451 Research® | PATHFINDER REPORT

Essential Building Blocks for the Next Era in Cybersecurity

COMMISSIONED BY

CyberProof®
A UST Global Company

MARCH 2020

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

ABOUT THE AUTHOR

AARON SHERRILL

SENIOR ANALYST,
INFORMATION SECURITY

Aaron Sherrill is a Senior Analyst for 451 Research covering emerging trends, innovation and disruption in the Information Security channel with an emphasis on service providers.

Aaron has 20+ years of experience across several industries including serving in IT management for the Federal Bureau of Investigation. He holds degrees in business and computer science, and has an MBA along with multiple certifications, including the Certified Information Systems Security Professional (CISSP) credential.

Executive Summary

Over the past decade, we have witnessed remarkable advancements in technology, tremendous changes in how enterprises consume and apply technology, and an overall paradigm shift in computing. Even so, the next decade will be accentuated by even greater disruptive technological advances, innovations and breakthroughs that will bring about transformative shifts in how societies and markets function.

While these transformational changes hold great potential, they will also give rise to new security threats and risks at an unprecedented rate. This evolving and increasingly complex threat landscape requires that security teams shed traditional security practices and become agile, scalable and resilient and build a foundation that can adapt to future demands.

The next era of transformation (and inevitable cybercrime) requires organizations to build robust automation and orchestration capabilities to enable security teams to work smarter and respond faster. To battle the adversaries of tomorrow, security teams must equip themselves with threat intelligence and analytics capabilities while building internal and external collaborative knowledge-sharing systems. And while preventative controls will remain a vital aspect of securing the enterprise over the next decade, organizations must shift their attention to detection and response to minimize the impact and scope of compromise through rapid identification and remediation of active threats.

Key Data Points

- Nearly all (97%) enterprises reported they are either underway with or expecting digital transformation progress in the next 24 months, and over half of enterprises reported that 30% or more of their IT budgets are now allocated to projects that grow and transform the business.
- A hybrid IT environment that leverages both on-premises systems and off-premises cloud and hosted resources is the formal IT strategy for more than 71% of enterprises.
- The speed of enterprise transformation and modernization is often outpacing the ability of the organization's security teams to adapt.
- Security teams are reaching a breaking point when it comes to the overabundance of tools they have deployed to protect their organizations.
- More than 87% of enterprises reported they are increasing security budgets by an average of 22%.
- Automation and orchestration are essential for security teams to scale and concentrate on productive problem-solving activities.
- Threat intelligence and analytics has an enormous impact on the effectiveness of investigative and intelligence processes.
- Collaboration is a crucial, yet often overlooked, part of cybersecurity.
- Because compromise is inevitable, robust detection and response capabilities are essential.

The Evolving State of Enterprise Cybersecurity

Enterprise Trends and Demands

The infrastructure and technology strategies of the past decade are quickly fading away as new norms take hold. As enterprises speed down the road of digital modernization and transformation, they are launching sweeping changes in pursuit of new business models, new revenue streams, and the ability to meet maturing customer expectations regarding products and services.

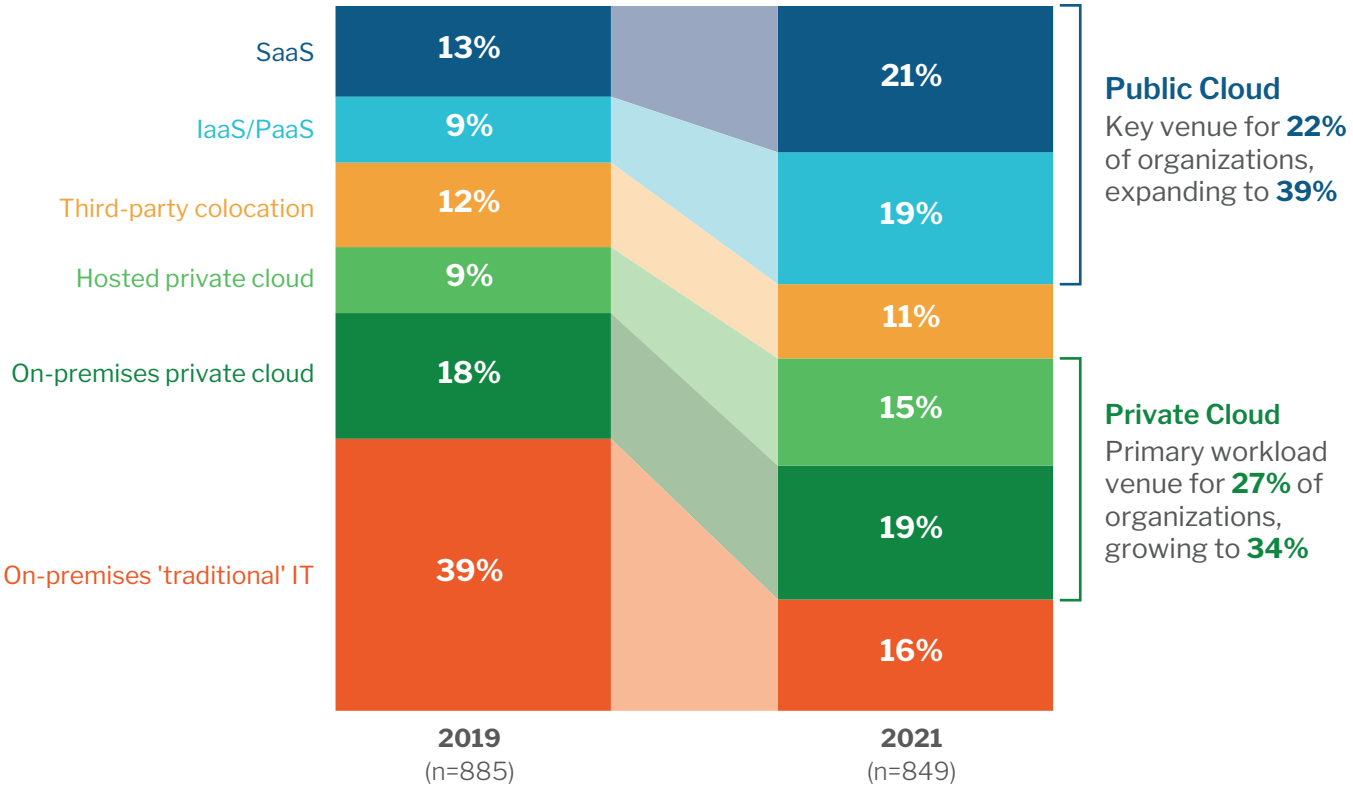
Technology giants like Google, Facebook and Amazon are delivering increasingly rich experiences that customers now expect from organizations in every industry. Fearful of being surpassed by competitors and losing customers, enterprises are radically rethinking how they leverage technology, people and processes to accelerate innovation and transform their business.

According to 451 Research's Voice of the Enterprise: Digital Pulse, Workloads & Key Projects 2019 survey, 97% of enterprises reported they are either underway with or expecting digital transformation progress in the next 24 months, meaning virtually all organizations in the survey are on their journey to digital transformation. Over half of enterprises reported that 30% or more of their IT budget is now allocated to projects that grow and transform the business. While the cloud is playing an increasingly significant role in transformation and modernization initiatives, a hybrid IT environment that leverages both on-premises systems and off-premises cloud and hosted resources is the formal IT strategy for over 71% of enterprises. This strategy is resulting in a significant shift of workloads to both public and private cloud environments (Figure 1).

Figure 1: Workloads shift from on-premises to cloud

Source: 451 Research's Voice of the Enterprise: Digital Pulse, Workloads & Key Projects 2019

Q: Which of the following best describes the primary environment used to operate your organization's [workload] today? Two years from now?



Although the cloud plays a significant role in most enterprise transformation and modernization initiatives, organizations are also considering other new and emerging technologies to gain a competitive edge and augment their services and capabilities. Enterprises believe technologies like artificial intelligence (AI) and machine learning (ML), sensor-based technologies, virtual assistants (e.g., AI-driven bots), robotics, biometrics, connected devices (IoT), 5G and immersive media will have a significant transformational impact on business operations and enable a variety of new competitive advantages.

Organizations are not just considering these emerging technologies as stand-alone tools; instead, they are seeking to gain exponential value, provide business impact and disrupt markets through the convergence of these and other technologies. The rapid rate of technology adoption is pushing enterprises to retool their IT ecosystems to provide the dynamic agility necessary to integrate these new technologies into business processes.

The current rate of change in the enterprise seems blistering. Unfortunately, it is likely at the slowest pace we will experience from here on out. While these vast changes promise great potential benefits and value, they are also resulting in a cascade of problems in the enterprise. The speed of enterprise transformation and modernization is often outpacing the ability of the organization's employees to adapt, leaving many initiatives slow to realize their full potential, or worse, fail altogether.

Enterprises are also finding that the seismic changes that accompany these new technologies are increasing complexity and exposing the organization to new risks. Implementing and integrating new technologies is rarely as simple as vendors may make it seem. Many organizations are adding new and emerging technologies to existing and legacy technology stacks as they systematically replace or rebuild systems for a modern, dynamic and agile digital world.

Not surprisingly, transformation and modernization initiatives are contributing to a significant rise in security issues and risks. The expanding, diverse and hybrid enterprise IT ecosystem coupled with the rapid adoption of new technologies and an increasingly mobile workforce is exponentially increasing the demands and workloads of already strained security teams that are struggling to keep pace with evolving and sophisticated threats, a growing attack surface and increasing compliance requirements.

Cybersecurity Challenges – Old and New

While enterprise security teams face a plethora of new and unforeseen challenges, most are also contending with the same challenges that have been plaguing cybersecurity efforts for the past decade. Expertise is at the top of this list of challenges. Building a security team is a significant investment that typically accounts for over a third of security budgets, according to 451 Research's Voice of the Enterprise (VotE): Information Security, Budgets and Outlook 2019 survey. Organizations are finding that recruiting and retaining security expertise can be one of the most challenging aspects of their cybersecurity programs, hampering their efforts to protect the enterprise.

The expertise shortage has been well-publicized over the past decade, but the problem may be worse than most organizations realize. According to 451's VotE: IT Security, Organizational Dynamics 2019 survey, over 61% of midsize and large enterprises believe their security staffing level is inadequate to handle the cybersecurity challenges their organizations are facing today. Organizations are finding it difficult to close the gap in security personnel, with over 89% of respondents reporting having difficulty in recruiting and hiring security professionals.

To combat the expertise shortage and recruiting challenges, 45% of organizations plan to train existing staff to learn new skills. However, organizations are discovering that not only does it take time to build the talent needed, but skills development also takes away time from short-staffed security teams and critical day-to-day tasks. Unfortunately, while organizations continue to build expertise and seek additional talent, they are also losing talent at a similar rate to a competitive job marketplace.

The cybersecurity skills gap spans every aspect of security, but emerging skills such as cloud, IoT and application security, as well as experience with frameworks like NIST and MITRE's ATT&CK are in particularly short supply. However, the demand for cybersecurity skills extends beyond dedicated and specialized cybersecurity roles. Cybersecurity skills are in demand across the entire organization, including IT, development and other roles such as project and business management.

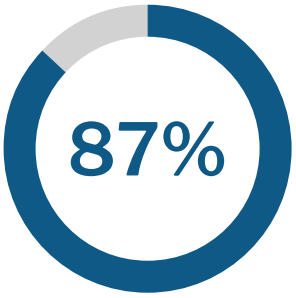
But it's not just the expertise and workforce shortages that are weighing down cybersecurity efforts. The very cybersecurity tools and technologies that organizations deploy to protect their critical assets often end up creating new challenges and placing additional burdens on security teams. Security teams are reaching a breaking point when it comes to the overabundance of tools they have deployed to protect their organizations. The shift to cloud-based and cloud-delivered security tools has made it easier for enterprises to deploy a wide range of security products and services. With good intentions, security teams have adopted a variety of tools to prevent, detect, mitigate, and respond to security incidents and breaches.

However, most enterprises are discovering that having an excess of security tools and one-off specialized products is creating unnecessary complexity, resulting in alert overload, a high rate of false positives, increased maintenance overhead and data silos. A lack of tool integration has hindered the security team's ability to protect the organization and quickly and effectively identify, understand and respond to threats. The problem is only becoming worse as enterprises continue to expand IT ecosystems across multiple diverse environments and rapidly adopt new, emerging technologies.

Security budgets have been one of the top pain points for security teams over the past several years. Security has traditionally been a line item in the overall IT budget, with security teams fighting for the same dollars that are funding digital transformation, infrastructure overhauls and cloud-migration initiatives. But now, more enterprises are giving security teams dedicated budgets, and over 87% of enterprises reported they are increasing security budgets by an average of 22% for this year.

Figure 2: Security budgets increasing

Source: 451 Research's Voice of the Enterprise: Information Security, Budgets & Outlook 2019



of enterprises report they are increasing security budgets over the next 12 months

Security budget increases tend to follow technology adoption fairly closely. Organizations that categorize themselves as early adopters are increasing their security spending at a significantly higher percentage than more conservative or characteristically late technology adopters. This dispels the notion that investment in modern IT architectures lowers the required amount of security investment. If anything, additional complexity is raising the rate at which security budgets are growing.

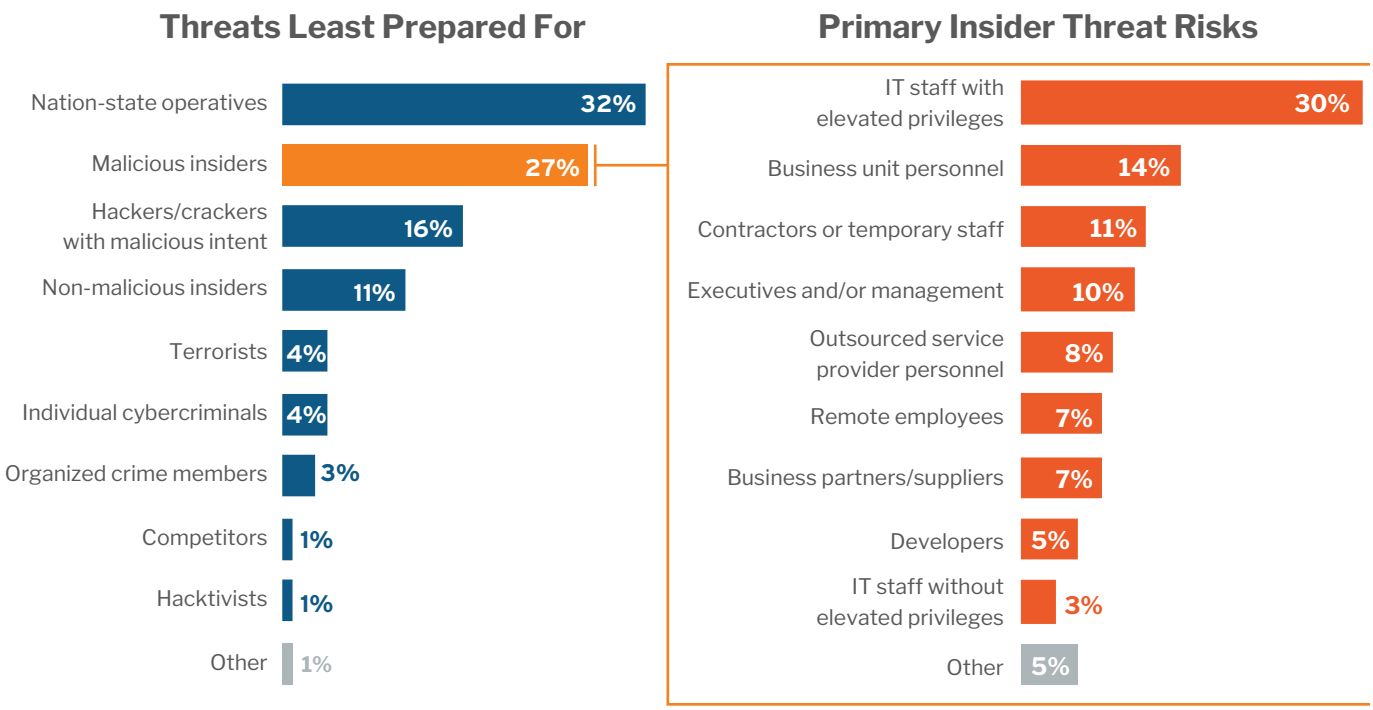
But for many, the increase in cybersecurity spending is not enough to overcome the complexity that comes with digital transformation, let alone secure emerging technologies, meet the demands from increased regulations, and stay ahead of evolving and increasingly sophisticated threats. Most organizations have made great strides in addressing many of the operational challenges that have hindered security efforts over the past decade. However, there are still significant gaps that will be exposed by the security challenges and threats of the near future.

The evolving threat landscape will continue to create new and unexpected challenges for enterprise security teams. Year after year we have seen a proliferation of new threats that seem to have greater impact and wreak greater havoc than their predecessors. We expect that trend to continue over the next decade. Cyberattacks will grow in scale and volume as attackers weaponize AI/ML to exploit vulnerabilities in the enterprise's security posture. Expect nation-state actors, in tandem with organized criminals, to develop sophisticated and multi-vector malware as cyber warfare comes in full force to the private and civilian sector. But enterprises may find more dangerous threats closer to home.

Organizations reported they are ill-equipped to deal with insider threats, and while not all insider threats are intentional or malicious, all are dangerous. A recent 451 Research survey (Figure 3) found that while IT staff with elevated privileges pose the greatest insider threat for most organizations, enterprises reported that executives, remote employees, contractors and temporary staff also pose significant insider risk. But many organizations are overlooking another avenue of insider threats – third-party suppliers, partners and vendors.

Figure 3: Organizations unprepared for threats

Source: 451 Research's Voice of the Enterprise: Organizational Dynamics 2019
Q: Which one of the following sources is your organization least prepared to deal with as a data security threat?
Q: Which of the following insiders do you think pose the greatest data security threat to your organization?



Enterprises are sharing data with an increasingly complex network of third parties, and these relationships are extending the organization's attack surface in ways that are difficult to secure and protect. The inherent trust that these partnerships are built upon make threats like business email compromise and account takeovers increasingly effective for attackers. Each vendor poses a potential weak spot for cyber defenses that even the most security-mature organizations struggle to keep in check.

As we move into the next era, security teams are recognizing they cannot continue to use yesterday's security strategies, processes and technologies to fight tomorrow's security battles. Regardless of the security technologies that will be used over the next decade, there are core, fundamental building blocks that organizations can put into place today to position their security teams to successfully secure and protect the organization from the next era of threats and challenges.

Building Blocks for the Next Era

Automation and Orchestration

Historically, security teams have been hesitant to leverage automation and orchestration to its full potential. Without proper tools, strategic planning and risk management, early endeavors into security automation were often riddled with missteps and service outages. As organizations automated complex processes, they often attempted to mimic poorly constructed manual processes, resulting in volatile automation efforts that were unable to handle unexpected situations. As a result, most security automation efforts have focused on small, isolated, low-risk tasks that only provide a minimal return.

But the challenges of the next decade demand robust automation and orchestration capabilities as security teams look to work smarter and respond faster. The increasing volume and sophistication of threats, the vast amount of data and assets spread across the diverse enterprise IT ecosystem, the exponential complexity of enterprise environments, the ongoing shortage of cybersecurity talent, and the growing number of privacy and security regulations are proving to be too much for overwhelmed security teams to manage through manual processes.

Automation and orchestration are essential for security teams to scale and concentrate on productive problem-solving activities, including tackling critical and complex security challenges like digital transformation and emerging technologies, rather than spending countless hours engaging in mundane, repeatable tasks. Automating security processes can improve security operations, enable more efficient use of security staff, enable teams to investigate more (if not all) alerts, improve the effectiveness and efficiency of detection and response activities, and enable better decision-making.

However, while automation and orchestration hold great potential, most organizations have found that implementing it beyond basic, rudimentary tasks is difficult. Many security teams have found that their lack of automation is preventing them from securing their entire security stack and improving their organization's security posture.

More than ever before, cybersecurity products are designed to automate specific processes within a particular tool's purview. While this type of automation provides some benefits, it often fails to integrate and orchestrate across the dozens of point security products that enterprises have in place. To solve these challenges, many enterprises are turning to security orchestration, automation and response (SOAR) and robotic process automation products. These purpose-built platforms are designed to dramatically reduce the time to detect incidents and accelerate the speed in which teams can respond. While these tools often provide robust APIs for custom integration, most enterprise security teams are finding they can integrate across their entire security stack with minimal or no coding expertise.

Although successfully implementing and operationalizing automation across the entire security stack is rarely quick and easy – requiring a significant investment in both time and resources to deploy and operate – SOAR platforms are crucial for security teams to remain effective in the next era of threats and attacks. Many organizations are finding that leveraging security service providers can not only expedite the adoption of automation but also enable in-house security teams to gain greater scale and efficiency.

Targeted Threat Intelligence and Analytics

To stay ahead, or even on pace, with determined and sophisticated attackers over the next decade, enterprise security teams must also incorporate threat intelligence and analytics capabilities into their security operations. Leveraging threat intelligence to make informed decisions is not a new concept. It has been used for decades in almost every industry to improve decision-making, better utilize resources and proactively identify issues. At first glance, threat intelligence and analytics may not seem like the disruptive or modern cybersecurity advancement enterprises are looking for to secure and protect their organizations in the coming decade. However, security teams are finding it can make an enormous impact on investigative and intelligence processes.

Historically, security teams have monotonously and iteratively gathered and searched through increasingly large volumes of threat data in hopes of distinguishing real threats from false positives. This time-consuming and overwhelming process has proven to be ineffective at rapidly identifying threats. Essentially, detecting threats in this manner is like looking for the proverbial needle in the haystack.

Threat intelligence provides security teams with continuously updated and insightful information about existing and emerging threats that may target their organization. Not only can threat intelligence help improve and accelerate threat detection, prioritization and incident response activities, but it can also enable security teams to proactively prepare for and even prevent attacks. Unfortunately, organizations tend to underutilize the threat intelligence they have available, focusing their efforts on basic use cases. By providing information about threat actors, indicators of compromise, attack patterns, tools, attacker motivations and capabilities, signatures, and common vulnerabilities and exposures, threat intelligence can help security teams better understand the tactics, techniques and procedures that adversaries leverage.

Most organizations find that while threat intelligence and analytics can be invaluable for security operations, the development and execution of an effective threat intelligence program can be difficult and expensive. Consuming, processing, enriching, analyzing and integrating multiple intelligence feeds spanning tactical, operational, strategic and technical intelligence often requires a dedicated effort to gain actionable insights that security teams can harness.

Organizations just getting started with threat intelligence, or struggling to maintain their threat intelligence program, should considering leveraging a managed threat intelligence platform. Often delivered as a security service, threat intelligence platforms streamline and automate the process of threat intelligence and analysis while facilitating the management and minimizing the overhead and requirements of a threat intelligence program.

Collaboration

Organizations that have effective cybersecurity programs are rarely differentiated by the security technologies they have in place but, rather, by the level of collaboration they have internally among all teams and stakeholders and externally with the greater community, both within their industry and the larger cybersecurity collective. Cybersecurity programs constructed for the next decade of challenges cannot be built on an island or in a vacuum. It is only when teams, organizations and industries collaborate and share knowledge can cybersecurity efforts be truly effective.

Collaboration is such a crucial, yet often overlooked, part of cybersecurity that the US federal government passed the Cybersecurity Act of 2015. The act encourages private organizations to collectively share threat intelligence, mitigation strategies, and incident response and handling tactics. Without collaboration, organizations risk limited situational awareness due to the biases of siloed teams and the narrow, individualized viewpoints found throughout the enterprise. Without robust collaboration, the risk of data loss and disruption increases as security events are prolonged and damages exacerbated due to confusion, a lack of communication and a lack of preparedness. Establishing strong cross-functional collaboration efforts and partnerships, both internally and externally, will greatly improve the organization's ability to tackle the adversaries of tomorrow.

Enhanced Threat Detection and Faster Response

A data breach is often a costly event both financially and through damage to the organization's brand and reputation. But failing to respond to security incidents with speed and efficiency can result in a situation that is often worse than the breach itself. There is a strong correlation between an organization's incident response preparedness and ability to execute and how well it will recover from an incident. Unfortunately, many organizations are ill-equipped or completely unprepared to handle security incidents quickly and effectively.

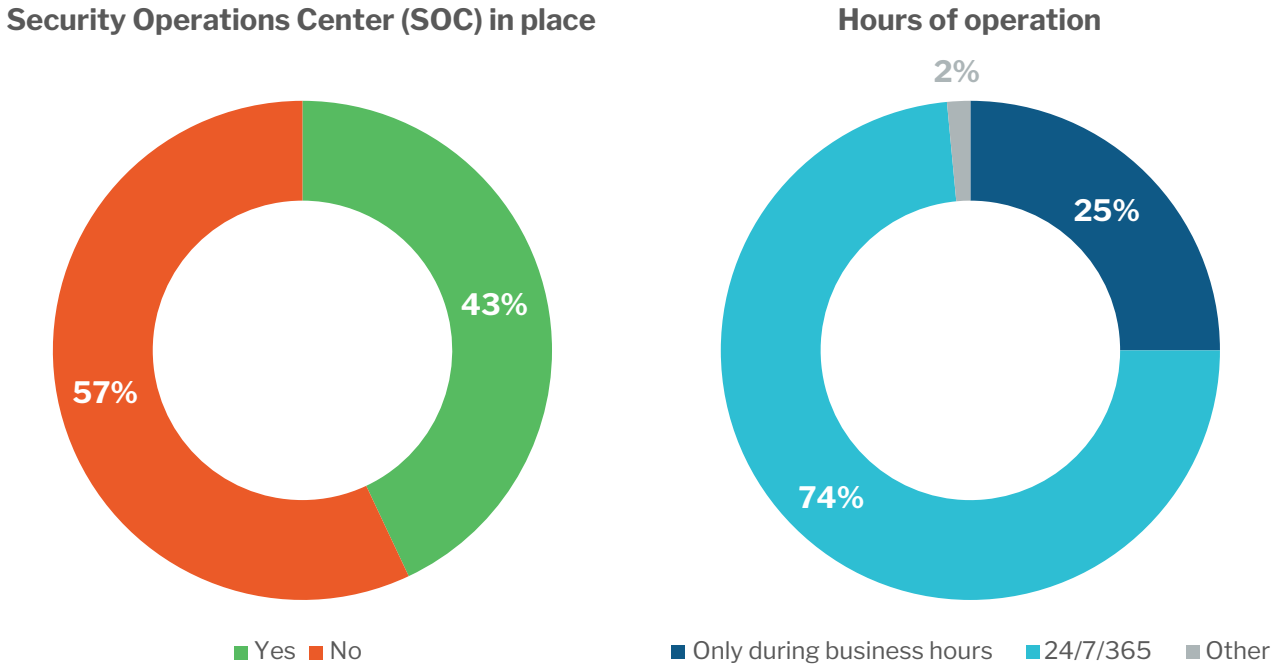
Organizations are starting to accept that not all attacks can be prevented. Compromise is inevitable. While preventive controls such as firewalls, antivirus and content filtering are effective at stopping known 'commodity' threats, they often fail to successfully defend against new complex and sophisticated cyberattacks designed to evade preventative security technologies. Underscoring these sentiments, more than 50% of midsize and large organizations believe it is likely they will experience a data breach in the next 12 months, according to 451 Research survey data.

While preventative controls will remain a vital aspect of securing the enterprise over the next decade, organizations are beginning to shift their attention to detection and response. This modern security strategy combines automation, AI/ML, threat intelligence, analytics, collaboration and human expertise to deliver threat hunting, threat detection, investigation and incident response. Employing these capabilities across endpoints, networks, clouds, applications, data and users, security teams are seeking to minimalize the impact and scope of compromise through rapid identification and remediation of active threats. The increasing complexity of the enterprise's IT ecosystem and rapid adoption of new technologies multiplied by an onslaught of new, sophisticated threats is making detection and response a vital but increasingly difficult endeavor.

Many security teams are finding they are missing foundational capabilities to make the shift to a detection and response strategy. Only 43% of enterprises reported that they have a security operations center (SOC) in place, and of those, 25% are operating their SOC only during business hours. The lack of a SOC may be worse than the data indicates because some enterprises attempt to deliver SOC operations and activities from their network operations center.

Figure 4: Organizations unprepared for threats

Source: 451 Research's Voice of the Enterprise: Organizational Dynamics 2019
Q: Does your organization have a security operations center (SOC) in place?
Q: When is the SOC at your organization staffed?



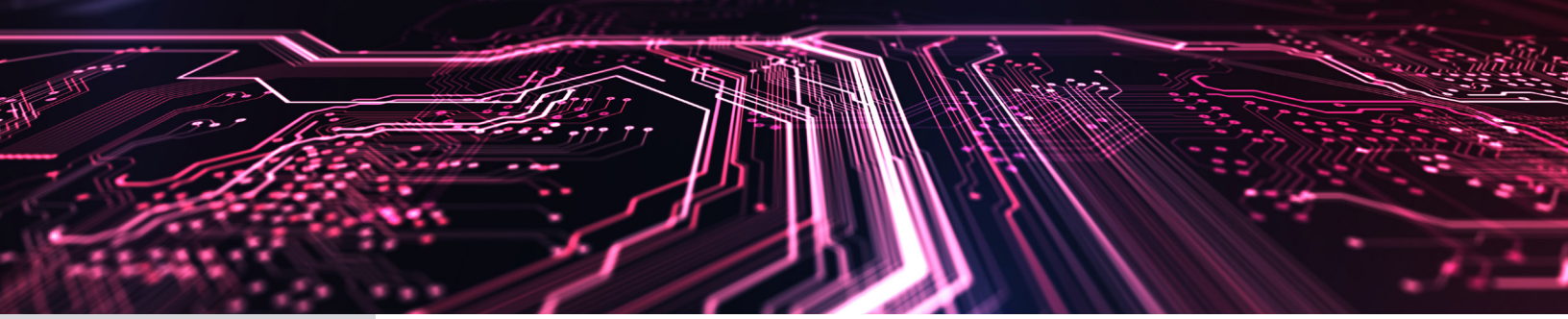
Managed detection and response (MDR) providers are filling the gap for many organizations. MDR providers deliver a range of capabilities to search for and detect vulnerabilities, indicators of compromise, suspicious behavior, and advanced threats across the entire IT ecosystem 24/7. Enterprises are finding that MDR providers deliver collaborative and personalized services tailored for their organization, enabling security teams to quickly deploy and leverage capabilities that would otherwise take months, if not years, to build and run on their own.

Conclusion

The last decade has been defined by the start of a digital transformation where every organization in every industry is becoming a technology company. And as technology continues to evolve at an increasingly rapid pace and the attack surface continues to grow in every direction, enterprise security teams are feeling the urgency to prepare for the next era of cybersecurity.

The evolution of cybersecurity will be marked by AI, ML and deep learning as security teams continue to adapt and shift their focus to resiliency and recovery. And while no one can accurately predict the challenges and risks that emerging technologies like 5G, quantum, IoT and AI will create, we do know there will be complexity, challenges and risks.

It is never too early or too late to start preparing for the rapidly evolving and diverse threat landscape of the next decade. By building a foundation of automation and orchestration, threat intelligence and analytics, collaboration, and detection and response, organizations can develop cybersecurity programs that can scale and flex against unknown future demands. Most organizations will find that security service providers can be a catalyst to reaching these goals and an invaluable partner in the never-ending evolution of cybersecurity.



CyberProof is a security services company that intelligently manages your incident detection and response. Our advanced cyber defense platform enables operational efficiency with complete transparency to dramatically reduce the cost and time needed to respond to security threats and minimize business impact. SeeMo, our virtual analyst, automates and accelerates cyber operations by learning and adapting from endless sources of data and responds to requests by providing context and actionable information. This allows our nation-state cyber experts and your team to prioritize the most urgent incidents and proactively identify and respond to potential threats.

We collaborate with our global clients, academia and the tech ecosystem to continuously advance the art of cyber defense.

CyberProof is part of the UST Global family. Some of the world's largest enterprises trust us to create and maintain secure digital ecosystems using our comprehensive cyber security platform and mitigation services.

For more information, see: *www.cyberproof.com*.

CONTENT PROVIDED BY:

CyberProof®
A UST Global Company

About 451 Research

451 Research is a leading information technology research and advisory company focusing on technology innovation and market disruption. More than 100 analysts and consultants provide essential insight to more than 1,000 client organizations globally through a combination of syndicated research and data, advisory and go-to-market services, and live events. Founded in 2000, 451 Research is a part of S&P Global Market Intelligence.

NEW YORK
55 Water Street
New York, NY 10041
+1 212 505 3030

SAN FRANCISCO
One California Street,
31st Floor
San Francisco, CA 94111
+1 212 505 3030

LONDON
20 Canada Square
Canary Wharf
London E14 5LH, UK
+44 (0) 203 929 5700

BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200

451 Research®