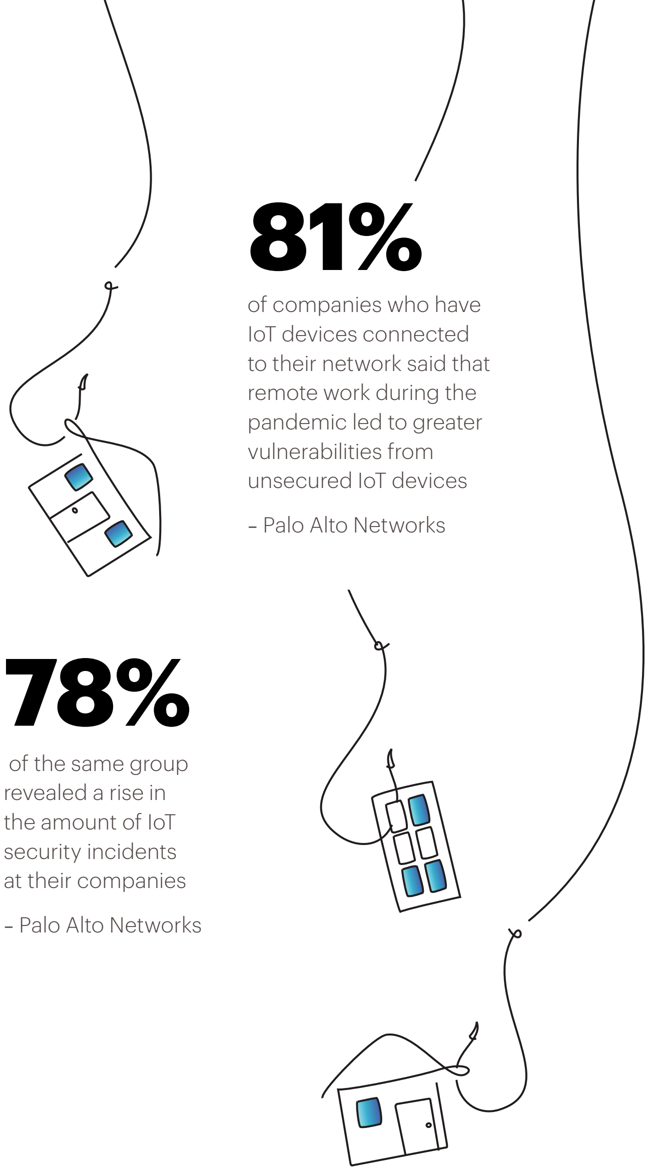
Progress in Internet of Things security

To this end, the growing number of IoT devices, increased connectivity, and the convergence of IT, OT, IoT and physical assets has also extended the vulnerabilities in cyber-physical systems for both the consumer and the enterprise. IDC predicts that there will be 55.7 billion connected IoT devices by 2025, and that almost 80% of the Forbes Global 2000 organizations in some industries will be digitally dependent by 2023.[24] All of these devices will need to be managed, monitored, secured, and patched in a unified and scalable way.

And like in other areas, the Covid-19 pandemic has compounded the problem. IoT security is very much still a challenge for organizations, many of which feel the issue has only gotten worse with the increase in remote work. 81% of companies who have IoT devices connected to their network said that remote work during the pandemic led to greater vulnerabilities from unsecured IoT devices, and 78% of the same group revealed a rise in the amount of IoT security incidents at their companies.[25]

U.S. IOT LEGISLATION

- The U.S. Internet of Things Cybersecurity Improvement Act of 2020 introduced requirements for more robust cybersecurity for IoT devices owned or controlled by the Federal Government. The act instructs the National Institute of Standards and Technology (NIST) to develop security standards and guidelines for the use and management of all relevant IoT devices, which will become mandatory in December 2022.
- This past summer, President Biden signed the National Security Memorandum on "Improving Cybersecurity for Critical Infrastructure Control Systems", which directs the Cybersecurity & Infrastructure Security Agency (CISA) and NIST to develop cybersecurity standards for critical infrastructure, and formally establishes the President's Industrial Control System Cybersecurity (ICS) initiative.



81%

of companies who have IoT devices connected to their network said that remote work during the pandemic led to greater vulnerabilities from unsecured IoT devices

- Palo Alto Networks

78%

of the same group revealed a rise in the amount of IoT security incidents at their companies

- Palo Alto Networks

DEFENDER'S PERSPECTIVE

In the same way the internet transformed how we interact with information, Cyber-Physical Systems (CPS) are transforming the way we interact with and control the physical world around us. Many IoT/OT-related security breaches may have impact which is realized directly in the physical world, such as with manufacturing. What will be critical in the next evolution of the Security of Things will be not just managing the security of individual things. As sensor networks and connected devices become more distributed and complex, future solutions must also take into consideration the holistic risks associated with the system as a whole.

John Petersen

CISO, Nestlé

Nestlé

An increase in IoT-related attacks is raising overall awareness. As a result, IoT vendors are facing pressure from both enterprises and governments for better security standards due to heightened consumer safety and privacy concerns. Such regulatory pressures have led to mandates and best practices, all of which have impacted the Security of Things.

Industrial Internet of Things (IIoT)

Within IoT Security, one of the most significant concerns is the security of industrial IoT (IIoT).[25] IIoT attacks are a particularly concerning trend as sensors that can gather data, connect to the internet, and control operational technology and machinery become installed in manufacturing and other industrial facilities. What makes industrial IoT that much more dangerous in the event of an attack is that the equipment it's connected to can be poisonous, explosive, high-voltage, life-critical, etc. An example of this is the recent attack on a water treatment plant in Florida where attackers attempted to poison the public water supply.[26]

IIoT environments can also be complicated by poor incident response capabilities. For example, if the IT team doesn't know where the connected device is, or there isn't a management interface for administration, options may be limited during a response scenario to unplugging or destroying the device. However, one of the biggest challenges in IIoT environments remains the notion of patching, especially in sectors like Food, Pharma, or Aviation, where change is difficult due to rigorous health and safety approval processes.

Impact

There continues to be a massive acceleration in the number and variety of IoT devices, creating new categories of attack that need to be planned for in order to protect individuals, data, and enterprises. In the context of industrial IoT, there are concerns regarding the resiliency of critical infrastructure, however, unfortunately much of this infrastructure is decades old and difficult to change rapidly.

TEAM8'S ATTACKER PERSPECTIVE

The most significant risk for consumer IoT is still "things" on the network that administrators aren't aware of, and what attackers like the most is finding old and unmanaged devices that can be compromised. But when it comes to these types of IoT devices, there hasn't been a lot of innovation from the attacker, since IoT has always been considered just another way into the target network. Rarely is the IoT device itself interesting - it's a beachhead, not the end goal. The regular endpoint is still the easiest and most common way of getting in. And if it's easy enough to go through the main door, why go through the window?

On the other hand, attackers love Industrial IoT because it's the pathway to remote execution of high-impact attacks. In this scenario, the IIoT itself is the target, which has driven some of the innovation from the offense.

Select Providers

CLAROTY TANIUM armis

SentinelOne CROWDSTRIKE SOPHOS

deepinstinct

Solutions

Attack Surface Management (ASM)	Extended Detection and Response (XDR)	IoT Security
Endpoint Detection and Response (EDR)	Unified Endpoint Security (UES)	OT Security
Endpoint Protection Platform (EPP)	Managed Detection and Response (MDR)	Antivirus (AV)
Mobile Threat Defense (MTD)		

Perimeterless World

The enterprise perimeter is nearly obsolete, and the dramatic shift to remote work during the pandemic is accelerating its demise. This requires enhanced processes for identity and access management, with a growing use of zero trust architectures that provide better control without requiring all traffic to pass through specific perimeter access enforcement points.

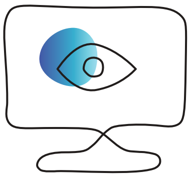
Drivers & Developments:

All signs point to the Perimeterless World continuing to accelerate well after the pandemic is over due to the impact of cloud and SaaS, as well as the shift to remote work. According to McKinsey, as the pandemic subsides, executives expect that the hybrid work model will become much more routine, with employees being in the office at most 4 days per week.[27]

Identity and access management

Identity lies at the heart of the issue of how to implement security in an environment where the perimeter can't be counted upon as a way to enforce policy. Identity and access management for remote work has become more complex as employees take a more dynamic and flexible approach, using a variety of devices to connect (including personal laptops, tablets, or smartphones) via open Wi-Fi networks. They also utilize remote collaboration tools, as well as a wide range of cloud/SaaS products and services to complete their tasks.

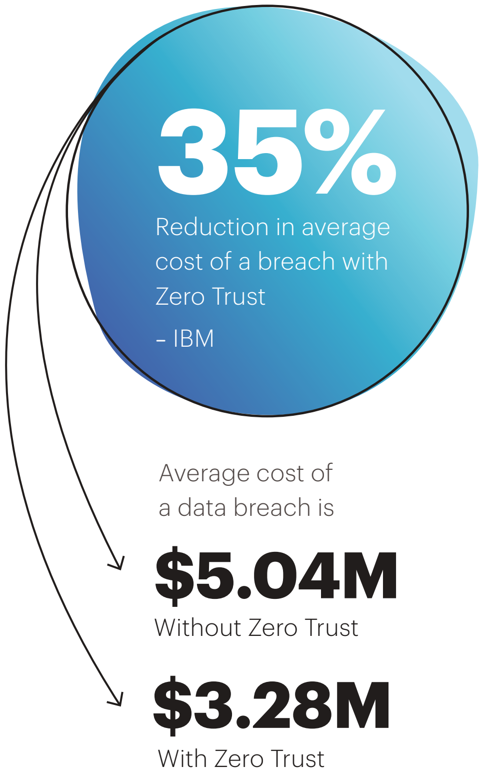
Going forward, technology solutions will focus even more on Identity and Access Management (IAM) that adaptively authenticate users across different environments in real-time and to varying degrees of granularity based on risk severity and confidence. Successful IAM technologies enable businesses to provide their employees or customers with the right access for the right reasons, at the right time, and with the right user experience (UX). This has driven interest in innovations such as passwordless authentication. By this year, Gartner predicts that 60% of large enterprises and 90% of midsized enterprises will utilize passwordless approaches in more than 50% of the relevant use-cases – up from just 5% in 2018.[28]



Zero Trust gains traction

Another security approach to identity that is gaining traction is zero trust. Zero trust is an architectural principle underlying products and services that create an identity-based and context-based access boundary around users, devices, and application services, which are hidden from discovery. Users are given access only to services to which they are entitled. Because zero trust does not allow full tunnel access to the network like a traditional VPN, lateral movement by attackers is much more difficult.

87% of companies would like to leverage a zero trust approach post-pandemic, not least because this can reduce the average cost of a data breach.[6] According to IBM, the average cost of a breach was $5.04 million for those without zero trust deployed, but the cost dropped by 35% to $3.28 million for those in the advanced stages of zero trust implementation.[1]



35%

Reduction in average cost of a breach with Zero Trust

– IBM

Average cost of a data breach is

$5.04M

Without Zero Trust

$3.28M

With Zero Trust

Secure remote access makes a comeback

The sudden rise in remote work has also shined a spotlight on secure remote access, with bring your own PC (BYOPC) and VPNs seeing renewed use over the short-term.

As applications move to the cloud and SaaS, there's less of a need to connect to the remote access VPN. As a result, the newer Secure Access Service Edge (SASE) model is gaining traction across businesses by replacing VPNs and point solutions with a combination of networking and security, delivered as a service. However, there are still questions over whether VPN and SASE are just transitional phases, as the market works towards a truly cloud-based network architecture, such as a secure virtual overlay network, particularly in the context of 5G networking.

As larger organizations develop SASE plans and look to consolidate their security tools, zero trust vendors with strong secure web gateway (SWG) and cloud access security broker (CASB) products will likely have an advantage. The endgame is either "cloud-first" or a "converged SASE appliance from one vendor," and best-of-breed point solutions probably will not be competitive in the long-term.

DEFENDER'S PERSPECTIVE

There's a greater potential threat from the insider world given the context of the last 18-24 months – more people are leaving their jobs, people are under a lot of stress, and there's less corporate loyalty. There was some oversight when we were all sitting in the office, but with the new Perimeterless World that structure is no longer there, and people are less aligned and less self-identified with their business. This leads to less oversight/control and monitoring, and thus, a greater potential or probability for insider threats. But the insider threat doesn't end with the employee – the disappearance of the perimeter also creates opportunities for casual/accidental 'insiders', e.g. an employee's child or a smart home assistant on the home network.

Admiral (Ret.) Michael Rogers
Former Director, NSA
Operating Partner, Team8

Solutions

- Identity and Access Management (IAM)
  - Privileged Access Management (PAM)
  - Multi-factor Authentication (MFA)
  - Self-Sovereign Identity (SSI)
- Secure Access Service Edge (SASE)
- User and Entity Behavior Analysis (UEBA)
- Zero Trust Network Access (ZTNA)
- Software Defined Perimeter (SDP)
- Secure Web Gateway (SWG)
- Virtual Private Network (VPN)
- Secrets Management

Select Providers

monogoto · AKEYLESS · TALON

illusive · okta · SILVERFORT

zscaler · paloalto NETWORKS · SECRET DOUBLE OCTOPUS

CATO NETWORKS

TEAM8'S ATTACKER PERSPECTIVE

The question for attackers has always been about where and how to get from the entry point to where they actually want to go. Zero trust authenticates individuals and limits what they can see, e.g. the default mode is that the user does not have access. This limits the ability of the attacker to land anywhere and still gain access to high-value assets.

Therefore, the nature of zero trust forces the attacker to be more deliberate about who to attack. The attacker now needs not only to collect technical data about the target network, but also to learn about and identify the people in it in order to target the right person as the entry point, thereby limiting the need for complex lateral movement. This requires the attacker to invest in better reconnaissance, making targets with zero trust protection that much more difficult to attack.

Impact

Today's security architecture was designed for network constructs that have subsequently been redesigned. The assumption used to be that the network was completely owned and managed by the enterprise, with everything outside of it a potentially uncontrolled hazard. But in the modern environment, there are many things outside of the network's control that still need to be trusted and depended upon. Thus, using network topology as the basis for trust simply isn't a valid assumption any more, and that's where identity comes into play.

Data Security

On one hand, globalization and the growth of the digital economy are accelerating the need for digital collaboration. On the other, emerging privacy regulations and consumer preferences are driving investment in privacy-enhancing technologies and the means for users to have more control over their data. The net result of these colliding forces will be new data protection- and privacy-driven strategies that impact underlying architectural design and business processes. The need to mitigate data breaches is also driving more Data Security and privacy regulation.

Drivers & Developments:

Data volumes are growing exponentially, and today data is an extraordinarily valuable asset. According to IDC's Worldwide Global DataSphere Forecast 2021–2025, business and consumer data had a compound annual growth rate (CAGR) of about 23% since 2020, and is expected to reach 180 zettabytes by 2025.[29] If this data is stolen or damaged, the fallout can be massive.

NEW DATA SECURITY & PRIVACY REGULATIONS

- GDPR enforcement is heating up. In July 2021, Amazon announced a GDPR fine of $877 million, which is nearly 15 times higher than any previous single GDPR fine in history.31
- The California Privacy Rights Act (CPRA) takes effect on January 1st, 2023. The CPRA adds new consumer rights such as the Right to Rectification or the Right to Limit Use and Disclosure of Sensitive Data, introduces annual cybersecurity audits and regular risk assessments, and calls for the creation of a California Privacy Protection Agency (CPPA) to enforce CPRA compliance.
- The CPRA has inspired two other states - Virginia and Colorado - both of which have signed new laws, due to go into effect in July 2023. The Virginia Consumer Data Protection Act (CDPA) and the Colorado Privacy Act (CPA) are the second and third comprehensive data privacy regulations in the U.S., respectively.
- China's Personal Information Protection Law (PIPL) was passed in August 2021. It is the first comprehensive data privacy law in China, and is expected to be a game changer for companies operating there.
- China also passed the Data Security Law (the "DSL") in June 2021, which governs data processing and management activities within China as well as those outside of the country that have the potential to harm Chinese national security or public interest, or damage any Chinese citizen's or organization's legal interests.

Correspondingly, data breaches are increasing in frequency and in cost. Verizon highlighted in its 2021 DBIR report that there were 5,258 confirmed data breaches across 16 industries and four global regions. This is up significantly from the 3,950 confirmed in the previous year.[14] The cost is going up too – the average total cost of a data breach has risen by nearly 10%, from $3.86 million in 2020 to $4.24 million in 2021, the highest one year cost increase in the previous seven years. This cost is being disproportionately borne by organizations with less mature security postures who lag in domains like security AI and automation, zero trust, and Cloud Security.[1]

Theft of personal information

The most common type of stolen information is usually the private information of consumers known as Personally Identifiable Information (PII), which is exploited through sale or ransom. PII accounts for 44% of breaches, and is also the most expensive at $180 per lost or stolen record.[1]

While PII is protected by law or regulation in most countries, the definition of what PII is and the specific protections vary by jurisdiction. Protected Health Information (PHI), on the other hand, is a more well-defined subset of PII where the protections are more consistent. However, hospital and healthcare providers lack sophisticated security systems embedded into their technology (even as the use of electronic medical records has increased). This is driving ransomware attacks that target these organizations to exploit their high-value data.

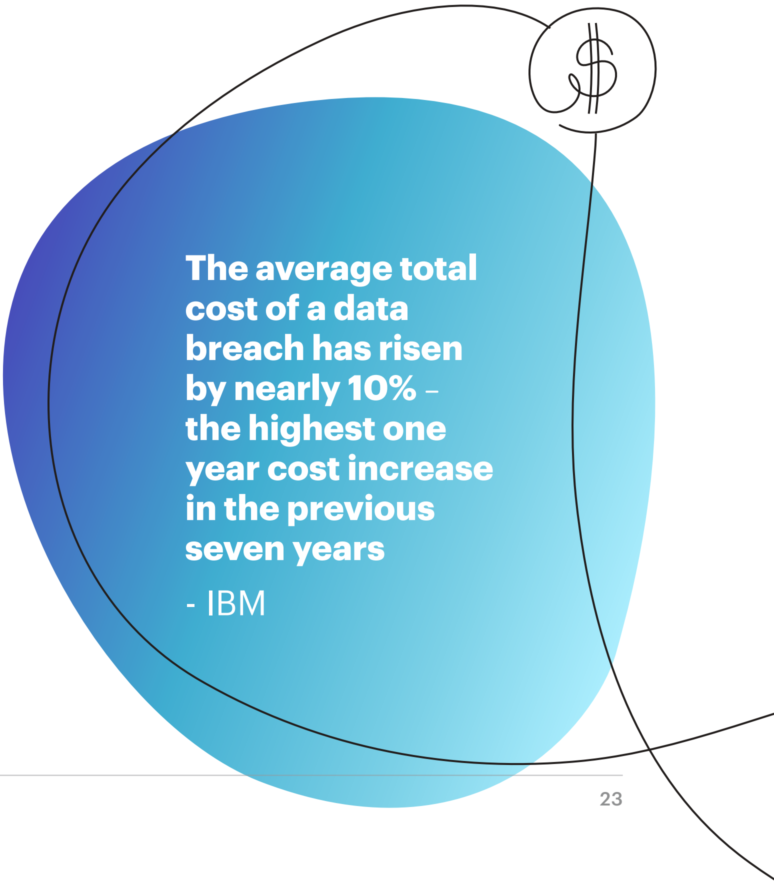
Citizens are increasingly aware of the risks, and now expect more transparency and control over how their information is being used. However, there is limited consistency in the approaches outlined by regulators, and the few industry-specific standards lack completeness. Corporate data is also at risk, with organizations fully aware that confidential information such as intellectual property and corporate emails with sensitive content are often targeted by ransomware actors in order to increase the probability or amount of payment.

In most instances, several Data Security controls and technologies will be required to address Data Security and privacy risks, and to protect data. Regulatory compliance and market requirements are growing in complexity, and vendors are struggling to consolidate and integrate technologies and security, leading to gaps or side effects due to overlap.

As these elements converge, they will consolidate into what are today being referred to as Data Security Platforms (DSPs). These platforms include capabilities such as encryption, data governance, data masking, database security and analytics, data discovery, tokenization, Data Loss Prevention (DLP), and more. Further innovation in data protection techniques has also seen the continued growth of specialized privacy-preserving technologies, such as confidential computing, differential privacy, Fully Homomorphic Encryption (FHE), zero-knowledge proofs, Secure Multi-party Computation (SMPC), and Key Management-as-a-Service (KMaaS).

TEAM8'S ATTACKER PERSPECTIVE

Two different things are happening simultaneously: first, companies that implement privacy and data protection solutions will be better at defending their customers' data. But at the same time, because of privacy laws and other factors, it's also becoming simpler for users to take their data out of the system and move it elsewhere. A good example is open banking, where it's easy for a customer to move/copy data from a bank to a startup. This will allow the advanced attacker to ask not "where" in the target network the data they need is - but "which startup/service" has a copy of it with a fraction of the security budget of the parent enterprise who originally collected it.



The average total cost of a data breach has risen by nearly 10% – the highest one year cost increase in the previous seven years

- IBM

Solutions

Data Discovery	Data Governance	Data Classification
Data Protection and Compliance	Database Security and Analytics	Consent-based Data Sharing & Verification (CDSV)
Tokenization	Fully Homomorphic Encryption (FHE)	Secure Multi-party Computation (SMPC)
Data Loss Prevention (DLP)	Anonymization and Synthetic Data	Key Management-as-a-Service (KmaaS)
Privacy Rights (DSAR)		

Select Providers

Duality

PIIANO

BigID

VARONIS

OneTrust

VERY GOOD SECURITY

DEFENDER'S PERSPECTIVE

The volume of data held by organizations, including data on factors such as purchases, preferences, and behaviors, is growing extremely quickly. All of this data needs protection from destruction and corruption, and especially from unauthorized disclosure. Incidents that disclose private data can be damaging, and the more sensitive the data that's disclosed, the greater the damage may be. So, it's no surprise that cyber and information security programs are focused on ways to locate, understand, and protect data, while protecting privacy.

Jerry Geisler
SVP & Global CISO, Walmart
Walmart

Impact

Data is at the heart of everything in the modern corporation, with concerns around confidentiality, data availability, and data integrity. While the focus has previously been on confidentiality, today there is an increased focus on availability. Integrity of data will be the next frontier for Data Security considerations. If people cannot trust that you are who you say you are, or that their doctor has their real medical records, or that a public official really got elected, the fabric of civilization could begin to deteriorate.

Shift-Left

Developing and managing software is more agile and faster than ever. However, developers currently have neither the expertise nor the tools to handle the security issues, while the security team doesn't have the staff to cover the gap. Cybersecurity needs to be shifted-left in the application development process to ensure that security considerations are embedded from the start.

Drivers & Developments:

The demand for new applications is so massive that businesses are developing them faster than they can implement proper security controls. This is exacerbated by also having to convert old applications to work securely in a new cloud environment.

Additionally, the use of open source has increased the risk, with developers sometimes using unknown vulnerable components and frameworks. So many developers are responsible for maintaining so much open source that, in these scenarios, one of the challenges becomes knowing where the code is used and exploitable, and getting them to respond to vulnerabilities in a timely manner when there is an emergency. Another, perhaps more grim challenge is malicious action by the open-source developers themselves.[30]

Embedding DevSecOps

As DevOps becomes more and more automated, 46% of companies are interested in DevSecOps in order to use security controls for continuous integration.[6] This is a positive sign that businesses are understanding the need to respond to security gaps by shifting-left, and are integrating security automation into their production lifecycle to both eliminate inefficiencies and protect against risks that result from services being released prior to security implementation. The challenges of adding application security controls into the continuous integration/continuous delivery (CI/CD) pipeline is motivating security teams to search for new tools that can integrate more easily and seamlessly into the DevOps stack without hindering it.

DevSecOps not only improves security, but also improves collaboration. 40% of organizations report that DevSecOps has facilitated stronger engagement between their development, infrastructure management, application owners, and cybersecurity stakeholders. Additionally, 40% also reported that DevSecOps has enabled them to achieve better operational efficiency via automation.[6]

Going forward, more solutions that enable application security from a "systems" point of view will be needed as the DevSecOps model becomes full stack. The microservice a developer creates that goes into the container comes bundled with an entire environment, and has everything from the application through the OS, all the way down to network drivers in a virtual machine. It is necessary to consider the entire development and all of the code together, not just the application logic.

Finally, if governments demand a "software bill of materials" (SBOM) for software sold to them, Shift-Left tools will be required to build accurate SBOMs at the time of code compilation and packaging, which is another business case for this class of technology.

DEFENDER'S PERSPECTIVE

Shift-Left is key to our 2022 strategy, and we are focused on making sure the "Sec" in DevSecOps is not forgotten by the development teams. Although the tools are there, they can be tricked by developers who feel pressured by the speed of the business. Therefore, as an industry, we will constantly need more scanning – not necessarily in the DevSecOps chain, but afterwards. We will also need real security experts to review code changes manually in order to give us the proof that what has made it to production is secure and robust for the future.

Olivier Nautet
Group CISO - Head of Cybersecurity
& Digital Fraud, BNP Paribas

BNP PARIBAS

Solutions

Static Application Security Testing (SAST)	Dynamic Application Security Testing (DAST)	Interactive Application Security Testing (IAST)
Software Composition Analysis (SCA)	Secure Development Lifecycle (SDL)	Developer Security Training
Application Security Orchestration and Correlation (ASOC)	API Security	

Select Providers

paloalto NETWORKS · snyk · tenable network security

WhiteSource · aqua · SECURE CODE WARRIOR

TEAM8'S ATTACKER PERSPECTIVE

Similarly to Data Security, there are two opposite forces at play. While Shift-Left can make code safer if good processes and tools for secure development are in place, it also makes everything code. The more code there is, the higher the chances that someone will make a mistake, and we may therefore see attackers shifting their focus from infrastructure vulnerabilities to infrastructure-as-code vulnerabilities.

40%

of organizations report that DevSecOps has fostered a high level of collaboration

40%

also noted that DevSecOps allows them to gain greater operational efficiency through automation

– Oracle

Impact

If Shift-Left works, the biggest impact will be that it enhances the relationship between security and AppDev, which will enable the faster creation of secure applications. This will be a win-win for all stakeholders, including the CIO and CISO. However, in order for Shift-Left to work, security has to adapt to the way developers think, act, buy, and consume tools. This concept can already be seen in the way security solutions are starting to operate "business-to-developer" (B2D) models in which the sales and go-to-market strategies are aimed at developers.

Final Thoughts

In the last 18 months, organizations have had to make huge changes, very quickly. Much of this has been in the cloud. This will have major implications for 2022 and beyond.

The huge acceleration in the use of the cloud, and the multiple impacts this has had on work processes, employees, technology policy, and, ultimately, cybersecurity, is playing a huge role in the way organizations are considering their technology and cybersecurity requirements. At the same time, the sheer volume and extent of the threats today, accelerated by the pandemic and changing working environments, means that cybersecurity not only has to get better, but it also has to get smarter. Cybersecurity must be implemented in a cohesive, integrated way that reduces complexity and increases efficiency. A driving force will be the use of Smarter Security technologies such as security automation and AI, which are likely to be game changers, and organizations at the forefront of these technologies are already seeing the benefits.

Resilience is also key. Cyber attacks are a fact and no security posture is likely to be able to eradicate them completely. Accordingly, ensuring that there are sufficient backups and resiliency measures in place reduces the impact and cost of successful attacks, and speeds up recovery time. It also reduces the likelihood of business-wide interruptions.

Finally, this is all having a huge impact on the role of the CISO because cybersecurity cannot, and should not, stand alone. CISOs and cybersecurity teams should be core to the business, and they should be working up, down, and sideways in order to take a strategic approach to the intersection of technology, security, and business operations.

Going forward, cybersecurity will be critical to any digital transformation strategy, and smart technology choices, including cybersecurity considerations, must be integrated into both the technology stack and the business from the start.

Contributors

Author

Aaron Dubin
VP of Strategy & Business Research,
Team8

aaron@team8.vc

Contributors

Nadav Zafrir
Co-Founder & Managing Partner, Team8

Bob Blakley
Operating Partner,
Team8

Charles Blauner
Operating Partner & CISO in Residence, Team8

Assaf Mischari
Managing Partner,
Team8

Tom Sela
VP of Technology Research, Team8

Gal Hochberg
Group CTO,
Team8

Liran Grinberg
Managing Partner,
Team8 Capital

Amir Zilberstein
Managing Partner,
Team8

Admiral (Ret.) Michael Rogers
Operating Partner, Team8

David Warshavski
VP, Enterprise Security,
Sygnia

Olivier Nautet
Group CISO – Head of Cybersecurity & Digital Fraud, BNP Paribas

Omkhar Arasaratnam
Engineering Director,
Google

Jerry Geisler
SVO & Global CISO,
Walmart

Stephen Sparkes
CISO,
Scotiabank

John Petersen
CISO,
Nestlé

Jean-Claude Chauveau
Founder & CEO,
FCME Global, Integrion

TEAM8™

For further information, visit
www.team8.vc

Team8 is a global venture group with deep domain expertise that creates companies and invests in companies specializing in enterprise technology, cybersecurity, and fintech. Leveraging an in-house, multi-disciplinary team of company-builders integrated with a dedicated community of C-level executives and thought leaders, Team8's model is designed to outline big problems, ideate solutions, and help accelerate success through technology, market fit, and talent acquisition.

References

1. IBM Cost of a Data Breach Report 2021. (2021). IBM Security and the Ponemon Institute. https://www.ibm.com/security/data-breach

2. Biden, J. (2021). Executive Order on Improving the Nation's Cybersecurity. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

3. Proposal on Digital Operational Resilience for the Financial Sector. (2020). European Commision. https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2020)595&lang=en

4. Dorries, N. (2021). Product Security and Telecommunications Infrastructure Bill. UK Parliament, Department for Digital, Culture, Media and Sport. https://bills.parliament.uk/bills/3069

5. Cybersecurity Market Review 1H 2021. (2021). Momentum Partners. https://momentumcyber.com/cybersecurity-market-review-h1-2021/

6. Oracle 2021 Cloud Security Trends. (2021). Oracle. https://www.oracle.com/a/ocom/docs/top-5-cloud-security-trends-for-2021.pdf

7. 2021 Cloud Security Report. (2021). Fortinet & Cybersecurity Insiders. https://www.fortinet.com/resources-campaign/dynamic-cloud-security/2021-cloud-security-report?utm_source=blog&utm_campaign=2021-cloud-security-report

8. The State of SaaS Sprawl in 2021. (2021). Productiv. https://productiv.com/resources/the-state-of-saas-sprawl-in-2021/

9. Croll, T. & Heiser, J. (2021). Hype Cycle for Cloud Security, 2021. Gartner. https://www.gartner.com/en/documents/4004061/hype-cycle-for-cloud-security-2021

10. (ISC)2 Cybersecurity Workforce Study, 2021. (2021). (ISC)2. https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

11. Feiner, L. (2021). Microsoft Announces Plan to Cut Cybersecurity Workforce Shortage in Half by 2025. CNBC. https://www.cnbc.com/2021/10/28/microsoft-aims-to-cut-cybersecurity-workforce-shortage-in-half-by-2025.html

12. Preparing for AI-enabled Cyberattacks. (2021). MIT Technology Review Insights. https://www.technologyreview.com/2021/04/08/1021696/preparing-for-ai-enabled-cyberattacks/

13. The State of Ransomware 2021. (2021). Sophos. https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469

14. 2021 Data Breach Investigations Report. (2021). Verizon. https://www.verizon.com/business/resources/reports/dbir/

15. Attacks From All Angles: 2021 Midyear Cyber Report. (2021). Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/attacks-from-all-angles-2021-midyear-security-roundup

16. Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. (2021). U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC). https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

17. The State of Ransomware 2020. (2020). Sophos. https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

18. Ransomware: The True Cost of Business. (2021). Cybereason. https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf

19. Balmforth, T. & Tsvetkova, M. (2022). Russia Takes Down REvil Hacking Group at U.S. Request – FSB. Reuters. https://www.reuters.com/technology/russia-arrests-dismantles-revil-hacking-group-us-request-report-2022-01-14/

20. Janardhan, S. (2021). More Details About the October 4th Outage. Meta. https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/

21. Summary of the AWS Service Event in the Northern Virginia (US-EAST-1) Region. (2021). AWS. https://aws.amazon.com/message/12721/

22. Rozeman, J. & Hoeck, M. (2021). Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults. Gartner. https://www.gartner.com/en/documents/4002031/innovation-insight-for-leveraging-isolated-recovery-envi

23. Blair, R. & Hewitt, J. (2021). Market Guide for Disaster Recovery as a Service. Gartner.

24. Hojlo, J. (2021). Future of Industry Ecosystems: Shared Data and Insights. IDC. https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights/

25. The Connected Enterprise: IoT Security Report 2021. (2021). Palo Alto Networks & Vanson Bourne. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/research/connected-enterprise-iot-security-report-2021

26. Mathews, L. (2021). Florida Water Plant Hackers Exploited Old Software and Poor Password Habits. Forbes. https://www.forbes.com/sites/leemathews/2021/02/15/florida-water-plant-hackers-exploited-old-software-and-poor-password-habits/?sh=5b57f8bc334e

27. Alexander, A., Cracknell, R., De Smet, A., Langstaff, M. Mysore, M. & Ravid, D. (2021). What Executives Are Saying About the Future of Hybrid Work. McKinsey. https://www.mckinsey.com/business-functions/people-and-organizational-performance/our-insights/what-executives-are-saying-about-the-future-of-hybrid-work#:~:text=In%20the%20postpandemic%20future%20of,executives%20across%20industries%20and%2–0geographies.&text=1

28. Omale, G. (2019). Embrace a Passwordless Approach to Improve Security. Gartner. https://www.gartner.com/smarterwithgartner/embrace-a-passwordless-approach-to-improve-security

29. Reinsel, D., Rydning, J. & Gantz, J. (2021). Worldwide Global DataSphere Forecast 2021–2025: The World Keeps Creating More Data — Now, What Do We Do with It All?. IDC. https://www.idc.com/getdoc.jsp?containerId=US46410421

30. Sharma, A. (2022). Dev Corrupts NPM Libs 'Colors' and 'Faker' Breaking Thousands of Apps. Bleeping Computer. https://www.bleepingcomputer.com/news/security/dev-corrupts-npm-libs-colors-and-faker-breaking-thousands-of-apps

31. 22 Biggest GDPR Fines of 2019, 2020, and 2021(So Far). (2021). Tessian. https://www.tessian.com/blog/biggest-gdpr-fines-2020/

Team8 Disclosure

This Team8 Cybersecurity Themes Report represents the opinions of Team8 Labs Inc. (“Team8”) and is for informational purposes only. You should not treat any opinion expressed by Team8 as a specific inducement to make an investment in any security, but only as an expression of Team8’s opinions. Team8’s statements and opinions are subject to change without notice. Team8 is not registered as an investment adviser under the Investment Advisers Act of 1940, as amended (the “Advisers Act”), and relies upon the “publishers’ exclusion” from the definition of investment adviser under Section 202(a)(11) of the Advisers Act. As such, the information contained in this Team8 Cybersecurity Themes Report does not take into account any particular investment objectives, financial situation or needs and is not intended to be, and should not be construed in any manner whatsoever as, personalized investment advice. The information in this Team8 Cybersecurity Themes Report is provided for informational and discussion purposes only and is not intended to be, and shall not be regarded or construed as, a recommendation for a transaction or investment or financial, tax, investment or other advice of any kind by Team8. You should determine on your own whether you agree with the information contained in this Team8 Cybersecurity Themes Report. Certain of the securities referenced in this Team8 Cybersecurity Themes Report may currently, or from time to time, be constituents of an index developed and maintained by WisdomTree Investments, Inc. using data provided by Team8, which has been or will be licensed for a fee to one or more investment funds. In addition, certain officers or employees of Team8 or funds or other persons or entities affiliated or associated with Team8 may hold shares of, be officers or directors of, or otherwise be associated with some or all of the issuers of the securities referenced in this Team8 Cybersecurity Themes Report or included in such index. Team8 expressly disclaims all liability with respect to any act or omission taken based on, and makes no warranty or representation regarding, any of the information included in this Team8 Cybersecurity Themes Report.

Important Information from WisdomTree

This material has been written by third parties not affiliated with WisdomTree or any of its affiliates. No information contained in the material has been endorsed or approved by WisdomTree, and WisdomTree is not responsible for the content. No information accessed through this material constitutes a recommendation by WisdomTree to buy, sell or hold any security, financial product or instrument discussed therein. This information neither is nor should be construed as an opinion regarding the nature, potential, value, suitability or profitability of any particular investment or investment strategy, and you shall be fully responsible for any investment decisions you make, and such decisions will be based solely on your evaluation of your financial circumstances, investment objectives, risk tolerance and liquidity needs.