

WHITE PAPER

Securing the Cloud-native Attack Surface with Unified XDR and CNAPP

Gain Greater Context and Efficiency to Mitigate Risk and
Protect Cloud Applications

By Dave Gruber, Principal Analyst; and Melinda Marks, Senior Analyst
Enterprise Strategy Group

August 2023

Contents

Executive Summary.....	3
Security Challenges with Digital Transformation.....	3
The Need to Support Increased IT Complexity.....	3
The Need for Security to Support Digital Transformation with Cloud Adoption.....	5
Challenges with Endpoints and Remote Work.....	7
Suffering a Range of Incidents.....	7
Too Many Siloed Tools and Data.....	8
The XDR Movement Is Helping, but Gaps Exist.....	9
Unifying XDR and CNAPP to Gain Control and Scale.....	10
The Need for Centralized Control.....	10
Incorporating Endpoint Security for Comprehensive Strategy from Desktops to the Cloud.....	12
A More Complete Picture for Software Supply Chain Security.....	12
Speeding Detection and Remediation.....	13
Shifting Up with Uptycs for a Unified Cloud-native Application Protection and XDR Platform.....	14
Conclusion.....	14

Executive Summary

Enterprises today require distributed environments with the prevalence of remote work and use of public cloud services for rapid cloud-native development. They need to support a wider range of infrastructure and services than ever before, including on-premises data centers, private cloud environments, public cloud environments, as well as workstations, endpoint, and mobile devices for employees and consumers. This creates new demands for security to enable employees to work securely and to support the increased scale and productivity of developers building and deploying software applications across multiple cloud providers.

While many security teams have already deployed a wide variety of security tools and solutions, they experience significant delays in data ingest, correlation, and analysis, enabling attacks to advance and carry out malicious objectives before security teams are even aware.

Despite having multiple security tools and platforms in place, organizations often suffer from security incidents because they are not able to act quickly enough to identify and remediate security issues in time to protect their cloud-native applications. They typically use endpoint

security products to secure mobile devices, desktops, and laptops, while leveraging separate products to help developers and DevOps teams secure their code and protect their applications running in cloud environments. They also use solutions like Security Information and Event Management (SIEM) or Security Orchestration Automation and Response (SOAR) solutions to go through event logs to help them detect, analyze, and respond to threats.

While these approaches are helping provide additional visibility into more complex threats, most organizations operate in siloes, requiring the transport, aggregation, and correlation of massive amounts of data and resulting in detection and response activity delays. Precious time wasted often results in further threat progression, leading to unnecessary operational and financial impact. A more efficient and effective approach is needed to eliminate these delays.

Modern attack techniques often have multiple asset types, leveraging endpoints to gain a foothold and acquire privileges, while moving laterally to cloud resources to access valuable assets. While many security teams have already deployed a wide variety of security tools and solutions, they experience significant delays in data ingest, correlation, and analysis, enabling attacks to advance and carry out malicious objectives before security teams are even aware.

Instead of operating separate mechanisms for cloud-native application protection (CNAPP) and extended detection and response (XDR), a unified approach can overcome these delays, providing visibility into early-stage attacks and enabling security teams to stop attack progression before critical resources are impacted.

A unified platform further breaks down silos and shares data across development, IT, and operations teams. This approach provides security teams with a more timely and complete picture and context to better understand vulnerabilities, exposures, and attacks in motion, enabling them to more efficiently and effectively mitigate risk and protect cloud-native applications.

Security Challenges with Digital Transformation

The Need to Support Increased IT Complexity

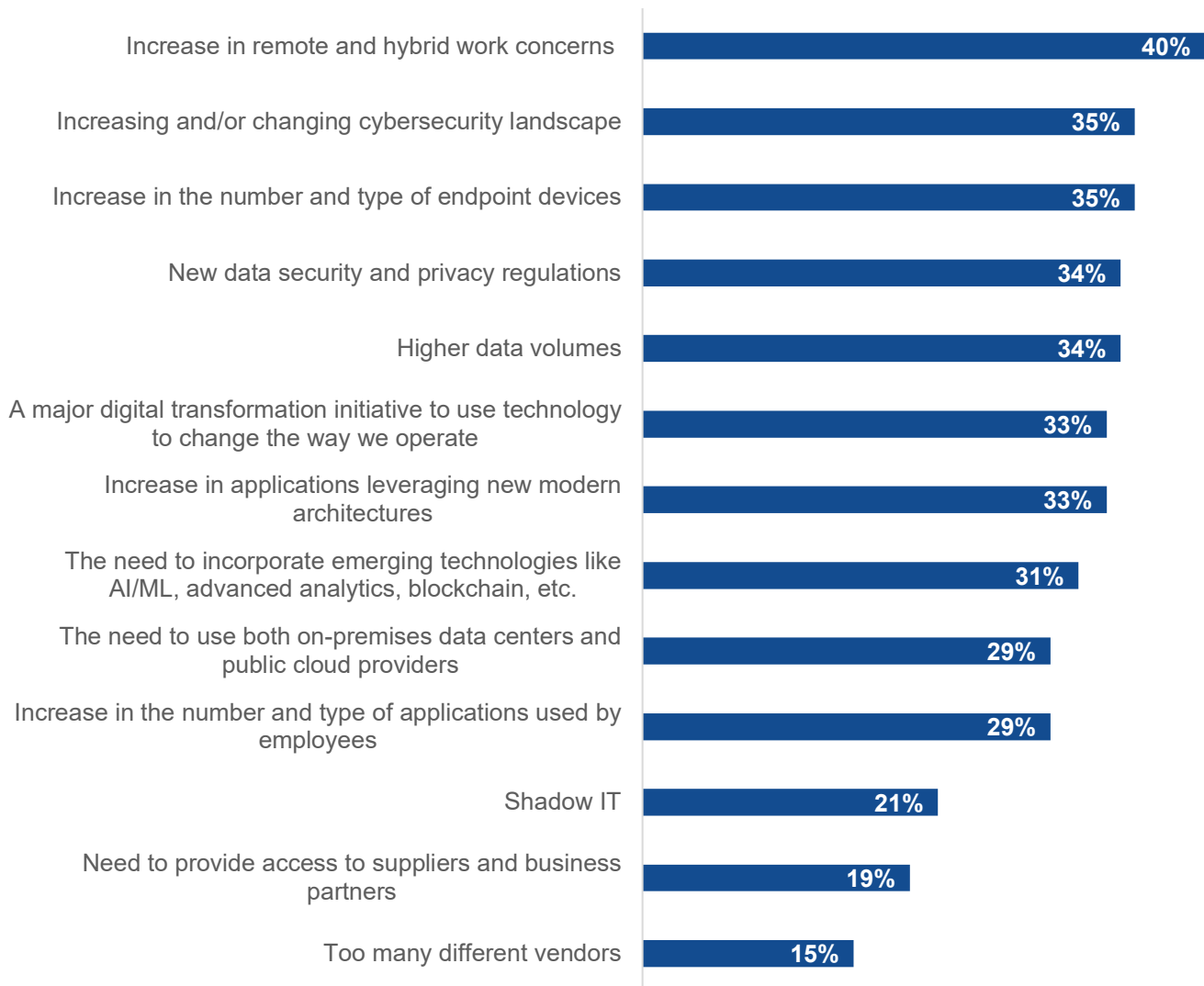
As organizations leverage digital transformation to increase productivity and gain a competitive advantage, increased complexity and new demands on IT and security emerge. TechTarget's Enterprise Strategy Group

research shows that more than half (53%) organizations say their IT environment is more complex or significantly more complex than it was two years ago.¹

In those organizations, the most commonly cited reason for the added complexity, cited by 40% of respondents, is the increase in remote and hybrid work. The top five most commonly cited reasons for increased complexity in IT environments also include the increasing or changing cybersecurity landscape (35%), an increase in the number and type of endpoint devices (35%), new data security and privacy regulations (34%), and higher data volumes (34%).²

Figure 1. Biggest Reasons for Increased IT Complexity

What do you believe are the biggest reasons your organization’s IT environment has become more complex? (Percent of respondents, N=392, five responses accepted)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

¹ Source: Enterprise Strategy Group Research Report, [2023 Technology Spending Intentions Survey](#), November 2022.

² Ibid.

Organizations are looking for ways to support growth and scale instead of being challenged or impeded by added complexity.

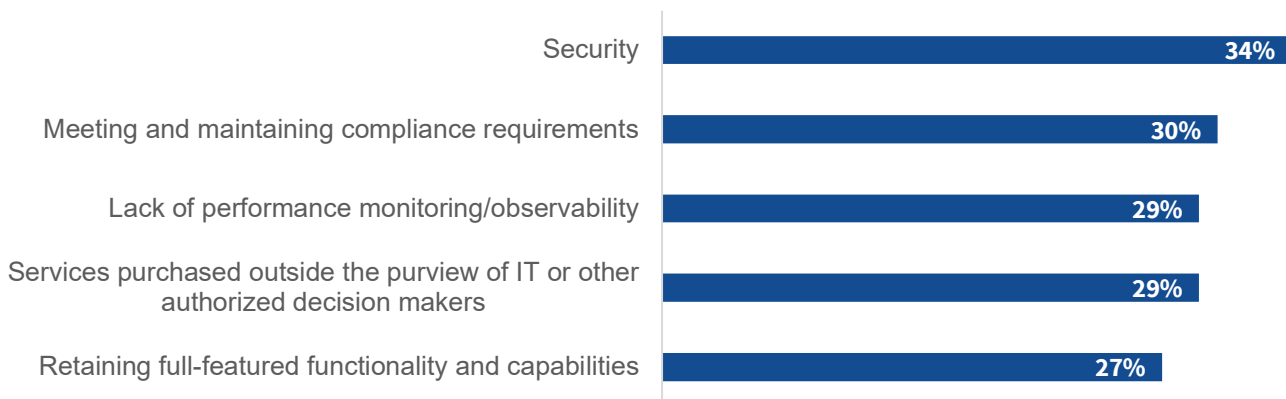
The Need for Security to Support Digital Transformation with Cloud Adoption

Organizations are also increasingly leveraging public cloud infrastructure to increase productivity and innovation with cloud-native development. By moving to cloud-native application development processes, developers can provision their own infrastructure instead of waiting for IT or operations teams to provision servers, enabling them to work efficiently with faster time to value than traditional application development methods.

However, security and meeting and maintaining compliance requirements were the two most commonly cited challenges for organizations with cloud-native applications (see Figure 2).³ With these challenges in mind, organizations need to ensure they can support the rapid growth as development scales.

Figure 2. Top 5 Biggest Challenges for Cloud-native Applications

What are the biggest challenges your organization has faced, or expects to face, with its cloud-native applications? (Percent of respondents, N=387, multiple responses accepted)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

As developers work on their laptops, using continuous integration and continuous deployment pipelines to facilitate collaboration and faster software releases and updates, security teams need to ensure the right tools and processes are in place to effectively mitigate risk.

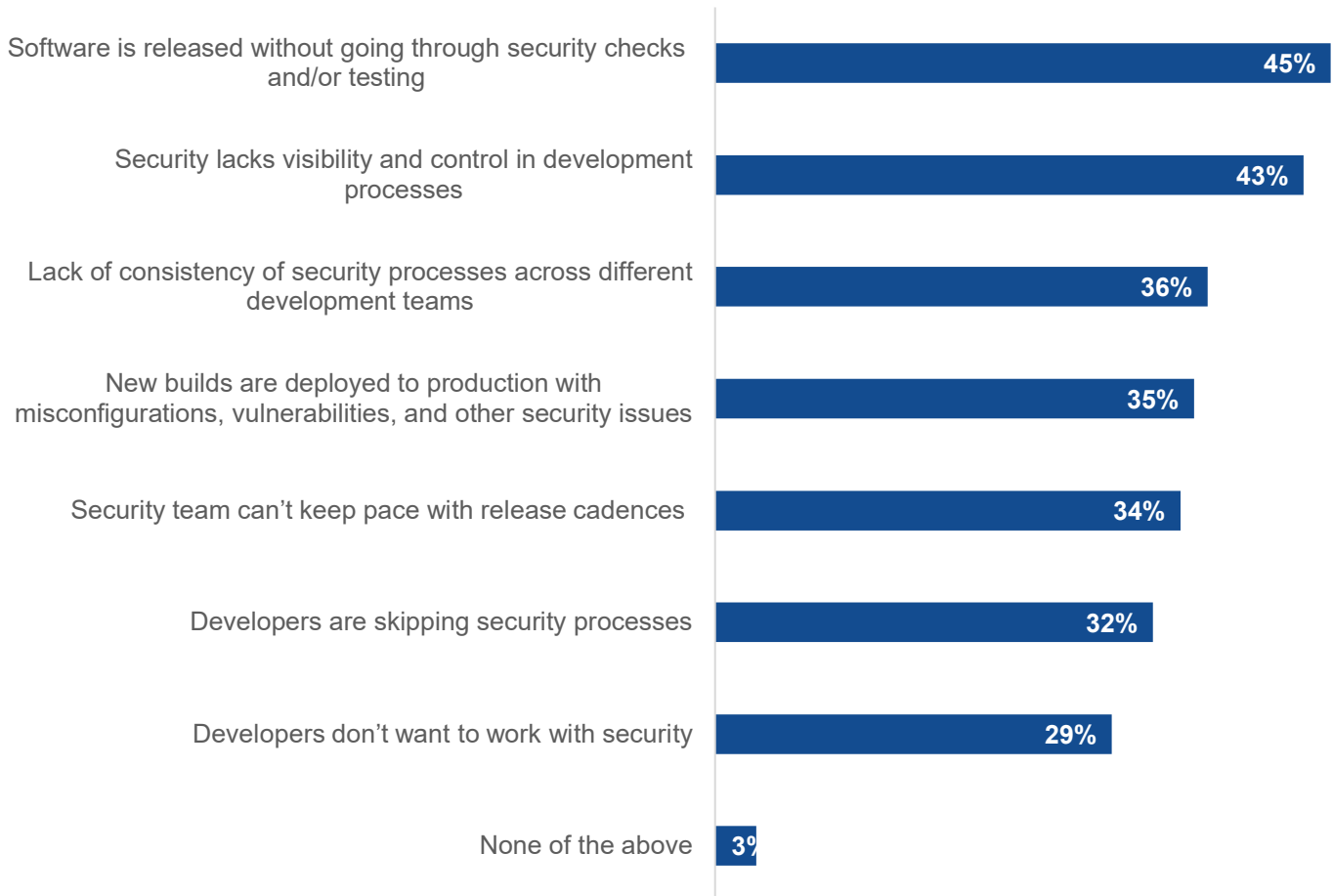
All too often, software is released without going through security checks and/or testing, and security teams often lack visibility and control over what is happening with development (see Figure 3).⁴

³ Source: Enterprise Strategy Group Research Report, [Cloud-native Applications](#), May 2022.

⁴ Source: Enterprise Strategy Group Research Report, [Walking the Line: GitOps and Shift Left Security](#), November 2022.

Figure 3. Security Challenges with Fast Release Cycles

What security challenges does your organization face with faster development cycles of CI/CD? (Percent of respondents, N=350, multiple responses accepted)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Security teams need a better way to scale with modern development, incorporating security processes and tools throughout the development process. It starts with their developer tools, workflows, and collaboration tools on their laptops, ensuring they have secure processes such as single sign-on capabilities for secure access.

They also need to incorporate the right security processes throughout the software development lifecycle (SDLC) in ways that work with developer tools and workflows so it is not disruptive for them to waste time fixing issues out of band. Having the right solutions in place helps security teams better collaborate with developers because the solutions should reduce the time that developers spend on rework or unneeded remediation efforts.

Challenges with Endpoints and Remote Work

Although organizations are increasingly providing flexibility for employees to work remotely using any device, remote work poses challenges for IT and security teams. Enterprise Strategy Group research shows that 70% of employees report interacting with four or more endpoint devices daily to accomplish their work.⁵

These additional devices mean security teams face a growing number of vulnerabilities to assess and manage, challenging 39% of organizations to keep up. In addition, 44% of organizations reported finding systems with open access, and only 43% said that they actively monitor 75% or more of their endpoints, leaving massive blind spots.⁶

This is problematic as development teams grow. Organizations need an effective way to correlate threat activity across developer machines, source code repositories, identity providers, and cloud Infrastructure. However, it takes time and manual effort to analyze data across tools. For example, it is difficult to tie identity information from an IAM solution to audit logs from a developer repository to reveal suspicious behavior as the developer moves code in and out of their repositories and into production.

As a result, endpoint security teams are prioritizing better threat detection and response capabilities and the alignment of their endpoint security strategies with their use of cloud computing services to better keep up. This is the only way for organizations to identify and stop threats before an attacker can access crown jewel data and services in the cloud.

Suffering a Range of Incidents

Although organizations typically have multiple security solutions in place, most of them have experienced security incidents on their cloud-native applications or infrastructure.

Enterprise Strategy Group research on cloud security posture management showed the incidents ranged from access and identity issues, to misconfigurations, to code vulnerabilities, to malware and ransomware (see Figure 4).⁷ These incidents occur either because the organization was unaware of the exposure to risk or because they could not prioritize addressing the issues needing remediation in time to prevent an incident. Organizations need scalable ways to support growth and scale while mitigating security risk to prevent security incidents.

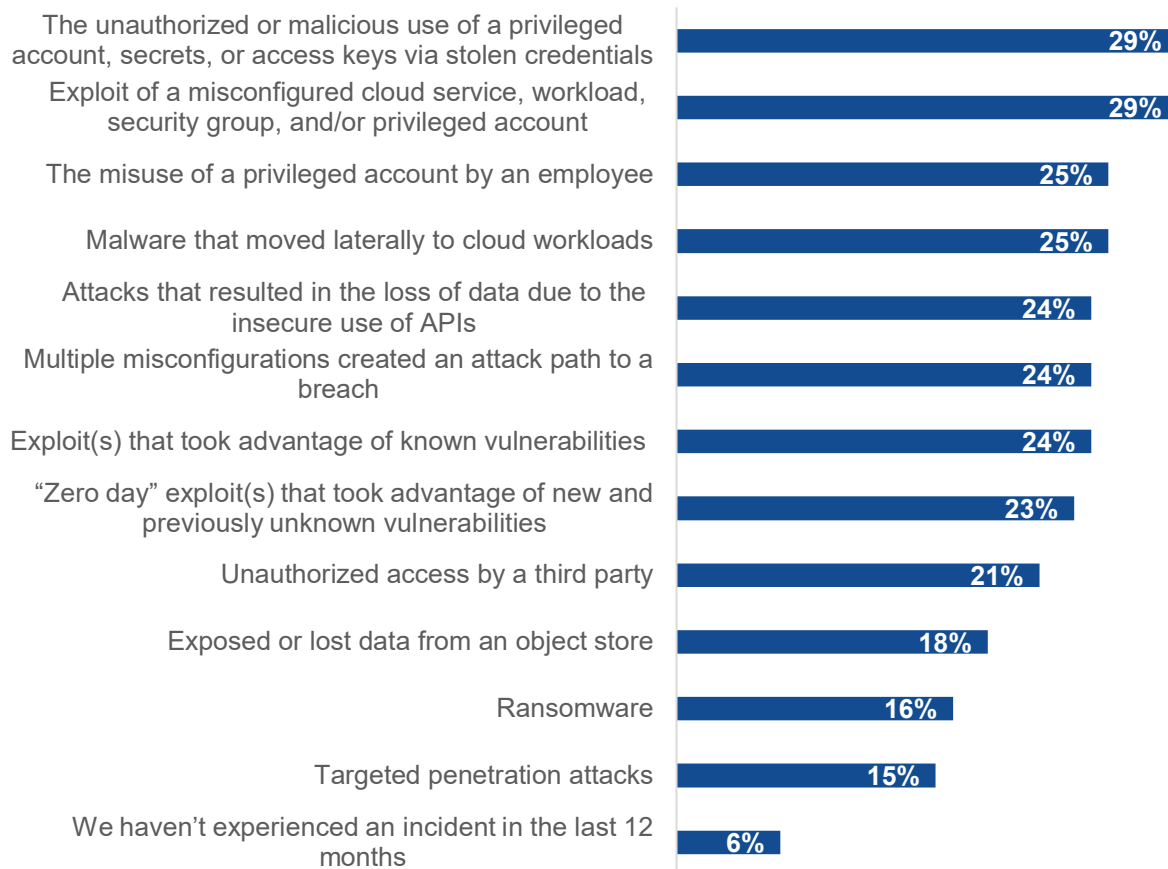
⁵ Source: Enterprise Strategy Group Research Report, [Managing the Endpoint Vulnerability Gap](#), May 2023.

⁶ Ibid.

⁷ Source: Enterprise Strategy Group Complete Survey Results, [Cloud Entitlements and Posture Management Trends](#), March 2023.

Figure 4. Security Incidents on Cloud Infrastructure and Cloud Applications in the Past 12 Months

Which of the following cybersecurity incidents, if any, has your organization experienced in the last 12 months related specifically to cloud-native applications and infrastructure? (Percent of respondents, N=383, multiple responses accepted)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Too Many Siloed Tools and Data

Another challenge is that organizations often use multiple siloed tools, slowing down security operations. While adding security products ensures coverage with testing and monitoring to detect security issues, it doesn’t work for cloud-native application security due to the speed of development cycles and the complexity of how the applications run in cloud environments.

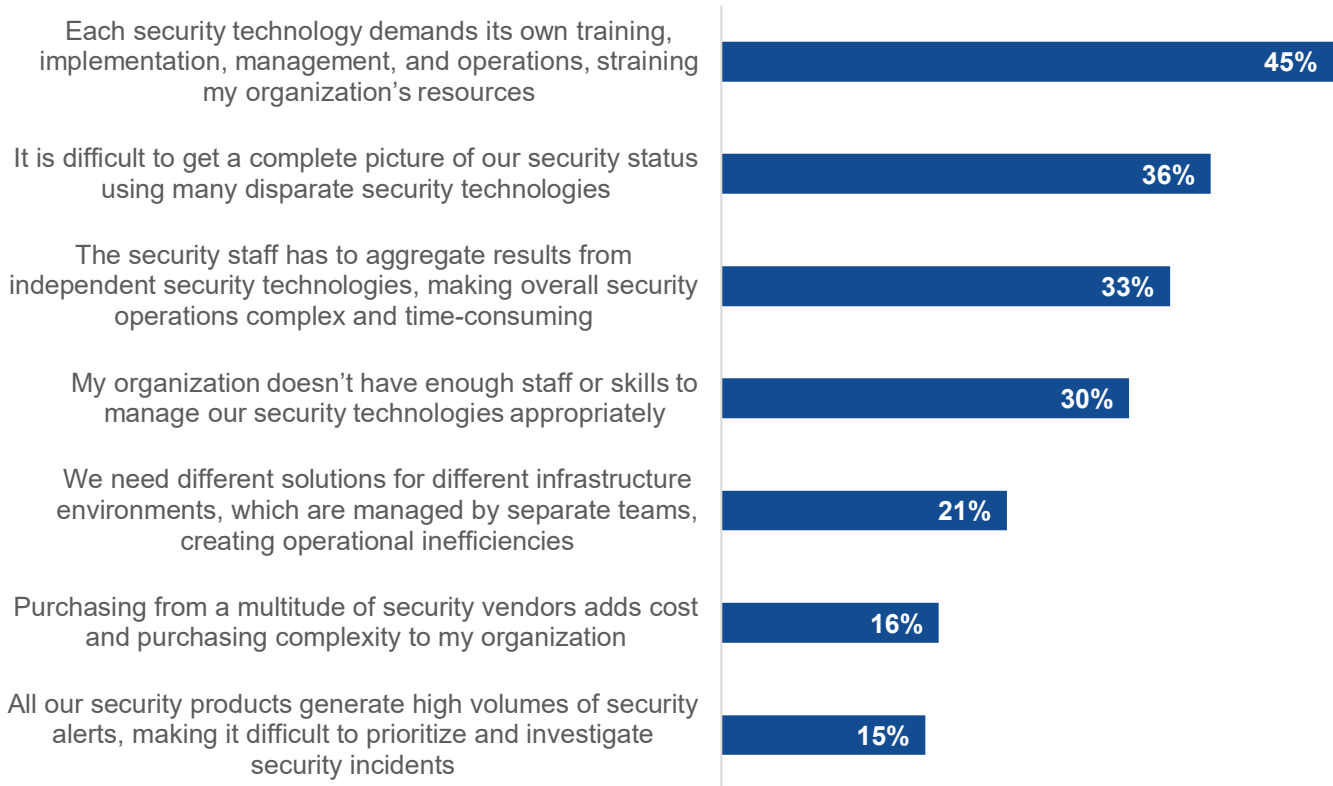
Testing and monitoring can disrupt development processes and/or affect application performance. Also, the ephemeral nature of cloud-native infrastructure and related resources that can be spun up and spun down create monitoring and detection challenges.

Separate tools are often built in different languages, making it difficult to integrate them, and they each generate alerts and/or false positives that are difficult to prioritize. They also bring more challenges (see Figure 5), including requiring training and time to deploy and manage them.⁸

⁸ Source: Enterprise Strategy Group Complete Survey Results, [ESG/ISSA Cybersecurity Process and Technology Survey](#), June 2022.

Figure 5. Management Challenges with Multiple Security Products

**Which of the following represent the biggest challenges associated with managing an assortment of security products from different vendors?
(Percent of respondents, N=280, three response accepted)**



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The security industry has a long history of tools convergence, as innovative new security solutions emerge to address new IT innovations. As these solutions gain traction and mature, opportunities to integrate with adjacent technologies emerge, resulting in the convergence of capabilities. Converged solutions frequently result in both efficacy and efficiency gains.

CNAPPs are one example of this trend, combining CSPM and CWPP solutions into a more integrated approach. XDR is another great example, converging EDR, NDR, CDR, and other DR solutions and driving improved detection and response capabilities over prior approaches such as SIEM.

The XDR Movement Is Helping, but Gaps Exist

The XDR movement was born out of a need for better visibility across an increasingly more distributed and diverse attack surface that attackers leverage to evade siloed security controls and analytics. Traditional detection and response mechanisms, such as endpoint detection and response (EDR) and network detection and response, cannot independently recognize these more complex and behavioral-based threats.

As XDR solutions mature, many face challenges in aggregating, correlating, and analyzing massive amounts of security telemetry in time to identify and stop threats underway. While providing significant value over siloed solutions, many struggle to keep up, allowing attacks to cause more damage than they should.

Research shows that gaps in cloud visibility top the list for where early XDR investments are focused. Yet EDR data is reported as one of the most valuable in detection and response activities.⁹ Analyzing endpoint and cloud telemetry, and other valuable signals from network, identity, and code repositories helps security teams gain early visibility as attacks emerge. Further adding risk data, including vulnerability and risk classification, helps security teams focus on the more important threats first.

Unifying XDR and CNAPP to Gain Control and Scale

Instead of holding organizations back and making it harder for security teams to manage multiple siloed tools as attack surfaces grow, a unified solution is needed to gain control, mitigate risk, and respond quickly to threats or attacks. CNAPPs help unify multiple cloud security capabilities, including cloud workload protection (CWP), cloud security posture management (CSPM), and cloud infrastructure entitlement management (CIEM). The concept behind moving to CNAPPs is to utilize the information across different areas to gain better context and understanding to prioritize remediation actions, speeding response because it minimizes the time needed for analysis across tools or alert triage.

But it misses a key area: developer workstations or laptops as they connect to the cloud. A unified CNAPP and XDR approach gives security teams the visibility and control they need to drive efficient remediation to effectively manage risk as they enable secure digital transformation to drive better business results.

The Need for Centralized Control

Enterprise Strategy Group research shows that organizations face challenges when attempting to gain the visibility and control they need to manage risk across environments and teams effectively. These include effectively managing standardized controls and policies, managing access, gaining visibility and control into development processes, gaining visibility into public cloud infrastructure, and better understanding cloud-native threats (see Figure 6).¹⁰

The research also showed how organizations are looking for ways to drive efficiency to enable security to scale to support cloud-native development. They need the right platform to assemble the data and perform the analysis needed for security teams to reduce time spent on tedious, manual tasks and focus on efficient actions that reduce risk to support growth and scale. 85% of organizations believe a CNAPP will give them a more efficient way to mitigate risk, and 87% believe a CNAPP will help drive efficiency in connecting application security processes to security posture management.¹¹

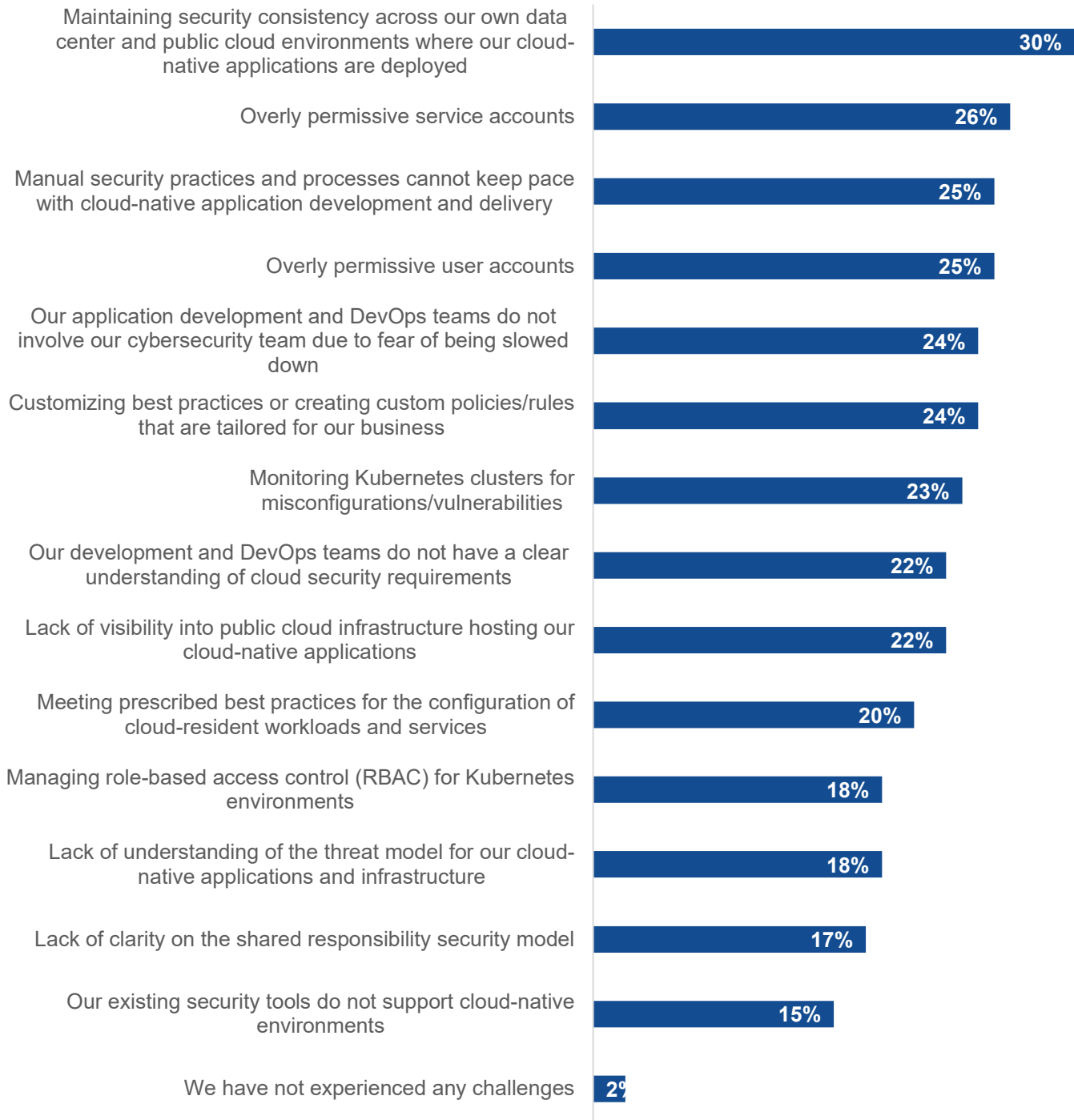
⁹ Source: Enterprise Strategy Group Research Report, [The Impact of XDR in the Modern SOC](#), March 2021.

¹⁰ Source: Enterprise Strategy Group Research Report, [Cloud Entitlements and Posture Management Trends](#), November 2022.

¹¹ Ibid.

Figure 6. Top Cloud Security Challenges Require Gaining Consistency, Visibility, and Control

Which of the following represent the biggest cloud security challenges for your organization? (Percent of respondents, N=383, multiple responses accepted)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

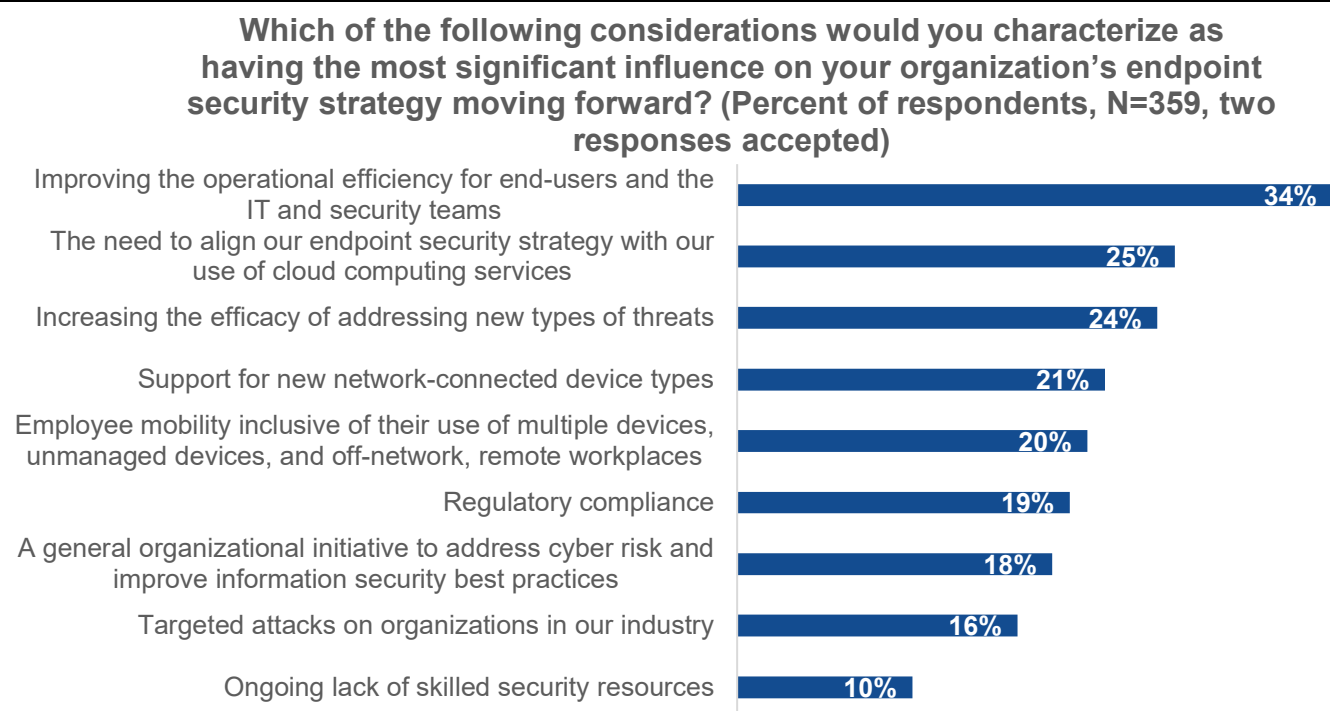
Incorporating Endpoint Security for Comprehensive Strategy from Desktops to the Cloud

While organizations look to CNAPPs to provide more context to drive efficiency and reduce risk, incorporating XDR and endpoint security provides more visibility for a more complete picture.

Securing workstations and laptops is critical to managing risk with rapidly scaling development teams and remote work. Using a platform approach with a unified data model helps map out potential attack paths to help security teams better understand their threat exposure.

As organizations plan to consolidate tools, it will drive operational efficiency with an aligned strategy from code to cloud and increase the efficacy of addressing threats (see Figure 7).¹²

Figure 7. Considerations with the Most Significant Influence on Organization’s Endpoint Security Strategies



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

A More Complete Picture for Software Supply Chain Security

A platform combining cloud-native application protection and XDR can also help security teams gain visibility and control of software supply chain issues. As developers utilize third-party code and resources, including consultants, integrations, and connections to other APIs, XDR expands the abilities of a CNAPP to give security teams visibility and control of the software supply chain.

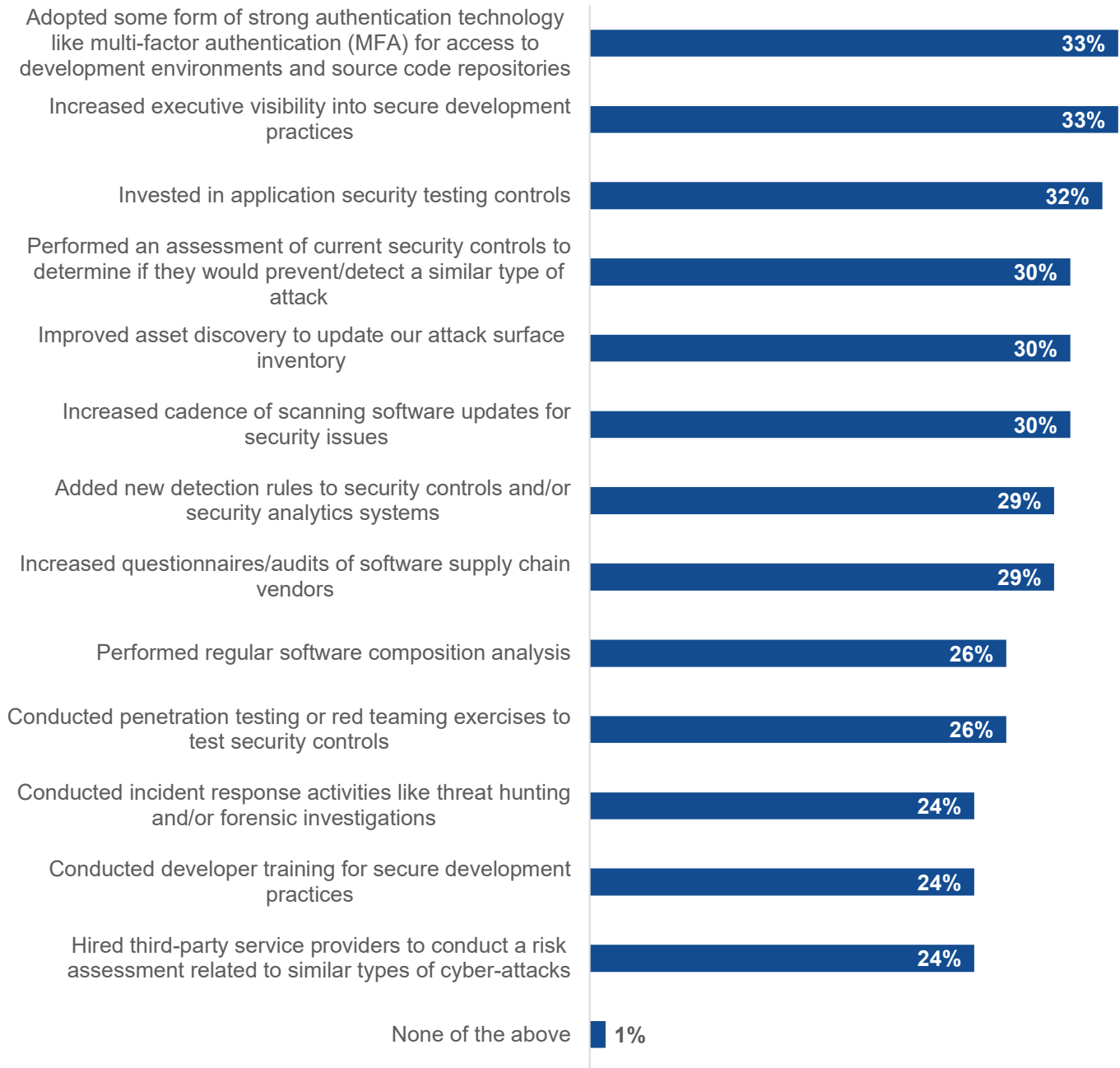
With the increase in software supply chain attacks, organizations are taking a wide variety of actions to better protect their cloud-native applications (see Figure 8).¹³ Combining CNAPP and XDR helps organizations gain better and more timely visibility into the assets, components, users, and remote access used within the software supply chain.

¹² Source: Enterprise Strategy Group Complete Survey Results, [Endpoint Security Trends](#), December 2021.

¹³ Source: Enterprise Strategy Group Research Report, [Walking the Line: GitOps and Shift Left Security](#), November 2022.

Figure 8. Actions Taken as a Result of Software Supply Chain Attacks

Which of the following actions has your organization taken because of recent software supply chain attacks? (Percent of respondents, N=350, multiple responses accepted)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Speeding Detection and Remediation

The key to effective cloud-native security is driving operational efficiency. Organizations should look to improve the two key metrics: mean time to detection and mean time to remediation.

This enables organizations to effectively mitigate risk with efficient remediation and to respond to threats and attacks quickly. A centralized platform with a unified data model can drive that efficiency from context and understanding that spans endpoints, where code is developed, to the cloud, where applications are deployed.

Shifting Up with Uptycs for a Unified Cloud-native Application Protection and XDR Platform

Uptycs helps organizations secure the modern attack surface utilizing a single data model. By streaming normalized data up into a data lake, Uptycs takes a “shift up” approach that delivers connected insights, control, and operational efficiency for security teams to effectively manage risk.

The Uptycs model provides:

- **A unified platform** with consolidated XDR and CNAPP capabilities, including cloud security posture management, cloud workload protection, Kubernetes and container security, cloud detection and response, identity analytics, cyberasset inventory, audit, and compliance.
- **Visibility and control** from endpoints to cloud environments, from where the code is developed to where it is deployed.
- **Normalized telemetry** with data collected from multiple sources, normalized, and streamed into a data lake for analytics processing.
- **Powerful analytics engine** using activity and flow logs and enabling security teams to enforce least-privilege policies, detect threats, and investigate incidents.

With a unified platform, organizations benefit from:

- Increased collaboration across teams.
- Increased operational efficiency, reducing manual work and analysis.
- Faster, more effective threat detection and response.
- A more complete picture of security posture that includes endpoints.
- Reduction in operating costs, including faster deployment and simplified management.

Conclusion

Moving to modern software development processes that leverage cloud services gives organizations a competitive advantage, but security teams need to support the growing attack surfaces as development scales to drive better business results.

Organizations have experienced challenges while managing risk and meeting compliance regulations, as their traditional security solutions and approaches are disruptive to cloud-native development processes and are often ineffective in complex cloud environments. Further, the use of multiple siloed tools requires more time to operate, manage, and analyze results, while adding delays in critical remediation actions.

While organizations are looking to CNAPP solutions to help drive remediation efficiency and better coordinate security processes for developers across the SDLC, organizations should look at Uptycs' approach to unifying CNAPP and XDR. The “shift up” approach provides a more complete picture of security risk from endpoints, where code is created, to the workloads in cloud environments, where software applications are deployed. Leveraging a unified data model, Uptycs helps security teams effectively and efficiently mitigate risk as cloud-native development activities continue to scale.

©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.


Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.

About Enterprise Strategy Group

TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

 contact@esg-global.com

 www.esg-global.com