SINC

The Cybersecurity Landscape

Challenges & How to Overcome Them

Commissioned by:

Attivo
NETWORKS

Introduction

About the Author

Keri Pearlson
Executive Director of Cybersecurity at MIT Sloan

Keri Pearlson is the Executive Director of the research group Cybersecurity at MIT Sloan: The Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (IC).

Dr. Pearlson has held positions in academia and industry including Babson College, UTexas-Austin, Gartner's Research Board, CSC, Hughes Aircraft Company, and AT&T. She has been a consultant for many Fortune 500 companies and provided expert witness testimony on numerous information system issues. She founded KP Partners, a CIO advisory services firm and the IT Leaders Forum, a community of next-generation IT executives. Previously, she was the founding Director of the Analytics Leadership Consortium, at the International Institute of Analytics.

About the Report

United States of America

1,000+

$25 million/yr+

Legal, Retail, Education, Energy, Finance, Government, High-Tech, Healthcare, Entertainment

CISO, CIO, VP Information Technology, VP of Information Security, Director of Information Security

Table of Contents

The Current State of Cybersecurity

Companies must protect their own and their customers' most private and essential information from cybercriminals, and it's a 24/7 job that requires constant preparedness and instant response. With attacks coming from many different types of attack vectors across many different attack surfaces, cybersecurity is an ever-evolving priority for executives in all industries.

This study measured the state of cybersecurity today in the United States. Approximately 100 respondents from the Legal, Retail, Education, Energy, Finance, High-Tech, Healthcare, and Entertainment industries as well as the Government, were included in the study. We contacted companies with 1,000+ employees, with over $25 million in annual sales. The title levels of respondents included: CISO, CIO, Cybersecurity Director, Security Risk Officer/Manager, Directory of Security, and VP of Security.

This study focuses on these executives' highest priority concerns and asked questions about their priorities, how they evaluate their activities, and what tools and resources they plan to use to improve their security posture.

High-level takeaways from the survey include that security executives continue to be concerned about their preparedness to fight cybercrime efficiently and are actively seeking enhanced coverage for a wide variety of attack types and surfaces. Attacks that disrupt services or that use credential theft are top concerns as well as the need to protect new environments such as cloud architectures or critical access resources such as Active Directory. New investment priorities are cited for combatting ransomware and for improving cloud security. However, they also mentioned the ability to detect across attack surfaces as the top priority for the next year.

Overall, businesses appear to still struggle with reducing dwell time and with their efficiency in responding to incidents. There appears to be an ongoing reliance on traditional security controls for detection; however, notably, deception technology was listed within the top two to three security controls for detection across a variety of top attack types. The value cited for deception was within its ability to detect threats comprehensively and to respond faster and more accurately to incidents.

Although spending on detection technology still ranked relatively low, organizations seem to be adopting security frameworks to help understand their security gaps and areas where they need to improve coverage. One such model is the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework* that highlights five core areas: Identify, Protect, Detect, Respond, and Recover.

As cybersecurity leaders address ways to increase resilience in their organizations, they must consider all five areas of the NIST framework. In the next year, the highest priority for security gaps to address is the detection across attack surfaces and to be vigilant on many fronts.

* For more information on the NIST Cybersecurity Framework, please refer to the Department Of Commerce page:
https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/nist-framework

Respondents Are Concerned About Being Prepared to Effectively Fight Cybercrime

In this ever-vigilant, constant state of hyper-awareness, there is cause for concern and focus on the preparedness to fight cybercrime. In this business environment of significant change and unknown, more than half of the respondents felt they could equip themselves better to fight cybercrime.

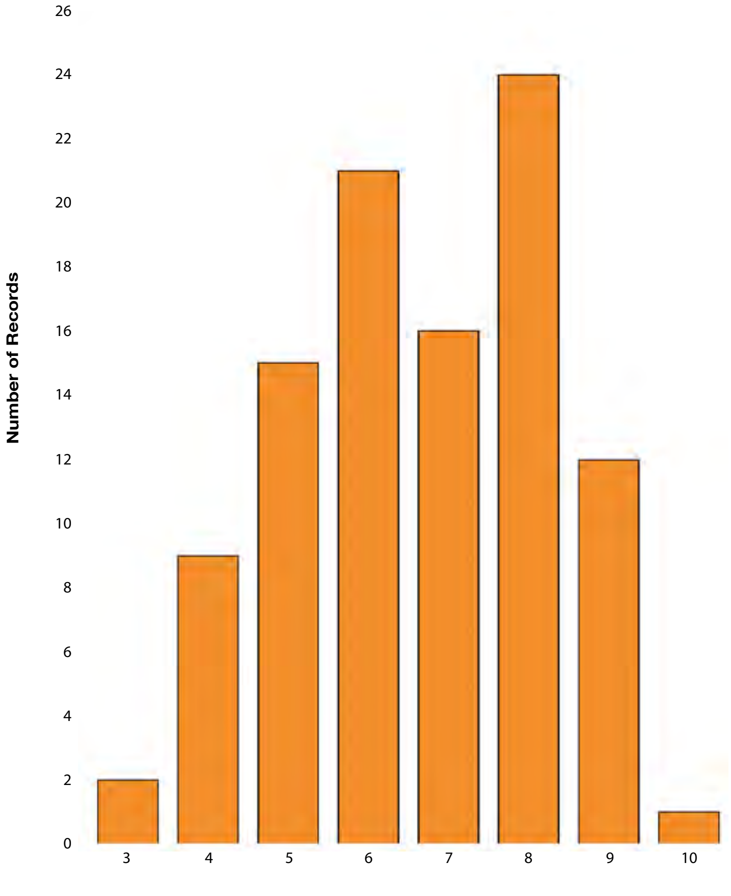
We asked respondents to rate themselves on a scale of 1 (Poor) to 10 (Excellent) on how well equipped they felt they are to fight cybercrime effectively. The results were somewhat surprising. As seen in the diagram (Figure 1), the responses formed a traditional bell-shaped curve trending towards the higher end of the scale. No one rated themselves poorly equipped (no one reported less than a 3). At the same time, more than 50% rated themselves a 7 or higher. Our conclusion from this data is that while people feel that they are well-prepared and well-positioned to fight cybercrime, the ongoing number of breaches and the increasing number of stolen records don't necessarily back this up. Additionally, with the recent disruption of COVID-19, there are gaps in security controls for which the consequences are currently unknown.

For those who reported feeling less prepared to fight cybercrime, this may reflect uncertainty with the rapid change of the current environment. For many, feeling prepared means knowing about vulnerabilities and having safeguards in place to detect, prevent, and respond to a cyber attack. Those reporting that they are less prepared maybe acknowledging that they are uncertain as to what attacks they should be preparing for in the future. They have implemented tools to cover the threats and attack surfaces they know about but realize that there are always new attack vectors that they have not yet addressed.

Interpreting why so many respondents feel prepared (over 50% rated themselves a 7 or higher) is more complicated. After all, it is difficult to be confident that the company has coverage for all types of attacks across all the possible attack surfaces during a period of daily highly accelerated changes. Perhaps respondents at this end of the curve believe that they have things under control for the threats they worry most about, but that could change over time as this dynamic environment settles down into a new normal, and new threats emerge.

The bell-shaped curve is not surprising since companies are each responding from their current and most recent experiences. Using the NIST framework lexicon, leaders might believe they are very prepared in one area, such as response, but are less ready in another area such as detection. Being prepared today does not automatically mean the company is ready for tomorrow.

Figure 1. On a scale 1 - 10 how equipped are you to effectively fight cyber crime?



Disruption of Service Followed by Credential Theft Are Top Attacks of Concern

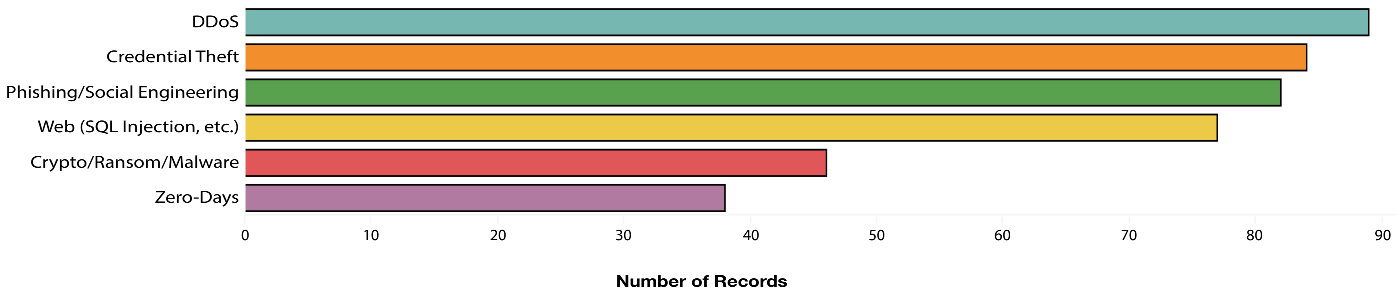
U.S. industries face multiple areas of concern, such as facing attacks on various levels for both customer data and company efficiency. As seen in the diagram below (Figure 2), companies listed Distributed Denial of Service (DDoS) as their top area of concern. They prioritized it as such because of the immediate ability to disrupt the business and keep services and operations from running. While DDoS is an external threat where attackers target network or site availability, organizations can address this by employing a DDoS-mitigation service that can absorb any potential DDoS traffic in another layer of the technology stack. For example, the attack can be prevented in the cloud before it reaches the network.

The next two top concerns, credential theft, and phishing/social engineering are user-level risks. When they occur, the attacker gains a foothold in the organization and often has access to credentials or systems necessary to hack. Security hygiene, user education, anti-phishing services, email filters, cybersecurity culture, and tools such as password managers can assist in mitigating these attacks.

The next concern, malware/ransomware/crypto-mining, was not as high on the priority list likely because they believe their Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) tools address these attacks. The challenge is that more sophisticated malware and new strains of code can slip past EPP and EDR since existing they are unknown to existing systems. Organizations can solve this by detecting abnormal traffic, or using deception technology to most quickly recognize an attack.

Reported as of least concern to organizations were zero-days threats. This finding is an interesting result, as it's well known that zero-day threats continue to be a significant challenge. Still, many believe that it's the tool of nation-state attacks, and it is such a low probability that their company would be a target. At the same time, these are very sophisticated attack vectors. CISOs often believe that absent a specific reason why they would be a target for a zero-day threat, it will not likely happen to them. The other types of attacks are much more common, in part because they still regularly succeed, and therefore higher priority.

Figure 2. Top Attacks of Concern



> "Cybersecurity has traditionally been a 'cat and mouse game' between security teams and attackers, with a cybercriminal's arsenal continually evolving. Defeating the modern cyber attacker requires expertise in thinking like an attacker and understanding how to create an active defense for an expanding threat landscape."
>
> – Tushar Kothari, CEO of Attivo Networks

Cloud Security and Active Directory are Top Priorities for Security Expansion

Virtually all respondents cite concern for security in the cloud, making it the #1 priority needing attention and increased cybersecurity investment. As organizations increase their use of the cloud for both systems and data, understanding how they maintain security is both problematic and unclear. Most organizations are wrestling with multi-cloud environments adding more confusion to their cloud security plans since every cloud platform has different security systems. Just having enough talent to manage security in a multi-cloud environment is a challenge.

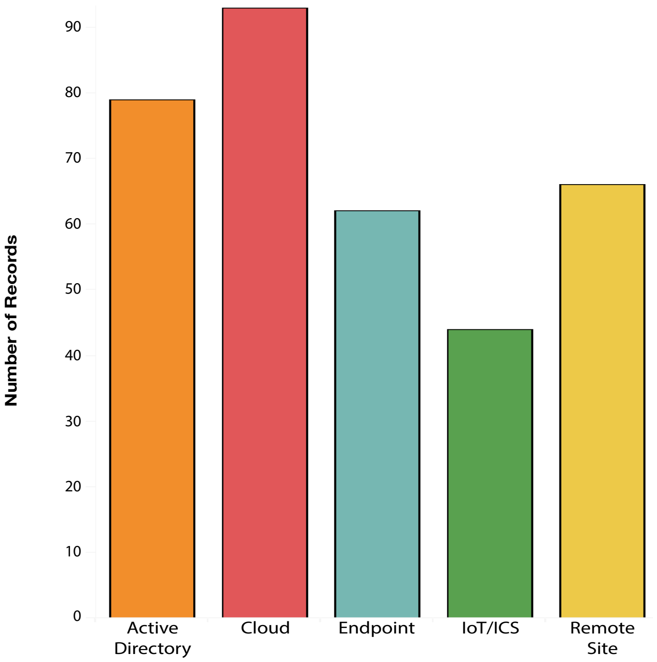
It is shown in the diagram below (Figure 3), almost 80% of respondents listed Active Directory security as a top priority. Active Directory is a primary target for attackers since it gives access to so much of the organization's systems. Adversaries can gain access to multiple levels of the organization, map relationships needed to carry out attacks, and elevate their access when they compromise Active Directory.

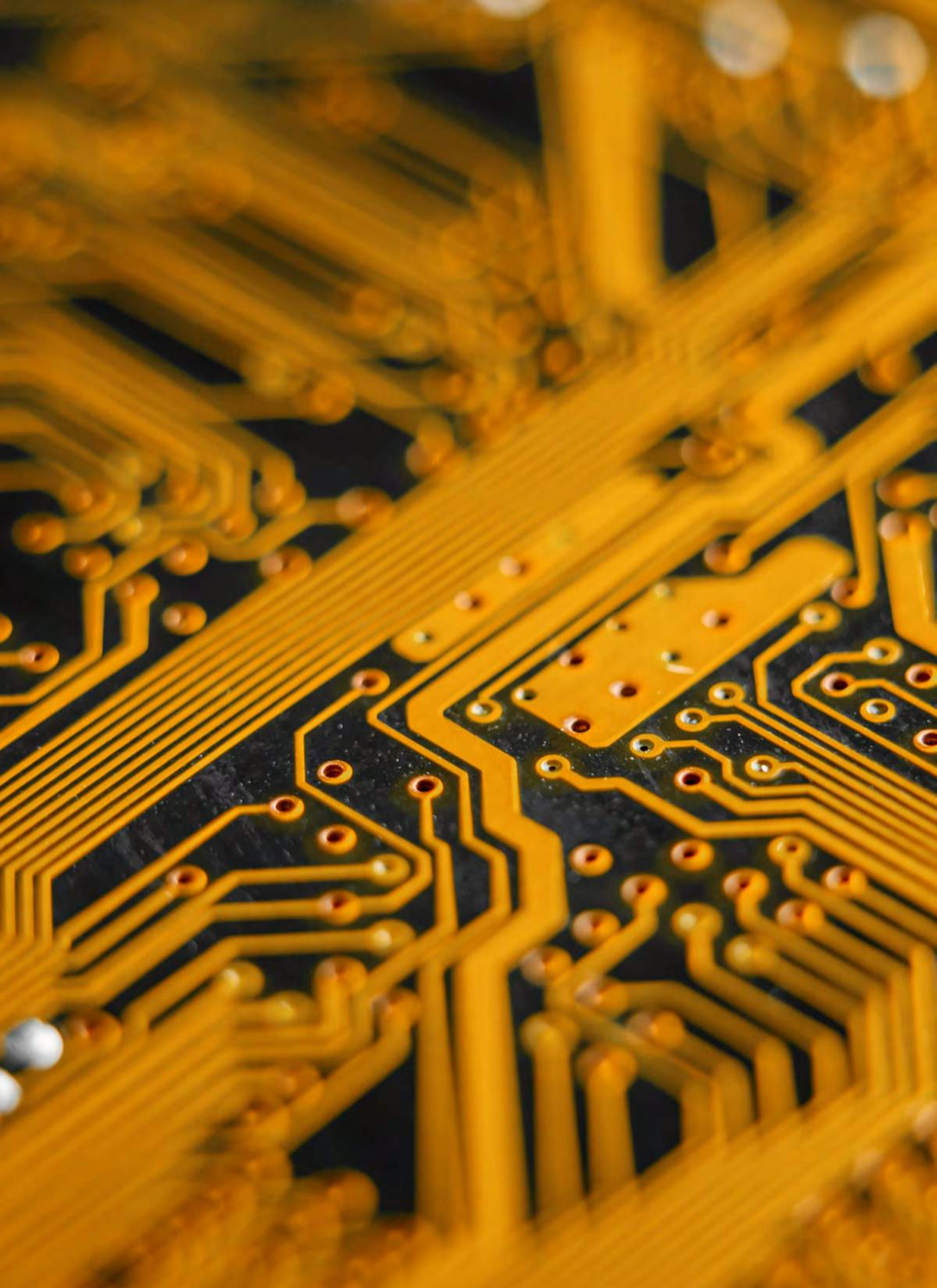
Endpoint and remote site security are also essential components in security expansion plans. As the number and variety of endpoints expand, the challenge of keeping each one secure grows. In today's environment, keeping security tight with almost every worker in an organization working remotely outside the firewall is a challenge. It's no surprise that remote worker security is a growing priority, considering the increasing number of remote workers, issues associated with VPN split-tunneling, and the fact that baselines and controls have become unreliable.

Internet of Things/Industrial Control System (IoT/ICS) devices are of concern, too, in part because they cannot typically run traditional antivirus software. These devices have much smaller processors, and standard endpoint security tools do not run on them. The customary manner of using log-monitoring of devices doesn't work here either, in part because these devices don't generate traditional logs. While respondents did not see this as a top priority for security expansion in this survey, organizations continue to see IoT and ICS as security challenges.

When looking at multiple attack surfaces and numerous attack vectors targeting these surfaces, organizations need ways to detect threats comprehensively and efficiently across the entire spectrum of their systems and devices.

Figure 3. Priorities for Security Expansion





Most Security Investments Are Driven by Disruption of Service Due to Ransomware

With so much to protect, executives are prioritizing their next security investments to help them fight disruption of service, ensure compliance, and secure cloud migration. Their most significant concern is disruption/ransom, as seen in the diagram (Figure 4), in part because business continuity and maintaining uptime are of utmost importance to keep operations running. Advanced ransomware attacks have had considerable impact and shut down businesses, as was seen in many recently well-publicized attacks. For example, NotPetya significantly disrupted transportation and many other industries not initially targeted by the cybercriminals who unleashed it. With the business disruption that ransomware could cause, it is not surprising executives prioritize security investments to minimize the effects on their organizations.

Compliance ranked second, reflecting an executive focus on meeting needs set up by governments, industry regulatory organizations, and supply chain partners. Meeting compliance and regulatory requirements came to the top of the list as the E.U. imposed GDPR, and U.S. states look to impose similar requirements. Companies found not in compliance can incur significant fines in addition to negative P.R. When assets utilize the cloud, compliance becomes even more of a priority. Where the processing takes place is often obscured by cloud services, yet regulations sometimes dictate rules around data flowing across borders and the location of the actual data processing.

Cloud mitigation was the third-ranked concern driving security investments. As described in earlier results, companies are increasingly moving critical assets to the cloud to take advantage of flexibility, efficiencies, and services. However, accompanying the benefits of cloud migration are increased concerns to ensure the security of assets placed in these new and complex environments. Security investments in this area could also represent business continuity priorities. Executives want to minimize service disruptions and address potential attack vectors for their cloud-based investments.

"Ransomware attacks can do a great deal of damage very quickly, making prevention, early detection, and the ability to slow an attacker's progress before it results in a disruption of service top priority. Organizations can immediately detect and slow an attack by giving the malware decoy targets to encrypt or corrupt. In ICS environments, this can make all the difference between interrupted operational processes and preserving business continuity while you execute your playbook."

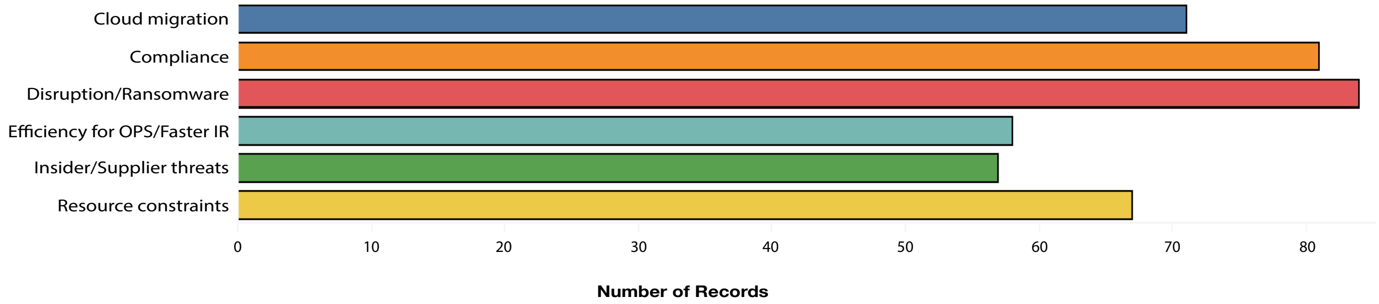
– Tony Cole, Chief Technology Officer at Attivo Networks

Attackers are targeting items of high value to secure ransomware payments. Ironically this was not the attack type of utmost concern as reported earlier in this report, but it is the area driving the highest investment. Respondents potentially assume that they can deploy new technologies to protect their organizations from this type of attack vector. Further, as they move critical data to the cloud, successful ransomware attacks could be highly disruptive if attackers gain access to cloud environments. Cloud-specific security measures, coupled with perimeter controls, can reduce vulnerabilities.

More than 50% of respondents ranked efficiency for operations as a driver of security investment. As the landscape of needs for security becomes clear, resource constraints kick in. It's impossible to be 100% secure, but executives are investing in tools and techniques that increase organizational efficiency and accelerate incident identification and response.

Another area driving investment for more than 50% of respondents is insider and third-party threats. Making sure supply chain partners are as secure as possible is increasingly vital to executives since their customers hold the company responsible for any breach, even if a supplier responsible for it. Executives are increasingly seeking solutions that help them understand and minimize vulnerabilities from insider and supplier threats.

Figure 4. Security Concerns Driving Investment



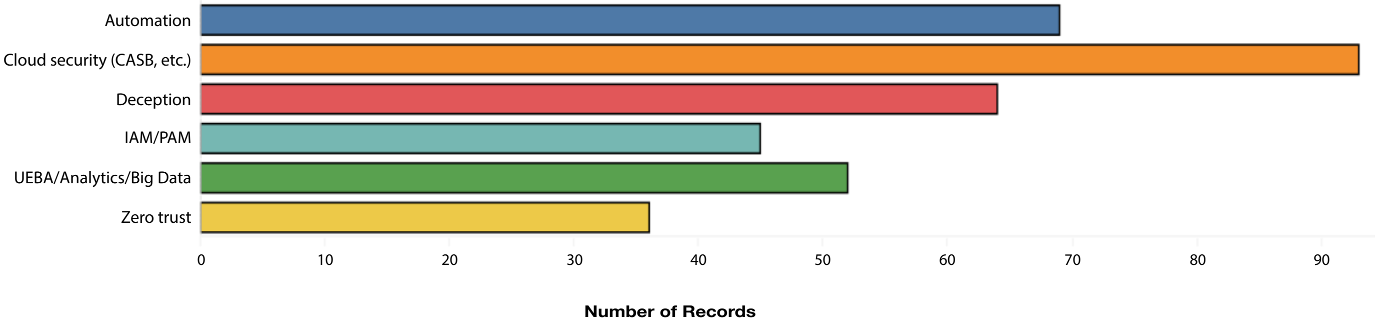
Technologies to Provide Cloud Security Top the List of Potential Future Spending

With security concerns on multiple fronts, companies are planning to invest in various new technologies. By far, first inline for spending is in Cloud Security, such as Cloud Access Security Brokers (CASB), shown in the diagram below (Figure 5), to protect investments in the cloud. Organizations consider CASB as the first cloud security control to implement, followed by Cloud Workload Protection Platform (CWPP) and Cloud Security Posture Management (CSPM). All assist in reducing the risk of cloud-based systems.

Next in priority are automation security technology and deception technology. Executives seeking efficiency improvements look to Security Orchestration Automation and Response (SOAR), but the fastest-growing segment of new technologies is deception technologies. This solution manages the detection process across multiple attack surfaces, address detection gaps, and quickly and accurately detect lateral movement. Deception technologies also increase efficiency in investigation and automation.

Only about 35% of the respondents considered zero-trust technologies, a surprising finding, given the extensive amount of publicity this concept has been receiving recently. Perhaps executives are ranking it lower in priority now as they investigate and learn more about its complexities, costs, and challenges in implementing it. Another possibility is that they have made what they consider enough investment in zero-trust technologies, and the next steps fall to policies and practices rather than in new technologies.

Figure 5. New Technologies Being Considered

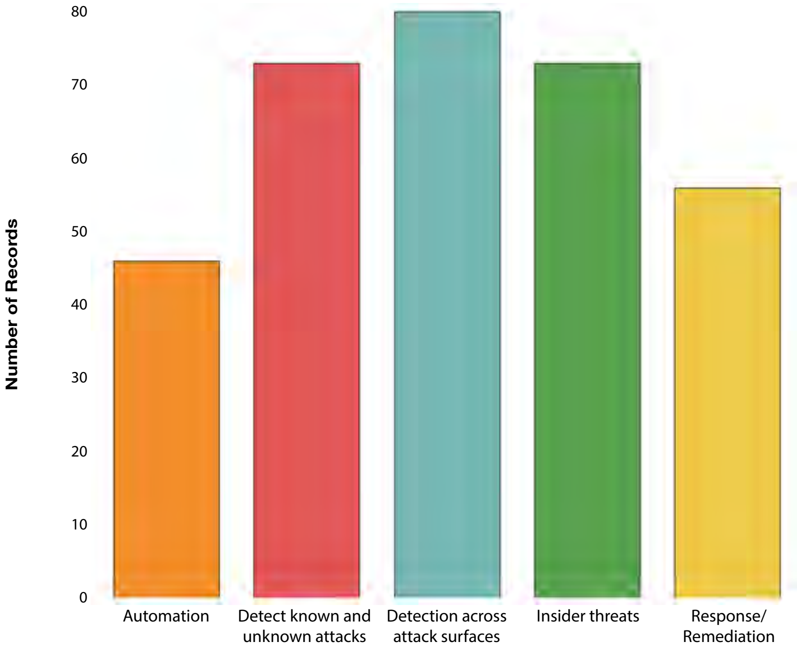


> "Data stored in the cloud is increasingly being targeted by both internal and external attackers. Securing cloud environments comes with its own set of very specific requirements, so security teams should look for solutions that can accurately and universally protect their data and infrastructure, regardless of the cloud environment they have chosen."
>
> – Carolyn Crandall, Chief Deception Officer and CMO at Attivo Networks

Detection Across Attack Surfaces is the Highest Priority to Address in the Next Year

When asked about priorities to address in the next 12 months, more than 70% of the respondents chose detecting unknown and known attacks, detection across attack surfaces, and insider threats, as shown in the diagram below (Figure 6). There is a theme emerging with these choices: universal coverage of all surfaces, attack vectors, and for both external and insider threats. Organizations are taking a broader look at their detection mechanisms across every part of their organization, not just the network and endpoints, as they must now address a greatly expanded attack surface. Detecting known and unknown threats speaks to the need for accurately detecting threats across this expanded attack surface, including all forms of lateral movements. Insider threats did not rank high in investments but ranked high in priorities to address in part due to the significant damage an insider could cause and a desire to make their security investments work for both internal and external threats.

Figure 6. Highest Priority Security Gaps



Top Detection Tools

As shown in the diagram on the next page (Figure 7), respondents reported that the top detection tools they use include EPP/EDR, Intrusion Detection/Prevention Systems (IDS/IPS), Deception tools, User and Entity Behavior Analytics (UEBA), and Security Information and Event Management (SIEM).

The tool of choice for the four most common threats facing organizations today are EPP/EDR. Since these are integrated solutions that combine many other types of security controls, it is not surprising that respondents selected them as the most common for detection. EPP/EDR tools detect and block threats, as well as include functions that hunt for, analyze, and respond to them. Since EPP/EDR often combine antivirus, antimalware, data encryption, firewalls, IDS, and data loss prevention (DLP) capabilities, they offer defense-in-depth in a single platform.

However, there could be an over-reliance on EPP/EDR and its capability to function as a security control technology. Security executives favor these tools and have heavily invested in them over the past 12 months. Some executives believe these tools solve a majority of cybersecurity problems, but that depends on how the organization implements them and which features or functions they configure. Attacks that rely heavily on credential-based exploitation or that circumvent controls may slip past EPP/EDR tools.

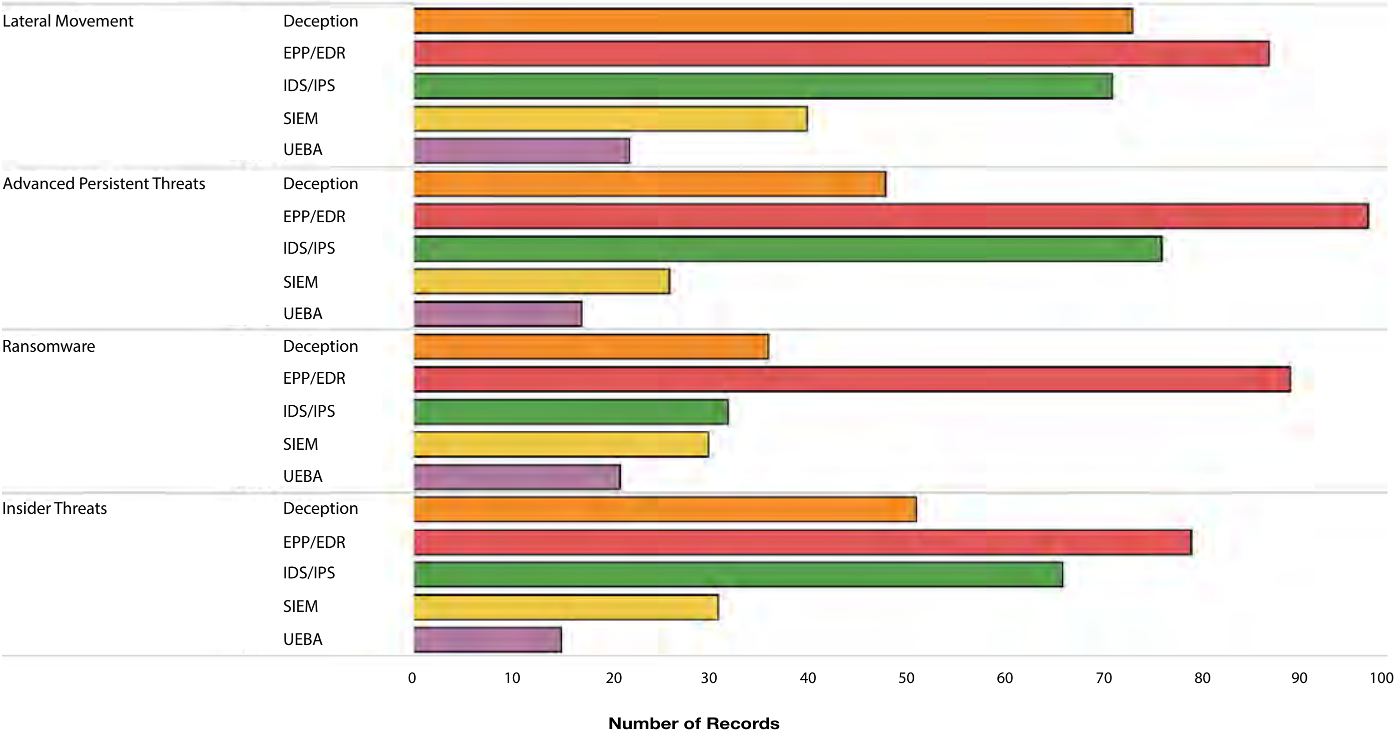
Likewise, IDS/IPS tools ranked high. Presumably, security executives have the most experience with these tools, which would account for their popularity across these threats. IDS/IPS form a baseline security control, which is the foundation for many security plans. These are useful for detecting known attacks, but newer attacks can bypass them since IDS/IPS relies on matching signatures. When a new attack appears, there is no signature to match. The rise in file-less malware attacks also pose a difficulty for IPS and IDS since there is no binary to match against a signature. Surprisingly, in the responses was the high rank of IDS/IPS tools for advanced persistent threats (APT). APTs are often more sophisticated attacks that seek information instead of financial gain. Newer APTs don’t usually have recorded signatures and, therefore, often bypass IDS/IPS.

> "Endpoints are the new battleground, and well-orchestrated detection and response capabilities are an organization's greatest weapon against attackers. By providing Active Directory query redirections and deceptive credentials and shares, organizations can feed attackers fake information and quickly redirect them away from production assets."
>
> - Srikant Vissamsetti, Senior Vice President of Engineering at Attivo Networks

Deception tools ranked in the top 2-3 positions for every threat. For an emerging security control, this is not surprising. These tools are complementary to EPP/EDR and IPS/IDS tools since they close detection gaps left by other security controls. Their flexibility makes them ideally suited for covering an expanded attack surface against multiple attack vectors such as insider threats, ransomware, and credential theft. We would expect to see the importance of these tools increase as they become more common since they provide more substantial and accurate alert signals for threats.

UEBA and SIEM tools ranked lower than the other tools. While these tools are useful for correlating data and finding missed incidents, they require significant intervention to keep them tuned and maintained for peak performance. False positives often result if organizations optimize these tools incorrectly. Large blind spots are another disadvantage to poorly tuned systems. A reliable baseline is necessary to set up these tools properly, and often, these require additional security resources that are unavailable or overcommitted. With the rise in the number of remote workers, network baselines have not adjusted to reflect the new user behavioral patterns, making them less effective at finding abnormal behavior.

Figure 7. Top Detection Tools



Protecting Active Directory is Most Frequently Done with Policy Management Tools

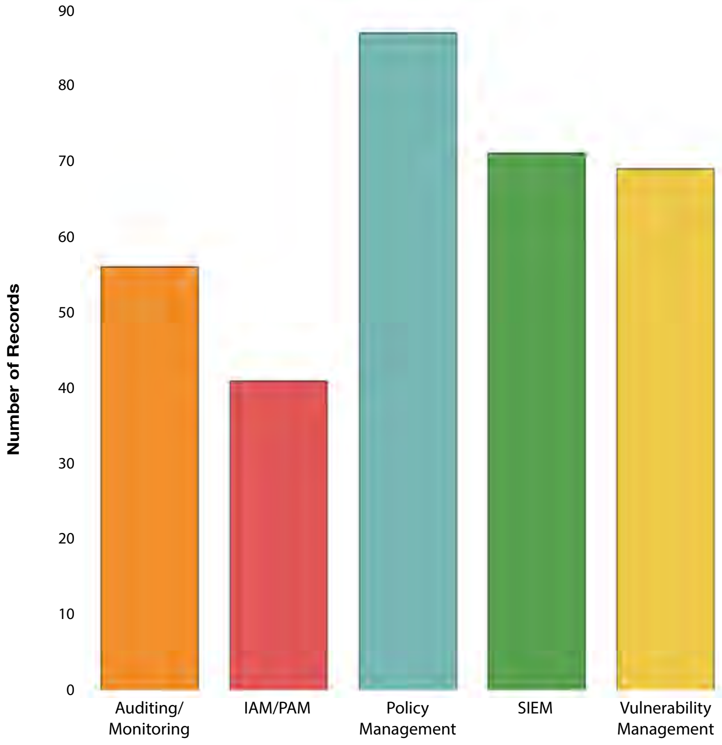
By far, respondents use Policy Management tools to protect Active Directory (AD). Next in line are Security Information and Event Management (SIEM) tools and Vulnerability Management tools. Fewer companies rely on Identity Access Management (IAM)/ Privileged Access Management (PAM) tools to protect Active Directory as shown in the diagram below (Figure 8).

Equally important, however, is that many organizations don't use actual AD security tools. They implement AD security by controlling access (as reflected in the high ranking of policy management, SIEM, and vulnerability management). These are in line with best practices today, but enabling auditing is quickly becoming a vital component of the AD protection plan since the SIEM system uses the data gained from audit logs to identify potential issues.

IAM/PAM ranked lower as security products of choice for AD. Perhaps this is because these tools are more difficult to set up and maintain properly.

Newer Active Directory protection technologies can hide AD objects and redirect attackers away from production objects. Organizations may consider these in future AD protection plans since they are often non-disruptive, and do not need to touch the production AD environment to work.

Figure 8. Security Products Used to Protect or Harden Active Directory



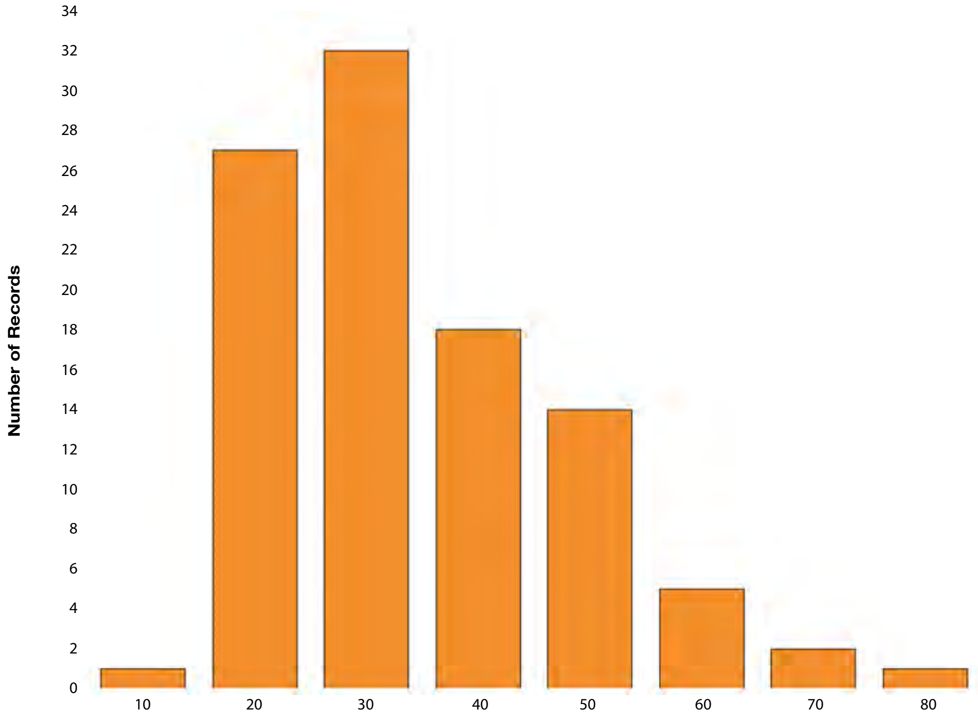
Security Budgets Show Priorities and Focus

Security budgets must cover all of the areas of the NIST framework: identification, protection, detection, responding, and recovery:

- **Identify** - Activities that record all assets of value that one must consider for cybersecurity such as equipment, software, data, and policies such as roles and responsibilities for all individuals with access to or management of valuable assets.
- **Protect** - Activities that control access, secure data and systems, patch vulnerabilities, and train everyone involved in keeping assets secure.
- **Detect** - Activities that monitor, investigate, and validate systems and users of the systems.
- **Respond** - Activities that prepare the organization should an incident occur, including notifying necessary individuals and organizations, keeping operations going, containing an attack, and reporting the incident to appropriate authorities.
- **Recover** - Activities that take place after an incident to get operations up and running or back to 'normal.' These include restoring equipment and other parts of the systems affected by the incident, informing employees and customers of new ways to operate, and putting additional layers of defense in place to reduce the change of a future occurrence.

When asked about the portion of the budget spent on detection solutions, the average was approximately 30%, as shown in the diagram below (Figure 9). From experience, 20% seems low for detection, and above 40% clearly demonstrates a priority focus on it. Companies spending only 10% on detection are taking unnecessary risks that they are catching threats in their systems. However, tools that incorporate detection may be the reason some executives reported 10-20%. If the tools they use for prevention and response include detection, separating the actual portion of the budget dedicated to detection controls would be lower.

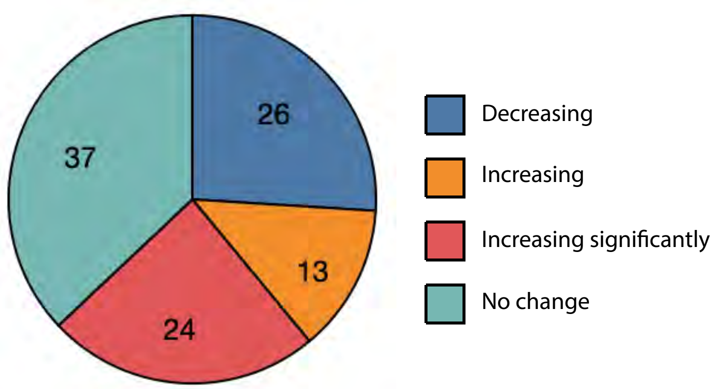
Figure 9. % of Security Budget Dedicated to Detection Solutions



Dwell Time Has Not Improved for the Majority of Companies

As seen in the diagram below (Figure 10), almost 75% of respondents believe that dwell time, the time between intrusion detection and eradication of a malware infection has either not changed or has increased. This finding is not good news. While it's encouraging that 37% reported dwell time has not changed, the goal must be to reduce it as much as possible. With average dwell time still measured in days, if not months, there is room for improvement in this area. Security experts say that anything above a few minutes is too long and increases the opportunity for malicious behavior.

Figure 10. Dwell Time



Triaging Incidents Has Room for Improvements

Rapidly examining an event to identify an incident and determining its priority, or triage, is taking place in minutes, rather than in days or hours in most companies. Shown in the diagram below (Figure 11), 66% of companies triage and identify malicious attacks in minutes compared to 33% who take hours. One organization reported that this process still takes days to complete.

Triaging an incident in hours means that attackers have plenty of time to move from one system to another (called breakout time) once they gain access. Studies have shown that breakout time for advanced attackers can be 20 minutes or less, and the average breakout time, according to Crowdstrike*, is 9 hours. Technologies that allow quicker triage must be part of the security program. This includes things like data analysis, data correlation, and forensic capture.

Figure 11. Triage Time

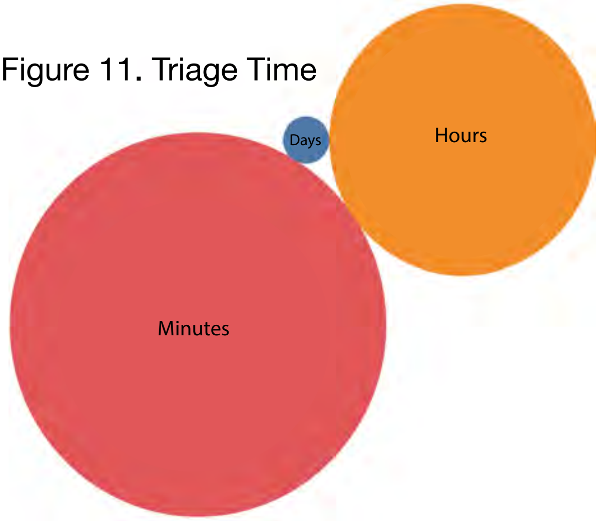


Figure 12. How many incidents did you experience last year?

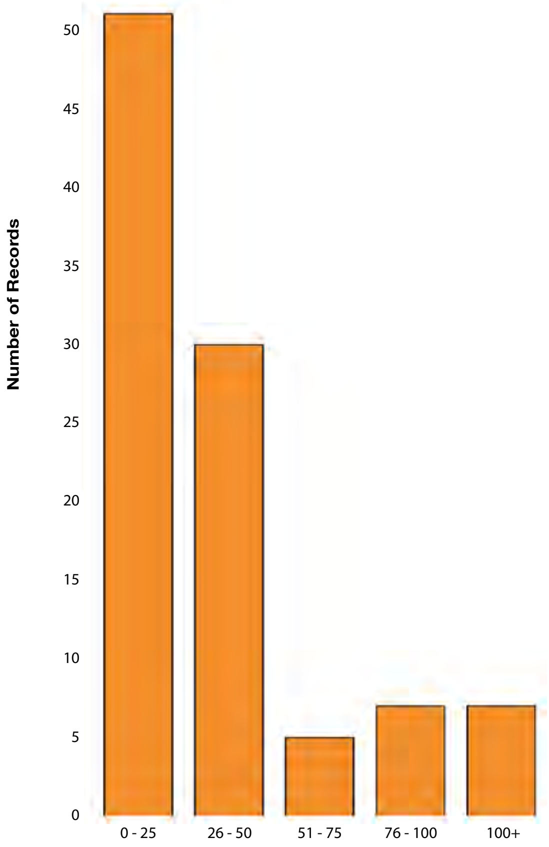
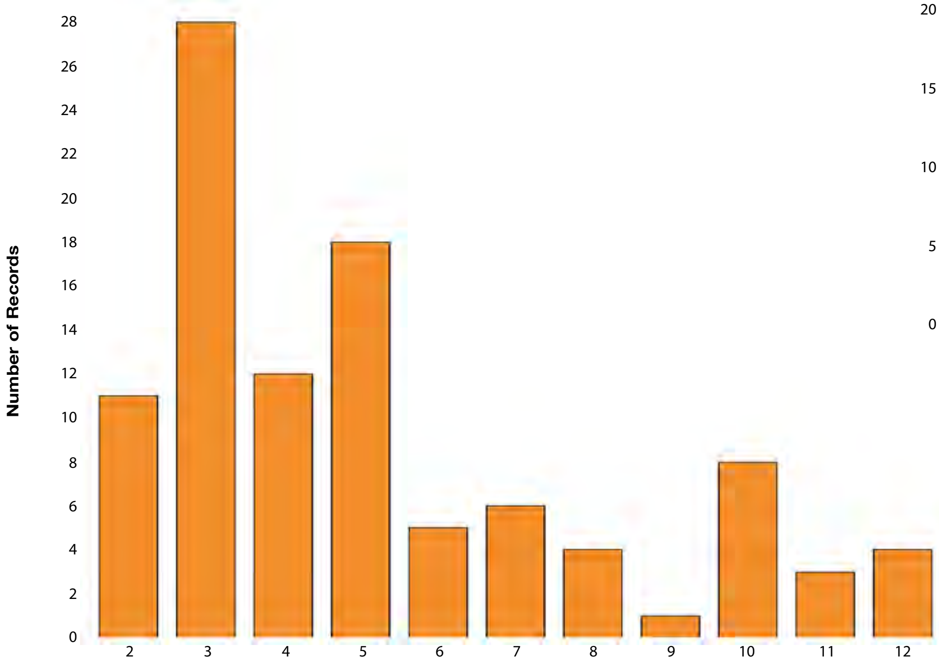


Figure 13. How many people on average are required to respond to an incident?

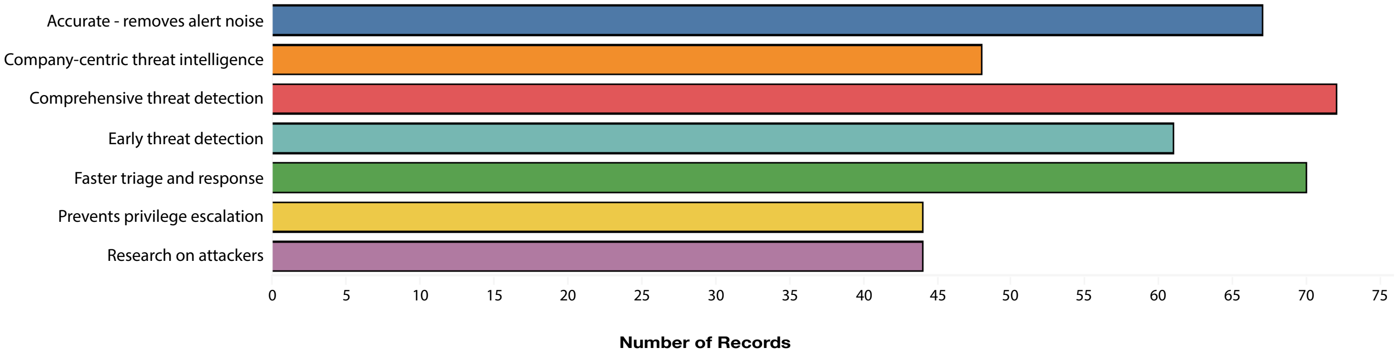


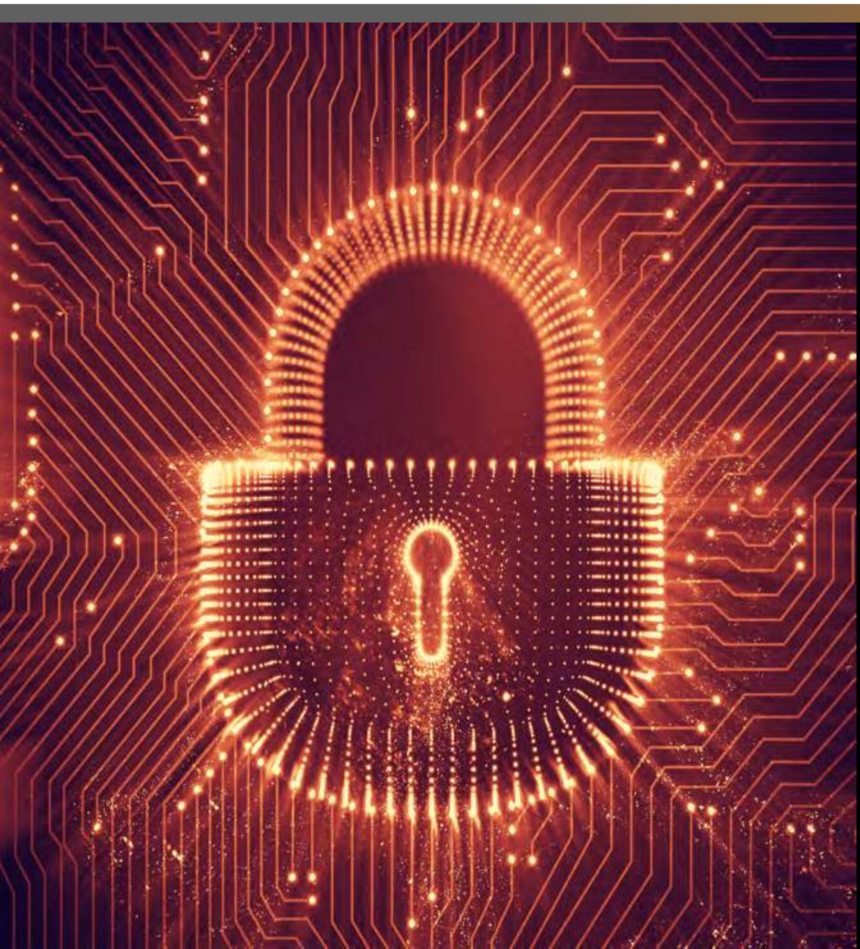
* For more information about the average breakout time, please refer to the Crowdstrike blog page: https://www.crowdstrike.com/blog/first-ever-adversary-ranking-in-2019-global-threat-report-highlights-the-importance-of-speed/

Deception Technology is Valued for Threat Detection

Shown in the diagram below (Figure 14), respondents valued deception technology for its accuracy as well as its ability to do early threat detection and accelerate triage and response. Most respondents mentioned comprehensive threat detection, which highlights the ability of deception technology to detect any attack vector across any attack surface without relying on known behaviors or signatures. Since detection across attack surfaces is the highest priority to address in the next year, we can expect to see increased deployment of deception technologies. Second in the respondents' opinion of the value of deception technology is faster triage, which indicates that respondents value the efficiencies it offers investigators and response teams. Efficiency was a driving concern for security investments. Also, highly valued is accuracy and removing alert noise. These also speak to the importance of operational efficiency, especially when dealing with resource constraints regarding personnel.

Figure 14. Value of Deception Technology





"Much of this year's research indicates a continued demand for in-network detection that works reliably across existing and emerging attack surfaces and is effective against all attack vectors. Our customers tell me that deception provides the easiest way to do gap analysis and in real-time see how dirty their network is. They also see the types of attacks present and the types of technologies needed to prevent those attacks."

– Sarah Ashburn, SVP of Sales and
Customer Success at
Attivo Networks

SUMMARY

In 2020, detection across all attack surfaces remains a priority for security executives. Of particular importance is security in the cloud. Investments in cloud security continue to be top of mind, in part because the responsibility is shared with cloud providers, thus making it challenging to understanding where the company's responsibility lies compared to what the cloud provider covers. Also, working in a multi-cloud environment, where each cloud provider has different cybersecurity procedures and processes, only complicates matters. At the same time, as companies move more of their critical business processes to the cloud, denial of service attacks, and disruption due to ransomware remain the top attacks of concern.

There appears to be a heavy reliance on IDS/IPS, which has historically been the primary security approach. Organizations are viewing newer EPP/EDR tools as a way to add detection coverage, and as multi-use security tools, but they can still have coverage gaps when working across varied attack surfaces and attack vectors.

Deception technology has emerged as a way to secure systems by providing the ability to better and more efficiently detect attack vectors across a wide variety of attack surfaces. Organizations are increasingly adopting deception technologies for comprehensive threat detection (along with faster triage and response) and provides extensive capabilities when used with tools like EPP/EDR or when used when in conjunction with IPS/IDS or other cloud security controls.

Of particular interest from this research is the focus on business continuity and maintaining service availability. Executives prioritize solutions that they think will keep their operations running. Efficiency remains a theme, as was demonstrated by the priority placed on accurate detection, faster triage and response, and automation.

As a new normal emerges due to the COVID-19 Pandemic, remote work has taken on new significance in just about every workplace. With more workers working from home, security managers must adapt their plans and practices to cover endpoints, credentials, and cloud environments. We expect top priorities to include cloud security, securing remote communication channels (VPN), and identifying new threat vectors arising from the transition into new ways of work. While no one could have predicted the extent of the disruption thrust upon the work environment, security leaders must adapt to address protection, detection, and recovery from cybercrime with what is now their new normal.

ABOUT SINC USA

SINC prides itself on being a partner to technology leaders across all industries and verticals. For senior IT and Security executives, SINC events and digital environments provide a valuable networking and educational experience. Through forums, private functions, virtual roundtables, webinars and industry reports, IT and Security leaders can rely on SINC to provide thought-provoking content to aid your personal and professional objectives.

ABOUT KPPARTNERS

Companies today must be able to respond instantly. Customers demand it. The environment in which we work demands it. The emerging social business environment enables it. KP Partners is an executive advisory services firm specializing in issues at the intersection of business strategy, organizational design, and information system. We most often work with CIOs and their executive teams on issues of strategic importance and strategy formulation. Utilizing our extensive and well-regarded network of IT and organization design experts, we provide executive coaching, team learning, multi-client programs, research and advisory services, and consulting services.

ABOUT ATTIVO NETWORKS

Attivo Networks provides a comprehensive deception platform that in real-time detects inside-the-network intrusions in networks, public and private data centers, and specialized environments such as Industrial Control System (ICS) SCADA, Internet of Things (IoT), and Point of Sale (POS) environments. Founded on the premise that even the best security systems cannot prevent all attacks, Attivo provides the required visibility and actionable, substantiated alerts to detect, isolate, and defend against cyber-attacks. Unlike prevention systems, Attivo assumes the attacker is inside the network and uses high-interaction decoys and endpoint, server, and application deception lures placed ubiquitously across the network to deceive threat actors into revealing themselves. With no dependencies on signatures or attack pattern matching, the BOTsink deception server is designed to accurately and efficiently detect the reconnaissance and lateral movement of advanced threats, stolen credential, ransomware, man-in-the-middle, and phishing attacks. The Attivo Multi-Correlation Detection Engine (MCDE) captures and analyzes attacker IPs, methods, and actions that can then be viewed in the Attivo Threat Intelligence Dashboard, exported for forensic reporting in IOC, PCAP, STIX, CSV formats or can be used to automatically update SIEM and prevention systems for blocking, isolation, and threat hunting. The ThreatOps offering simplifies incident response through information sharing, incident response automation, and the creation of repeatable playbooks. Learn more at https://attivonetworks.com/.

SINC