TEAM8™

2021 Cybersecurity Brief

Table of Contents

Introduction

The world of cybersecurity is changing and cyber risk is taking on a whole new meaning for enterprises, not only technologically, but also financially, reputationally, and operationally.

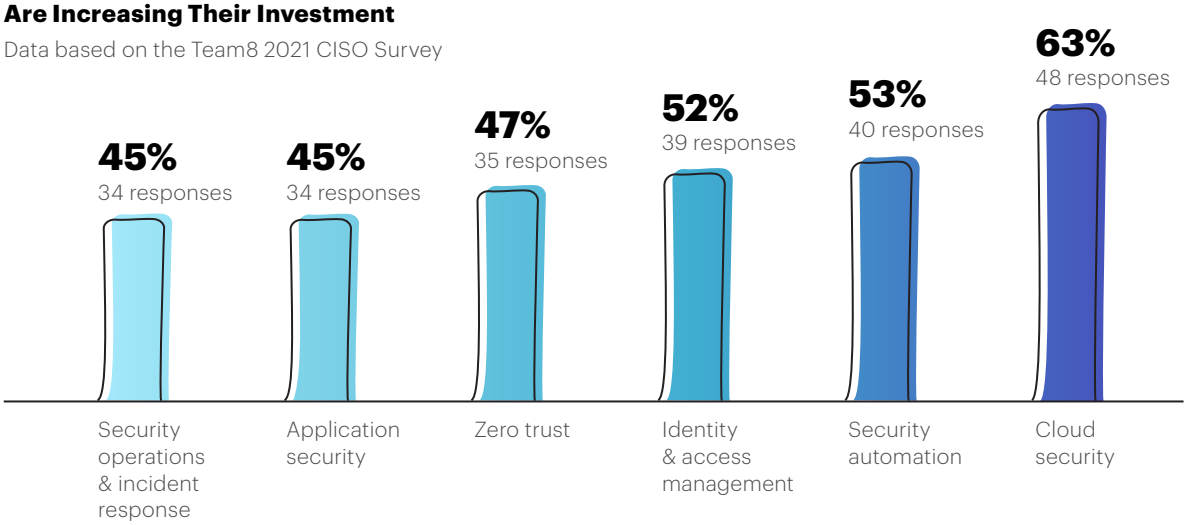
Prior to the Covid-19 pandemic, cybersecurity was already approaching a tipping point — attackers were getting more sophisticated, attack surfaces were expanding, and the bad actors' advantage was becoming more asymmetrical. Luckily, the pandemic may have also accelerated some positive shifts in the way organizations fundamentally think about cybersecurity. The pandemic caused enterprises to become more reliant on their digital infrastructure as a building block critical to business operations. A second order consequence of the expansion in scope of digital transformation has been a spotlight on the importance of resilient infrastructure, vetted third-party suppliers, and a sound supply chain. The recent SolarWinds attack illustrated how these concepts have been elevated in a digitally transformed and interconnected economy. Enterprises should seize this opportunity to reexamine their infrastructure and make investments to solve root cybersecurity problems and vulnerabilities, ultimately leading to greater security and resilience.

To help navigate this path forward, we are excited to introduce our 2021 Cybersecurity Brief outlining the main themes, drivers, and implications that we believe will be of critical importance to the industry in the next few years. The seven themes help shed light on the way the overall cybersecurity environment is changing and the forces behind them. This brief was created as much for ourselves as it was for innovators, operators, and technologists, as we have used it to guide our company building strategy and how we see the world of cybersecurity evolving.

How we identified our themes. We collaborated with our Village — our community of 350+ C-level security executives from 300 enterprises across 20 countries, 25% of which are Fortune 500, and 55% of which are Forbes Global 2000. We also worked closely with our Team8 cybersecurity experts, many from Israel's elite 8200 military intelligence unit, and our global advisors to highlight the areas of immense future business growth and product depth from a technology, market trend, regulatory, and venture funding standpoint. 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. We also considered Team8's "Attacker Perspective" (our unique insights into how attackers think and operate), and other Team8 internal resources, in addition to publicly-available information. We then cross-referenced our findings with the responses from our proprietary 2021 CISO Survey, confirming the top areas where security leaders are increasing their investment (see below).

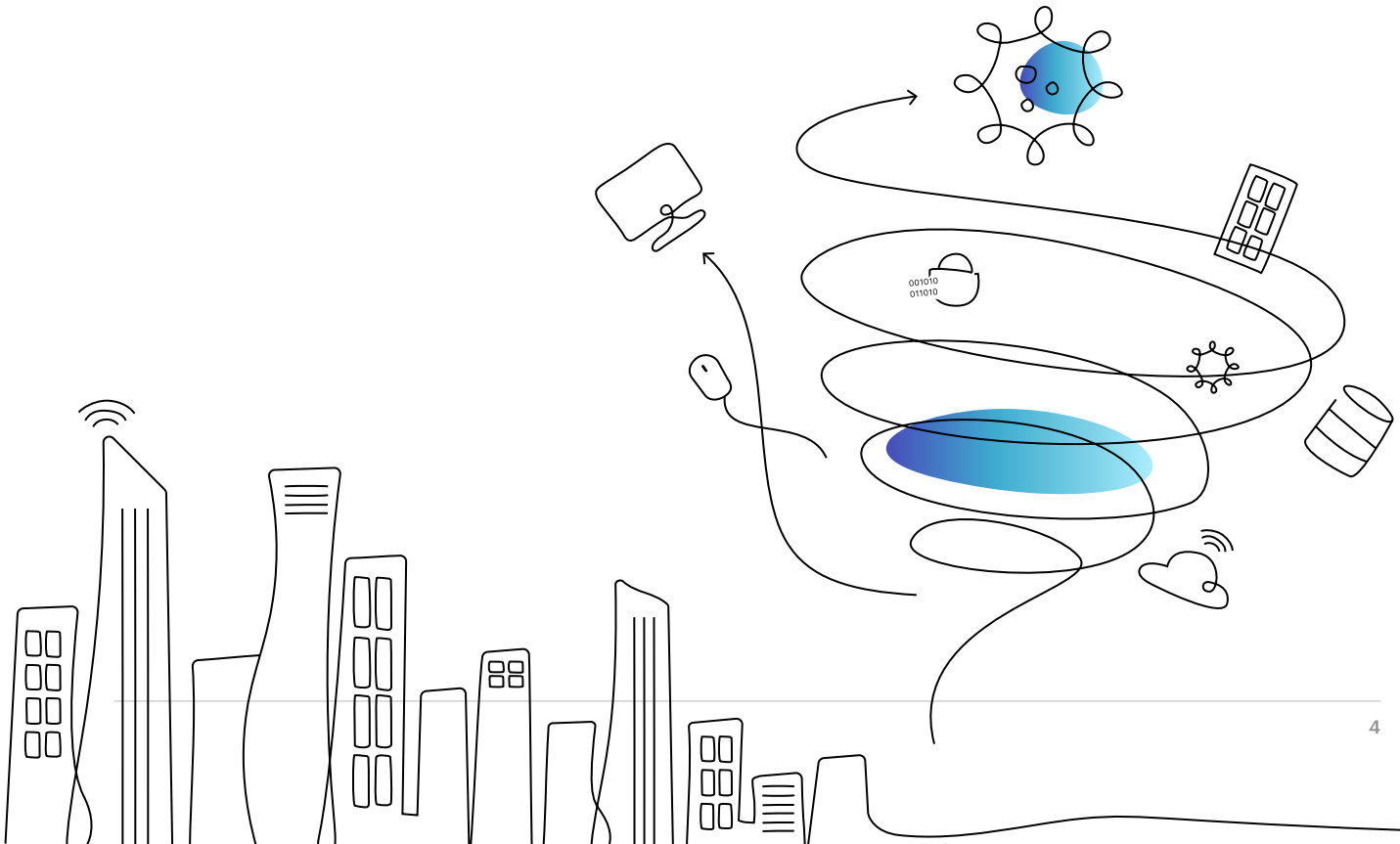
Top Areas Where Security Leaders Are Increasing Their Investment

Data based on the Team8 2021 CISO Survey



Our 7 Themes Driving the Future of Cybersecurity

The following represent Team8's seven cyber themes. Each theme includes the threats and technology trends driving the theme, as well as some suggested products and services that can serve as solutions to the challenges created. To enrich the discussion, we've included perspectives from CISOs in our Village to illustrate how defenders are thinking about these themes and operationalizing them, as well as Team8's Attacker Perspective to reflect the adversary's viewpoint.



Team8 Cyber Themes

	Drivers	Impact
01 Cloud Security		
Cloud adoption is on the rise and enterprise cloud migrations are expanding from experiments to business-critical initiatives. Security capabilities are evolving so that enterprises can retain control over their security posture, data protection programs, and application integrity.	• Reliance on cloud as a business critical system • Ubiquity of container technology (e.g. Kubernetes) • Complex hybrid and multi-cloud environments	Security solutions must be architected for the cloud, combining control and integrity with scalability and agility.
02 Security of Things		
IoT device connectivity unlocks new business value in the industrial economy. But as IT networks and operational technology (OT) networks converge, the attack surface expands, and adversaries can move from stealing data to threatening health and safety.	• Explosion of connected devices • Convergence of IT and OT • Ramifications on the supply chain and physical world, including personal safety	Ransomware and 5G are changing the OT threat landscape. To mitigate risk, new models and mindsets are needed.
03 Perimeterless World		
The enterprise perimeter is nearly extinct and the shift to remote work during COVID-19 is accelerating its demise. Identity and zero trust architectures will become increasingly important in governing access management.	• Remote work • SaaS • Cloud migration • Insider threats	Security strategies must change to support new ways of doing business that drive growth, productivity, and competitive advantage.
04 Privacy & Digital Trust		
Globalization and growth of the digital economy are colliding with emerging privacy regulations and consumer preferences, providing users with more control over their data. Architectural design and business processes must accommodate new privacy and zero trust-driven strategies.	• Globalization combined with different geopolitical approaches to privacy and data protection • Growth in data breaches • Growth in privacy regulations • Changing consumer preferences	Knowing what data you have, storing only what is needed, and leveraging technologies that enable business without sharing data will become critical.
05 Resilience & Recovery		
Digital infrastructure is now business critical, and therefore, recovery from cyberattacks is now a core tenet of risk mitigation and business continuity. Any sound security strategy necessitates capabilities that enable rapid recovery and reconstitution of assets and capabilities.	• Increasing pace of cyber attacks • Ransomware • Not just about security but also relates to operational resiliency • Getting it wrong could be fatal	Companies need a reboot plan designed for the digital age, to build resiliency and accelerate recovery from damage or disruption.
06 Shift-Left		
Developing and managing software is becoming more agile and faster than ever. Security can't come after the fact, but needs to be shifted-left to the developers, embedding security considerations from the start in a DevSecOps model.	• Code to production is the new pace of business • DevSecOps • Security by Design	Security professionals must understand coding, and developers must be able to code with security in mind.
07 Smarter Security		
Response capacity is stretched to its limits as organizations face immense security complexity — dozens of products that aren't integrated, an expanding enterprise network, a cyber talent shortage, and an adversary leveraging increasingly sophisticated capabilities. Smarter security can plug the gaps.	• Growing attack surface • Increase in number of security tools • Shortage of cyber talent • Pace of attacks	Smarter security solutions can leverage automation, data, and AI to handle routine tasks, so humans can focus on managing exceptions.

01

Cloud Security

Buoyed by tailwinds from the pandemic and remote work, cloud adoption is on the rise and enterprise cloud migrations are expanding from fringe 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.

Cloud security is the number one investment area for 2021 according to the Team8 2021 CISO survey

Drivers

2020 will go down as a pivotal year for cloud adoption as businesses sought to cut costs, retain flexibility, and throttle demand due to dislocation caused by the pandemic. In fact, cloud security is the number one investment area for 2021 according to the Team8 2021 CISO Survey, followed by Security Automation and Identity and Access Management. In retrospect, we expect that 2020 will be remembered not only as the year where cloud became the default, but also where the dynamics governing enterprise networks and workload deployments changed forever. In a world where containers offer the capability to combine hybrid, multi-cloud and on-premise compute and storage strategies, security tools and techniques will need to evolve to reduce complexity created by a multitude of new offerings within and beyond the enterprise perimeter. For example, workloads moving between different cloud environments to optimize for speed, scalability, cost, and compliance have created a new "shared responsibility" model between the enterprise and its different cloud providers. If not managed properly, this model could open the door for threat actors to identify and leverage misconfigurations as a way to gain access.

DEFENDER'S PERSPECTIVE

The next big thing with regards to cloud security is automated remediation. Most cloud vulnerabilities can be automatically fixed rather than fixing them one by one, by hand. When you describe things with code, they can be easily applied to multiple instances. This characteristic offers an opportunity to automatically remediate these vulnerabilities as opposed to waiting for DevOps to do it.

Jonathan Jaffe
CISO, Lemonade
Lemonade

TEAM8'S ATTACKER PERSPECTIVE

The complexity of an environment usually plays into the hands of the attacker, and it would be hard to find infrastructure more complex than modern cloud. It is a mesh of services, identities, logs, networking, compute, and storage. For attackers, it's the wild west. When moving to the cloud, many enterprises lose the visibility, understanding, and control they had when their infrastructure was on-premise. This is a new playground for attackers, especially since they have plenty of opportunities for target practice on cloud networks.

Impact

Cloud is becoming so complex it should be perceived as an operating system. Many of today's security solutions are just modern-day equivalents of endpoint security and other on-premise techniques that had limited effectiveness. Attacks are not only still happening, but are being amplified by the pervasiveness, speed, and connectedness of the cloud. Instead of applying legacy solutions to the cloud, organizations need security solutions that are architected for the cloud, combining control and integrity with scalability and agility.

Solutions

Cloud Workload Protection Platform (CWPP)	Cloud Security Posture Management (CSPM)
Cloud Infrastructure Entitlement Management	Cloud Access Security Broker (CASB)
Extended Detection and Response (XDR)	Container Security

Select Providers

paloalto NETWORKS · zscaler · Check Point SOFTWARE TECHNOLOGIES LTD. · netskope · orca security

02

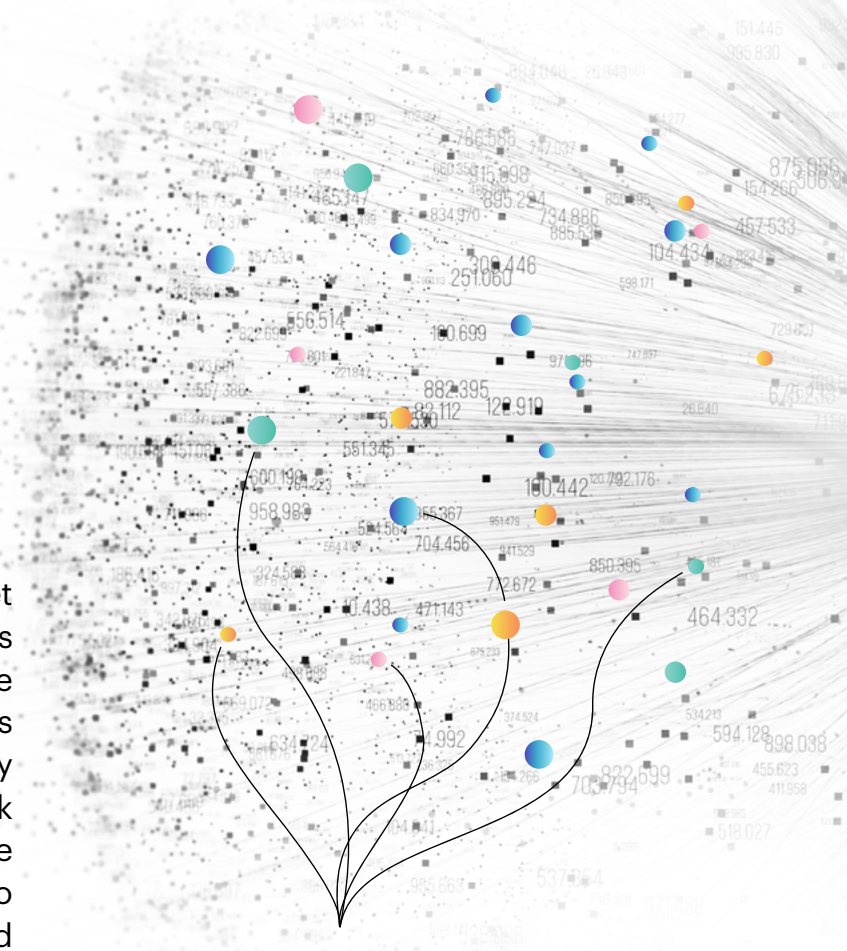
Security of Things

Technology advances are fueling Internet of Things (IoT) device connectivity that is driving the Industrial Economy to digitize and unlock new business value. But as IT networks and operational technology (OT) networks converge, the attack surface expands, and the stakes are raised. Cyber threats move from data to people — disrupting supply chains and infrastructure critical to health and safety.

DEFENDER'S PERSPECTIVE

The global supply chain is immense and growing with more connectivity and automation in the Internet of Things driving efficiencies and improved performance throughout. Concurrently, this growing web of interconnectivity has the potential to make our production systems more fragile because one change can have a cascading and tangible impact in the overall physical world. The ability to adapt cyber techniques, such as security monitoring, visibility, and remediation, to a totally different environment of inter-connected devices operating our physical manufacturing world, will be foundational to creating a safe and resilient global supply chain. The industry must grow beyond managing this retroactively and manually via spreadsheets toward a real-time, always available and highly precise, layered network design approach.

Jim J. LaBonty
Head of Global Automation Engineering, Pfizer, Inc.



55.7 Billion

Connected devices worldwide by 2025
- IDC

Drivers

Fueled by advancements in lower-power compute and communication, there's an explosion of connected devices, with IDC predicting there will be 55.7 billion connected devices worldwide by 2025.[1] Entirely new devices are coming online, while old technologies that have been online for years under the radar, such as in manufacturing, remain vulnerable. The 5G spectrum enables ubiquitous connectivity because it expands the frequencies and bandwidth for data transfer. As critical infrastructure and manufacturing sectors go online, spurred by advancements in smart machinery, IT and OT networks are converging. Legacy systems are being connected to the Internet, along with Industrial IoT (IIoT) technologies like smart meters, automated asset distribution systems, and self-monitoring transformers, or production lines and farm equipment outfitted with sensors.

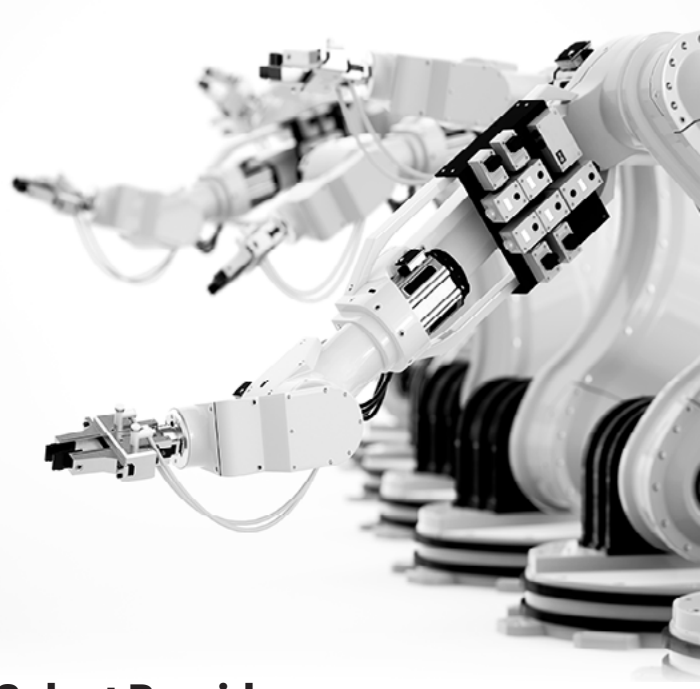
Done right, IT-OT convergence unlocks tremendous business value — enabling improvements in operational efficiency, performance, and quality of service. But new threat types expose the need for better endpoint defense. Novel attack patterns and approaches are cropping up every day - ransomware, cryptojacking, new kinds of advanced persistent threats (APTs) - that require a shift from signature-based detection to more advanced and dynamic behavioral-based techniques. Enterprise security teams simply can't stop them all and a lack of asset visibility and management, and security updates compounds the problem. Successful attacks go beyond data breaches — widespread disruption and harm, both physically and economically, is often the attacker's endgame.

TEAM8'S ATTACKER PERSPECTIVE

IoT devices are prime targets for attackers. These devices contain all the hallmarks attackers like - they are black boxes, are rarely designed with security in mind, and use embedded code that isn't updated and is full of security holes that are usually not patchable. Adding connectivity to the corporate network transforms IoT into the perfect entry point for the sophisticated APT.

Solutions

OT Security	IoT Security	EDR & EPP
User Behavior Analytics	Vulnerability Management	Managed Detection and Response (MDR)
Deception	Antivirus	



Impact

Although there has been an evolution in this field over the last few years, the shift in ransomware from focusing on data and IT infrastructure, to disrupting OT environments is accelerating and is perhaps the single greatest threat facing CISOs and CIOs today. Furthermore, as 5G proliferates, everything will become "a thing" and even in domains like OT, the concept of networks will dramatically change. IT security controls can't adapt to work in OT environments. To mitigate risk of threats that cross the IT/OT boundary, new models and mindsets are needed.

Select Providers

CLAROTY · CROWDSTRIKE · armis · TANIUM · VDOO

03

Perimeterless World

The enterprise perimeter is nearly extinct and the dramatic shift to remote work during the pandemic is accelerating its demise. Security needs rethinking in a world without perimeters, where identity and zero trust architectures will need to play increasingly important roles governing access management.

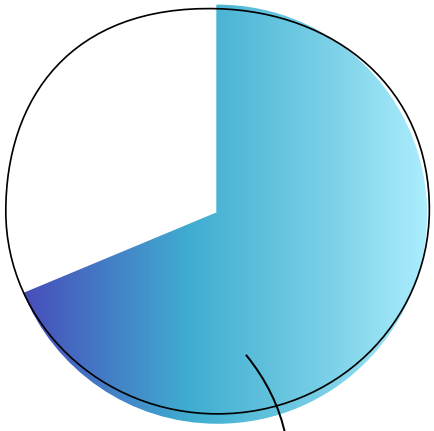
Drivers

The traditional firewall approach assumed that enterprises could establish a strong perimeter and then intrinsically trust everyone inside. Yet, even before the pandemic, cloud migration and the adoption of Software-as-a-Service (SaaS) applications were on the rise causing perimeter-based controls to become increasingly hard to maintain and scale. Many enterprises also had existing Bring Your Own Device (BYOD) programs and robust mobile-first initiatives that perimeter-based controls were never designed to protect.

DEFENDER'S PERSPECTIVE

The network as a decision maker has been outmoded, and has not been a particularly useful gating mechanism for some time. Instead, trust ought to be treated as a gradient and neither as a static nor binary state of being. With the evolution to zero-trust, enterprises can reevaluate trust levels dynamically, so they can constantly reassess the extent to which to trust an identity. With an access management approach rooted in a perimeterless reality, security teams can make more nuanced decisions with inputs from the business about risk tolerance and acceptance. The shift from caring about "where" to "who" is the natural evolution of security that enterprises can choose to either lead or lag.

Justin Berman
Former Head of Security, Dropbox
Dropbox



72%

of office workers indicate a desire to retain the flexibility to work remotely

- PWC Remote Work Survey

Remote-first work will remain with us in a post pandemic environment, with 72% of office workers indicating a desire to retain the flexibility to work remotely.[2] As such, the global workforce has become reliant on at-home WiFi networks, non-hardened work devices, and online collaboration tools. Without reliable connectivity, employees may not be getting the protection they need and their non-hardened devices can also pose a significant risk to enterprise network security. A more porous perimeter with less oversight is also naturally more susceptible to insider threats, malicious or unintentional. Organizations must quickly move beyond perimeter-based solutions to secure the growing number of applications and resources hosted in the cloud, available as a service, and on mobile systems.

Solutions

Identity Access Management	Zero Trust	User Entity Behavior Analysis
Secure Access Server Edge (SASE)	Software Defined Perimeter (SDP)	Cloud Access Security Brokers (CASB)

TEAM8'S ATTACKER PERSPECTIVE

In a perimeter-driven strategy, once attackers successfully infiltrate a perimeter, they can easily navigate laterally within a wide internal enterprise environment. While breaking through the perimeter is hard, moving within it is easier. On the downside, the death of the perimeter and the move to zero trust has theoretically exposed some internal crown jewels to the outside. The upside is that, in most cases, zero trust breaks the network into smaller fragments, removing much of the lateral movement options for an attacker.

Impact

With less and less behind the walls of the enterprise, companies can no longer take a fortress approach to defend against threat actors. Employees, vendors, contractors, and customers are all connecting to the network from everywhere. Security strategies need to evolve to support new ways of doing business that drive growth, productivity, and competitive advantage.

Select Providers

okta Auth0 CATO NETWORKS

zscaler illusive

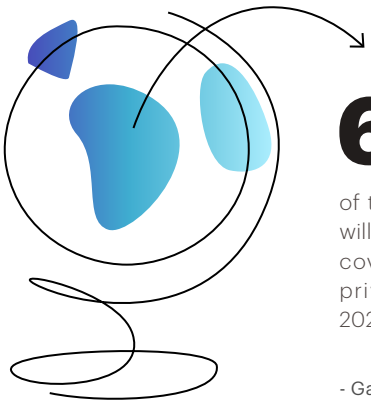
04

Privacy & Digital Trust

On one hand, globalization and the growth of the digital economy are accelerating the need for safe and trustless means of digital collaboration to remain competitive. On the other, emerging privacy regulations and consumer preferences are driving more investments in privacy-enhancing technologies and providing users with more control over their data. The net result of these colliding forces will be new privacy- and zero trust-driven strategies that impact underlying architectural design and business processes.

Drivers

The recent history of high-profile data breaches is accelerating privacy regulations and eroding consumer trust in companies. Cisco's 2020 Consumer Privacy Survey revealed that one-third of consumers are "Privacy Actives" who have stopped doing business with organizations over Data Privacy concerns.[3]



65%

of the world's population will have its personal data covered under modern privacy regulations by 2023, up from 10% in 2020

- Gartner

DEFENDER'S PERSPECTIVE

In today's digital world, privacy sometimes, albeit superficially, seems at odds with business objectives. Businesses must reconcile a vigorous appetite to collect, leverage, and exchange data that could be monetized with a growing demand for enhanced privacy from consumers and regulators. In particular, businesses need to carefully consider reducing their liability as related to data loss or misuse.

Privacy preserving technologies such as homomorphic encryption help businesses to achieve new and existing objectives by enabling the processing of data while keeping it encrypted, and outsourcing computation to untrusted servers and clouds without compromising on privacy. Such mathematical approaches may not only help to improve existing data sharing practices, but even more importantly can unlock hidden value, new business models, and unique approaches to collaboration for organizations who are willing to adopt a new privacy paradigm.

Professor Shafi Goldwasser
Director of the Simons Institute for the Theory of Computing, UC Berkeley

Berkeley
UNIVERSITY OF CALIFORNIA

This trend is likely to continue as 65% of the world's population will have its personal data covered under modern privacy regulations in the next two years, up from 10% in 2020.[4] Yet, many organizations have a hard time keeping up with growing and ever-changing regulations because they lack an effective Governance Risk and Compliance (GRC) program and regulations often conflict with one another, making it costly and complicated to comply. To satisfy regulations and earn consumer confidence, organizations need to take a proactive approach with tools, systems, and services that help them get ahead of business risk by identifying and managing personal information within their enterprises and throughout the supply chain, respecting regional variations in data regulations, and transparently supporting consumers' intentionality about data sharing.

TEAM8'S ATTACKER PERSPECTIVE

The use of privacy-preserving technologies and a decreasing number of large hackable open datasets are pushing bad actors to attack the edges and collect data before it can be secured. PCI removal of credit card numbers from databases pushed attackers towards attacking the Point-Of-Sale system, where the card number was "in the clear". Similarly, privacy-preserving technologies will make the edge devices increasingly important to attackers who are after the raw data.

Solutions

Data Discovery	Data Classification	Privacy Rights (DSAR)
Data Protection and Compliance	Homomorphic Encryption	Anonymization & Synthetic Data
Distributed Machine Learning	Multi-Party Computation	

Select Providers

Duality VARONIS OneTrust BigID

Impact

In the future, personal data may be controlled by the consumer, which will drive changes in business models, regulations, and security. As consumers and companies become more scrupulous, technologies that enable doing business without sharing data will take center stage and drive competitive advantage. Storing data that an enterprise doesn't need has become a liability not worth taking. Not knowing what data it has and who has access to it has become unconscionable.

Resilience & Recovery

In a world where digital infrastructure is now synonymous with business-critical infrastructure, cybersecurity cannot afford to stop at "protect, detect and respond". Recovery can no longer be an afterthought — it must become a core tenet of risk mitigation and business continuity. Any sound security strategy necessitates capabilities that enable rapid recovery from degradation, disruption, or denial of access to enterprise systems or data, and swift reconstitution of assets and capabilities.

DEFENDER'S PERSPECTIVE

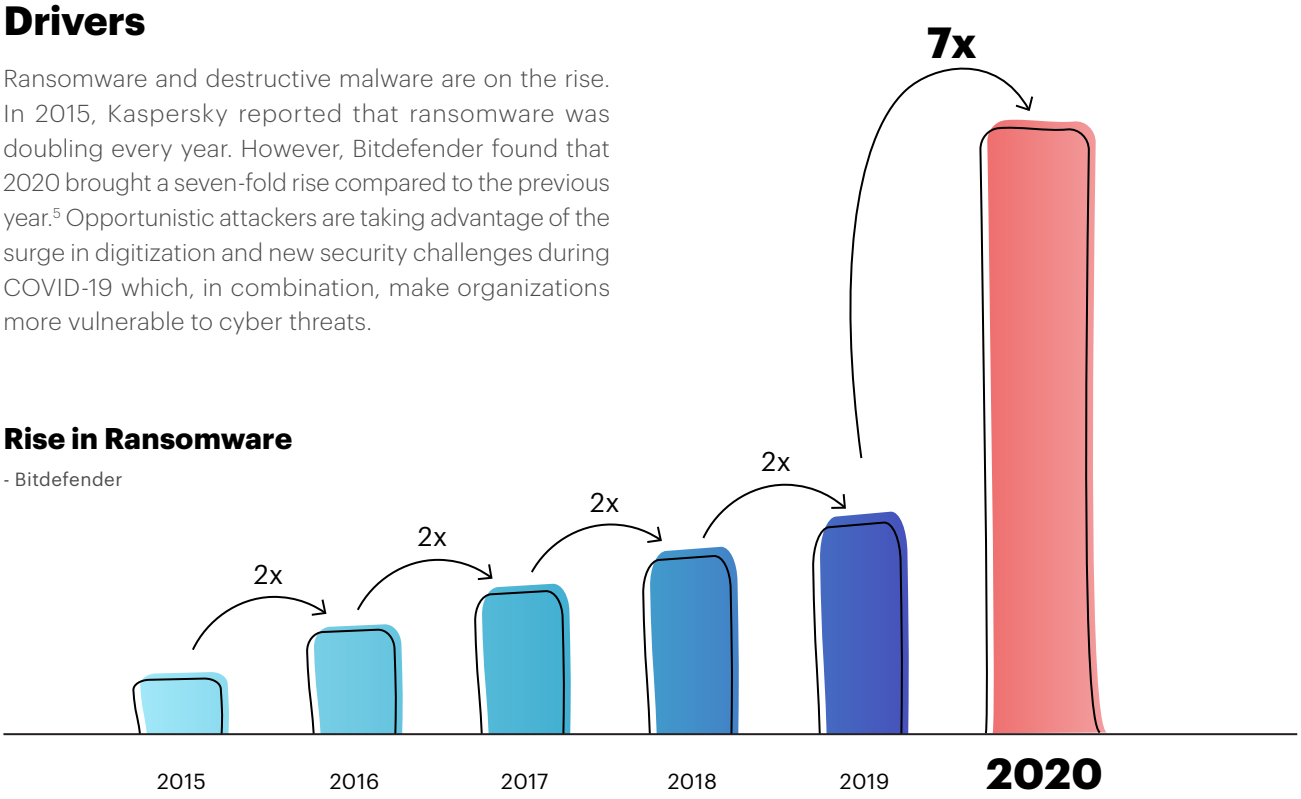
We've made great improvements to our cyber posture that have pushed down the probability of an attack. However, the magnitude of impact has stayed the same or risen because we're more digitally reliant. What COVID-19 has shown us is that low probability, high impact events can happen. Defense is still a core component of any good strategy, but there is an increasing importance for enterprises to quickly reboot in the event of digital catastrophes.

Paul Branley
Director, Strategy, Innovation & Testing
Lloyds Banking Group

Drivers

Ransomware and destructive malware are on the rise. In 2015, Kaspersky reported that ransomware was doubling every year. However, Bitdefender found that 2020 brought a seven-fold rise compared to the previous year.[5] Opportunistic attackers are taking advantage of the surge in digitization and new security challenges during COVID-19 which, in combination, make organizations more vulnerable to cyber threats.

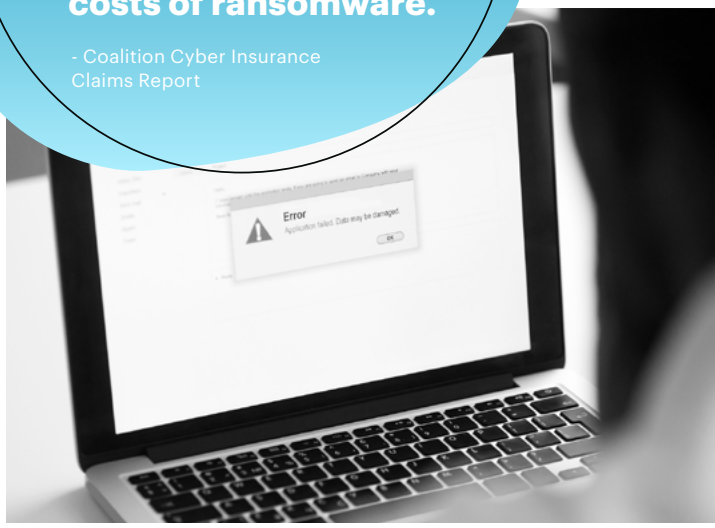
Rise in Ransomware
- Bitdefender



Overall, the average severity of insurance claims reported by policyholders jumped by 65% from 2019 to 2020, driven largely by the rising costs of ransomware as cybercriminals ask for higher amounts of money and increasingly threaten to release stolen data publicly unless the ransom is paid.[6] An October 2020 US Treasury directive, aimed at stymying ransom payments by threatening enterprises who pay with sanctions, could either provide a much needed headwind against this alarming trend or put enterprise leaders, staring down the barrel of a severe ransomware attack, between a rock and a hard place.[7] As enterprises adjust to the business disruptions caused by the pandemic, disaster recovery and business continuity plans are critical. This isn't only a matter of cybersecurity but also of operational resiliency. Any network outage or other disruption to infrastructure can put companies on the sidelines or entirely out of business for months. For many companies, there is no "Plan B" and in today's climate that is a particularly dangerous position in which to be. Even the best security teams will succumb to attacks and knowing how to continue to offer services to customers is essential.

65% rise in average severity of insurance claims between 2019 and 2020, driven largely by the rising costs of ransomware.

- Coalition Cyber Insurance Claims Report



Solutions

Cyber Exercise Facilitation	Cyber Ranges	Self-Healing Systems
Application Performance Monitoring	Backup and Disaster Recovery	

Impact

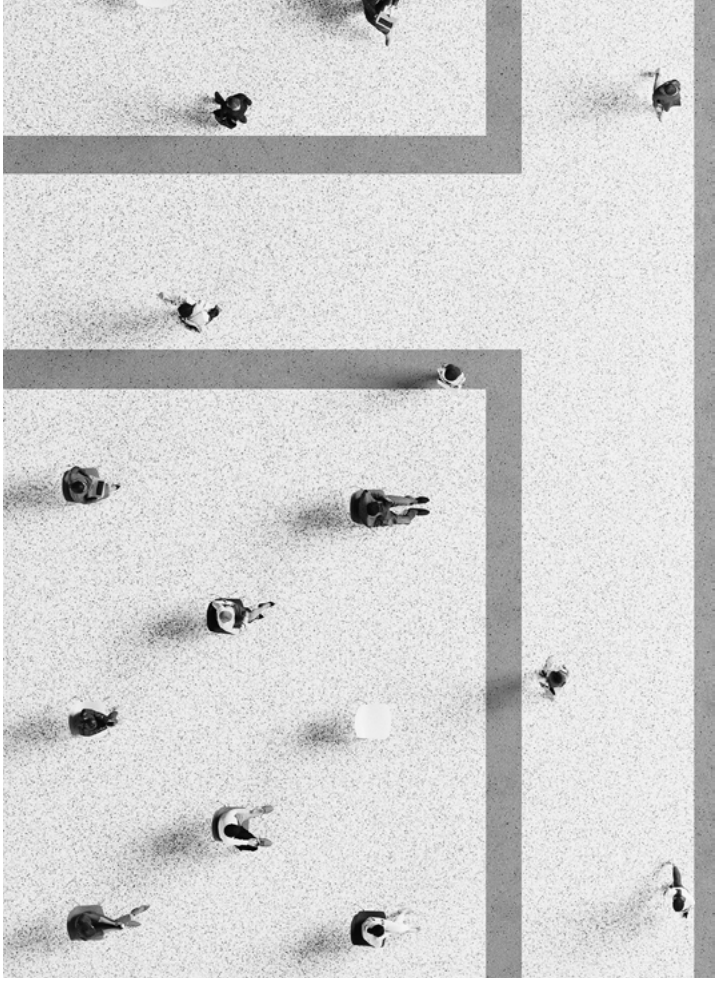
Ransomware is just one example of the damage threat actors are causing businesses. Systems can be modified, data stolen, and infrastructure brought down for a variety of reasons. Companies need a reboot plan designed for the digital age, to build resiliency and accelerate recovery from damage or disruption.

TEAM8'S ATTACKER PERSPECTIVE

Ransomware attacks have evolved beyond holding production and productivity hostage. Improvements in business continuity planning (BCP) and resilience have pushed attackers to make additional threats, such as publishing data if a payment isn't made. This creates a problem for organizations that want to minimize the effects of ransomware by introducing resilience. As systems become more resilient, this two-pronged approach [used by attackers] will proliferate. The latest US Treasury directive threatening prosecution or sanctions to enterprises who pay off certain ransoms could alter this dynamic by pushing attackers to find other ways to monetize their ransom.

Select Providers

COMMVAULT · Zerto · SEMPERIS · Own{backup}



06

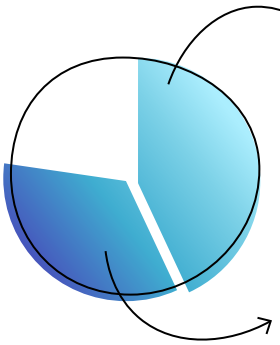
Shift-Left

Developing and managing software is more agile and faster than ever. Security can't come after the fact, but needs to be shifted-left to the developers, embedding security considerations from the start in a DevSecOps model.

Drivers

Time to market is often prioritized over security. Developers are measured by how fast they can code, rather than on how securely. And business leaders are measured on time to market. With no time to fix insecure code at the source, security is often "bolted on" once the application is fully developed — a subpar approach. As a result, 42% of organizations that experienced an external attack blame the incident on a software security flaw and 35% blamed a buggy web application.[8]

In today's dynamic environment of micro-releases and daily or weekly software updates, to get ahead of security, software developers need to maintain a security mindset and rely on controls throughout the coding process. Yet, the migration of a developer-driven security paradigm has been slow as Google reports only 20% of firms are considered "elite performers" with DevOps.[9] Minimally, shift-left highlights the need for security teams to work with developers throughout the development lifecycle to build-in information security and security automation. Ideally, developers are empowered to embed security while creating a product or service, with tools that not only make code more secure, but also codify intent.



42%
of organizations blamed an external attack on a software security flaw

35%
blamed a buggy web application

- Forrester

DEFENDER'S PERSPECTIVE

One way to measure speed of business is developer velocity. Developers are constantly adding features to applications, and if companies wish to remain competitive, modern day security has to move at the speed of business.

Stephen Garcia
VP of Cybersecurity, FanDuel
FANDUEL

Solutions

Static Application Security Testing (SAST)	Dynamic Application Security Testing (DAST)	Interactive Application Security Testing (IAST)
Software Composition Analysis (SCA)	Secure Development Lifecycle	Developer Security Training
Container Security		

Select Providers

paloalto NETWORKS · tenable network security · snyk · aqua

TEAM8'S ATTACKER PERSPECTIVE

Shift-left creates several problems for the attacker. As software becomes more security robust, the chance of zero days is getting slim. But sophisticated attackers can also shift left, adding malicious code or backdoors early in the development cycle before the source code is compiled. A great example of this is the build system for the SolarWinds attack. Instead of waiting for or finding a vulnerability, they changed the system just like a coder would, and created their own vulnerability.

Impact

The farther left the shift, the more deeply security is integrated into the application development process. To achieve this, security professionals should hone their coding skills, and developers must be able to code with security in mind.

07

Smarter Security

The pace of change in technology brings immense complexity to security causing organizations to integrate dozens of products. Orchestrating this is a growing challenge and contributes to technology debt and overhead. Further, an expanding enterprise network and shortage of cyber talent, combined with an adversary leveraging increasingly sophisticated capabilities, is stretching response capacity to its limits. Smarter security solutions can incorporate automation, data, and AI to plug the gaps and provide teams with greater leverage on their human capital.

DEFENDER'S PERSPECTIVE

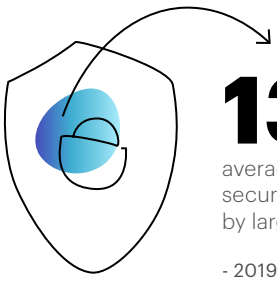
In a post SolarWinds environment, there will be a renewed focus on integrity of the code base, digital supply chain, and APIs to monitor and distinguish between purposeful changes and malicious ones. Even the most robust security teams will need creative solutions to handle the growing number of alerts and identify tamper evidence with enough fidelity to subvert a sophisticated attack. Smarter security can not only aid security professionals in executing on their mission, but will enable human capital to run more investigations and prevention activities in parallel.

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

TEAM8

Drivers

Organizations are deploying and managing an increasing number of security tools to manage ever-expanding networks. In fact, larger organizations deploy 130 cyber tools on average.[10] CISOs are being bombarded by vendors with tools that solve specific problems but don't interoperate. Beyond the initial purchase price, the hidden costs of managing these tools, making sense of the data generated, and the time it takes for the security operations center (SOC) to tie it all together for actionable information are overwhelming.



130
average number of security tools used by large organizations

- 2019 RSA Conference

The global shortage of skilled cyber talent exacerbates the problem. The United States faced a shortfall of almost 314,000 cybersecurity professionals as of January 2019. By 2022, the global cybersecurity workforce shortage has been projected to reach upwards of 1.8 million unfilled positions.[11] Employers today are desperate for people with real technical skills who can design secure systems, create new tools for defense, and hunt down hidden vulnerabilities in software and networks. At a time when attackers are accelerating attacks by employing AI tools, the talent shortage is more pronounced. Smarter security can alleviate the deficit facing defenders by using automation not purely to eliminate human error or save money, but also to empower security teams to be able to defend against attacks at the same rate at which they're happening.

TEAM8'S ATTACKER PERSPECTIVE

As security automation allows the defender to react faster and augment the human element, and in some cases take it out of the loop, the attacker will do the same. Attacker automation will try to "outpace" the defense in a bot-to-bot war.

Solutions

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

Select Providers

paloalto NETWORKS · tufin · DATADOG · splunk> · exabeam · VULCAN.

Impact

Enterprises need software engineers and systems that are focused on APIs and more useful interfaces to enhance security analyst productivity. They need tools that facilitate comprehensive security orchestration. And they need smarter security that leverages automation, data, and AI so that humans can focus on decision making around exceptions, while security solutions analyze data, automate processes, learn over time, and automatically enforce policies.

Final Thoughts

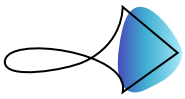
Cybersecurity is going through a historic shift as companies accelerate their digital transformation, systems become more complex and expansive, and attacks become more sophisticated and frequent. We are entering a new age for the industry as it grows and matures, and what happens now will help set the stage for the next cybersecurity cycle and the corresponding generation of companies it yields.

What cybersecurity has going for it

At long last, cybersecurity as a whole is coming into the mainstream spotlight. The CISO is finally starting to be viewed as a business decision-maker and profit enabler, as much as a leader of risk and cost avoidance. Employees and individuals are generally more educated than they used to be about the need for cybersecurity and common ways to avoid falling victim. Finally, due to the pandemic, organizations are on high alert and are catching phishing and other forms of attacks and scams that can lead to a data breach.

Challenges cybersecurity still faces

As the industry matures, what cybersecurity needs is more standardization and compatibility. More intuitive application interfaces that are optimized for the behavior of security professionals. More security by design and more collaboration with engineering teams. More automation and consolidation. Less reliance on trust and less human involvement. The companies that rise to the moment with innovative solutions to tackle these challenges are the ones to watch.



Future trends in cybersecurity

Team8 is always tracking the next major trend or technology leap in cybersecurity — and enterprise technology more broadly. From quantum computing to deep fakes, self-healing machines, security for AI, and semantic security, we aim to monitor how these trends will evolve. Our goal is to help identify which trends have real world implications, and which companies are taking active, commercial steps to address them. While these themes are still emerging, we expect them to heavily influence the companies of tomorrow.

Contributors

Co-Authors

Aaron Dubin
Director of Business Research, Team8

Ben Borodach
VP Strategy & Operations, Team8

Contributors

Nadav Zafrir
Managing Partner, Team8 Platform

Admiral (Ret.) Michael Rogers
Operating Partner, Team8

Amir Zilberstein
Managing Partner, Team8 Enterprise

Assaf Mischari
Managing Partner, CTO, Team8

Charles Blauner
Operating Partner & CISO in Residence, Team8

Bob Blakley
Operating Partner, Team8

Liran Grinberg
Managing Partner, Team8 Capital

Tom Sela
Director of Research, Team8

Stephen Garcia
VP of Cybersecurity, FanDuel

Jonathan Jaffe
CISO, Lemonade

Jim J. LaBonty
Head of Global Automation Engineering, Pfizer, Inc.

Paul Branley
Director, Strategy, Innovation & Testing Lloyds Banking Group

Justin Berman
Former Head of Security, Dropbox

Professor Shafi Goldwasser
Director of the Simons Institute for the Theory of Computing, UC Berkeley

Simon Hodgkinson
CISO

Prashant V Jethwa
CISO, Cyber Defence Alliance (CDA)

Contact: info@team8.vc

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. Mukherjee, A., Rojas, B., & Ujhazy, H. (2020). Business Models for the Long-Term Storage of Internet of Things Use Case Data. International Data Corporation (IDC). https://www.idc.com/getdoc.jsp?containerId=prAP46737220

2. Caglar, D., Faccio, E., Couto, V., & Sethi, B. (2021). PwC's US Remote Work Survey. PwC. https://www.pwc.com/us/remotework?WT.mc_id=CT3-PL300-DM1-TR1-LS2-ND30-PR2-CN_FFGFY21-remotework&gclid=Cj0KCQiA6Or_BRC_ARIsAPzuer_gm2fNjf4Akh9BKVNyX0Vb_zhv3pmGEGwKZZp6t79BO562DNY6YfwaAoTgEALw_wcB

3. Waitman, R. (2020). Cisco 2020 Consumer Privacy Survey. Cisco. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cybersecurity-series-2020-cps.pdf

4. The State of Privacy and Personal Data Protection, 2020-2022. (2020). Gartner, Inc. https://www.gartner.com/en/newsroom/press-releases/2020-09-14-gartner-says-by-2023--65--of-the-world-s-population-w#:~:text=September%2014%2D17-,By%202023%2C%2065%25%20of%20the%20world's%20population%20will%20have%20its,%2C%20according%20to%20Gartner%2C%20Inc.&text=Gartner%20analysts%20presented%20these%20findings,Americas%20and%20EMEA%20through%20Thursday

5. Bitdefender Mid-Year Threat Landscape Report 2020. (2020). Bitdefender. https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf

6. Coalition H1 2020 Cyber Insurance Claims Report. (2020). Coalition. https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2020-09-Coalition-Cyber-Insurance-Claims-Report-2020.pdf

7. Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. (2020). Department of the Treasury. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

8. Carielli, S., DeMartine, A., Bongarzone, M., Dostie, P. (2020). The State of Application Security. Forrester. https://www.forrester.com/report/The+State+Of+Application+Security+2020/-/E-RES159057

9. Forsgren, N., Smith, D., Humble, J., Frazelle, J. (2019). Accelerate: State of DevOps 2019. DORA & Google Cloud. https://services.google.com/fh/files/misc/state-of-devops-2019.pdf

10. Chiodi, Matt. (2019). 99 Security Products and You Still Got Breached? RSA Conference 2019, San Francisco. https://biztechmagazine.com/article/2019/03/rsa-2019-most-organizations-use-too-many-cybersecurity-tools

11. Crumpler, W. Lewis, J. A. (2019). The Cybersecurity Workforce Gap. Center for Strategic & International Studies. https://www.csis.org/analysis/cybersecurity-workforce-gap

Team8 Disclosure

This Team8 Cybersecurity Brief 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 Brief 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 Brief 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 Brief. Certain of the securities referenced in this Team8 Cybersecurity Brief 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 Brief 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 Brief.