IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Sponsored by:

Information Security and Compliance Future Trends 2024:

How Regulation, Sophisticated Attacks, and Artificial Intelligence will Shape Security Spending in 2024

April 2024 EMA Research Report

Christopher M. Steffen, CISSP, CISA, VP of Research and **Ken Buckler, CASP**, Research Director

Information Security, Risk and Compliance Management

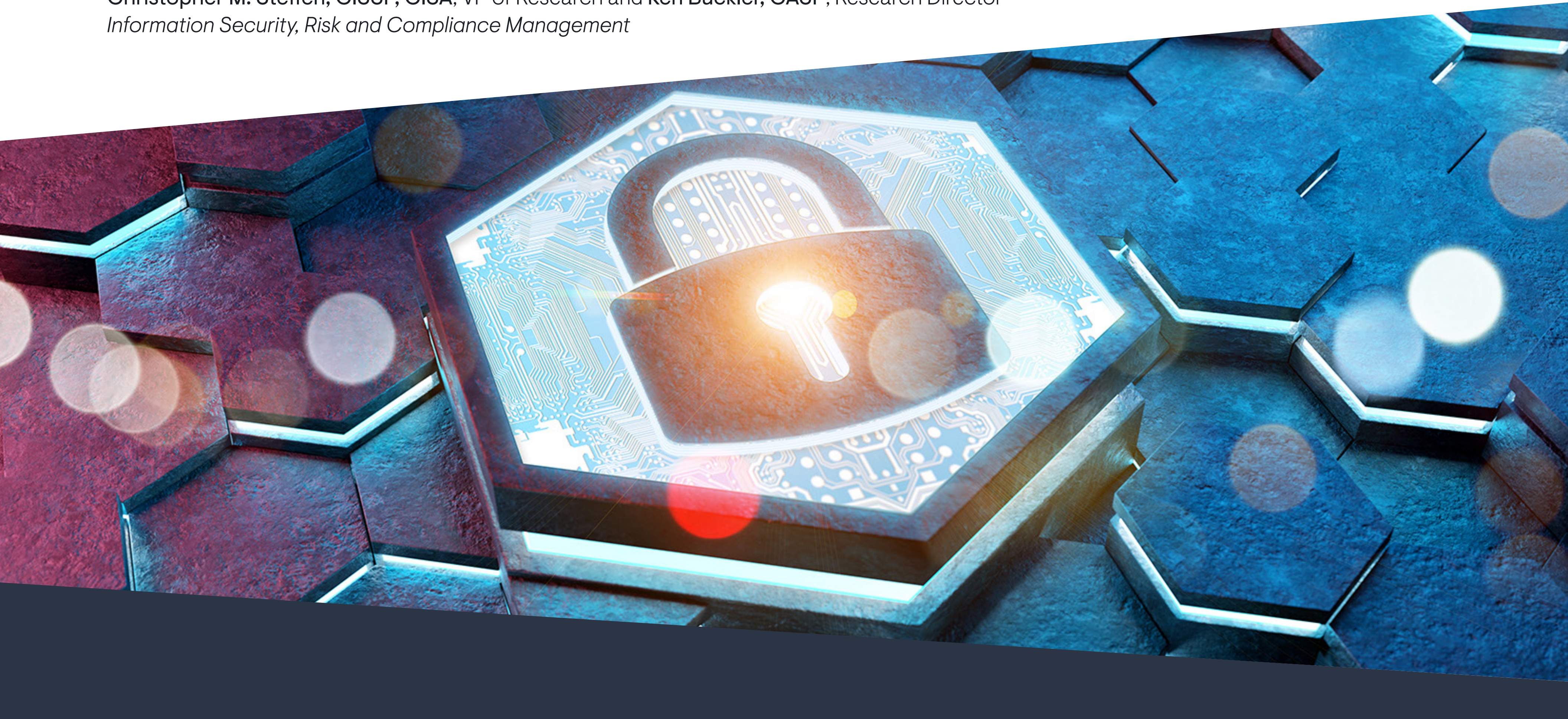
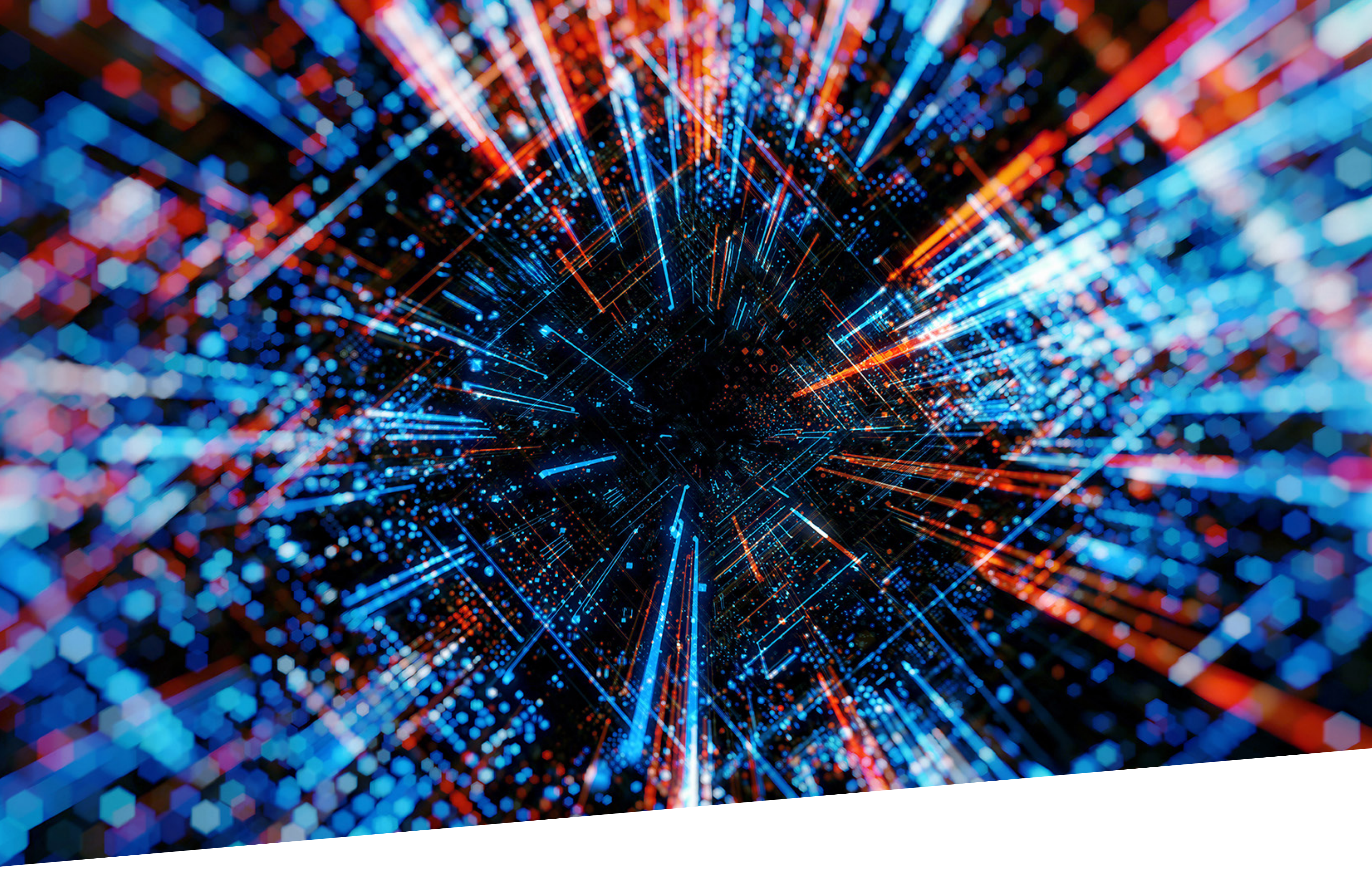


Table of Contents



Introduction

If you've ever visited a carnival, it's likely you've encountered a fortune teller. Many fortune tellers engage in a practice known as "cold reading" in which they seem to magically know things about your personal life. Through this process, the fortune teller reads "signals" from your body language to identify insights into your life based on context clues from your mannerisms in order to gain your trust and provide a believable prediction of something that might happen in your future. Often, this involves objects such as crystal balls, magical tea leaves, or tarot cards for extra dramatic effect.

While we certainly don't have a crystal ball or magical tea leaves here at EMA, we can look at the "signals" we've gathered over the past several years to provide a good idea of current trends and where the industry is headed. In this report, through the utilization of multiple recent research reports as well as publicly available data, we take a look at the future of the cybersecurity industry and identity the key shifts that IT managers and CISOs need to prepare for, if they're not already doing so.

Of course, it won't take a crystal ball for anyone to point out that artificial intelligence (AI) is taking center stage in much of the cybersecurity industry. Whether it is leveraging AI for cybersecurity usages, such as security automation, or for securing generative AI models, such as ChatGPT, AI seems to be on everyone's minds. However, it's important to note that the cybersecurity industry is seeing other radical changes taking shape – some influenced by the AI revolution – and these changes have the potential to alter the trajectory of much of the industry. Data security is also increasingly becoming a challenge, with 22% of organizations declaring their greatest data security challenge is developing a unified security strategy across their enterprise. This isn't surprising, given significant shifts toward privacy regulations, such as GDPR and CPRA, with 34% of organizations stating that these regulations are their greatest IT compliance challenge.

No one can predict when a successful cyber attack will occur, and that's why endpoint security, security information event management (SIEM), and extended detection and response (XDR) are all closely becoming unified core parts of enterprise strategies, with 60% of organizations now leveraging XDR as well as SIEM. This usage adoption is only predicted to increase as organizations look to improve their detection of advanced threats. All of this is wrapped up in continuing efforts to shift to a more proactive approach through zero trust, with 62% of organizations planning or implementing a zero trust project, but only 28% of organizations having at least started implementation.

Data sources for this report

Multiple EMA research projects, including but not limited to:

- EMA 2023 Observability Research
- EMA 2024 Artificial Intelligence Research
- EMA 2023 API Security Research
- EMA 2023 Data Security Research
- EMA 2023 Transcending Passwords Research
- EMA 2023 Observability Research
- EMA 2023 XDR Research
- EMA 2023 Zero Trust Research
- EMA 2024 Trends in SaaS Research

Additional Data Sources:

- Google Trends
- Google Search API
- IC3.gov Internet Crime Report – 2018 to 2022

FAN
TV
SECURITY
NETWORK
CCTV
LIGHT
TEMP
LOCK
_DaTa_0001_
060_%
020_%
BAB_0001101
Project Timeline
Research
Develop
Start

Baselines

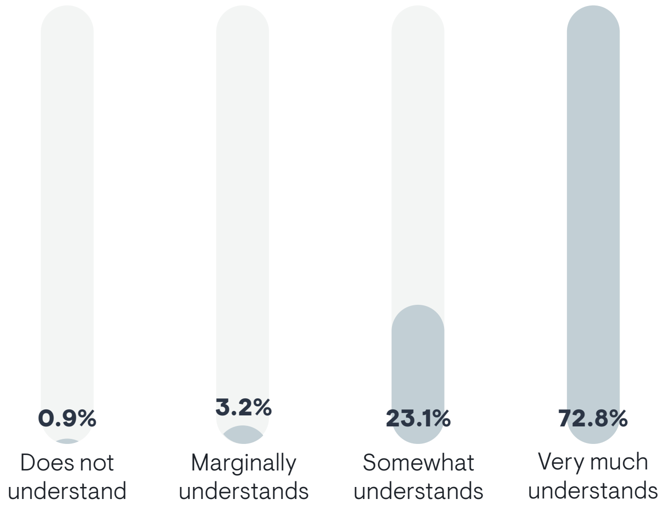
In nearly every piece of security research that EMA conducts, one of the baseline questions asked is whether the respondent feels their executives and organizational leadership grasp the importance of information security. The overwhelming majority believes that their leaders understand information security's importance. Still, there is a fraction (over 4%) with organizational leaders that barely or do not understand information security.

In a smaller sample, this might be considered an aberration. With over 1,000 samples in 2023 alone, the results are significant. Maybe 4% doesn't seem like a statistical concern, but – in this climate and technology-driven age – the fact that there is still a large number of executives out of touch with security concerns or priorities highlights the need for better communication of security priorities by technology practitioners.

In the immediate future, we will see the following trends:

- **AI as the equalizer.** Practitioners may not speak the language of their organizational leaders, but large language models (LLMs) can/do, and summarizing a technical brief or a CVE to business language by one of these AI sources is the perfect use of AI.
- **The CISO has a REAL seat at the table.** No longer relegated to the "Chief Tech Nerd" at the executives' table, the role of the CISO will continue to gain importance and influence as the Security and Exchange Commission pushes to hold organizations responsible for their information security. Finding a qualified security leader who also has a strong business background may become the new "unicorn" tech position.

DO YOU FEEL THAT THE EXECUTIVE MANAGEMENT/BOARD OF DIRECTORS OF YOUR ORGANIZATION UNDERSTANDS THE IMPORTANCE OF INFORMATION SECURITY?



On the surface, this seems like a fairly benign question to ask in a survey, but the consistent results indicate something that should be concerning to every security professional.

When asked who provides the security administration for your organization, the majority (58%) indicated that the corporate team performs security administration while the security team came in a distant second (18%). The alarming trend – in over 1,000 technical managers and leaders surveyed – is that they believe the cloud services provider is responsible for their security administration.

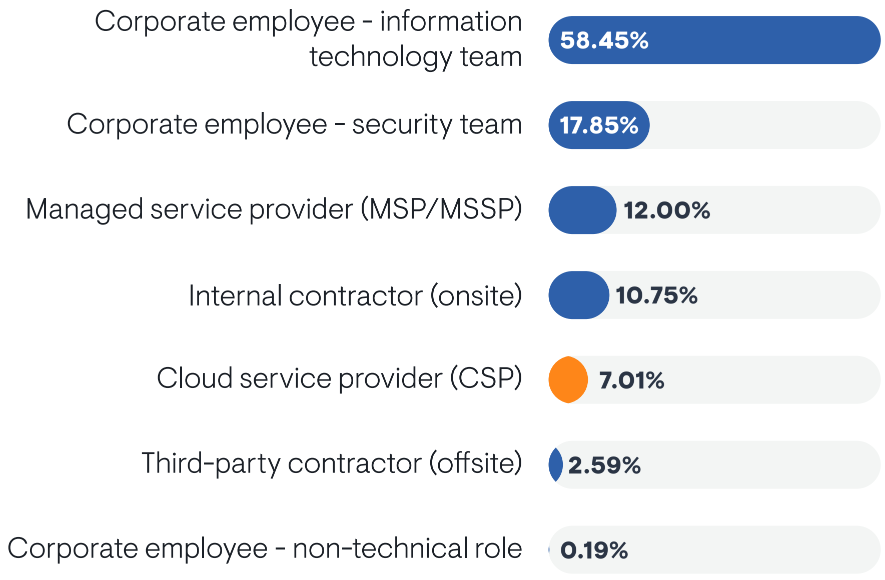
The cloud providers – such as Amazon, Microsoft, and Google – have spent millions in advertising and educating their customers on the shared responsibility model, meaning that some of the aspects of securing a cloud infrastructure (hardware, physical access, etc.) would fall to the CSP, but most of the basic considerations would be the responsibility of the end customer.

Another interesting trend is that in recent EMA research, 43% of organizations responded that they believe AI-powered MSP/MSSPs will begin replacing entire IT and security departments.

We believe that we will see the following trends:

- **Continued evangelism of the shared responsibility model.** The cloud providers have no choice but to continue to educate their customers on the specifics of the shared responsibility model. While the number of incidents is low, from the data, you can safely assume that 1 out of 20 workloads in the cloud are not properly secured.
- **Cloud incidents will continue.** The bad actors know this and will continue to exploit cloud instances that have weak security. Before blaming the cloud provider, though, find out how the end user secured the instance.
- **Increased MSP/MSSP presence:** With AI-powered MSP/MSSPs presenting a cost saving opportunity for organizations, and the continued qualified cybersecurity workforce shortage, there is no doubt that organizations will continue to shift toward this IT and security model, and even larger enterprises may begin to participate in this shift.

WHO PROVIDES SECURITY ADMINISTRATION FOR YOUR ORGANIZATION?



AI Security

Technology Overview

Artificial intelligence (AI) is revolutionizing cybersecurity through a range of impactful use cases. AI-powered threat detection and analysis enhance the identification of sophisticated cyber threats in real time, enabling proactive defense mechanisms. Behavioral analytics leverage machine learning to monitor user activities and detect anomalies, providing a dynamic approach to identifying potential security incidents, including insider threats. Endpoint security benefits from AI's ability to detect and respond to malware and ransomware, fortifying individual devices against evolving cyber threats. In identity and access management (IAM), AI contributes by implementing adaptive authentication, utilizing biometrics, behavioral analysis, and contextual information to verify user identities and secure access. Additionally, AI facilitates automated response and mitigation strategies, streamlining incident response and reducing the time to remediate security incidents. These use cases collectively demonstrate AI's transformative impact on bolstering cybersecurity measures in today's dynamic and evolving threat landscape. Due to the potential positive impacts of artificial intelligence in cybersecurity, many vendors are adopting it and making it part of their core offerings.

In EMA's 2024 research, 92% of organizations stated that changes in technology (such as AI) have had a noticeable or significant impact on their organizations.

Significant Vendors in the Space:

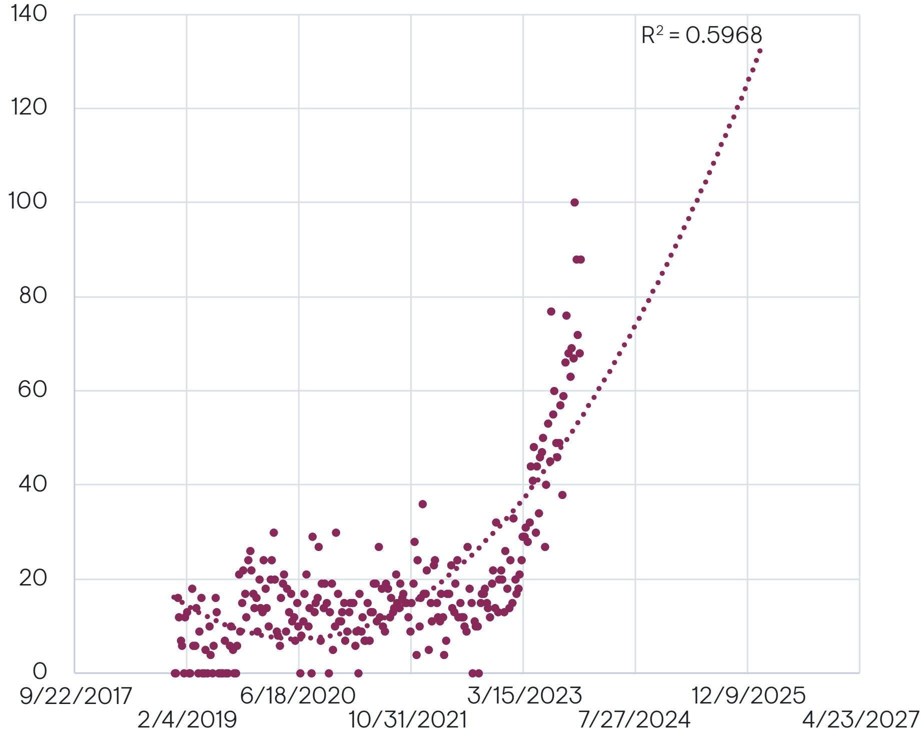
BforeAI
CLOUDFLARE®
CROWDSTRIKE
cybereason®
DARKTRACE
paloalto® NETWORKS
portal26
sparkcognition™
TESSIAN
VECTRA®

The noticeable uptick in Google search interest in AI security, starting with a slight incline in 2022 and a more substantial surge in early 2023, signifies a paradigm shift in the perception of artificial intelligence within the cybersecurity landscape. The pivotal factor contributing to this surge is likely the widespread adoption and application of generative AI across diverse industry verticals. As generative AI technologies become increasingly pervasive, organizations are grappling with the imperative to secure these advanced systems against potential vulnerabilities and threats.

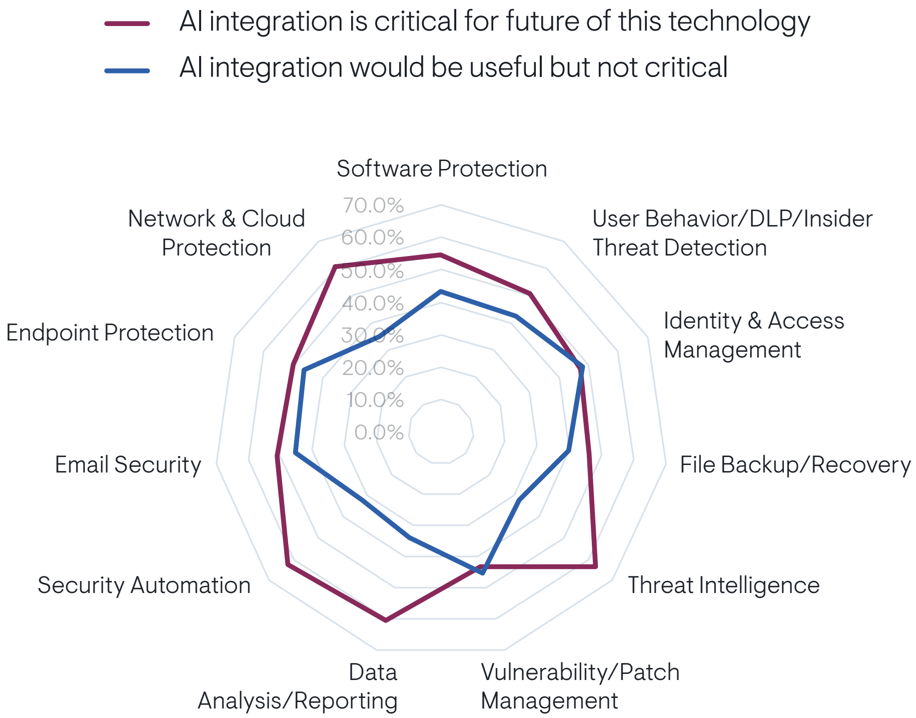
The heightened interest in AI security suggests a growing awareness of the intricate challenges associated with safeguarding AI models and the sensitive data they process. Even the Open Worldwide Application Security Project (OWASP) has taken note of the increasing security concerns regarding AI, specifically large language models (LLMs), by releasing their own Top 10 vulnerabilities list for LLMs.

This shift underscores the recognition that, as AI continues to revolutionize various sectors, ensuring the security and resilience of these intelligent systems is paramount. The surge in interest places AI security at the forefront of discussions, emphasizing the need for robust strategies and solutions to protect against evolving cyber threats in the age of advanced artificial intelligence applications.

AI SECURITY RELATIVE SEARCH TRENDS



EMA conducted our 2023 AI survey among IT/security professionals and decision makers. It provides insights into the perceived value of integrating artificial intelligence into various cybersecurity technologies. Notably, the majority of respondents (63.2%) sees threat intelligence as the area in which AI integration holds the most value, emphasizing the potential for AI to enhance threat detection and response capabilities. Security automation closely follows at 62.3%, indicating a recognition of AI's role in streamlining and fortifying automated security processes. Data analysis & reporting (60.4%) and network & cloud protection (60.4%) also emerge as critical areas for AI integration, underlining the importance of AI-driven insights in handling vast datasets and securing modern IT infrastructures. The acknowledgment of these technologies as critical aligns with the broader industry trend of leveraging AI for proactive and adaptive cybersecurity measures. On the other hand, technologies like identity and access management, endpoint protection, email security, and vulnerability and patch management are deemed "useful," but not critical for AI integration. This nuanced perspective suggests that while AI can enhance these areas, they may currently rely on more traditional approaches or have lower priorities for AI integration compared to the critical technologies. Overall, 83% of organizations believe that AI represents a cost savings opportunity for cybersecurity budgeting, helping organizations do more with less. While organizations did not indicate they will see increased security budgets due to AI, 88.6% of organizations predict an increase in security budget allocation toward AI for cybersecurity.



API Security

Technology Overview

API security is an essential framework of strategies and protocols designed to safeguard application programming interfaces (APIs) from unauthorized access, data breaches, and cyber threats. APIs serve as connectors between different software systems, enabling smooth communication and data exchange. Securing these interfaces is crucial to protect sensitive information, preserve user privacy, and prevent potential attacks.

Authentication and authorization are fundamental components of API security, verifying user identities and controlling their access rights. Encryption methods like HTTPS/SSL ensure that data transmitted via APIs remains confidential and tamper-proof. Implementing rate limiting and throttling helps prevent abuse and denial of service attacks by managing the number of requests an API can handle.

Furthermore, input validation techniques validate and sanitize incoming data to prevent common vulnerabilities, like SQL injection or cross-site scripting. Consistent monitoring, logging, and timely updates through patch management form a robust defense against evolving cyber threats, ensuring the resilience of API systems.

> “Securing an organization’s API is critical for business since it prevents private data from being accessed or abused. Businesses may guarantee that only authorized users can use the API and that the data is safe from bad actors by implementing encryption and authentication mechanisms.”
>
> *CIO, Midsized Services Company*

Significant Vendors in the Space:

42crunch

Akamai

Checkmarx

CLOUDFLARE

f5

FORTINET

neosec

noname

SALT

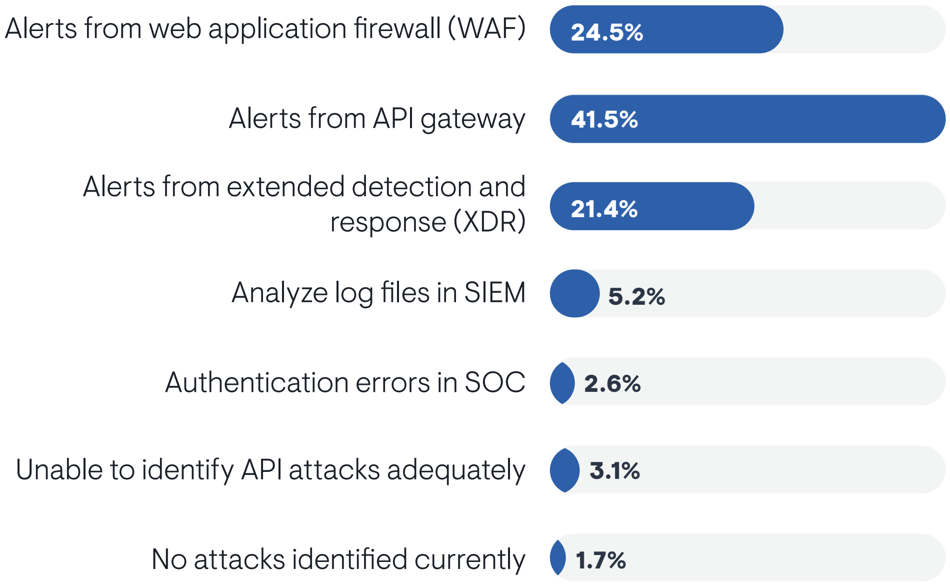
TREND MICRO

API security is at the forefront of security technologies that organizations are investing. In a recent survey, EMA found that organizations are using a variety of methods for securing their APIs, including API gateways (42%), web application firewalls (WAFs) (25%), and extended detection and response (XDR) solutions (21%). More concerning is that just under 5% of the organizations surveyed indicated that they cannot identify attacks or do not have the solutions to identify an attack on their APIs.

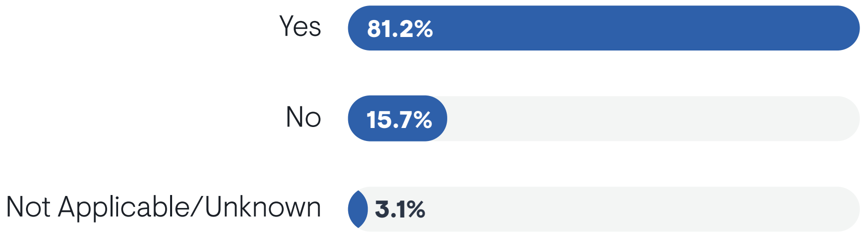
Looking ahead, these findings suggest several key trends.

- **API-Specific Security:** Dedicated API security solutions that go beyond traditional WAF functionalities are likely to gain traction.
- **Integration with Broader Security Strategies:** API security will become a more integrated part of overall security strategies, leveraging XDR and other tools for a holistic view, such as consolidated web application and API protection (WAAP) solutions.
- **Focus on Improved Detection:** Organizations will prioritize continuous improvement of their API security posture to identify and mitigate threats more effectively.

WHAT IS THE PRIMARY METHOD YOUR ORGANIZATION CURRENTLY USES TO IDENTIFY AN ATTACK ON YOUR APIS?



IF YOU DO HAVE A TOOL TO SECURE APIS, DO YOU USE THE SAME TOOL TO ALSO BUILD AND MANAGE THEM?



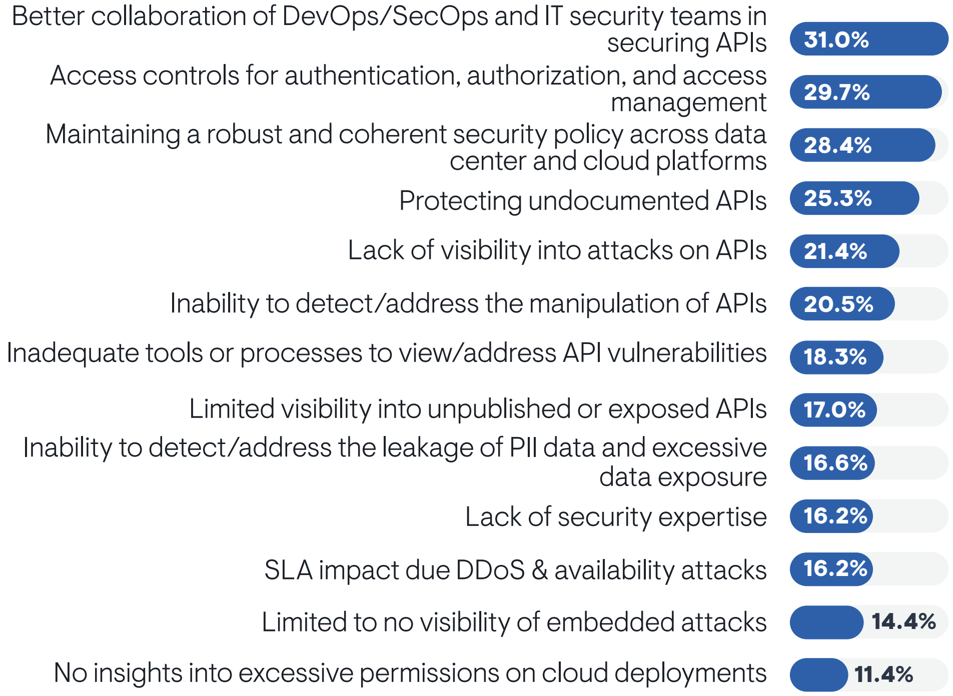
One of the best ways to determine how mature an API environment might be is to evaluate how well documented the organization's APIs actually are. In this survey, almost 70% of organizations had 30% or more of their APIs undocumented. That speaks only to the APIs they specifically know about in their environment.

Developers rarely love documentation, but the quality of the code is directly related to how well the code is documented, as well as how mature the organization actually is with their security and technical processes. In this survey, the fact that over one-quarter of an organization's APIs are undocumented (meaning there is little to no understanding of their function, the data they handle, and possibly how or what they connect to) is the strongest evidence that organizations that believe they have a "mature" API security strategy have subscribed to a false narrative.

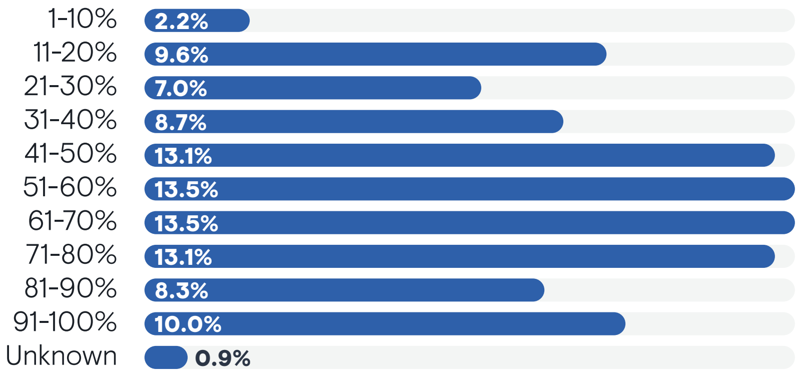
Looking ahead, these findings suggest several key trends.

- **Management Awareness Isn't Enough:** Ninety-five percent believe their existing security tools are effective at protecting their APIs and believe that the solution purchased will safeguard their organization. They feel they have done all the right things, but a deeper look at the environment shows that there are still significant gaps that need to be remediated.
- **Undiscovered APIs are a Major Risk:** With only 10% of APIs fully documented, a significant portion of the attack surface remains invisible. Organizations need better discovery and documentation processes to ensure comprehensive API security.
- **Security Starts Early:** Waiting until production to implement API security standards is too late. Security controls and procedures should be integrated into the design and development phases to prevent vulnerabilities from being baked in.
- **Integration is Crucial:** Customers would be wise to have a broader understanding of how their existing API management tools integrate with their overall security solutions and seek vendors that provide guidance on how to maximize their integrations.

IN YOUR ORGANIZATION, WHAT ARE YOUR PRIMARY CONCERNS REGARDING API USAGE?



HOW MANY APIS ARE DOCUMENTED (PERCENTAGE)?



Data Security/Privacy

Technology Overview

Data security and data privacy are paramount in the digital age, governing the protection and ethical use of sensitive information. Data security involves safeguarding data from unauthorized access, breaches, and malicious attacks. This encompasses encryption, access controls, and secure storage methods to maintain the confidentiality, integrity, and availability of data.

Data privacy, on the other hand, pertains to controlling how data is collected, shared, and used. It involves ensuring that individuals have control over their personal information, dictating who can access it and for what purposes. Compliance with regulations like GDPR and CPRA is crucial to uphold data privacy rights, requiring transparent data handling practices, user consent mechanisms, and the ability to manage and erase personal data when necessary.

Data security and data privacy are intertwined, forming the foundation for trustworthy and ethical handling of information. Establishing robust security measures while respecting individuals' privacy rights is essential in fostering trust with users and maintaining the integrity of data systems.

Significant Vendors in the Space:

CLOUDFLARE®

DIGITAL GUARDIAN

Forcepoint

IBM Security

KEEPER®

McAfee™

netskope

Symantec

VARONIS

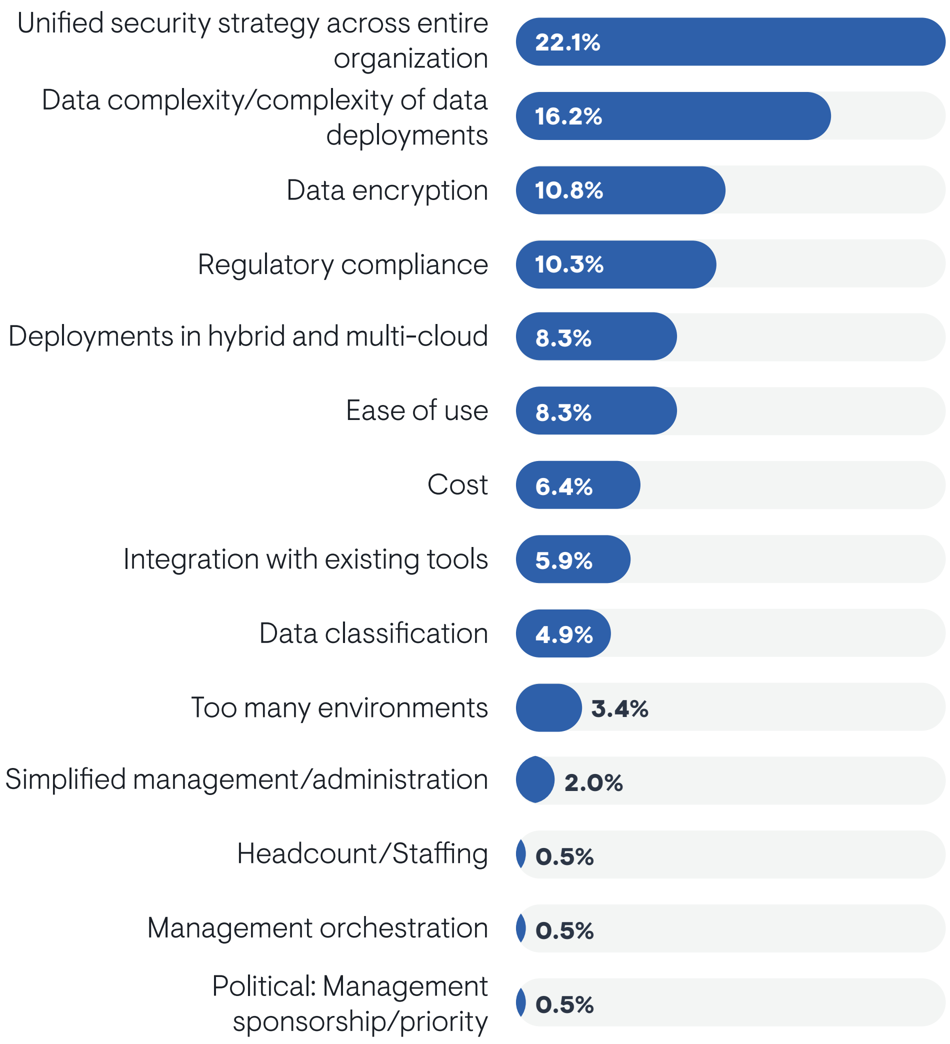
zscaler™

Data security is a factor that impacts nearly every division of an organization. The two challenges outlined in this survey showed that a unified security strategy (that encompasses data security), along with the complex nature of data and where it is deployed, ranked as the greatest challenges, followed by encryption of data, compliance requirements, and data deployed into cloud environments. Recent EMA research showed that 91% of organizations experienced growth in data associated with digital transformation, with 36% of organizations experiencing data growth over 20%.

Integrating data security as the primary (or a major) priority in an organization's overall security strategy is critical. So many organizations have regional or divisional plans for security operations, making protecting the organization's critical data even more difficult. When combined with differing classification standards and struggles for data ownership and custody, it becomes obvious why a unified security strategy ranked as the greatest data security challenge.

Regulatory compliance remains a major driver for security spending. Solutions that effectively address compliance requirements like GDPR, CPRA, HIPAA, and PCI will continue to see increased investment. Security professionals should collaborate with other departments to find solutions that meet both business needs and security goals. In EMA's 2024 research, 74% of organizations reported that compliance changes had a noticeable or significant impact on their organization.

WHAT IS YOUR ORGANIZATION'S GREATEST DATA SECURITY PROBLEM/CHALLENGE?

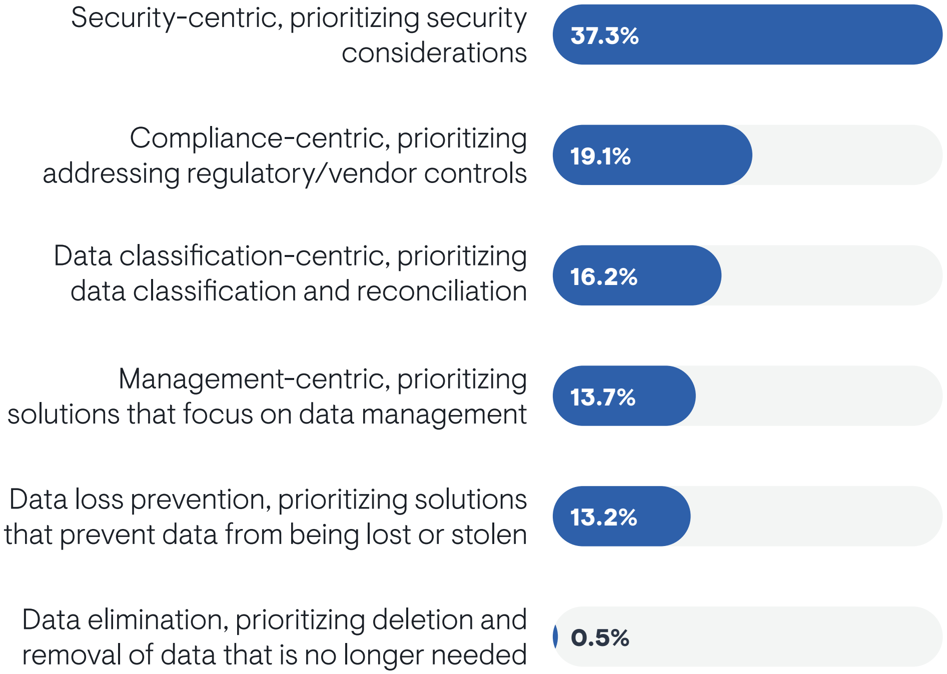


Data privacy is a major driver for organizations trying to implement a data security project. Many organizations (37%) have decided to take a security-centric approach to data privacy, prioritizing the security considerations first. Compliance (19%) and data classification (16%) round out the top three approaches to address data privacy.

As organizations embark on their data privacy projects, the key stakeholders need to determine the priority and approach to addressing data privacy concerns. In this survey, security was determined to be the primary motivator, but that answer could have just as easily focused on compliance if the survey respondent pool had been different. Both are valid approaches, and it is critical to agree on an approach before starting the project. There is no reason that the project cannot accomplish both, since the tools and vendors are designed with these approaches in mind.

Organizations will continue to seek comprehensive, user-friendly solutions that integrate seamlessly with existing tools and offer robust reporting. They will avoid complex, multi-part solutions and favor vendors with a proven track record of long-term support. In EMA's 2024 research, 39% of organizations considered ease of use the most important, or second most important, priority when investing in tools or solutions.

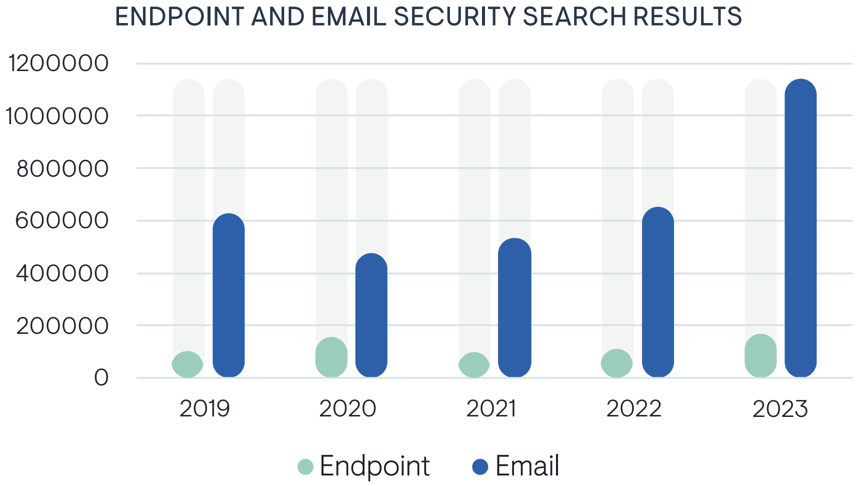
WHEN CONSIDERING THE METHODS YOUR ORGANIZATION USES TO ADDRESS DATA PRIVACY, WHICH OF THE FOLLOWING BEST DESCRIBES THE APPROACH?



Endpoint and Email Security

Technology Overview

Endpoint security focuses on protecting individual devices, such as computers, laptops, smartphones, and servers, from security threats. The goal is to secure the endpoint devices and the data they contain. Email security aims to protect organizations from threats that may be delivered through email, such as phishing, malware, and spam. Combining these endpoint and email security technologies provides a comprehensive defense strategy, safeguarding both individual devices and the communication channels that cyber threats commonly target.



Significant Vendors in the Space:

AVANAN
A Check Point Company

Barracuda

Bitdefender

CLOUDFLARE

CROWDSTRIKE

McAfee™

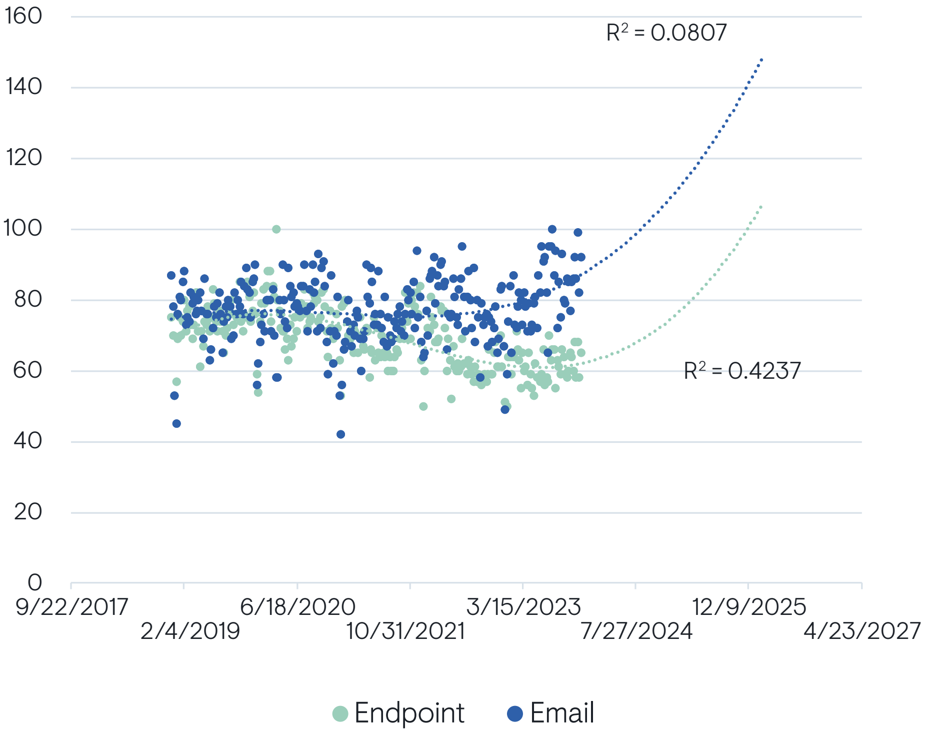
Microsoft Defender
for Endpoint

mimecast

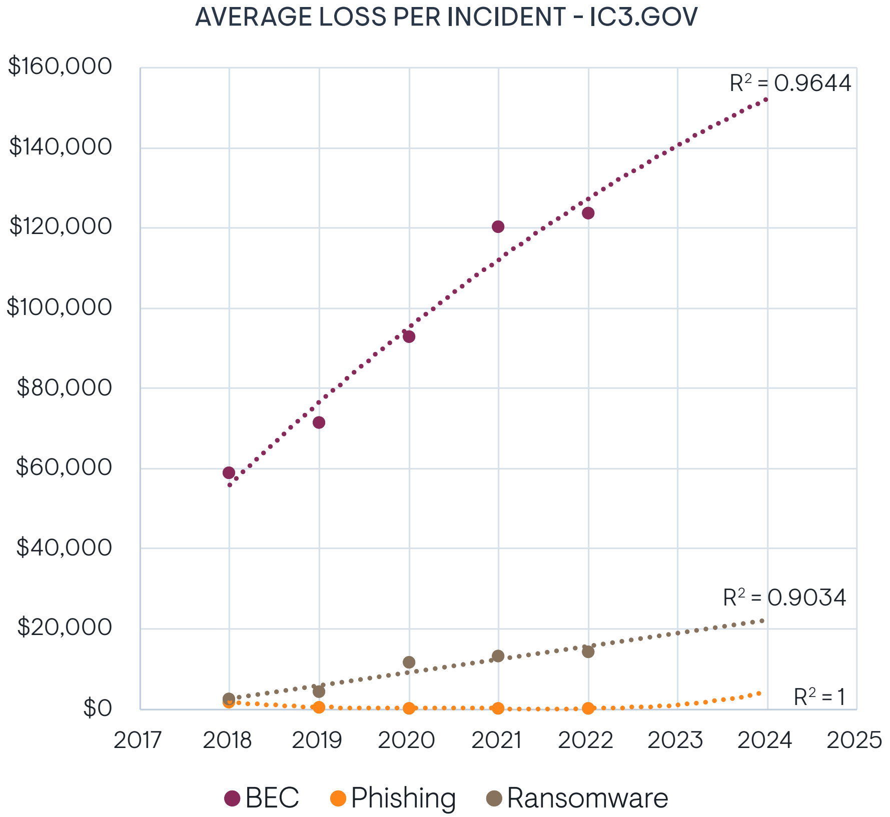
proofpoint

The contrasting trends in Google searches for endpoint security and email security unveil a nuanced landscape in the cybersecurity domain. The initial decrease in searches for endpoint security starting in 2019, followed by a sharp increase in mid-2023, signifies a notable shift in organizational priorities. The surge in interest is likely a response to the evolving challenges the widespread adoption of remote and hybrid work models pose, emphasizing the critical need to secure individual endpoints in dispersed environments. This trend is expected to persist and intensify in the coming years as organizations grapple with the intricacies of safeguarding remote devices. On the other hand, the consistent and progressively increasing search interest in email security, particularly with sharper upticks in the latter half of 2023, underscores the enduring importance placed on securing communication channels. This sustained interest suggests a growing recognition of the persistent threats associated with email-based attacks and the need for robust email security solutions. The concurrent trajectories of these trends highlight the dynamic nature of cybersecurity concerns, with organizations increasingly prioritizing measures to fortify both individual endpoints and communication channels in response to the evolving work landscape and the ever-present cybersecurity threats.

ENDPOINT/EMAIL SECURITY RELATIVE SEARCH INTEREST



The consistent and steady increase in the average loss per incident for business email compromise (BEC) over the past five years signifies a growing financial threat that sophisticated email-based attacks pose. This trend reflects the evolving tactics cybercriminals employ to manipulate communication channels and exploit vulnerabilities within organizations. The relatively flat trajectories for phishing and ransomware losses suggest a level of stabilization in the effectiveness of defenses against these types of attacks, though they remain significant threats. The predicted slight increase in phishing and ransomware losses per incident in 2024 indicates an ongoing need for vigilance and enhanced security measures. However, the stark contrast in the predicted average loss of $150,000 per incident for BEC in 2024 underscores the urgent necessity for organizations to prioritize advanced security strategies and invest in technologies that specifically address the nuances of email compromise threats. This emphasizes the critical importance of bolstering defenses against increasingly sophisticated and financially impactful endpoint-focused and email-based attacks in the coming years.



Identity and Access Management

Technology Overview

Identity and access management (IAM) is a comprehensive framework and set of technologies designed to manage digital identities, control user access to systems and resources, and ensure that the right individuals have the appropriate level of access within an organization's IT environment. Privileged access management (PAM) focuses specifically on securing and managing elevated or privileged access within an organization. Privileged accounts, often held by administrators, present a higher security risk due to their extensive access rights. IAM and PAM technologies work together to establish a robust and secure access management framework. IAM focuses on managing user identities and their access to resources, while PAM specifically addresses the unique security challenges associated with privileged accounts and elevated access within an organization's IT infrastructure.

Significant Vendors in the Space:

BeyondTrust

BROADCOM®

CYBERARK®

KEEPER®

ManageEngine

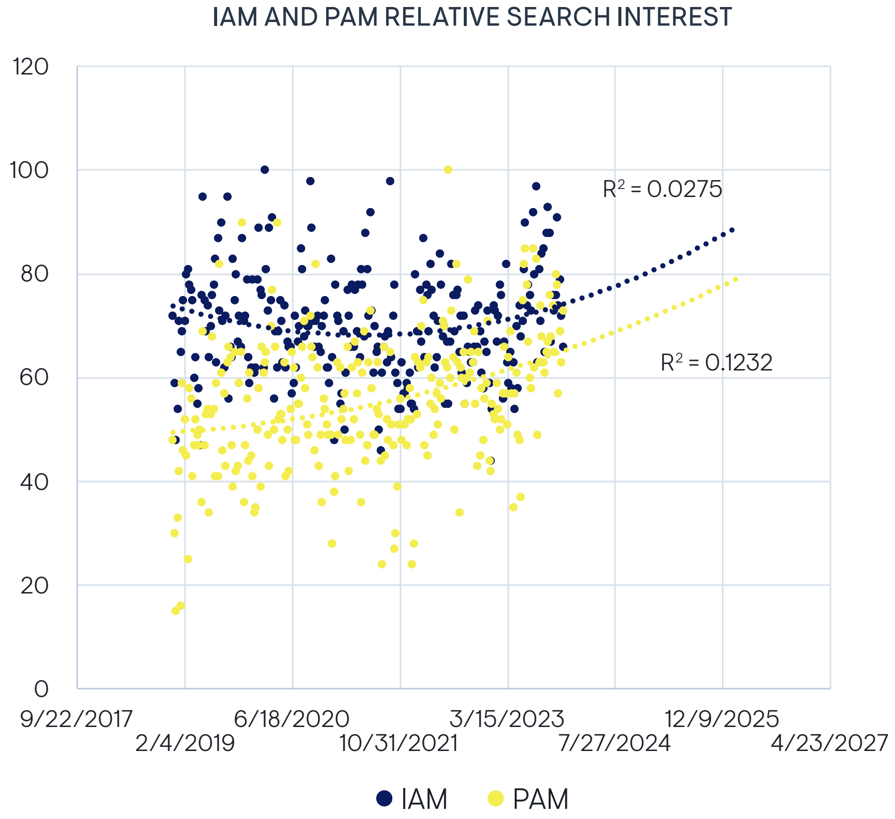
okta

typingdna

yubico

A decline in search result pages for new identity and access management and privileged access management solutions was observed during 2020 and 2021, likely influenced by the heightened focus on remote work enablement technologies during the pandemic. The decline indicates a temporary shift in organizational priorities. However, the subsequent significant increases in search results for IAM in 2022 and PAM in 2023 point to a renewed emphasis on strengthening security postures. The apparent disparity between the declining search result pages and the increasing search interest in IAM and PAM from 2019 through 2023 suggest a nuanced evolution in the perception and prioritization of identity-related solutions. The initial decline in search result pages could reflect a potential underestimation by web publishers regarding the pivotal role of identity in addressing the challenges remote work posed during the early stages of the pandemic.

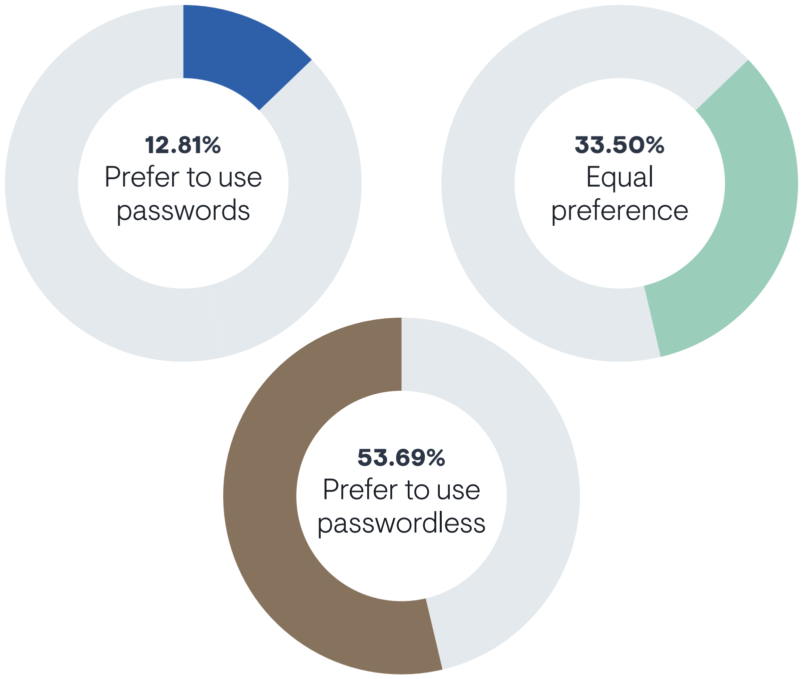
However, the concurrent increase in actual search interest implies that organizations and individuals recognized the growing significance of IAM and PAM even as they sought solutions to adapt to remote work requirements. The subsequent rise in both search results and interest indicates a maturation in understanding and an acknowledgment of the critical role that identity and access security plays in safeguarding digital environments. This trend underscores a collective recognition of the need for robust IAM and PAM solutions, aligning with a broader understanding of the evolving cybersecurity landscape and the imperative of securing identities in the context of remote and distributed work models.



The 2023 EMA research report "Transcending Passwords: The Next Generation of Authentication," along with a concurrent surge in Google search interest toward the end of the year for passwordless authentication, highlights a notable and accelerating shift toward these methods.

The increasing interest, particularly in authenticators and biometric authentication, underscores a collective recognition within the cybersecurity landscape that traditional password-based security models are facing heightened vulnerabilities, exemplified by the rising threat of credential stuffing attacks. The sharp uptick in search interest at the close of 2023 indicates a growing urgency among organizations and individuals to explore more secure and user-friendly alternatives.

Passwordless authentication methods, such as authenticators and biometrics, offer a promising avenue to enhance security while simplifying user experience. This trend reflects a broader industry acknowledgment that innovative approaches to authentication are imperative to staying ahead of sophisticated cyber threats, and the momentum is likely to persist as these technologies become integral components of modern cybersecurity strategies.

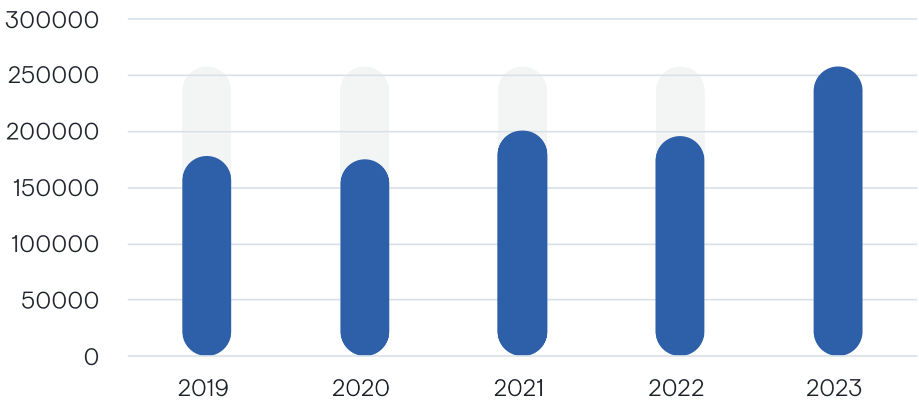


Network Security

Technology Overview

Network security technology encompasses a range of tools and practices designed to protect an organization's computer networks from unauthorized access, cyber attacks, and data breaches. Implementing a combination of these network security technologies helps organizations create a robust defense against a wide range of cyber threats, safeguarding the integrity, confidentiality, and availability of their network infrastructure.

NETWORK SECURITY SEARCH RESULTS



Significant Vendors in the Space:

CISCO

CLOUDFLARE®

FORTINET®

IBM Security

JUNIPer® NETWORKS

paloalto® NETWORKS

TREND MICRO™

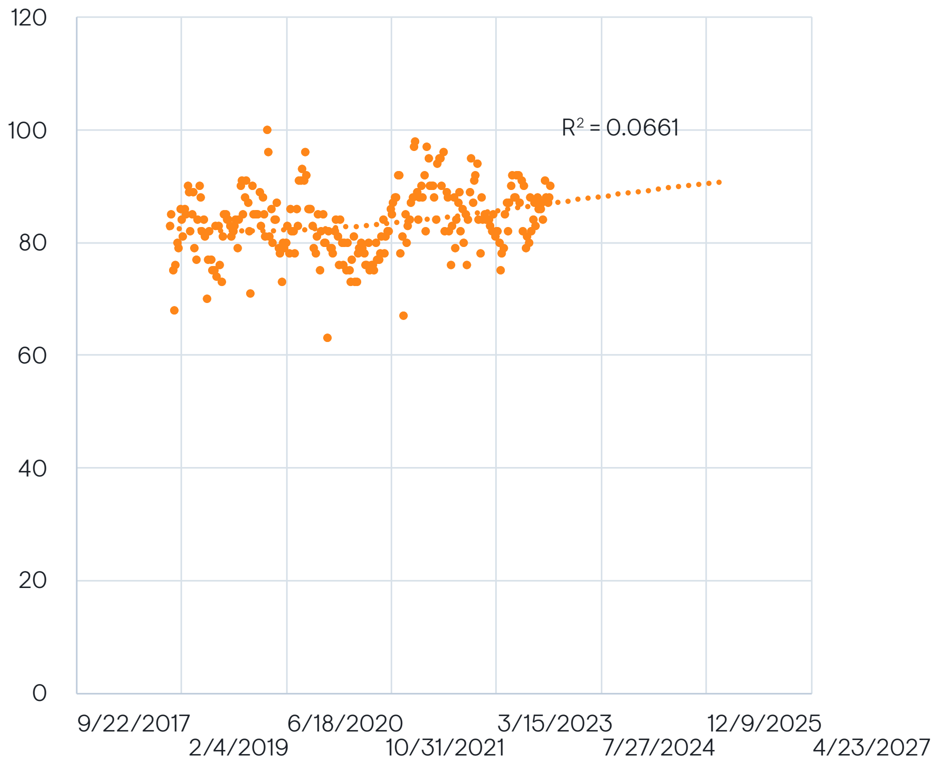
zscaler™

The consistent increase in Google searches for network security over the past five years reflects a growing and sustained awareness of the critical role that network security plays in the overall cybersecurity landscape. The upward trajectory suggests a heightened focus on fortifying digital infrastructures against evolving threats, likely fueled by a combination of escalating cyber risks and the rapid expansion of digital connectivity.

As organizations continue to digitize their operations and leverage interconnected technologies, the emphasis on securing networks becomes paramount. This trend indicates that businesses and individuals alike are proactively seeking information, solutions, and best practices to enhance the resilience of their networks against a backdrop of ever-evolving cyber threats.

The persistent and year-over-year growth in search interest underscores the enduring importance of network security as a fundamental pillar in the ongoing efforts to safeguard digital assets and maintain the integrity of online environments.

NETWORK SECURITY RELATIVE SEARCH INTEREST

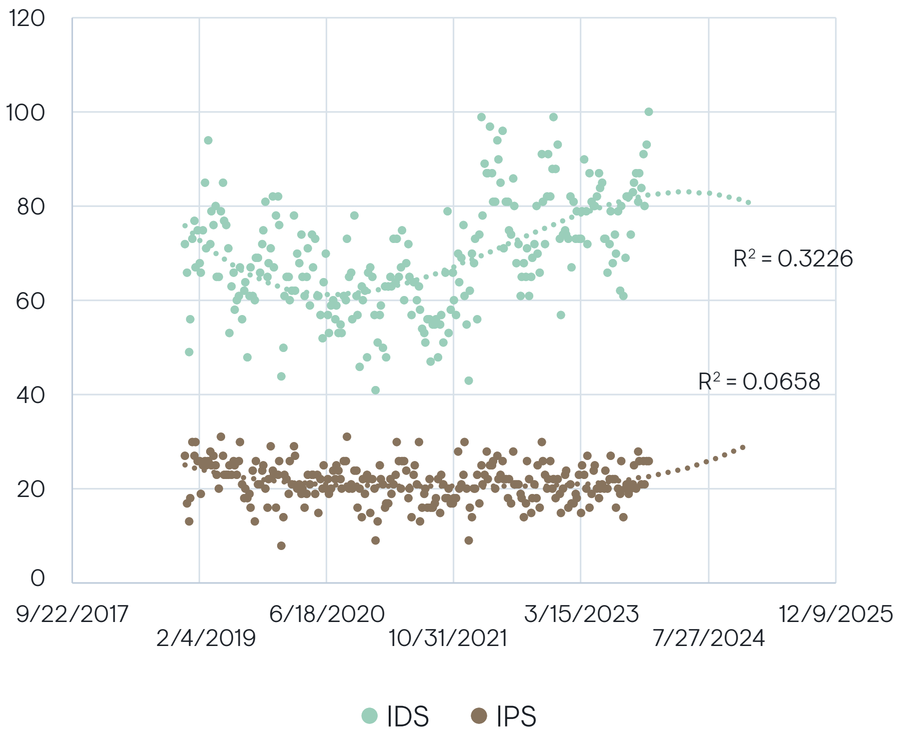


The shift in Google search trends, with searches for intrusion detection (IDS) showing a decline while intrusion prevention (IPS) searches are on the rise, indicates a notable transition in the approach of organizations toward network security.

The historical preference for intrusion detection suggests a more reactive stance, emphasizing the identification and response to security incidents after they occur. However, the increasing interest in intrusion prevention signifies a growing inclination toward a proactive defense strategy.

This shift likely reflects a recognition within the cybersecurity landscape that preventing intrusions before they happen is crucial for mitigating potential risks and minimizing the impact of security breaches. The trend underscores a maturation in security practices, with organizations prioritizing preemptive measures to fortify their networks against evolving threats, aligning with the broader industry push toward proactive cybersecurity postures.

IDS/IPS RELATIVE SEARCH TRENDS



Regulatory Compliance

Technology Overview

Information security serves as a crucial pillar in achieving regulatory compliance across industries. Various regulations like GDPR, HIPAA, or PCI DSS set stringent guidelines for data protection and privacy, demanding robust security measures from organizations.

The role of the Chief Information Security Officer (CISO) evolved significantly in response to these regulations. CISOs are pivotal in ensuring that businesses not only adhere to these standards, but also proactively implement effective security strategies. They oversee the development, implementation, and monitoring of security protocols and policies, ensuring alignment with regulatory requirements.

The latest regulations emphasize the CISO's role as a strategic leader responsible for integrating security measures into the business's overall objectives. Their expertise helps in navigating complex compliance landscapes, mitigating risks associated with non-compliance, and building trust with customers by safeguarding sensitive data. Ultimately, the CISO's involvement and understanding of evolving regulations are instrumental in enabling businesses to thrive while maintaining data integrity, security, and regulatory adherence.

In EMA's 2024 research, 74% of organizations reported that updated compliance regulations had a noticeable or significant impact, and 77% of organizations reported similar impacts due to updated vendor requirements.

> "In our organization, we consider IT compliance and audit to be a top priority. We hired a third party that carries on unbiased checks on the company's operations. Various intermediate checks are internally done, too, to keep the operations on track and secured."
>
> *CISO, Financial Services*

Significant Vendors in the Space:

ARCHER

baffle

BITSIGHT

CLOUDFLARE®

CERBERUS SENTINEL

COALFIRE®

IBM Security

ProcessUnity

protiviti® Global Business Consulting

servicenow®

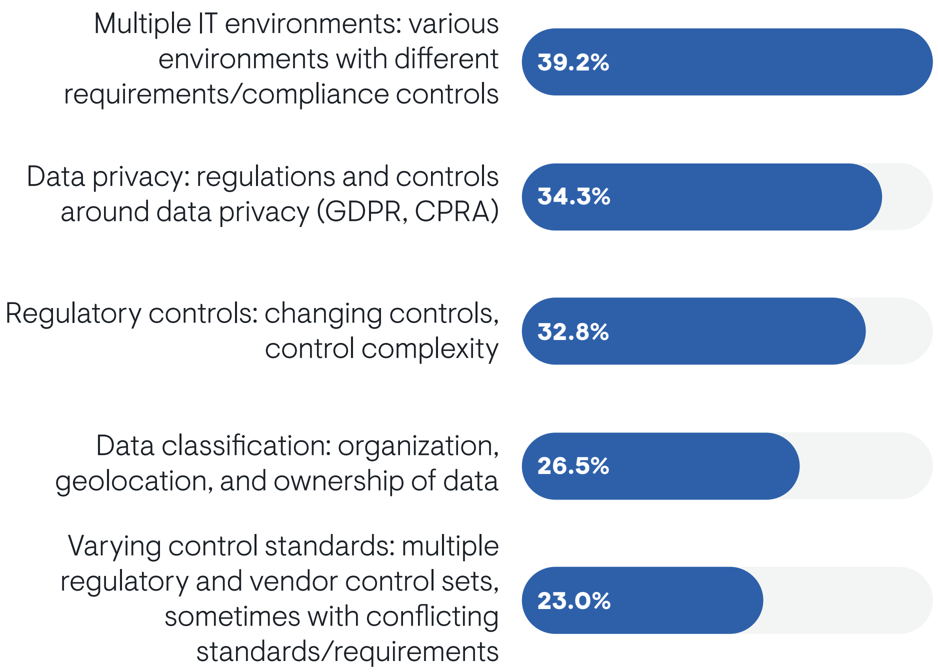
sumo logic

Data regulatory compliance across multiple IT environments will undoubtedly continue to be a major challenge for organizations in the coming years. EMA research shows that 70.8% of organizations have over ten different services and platforms in their technology stack, with 36.9% of organizations having over 20 different services and platforms, resulting in a security regulatory compliance nightmare.

This challenge will only become more complex as organizations continue to adopt artificial intelligence and large language models, with EMA research showing that 33% of organizations have experienced an unintentional material security or privacy incident due to usage of artificial intelligence.

The complexity of IT environments is also greatly increasing, with 90% of organizations experiencing an increased number and complexity of regulatory compliance considerations and 38% seeing a significant increase of 20% or more. This also resulted in budget impacts, with 80% of organizations reporting a noticeable or significant impact to their IT budgets and 75% of organizations reporting similar impact to their information security budgets.

WHAT IS YOUR ORGANIZATION'S GREATEST IT AUDIT/COMPLIANCE CHALLENGE?



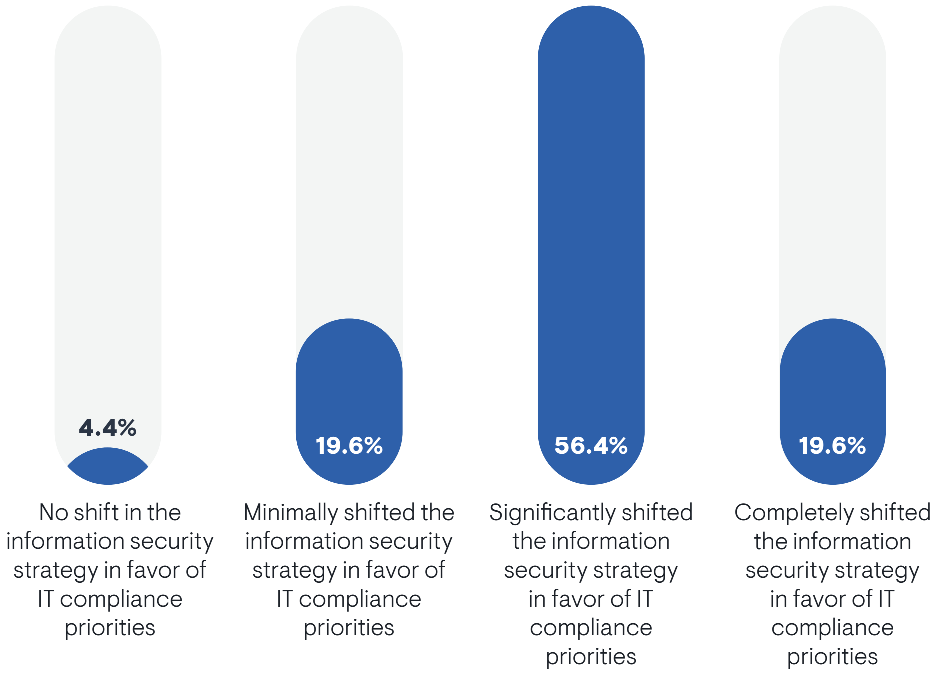
With IT compliance priorities significantly shifting organizations' information security strategy, many trends can be identified based on new and proposed compliance regulations.

SEC's new rules on cybersecurity risk management, strategy, governance, and incident disclosure sent ripples through industries across the United States in 2023. The increased focus on cybersecurity by government regulatory bodies will undoubtedly only increase in the coming years.

Of significant focus for the upcoming years will be software supply chain and software bill of materials (SBOM). New regulations, such as the Cybersecurity Maturity Model Certification (CMMC), will likely have a domino effect across much of the IT industry. Even if a specific organization does not have defense contracts, it's possible that one of their customers does, resulting in the need for many organizations to focus on supply chain compliance even if they never deal directly with the DoD.

Additionally, with increasing focus on privacy through regulations such as the EU's General Data Protection Regulation (GDPR) and California Privacy Rights Act (CPRA), regulatory compliance will continue to require organizations to shift toward a data-centric security approach, keeping sensitive data protection paramount.

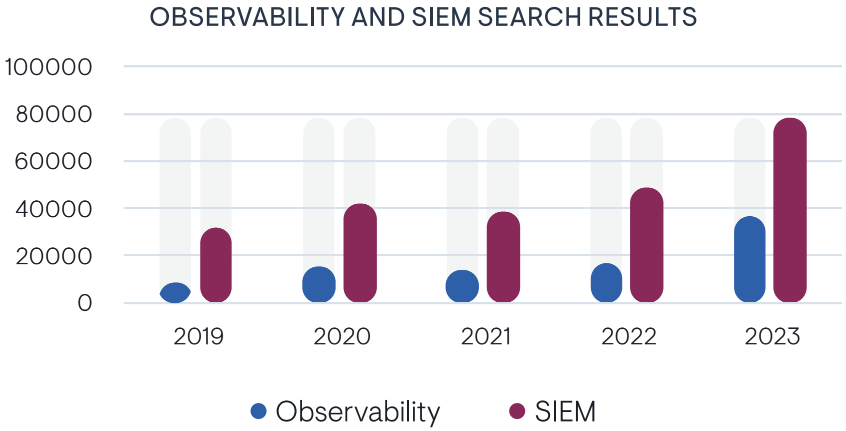
HAVE IT COMPLIANCE PRIORITIES IMPACTED YOUR ORGANIZATION'S INFORMATION SECURITY STRATEGY?



SIEM/Observability

Technology Overview

The security information and event management (SIEM) and observability technology spaces are crucial domains within the realm of information technology that focus on ensuring the security, reliability, and performance of digital systems. These technologies play a vital role in proactively identifying and mitigating security threats, monitoring system health, and optimizing the overall operational efficiency of an organization's IT infrastructure. SIEM covers security monitoring, event correlation, incident response, and compliance management. Observability focuses on monitoring and logging, metrics and tracing, anomaly detection, troubleshooting and root cause analysis, application performance management, and end-to-end visibility. It focuses on the availability and performance of the enterprise. The SIEM and observability technology spaces collectively address the diverse needs of organizations in terms of security, performance, and operational efficiency. These technologies are integral components of modern IT infrastructures, helping businesses stay resilient, secure, and responsive to the evolving digital landscape. Both SIEM and observability are seeing increased prominence within the cybersecurity industry, as highlighted by ongoing trends in internet content focused on these two technologies.



Significant Vendors in the Space:

DATADOG

elastic

IBM QRadar

LogRhythm™

solarwinds

splunk>

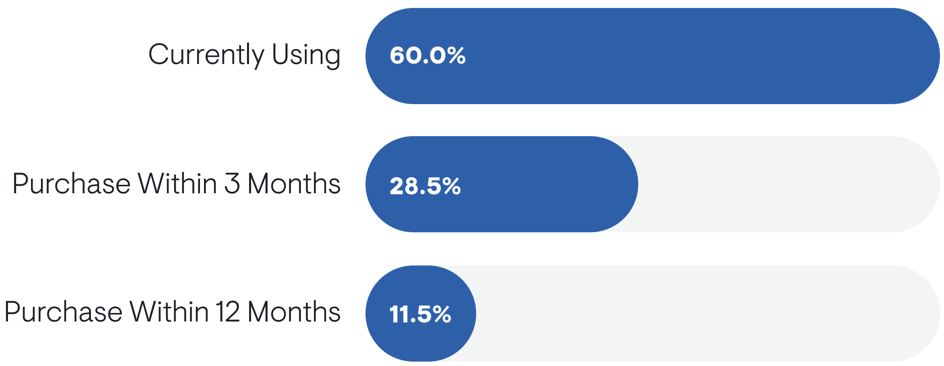
sumo logic

EMA conducted a 2023 survey among IT/security professionals and decision-makers that reveals a significant trend in the adoption of observability platforms within organizations.

With 60% of respondents already utilizing observability platforms, this indicates a growing recognition of the importance of comprehensive insights into complex IT environments. Moreover, the noteworthy statistic that 40% of organizations plan to invest in an observability platform within the next year underscores a continuing surge in demand. This suggests a proactive approach to enhancing operational visibility, troubleshooting, and performance optimization within digital infrastructures.

The anticipated influx of new adopters indicates a trajectory toward mainstream acceptance of observability platforms, highlighting their pivotal role in shaping the future of IT and security practices. As organizations increasingly prioritize real-time data and holistic visibility, the observability space is poised for further growth and innovation to meet the evolving needs of the tech landscape.

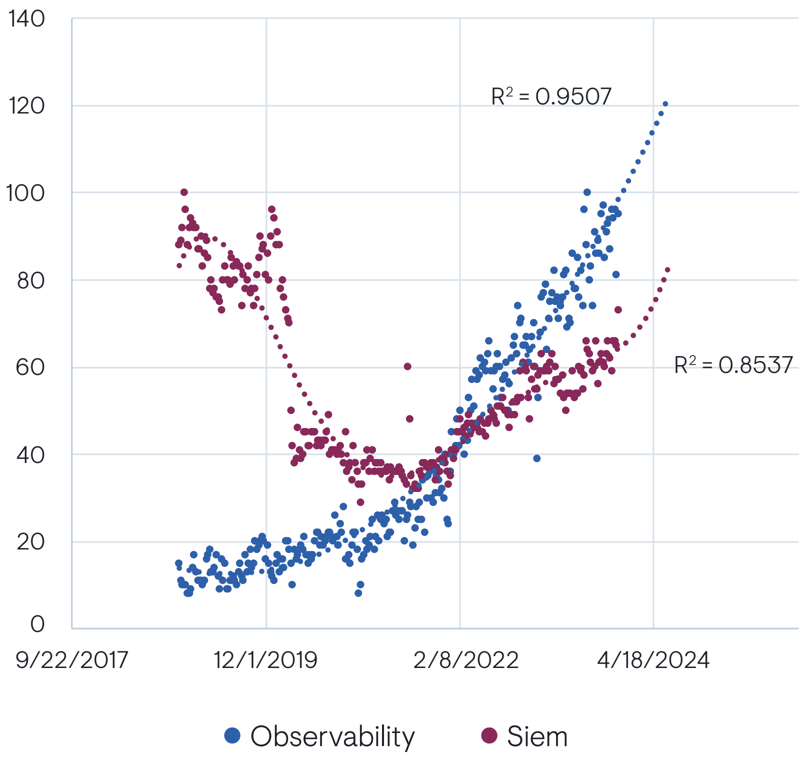
OBSERVABILITY PLATFORM USAGE – 2023 SURVEY



Google search trends indicate a decline in SIEM interest from 2019 to 2021, followed by a resurgence in 2022 and a more rapid increase in 2023, which suggests a dynamic shift in cybersecurity priorities. Simultaneously, the steady and continuous rise in search interest for observability since 2020 reflects a parallel recognition of the importance of comprehensive system monitoring and performance visibility.

The concurrent upward trends in both SIEM and observability suggest a nuanced approach by organizations, recognizing the complementary nature of these technologies. As cybersecurity and operational efficiency become increasingly intertwined, the trends imply a strategic pivot toward integrated solutions that combine threat detection and comprehensive system observability for a more robust and adaptive cybersecurity posture.

OBSERVABILITY AND SIEM RELATIVE SEARCH INTEREST



Extended Detection and Response (XDR)

Technology Overview

Extended detection and response (XDR) represents a significant evolution in cybersecurity, addressing the complexity of modern threats across diverse digital environments. It consolidates and enhances threat detection and response capabilities, integrating multiple security data sources and technologies into a unified platform. XDR goes beyond traditional endpoint detection and response (EDR) by correlating data from various sources like endpoints, networks, emails, and cloud environments. By leveraging advanced analytics, machine learning, and automation, XDR enables quicker threat detection and more effective response actions. It allows security teams to connect the dots between disparate security alerts and events, reducing response times and improving overall cybersecurity posture. As organizations continue to migrate toward a cloud-first approach, extending traditional detection and response to cloud must become part of organizations' digital transformation.

EMA proposed a unifying definition of XDR in 2023, and that definition has been widely adopted. It states that extended detection and response, or XDR, is a cybersecurity solution that:

- Integrates with existing and future security and operations tools
- Provides in-depth insights and reporting to technicians and decision-makers
- Streamlines security operations across users, endpoints, data, networks, cloud resources, applications, and other workloads
- Applies analytics and automation to detect, analyze, hunt, and mitigate threats

> One of the hardest parts about our security program is deploying a solution that protects our environment from outside intrusions. With the evolving nature of security threats, it becomes a never-ending struggle to make sure that our security monitoring is up to date.

CTO, Healthcare Organization

Significant Vendors in the Space:

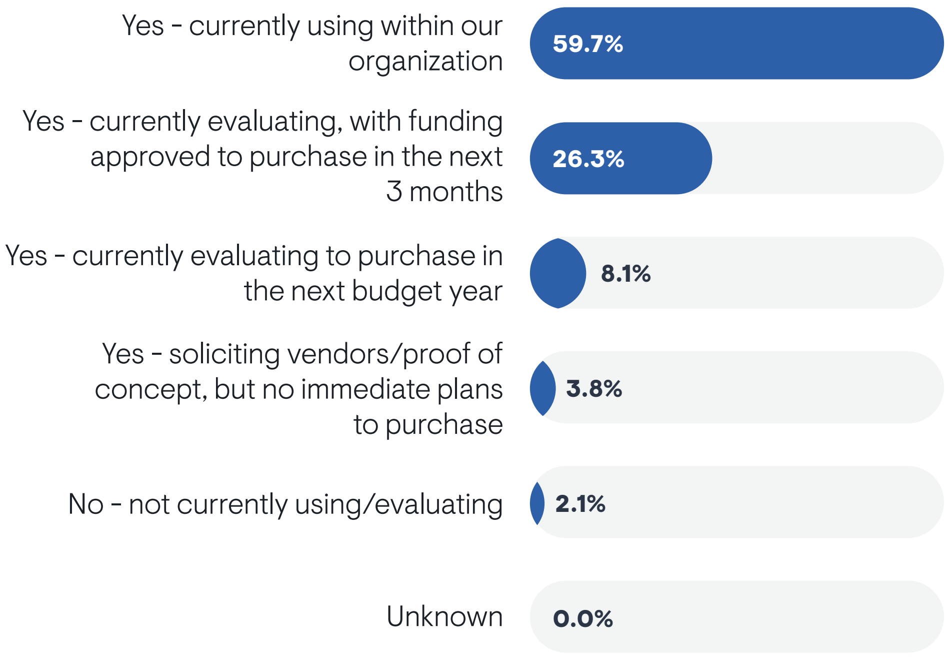
Bitdefender®
Carbon Black.
CROWDSTRIKE
cybereason®
elastic
FIREEYE™
Microsoft
paloalto® NETWORKS
SentinelOne®
SOPHOS

Traditional security solutions often operate in isolation, with each product focusing on specific areas such as endpoint protection, network security, or cloud security. However, this fragmented approach can lead to blind spots and gaps in visibility, allowing attackers to exploit vulnerabilities across multiple attack vectors. XDR addresses these shortcomings by integrating and correlating data from various security tools and sources, including endpoints, networks, and cloud environments. By analyzing this unified dataset in real time, XDR enables organizations to detect and respond to threats more effectively, regardless of where they originate or how they evolve over time.

In recent years, the information security landscape witnessed a significant shift toward the adoption of XDR solutions. According to EMA research in 2023, a staggering 86% of organizations either already implemented XDR or were actively planning to procure it within the next three months. This statistic underscores the rapid pace at which XDR became a cornerstone of modern information security strategies.

Overall, the widespread adoption of XDR represents a paradigm shift in how organizations approach cybersecurity, moving away from reactive, siloed approaches toward a more integrated, proactive, and adaptive model that is better suited to addressing the complex and dynamic nature of modern cyber threats.

IS YOUR ORGANIZATION CURRENTLY USING/EVALUATING AN EXTENDED DETECTION AND RESPONSE (XDR) SOLUTION?



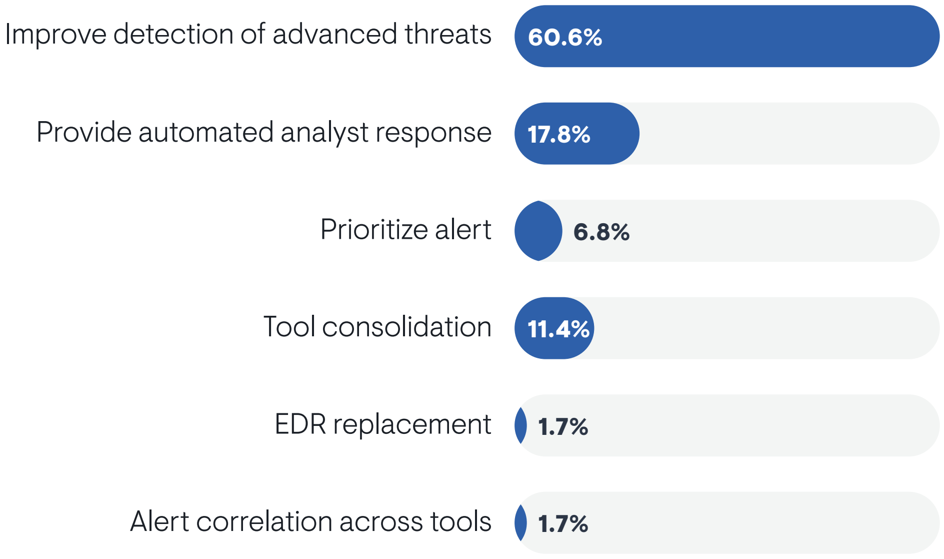
There are several reasons why many organizations are increasingly adopting XDR solutions. Traditionally, organizations relied on a bunch of separate security tools, each generating its own data. This made it hard to get a holistic view of what was happening on the network. XDR consolidates data from various security tools into a single platform, allowing for better analysis and threat detection.

Additionally, by correlating data from different sources, XDR can identify complex threats that individual security tools might miss. This allows for faster and more effective incident response and even security automation. XDR leverages machine learning and automation to streamline security tasks. This frees security analysts to focus on more strategic work, such as threat hunting and incident response.

Of interesting note is that only 1.7% of organizations are looking to XDR to replace EDR as the primary usage case. This is likely because XDR is not viewed as a direct replacement of EDR, but more of an extension. Tools consolidation and automated response both provide significant cost savings in either tool cost or human work costs, highlighting that after the improved detections XDR offers, budget impact is an important factor.

Overall, XDR offers a more cost-efficient and effective way to manage security in today's complex threat landscape.

WHAT IS THE PRIMARY USE CASE YOU ARE LOOKING TO SOLVE WITH XDR?



Zero Trust

Technology Overview

Zero trust is a cybersecurity approach centered on the principle of distrust by default, requiring continuous verification and validation for any access to resources within a network. Unlike traditional perimeter-based security models, zero trust assumes that threats exist both inside and outside the network. It emphasizes strict access controls and authentication measures, requiring users and devices to undergo rigorous verification before accessing any resources, regardless of their location. This approach aims to minimize the attack surface and prevent lateral movement within networks, reducing the potential impact of security breaches.

Zero trust relies on identity verification, microsegmentation, and continuous monitoring to enforce least-privilege access, limiting users and systems to only what is necessary for their tasks. This dynamic and adaptive model prioritizes real-time risk assessment and response, enhancing overall security posture against evolving cyber threats.

Implementing a zero trust architecture involves a cultural shift alongside technological changes, promoting a more proactive and adaptive security strategy. By continuously validating trust and implementing stringent access controls, organizations can better protect their assets and data, adapting to the evolving threat landscape with a more resilient security framework.

Significant Vendors in the Space:

appgate

BeyondCorp Enterprise

CSA cloud security alliance®

CLOUDFLARE®

illumio

netskope

NIST

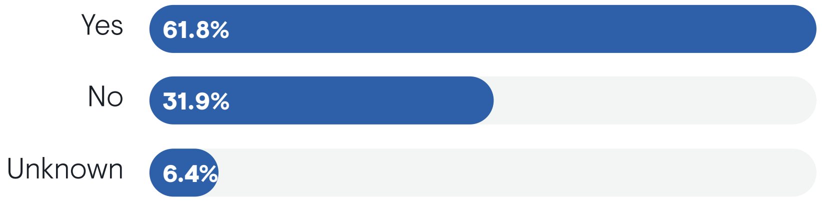
okta

perimeter 81
A Check Point Company

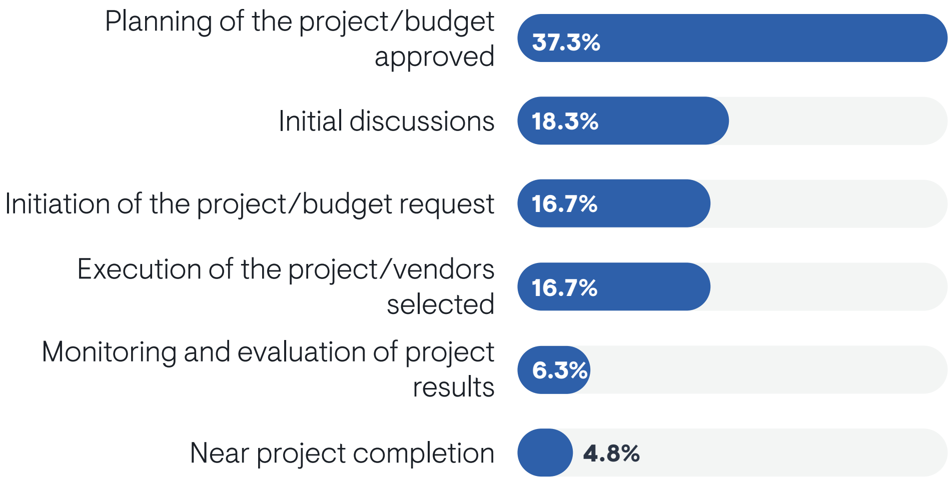
THREATLOCKER

Zero trust is not a buzzword. There are always emerging trends in the security industry, with plenty of vendors jumping on the bandwagon to ride the publicity around the current buzzword or phrase. Without question, there is a lot of buzz about zero trust, but unlike other fly-by-night trends, zero trust is a philosophy that will drive security innovation for the foreseeable future. Organizations are excited to start their zero trust implementations, but require guidance to make all the pieces work. Also, organizations can smell a fraud. They know that the organization that sold them sprockets yesterday and wants to ride the zero trust wave is not likely the zero trust leader that they need today.

In a survey conducted by EMA on organization' preparations for their Zero trust initiatives, we polled 209 technology leaders and about 62% indicated they were starting a zero trust journey. Of the 126 that indicated that nearly half were at some point in the implantation process.



IS YOUR ORGANIZATION INVESTIGATING/PLANNING A ZERO TRUST PROJECT?



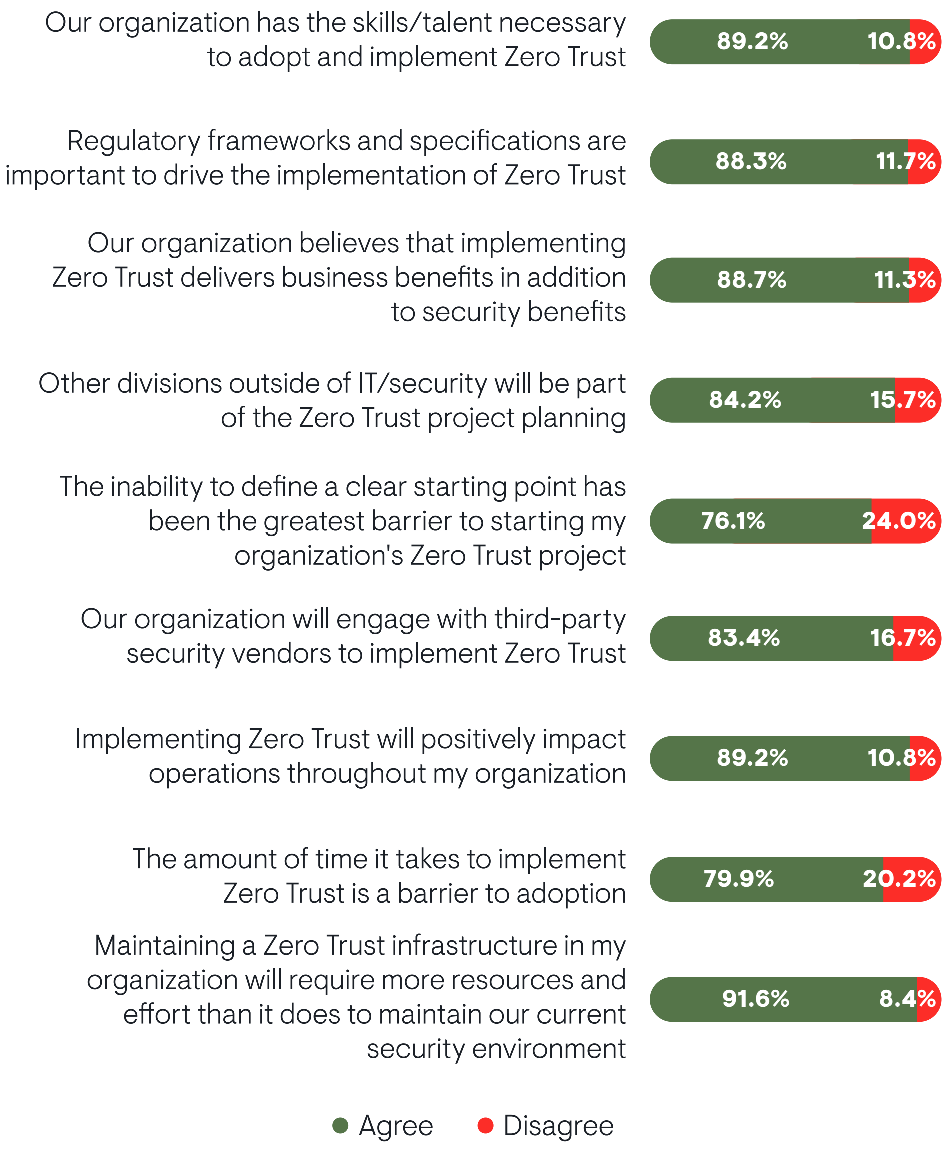
AT WHAT STAGE IS YOUR ORGANIZATION REGARDING YOUR ZERO TRUST PROJECT?

While most organizations believe they have the talent necessary to adapt and implement zero trust, one of the biggest concerns when it comes to zero trust is the increased resources and effort. Ninety-one percent of respondents in EMA's zero trust research indicated that zero trust infrastructure will require more effort than is currently being used for managing their IT and security infrastructure.

Ultimately, despite the increased effort required, most organizations believe that zero trust will result in a positive impact to organizational operations, once they can overcome barriers such as length of implementation time.

The demand for zero trust solutions and methodologies will only increase alongside adoption efforts. While zero trust cannot be achieved overnight and should be viewed more as a journey than a single solution, this holds the potential to completely revolutionize the future of the cybersecurity industry and fundamentally change how our information systems work and communicate.

PLEASE RATE THE FOLLOWING STATEMENTS ABOUT A POTENTIAL ZERO TRUST IMPLEMENTATION.



EMA Perspective

As the cybersecurity landscape evolves, organizations must adapt to emerging trends and technologies to protect against evolving threats effectively. While we may not have a crystal ball, we believe that through analyzing key shifts in the cybersecurity industry, this report offers insights into current trends and future directions based on recent research and industry data.

Only regulatory compliance will continue to be one of the primary driving factors of all technologies mentioned within this report. Notably absent from this report is a dedicated section to software supply chain security and software bill of materials (SBOM). This was instead integrated into the regulatory compliance part of this report. While it would have been easy to incorporate a dedicated section for this challenge, EMA believes that a much more holistic approach to software supply chain security is necessary, rather than a single SBOM solution. Obtaining an SBOM is only the first step in properly securing the full software supply chain, and all technologies mentioned in this report must be utilized in conjunction to fully secure the entire software supply chain. While regulatory compliance will absolutely be the driving force behind software supply chain and other security technologies, it is our hope that compliance will only be the starting point of this effort and organizations will go above and beyond the minimum requirements.

Another significant driving factor across multiple verticals in this report is tool consolidation. EMA research from 2024 shows that 45% of organizations stated tool consolidation was their most important factor when considering investments in new tools or solutions. Organizations will continue to seek out more simplified solutions to their existing number of cybersecurity and IT tools.

Looking ahead, organizations must prioritize investments in AI-powered solutions, data security, and compliance efforts to navigate evolving cybersecurity challenges effectively. By embracing proactive defense strategies and adopting emerging technologies, organizations can strengthen their security posture and mitigate risks in an increasingly complex threat landscape. Cybersecurity and IT budgets may not increase, but changes in the landscape require strategic shifts in investment priorities for the years to come.

If you made it this far, you have undoubtedly been overwhelmed with a significant amount of information, so here is a recap of the five most interesting trends we're predicting for the remainder of 2024 and beyond:

- Increased focus on artificial intelligence and large language models, especially with shifting budget priorities toward AI
- Increased adoption of zero trust across the entire technology stack, including networking and in the cloud
- Increased data-centric security and data privacy, especially driven by increasing compliance regulations
- Increased focus on API security as organizations continue to adopt cloud applications through digital transformation
- Increased focus on identity and email security as business email compromise becomes the dominant attack vector, outpacing ransomware in total business losses and requiring rigorous identity protection

Overall, the cybersecurity industry is poised for continued innovation and transformation, driven by advancements in AI, regulatory mandates, and shifting security paradigms. Organizations that proactively adapt to these changes will be better positioned to safeguard their assets and data against emerging threats and cyber attacks.

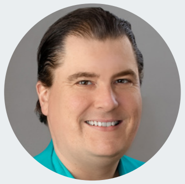
As always, if you'd like to examine these trends or others more in depth, please reach out.

About Cloudflare

Cloudflare, Inc. (NYSE: NET) is the leading connectivity cloud company. It empowers organizations to make their employees, applications and networks faster and more secure everywhere, while reducing complexity and cost. Cloudflare's connectivity cloud delivers the most full-featured, unified platform of cloud-native products and developer tools, so any organization can gain the control they need to work, develop, and accelerate their business. Powered by one of the world's largest and most interconnected networks, Cloudflare blocks billions of threats online for its customers every day. It is trusted by millions of organizations – from the largest brands to entrepreneurs and small businesses to nonprofits, humanitarian groups, and governments across the globe.

IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Christopher M. Steffen, CISSP, CISA
Vice President of Research
CSteffen@enterprisemanagement.com



Ken Buckler, CASP
Research Director
KBuckler@enterprisemanagement.com

Check out the CyberSecurity Awesomeness Podcast:
https://www.cybersecurityawesomeness.com

CYBERSECURITY
AWESOMENESS PODCAST

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT analyst research firm that specializes in going “beyond the surface” to provide deep insight across the full spectrum of IT management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services at www.enterprisemanagement.com or follow EMA on X or LinkedIn.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 www.enterprisemanagement.com

4407.050224