2023

STATE OF SECURITY REPORT

Forcepoint

INTRODUCTION

Organizations are experiencing significant cybersecurity challenges intensified by rising threat levels, new attack vectors, hybrid work environments, and the continued shortage of skilled cybersecurity professionals.

The 2023 State of Security Report surveyed over 340 cybersecurity professionals from North America to reveal the key challenges cybersecurity teams are facing, how they solve cyber issues, and the security technologies organizations prioritize.

Key findings include:

- 84% of companies feel cybersecurity policy management has become more difficult. One key reason is policy sprawl, as it increases the complexity of security and meeting compliance.
- 84% of companies report security alerts are becoming increasingly overwhelming as more security tools are added to the mix. This adds to the desire to consolidate tools and dashboards to introduce simplicity and increase control and visibility.
- Nearly half of all companies (44%) believe consolidated platforms will be the most effective approach to security over the next decade.
- The top three benefits companies have gained after adopting Zero Trust are secure user access (35%), simplified security controls (19%), and malware prevention (15%).
- One in three companies believes simplified security functionality is the top benefit of SASE (33%).

We would like to thank Forcepoint for supporting this important industry research. We hope you find this report helpful as you continue your efforts to protect your organizations against evolving threats.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

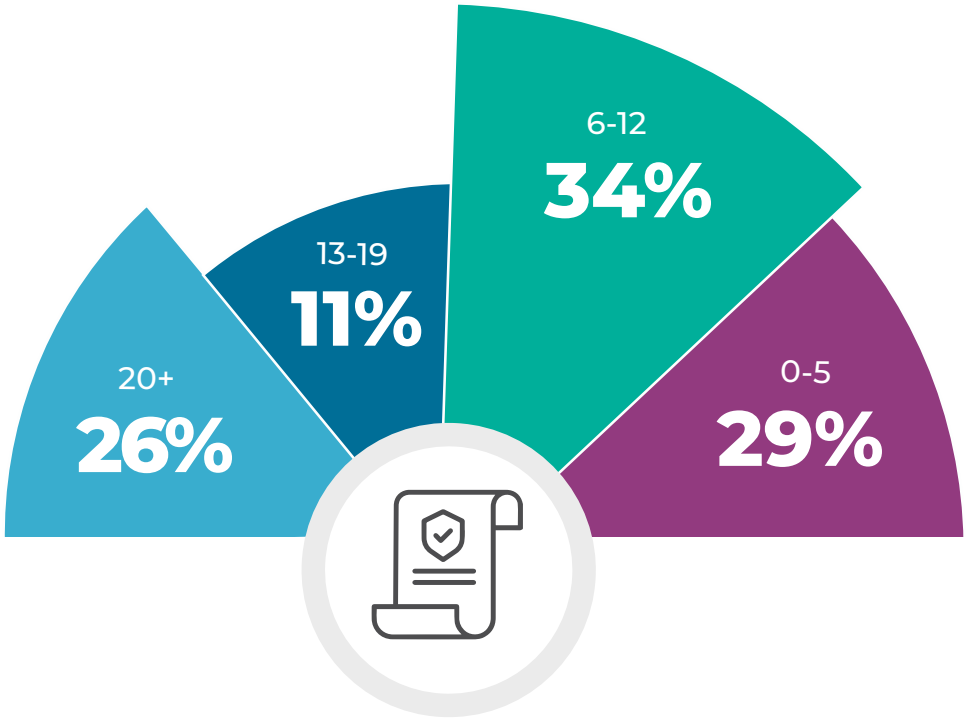
Cybersecurity
INSIDERS

SECURITY POLICY MANAGEMENT

Eighty-four percent of companies report that managing cybersecurity policy across the entire cybersecurity stack has become more difficult. One key reason is policy sprawl, as it increases the complexity of security and meeting compliance. Approximately one in four companies (26%) juggles over 20 security policies across the web, and public and private clouds.

Based on your organization's experience over the last few years, do you agree or disagree with the following: Managing policies across the entire cybersecurity stack has become more difficult.

How many security POLICIES does your organization have in place to secure access to and protect data in private and public cloud apps, and the web?



SECURITY INTEGRATION AND VISIBILITY

Lack of visibility is a perennial problem for cybersecurity teams. It is further exacerbated by the proliferation of tools that often don't integrate with each other, making it difficult to get full visibility of security issues. Eighty-seven percent of companies confirm they can't get the security visibility they need due to lack of integration.

Based on your organization's experience over the last few years, do you agree or disagree with the following:

Not all of our security tools integrate fully with each other, making it difficult to get full visibility of potential security issues.

Alert fatigue due to false positives is a real problem for cybersecurity teams. Additional security tools compound this issue, adding more alerts and dashboards to the mix. This clearly overwhelms the vast majority of cybersecurity professionals in our survey (84%) and adds to the desire to consolidate tools and dashboards to introduce simplicity and increase control and visibility.

The number of security alerts you receive gets more overwhelming depending on the number of security tools you use.

INSTITUTIONAL KNOWLEDGE AND STAFFING

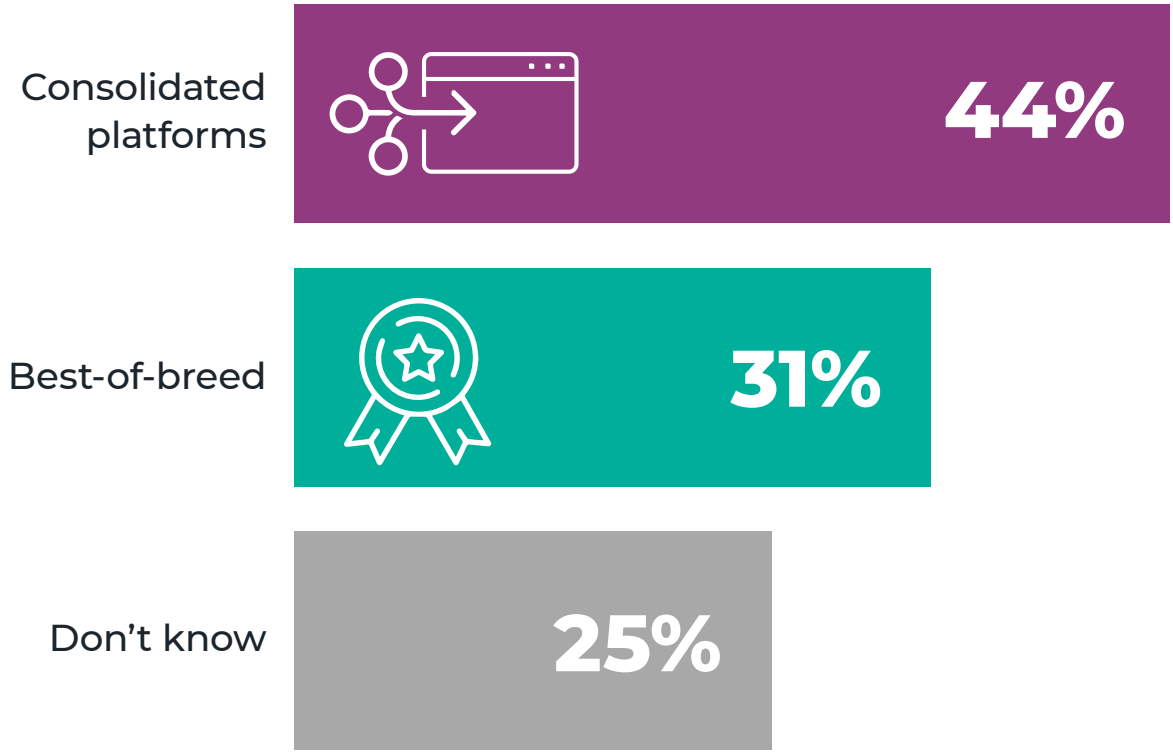
Employee turnover has increased significantly in recent years, negatively affecting organizations with an already understaffed security workforce. Over half of all companies (56%) believe security employee turnover has disrupted their planned security integrations and migrations due to a drain of institutional knowledge.

Has security employee turnover materially impacted any of your planned security integrations or migrations due to a lack of institutional knowledge or the need to upskill new hires?

BEST-OF-BREED VS PLATFORM

Nearly half of organizations (44%) believe consolidated platforms will be the most effective approach to security over the next decade as vendor consolidation initiatives gain momentum. The best-of-breed approach, in contrast, increases complexity and SOC workload especially when there is a lack of skilled security professionals and the need for better control over, and visibility into, the IT environment.

Do you believe that best-of-breed OR consolidated platforms will be the most effective approach to security over the next decade?



ZERO TRUST ADOPTION

We asked cybersecurity professionals about their adoption of Zero Trust - a security framework requiring all users to be authenticated, authorized, and continuously validated before being granted access to applications and data.

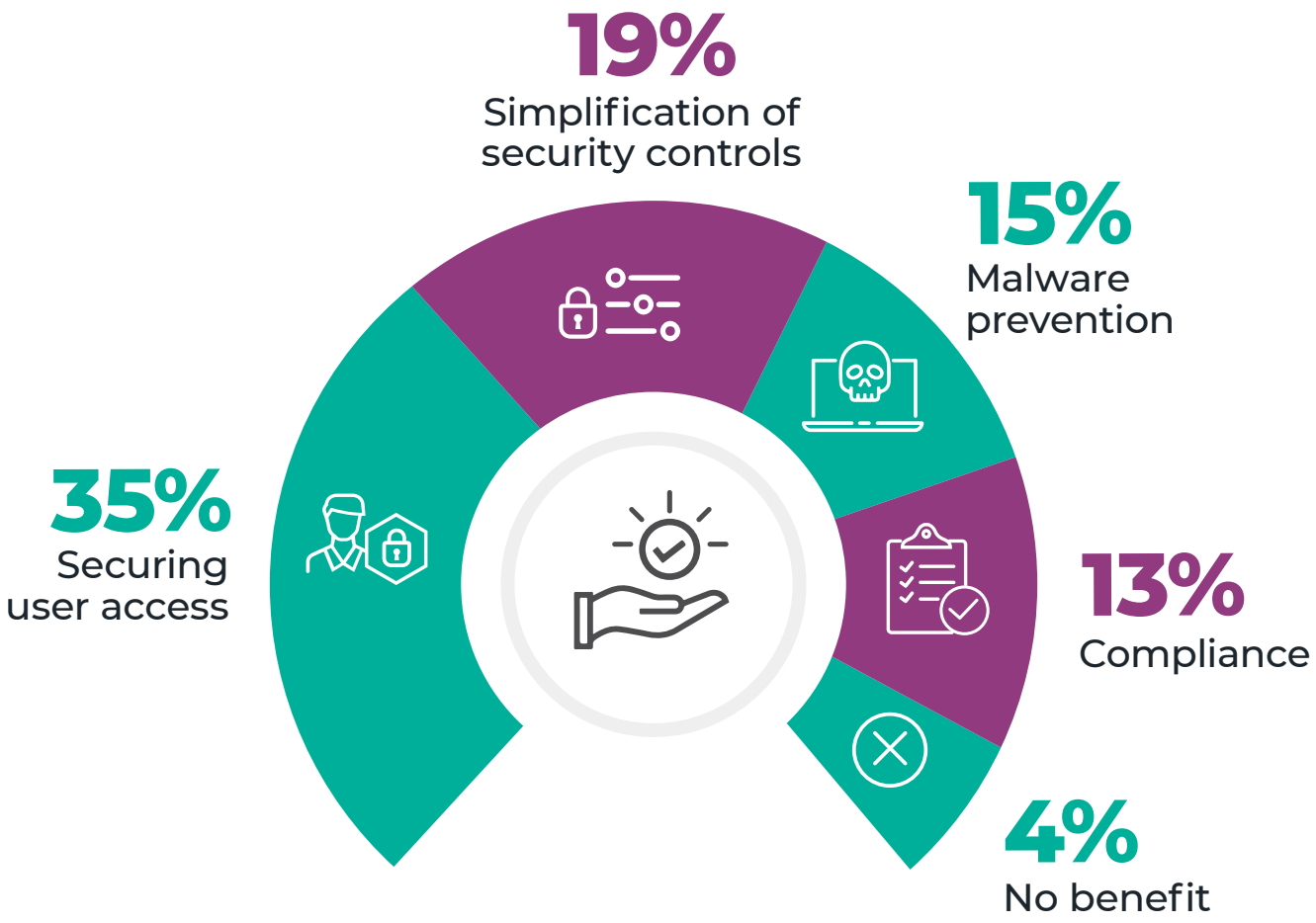
Three quarters of organizations confirm they are using elements of Zero Trust or are planning to do so (76%).

Has your organization adopted or does it plan to adopt elements of Zero Trust?

ZERO TRUST BENEFITS

Cybersecurity professionals in this survey report a variety of primary benefits from Zero Trust, including secure user access (35%), simplification of user controls (19%), and malware prevention (15%).

What is the primary benefit you have gained with Zero Trust?



We have not adopted Zero Trust 10% | I am not sure what Zero Trust is 2% | Other 2%

ZERO TRUST AND CYBERTHREATS

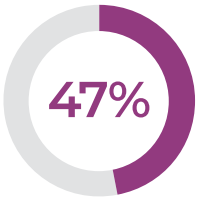
Zero Trust has the capacity to address a variety of security threats facing organizations, including compromised access (69%), insider threats (56%), and data theft (53%).

What threat(s), if any, do you believe Zero Trust has the potential to eliminate?

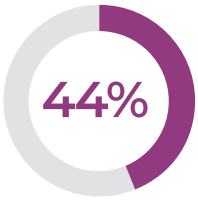
69%
Compromised access

56%
Insider threat

53%
Data theft



Cyberespionage



Ransomware

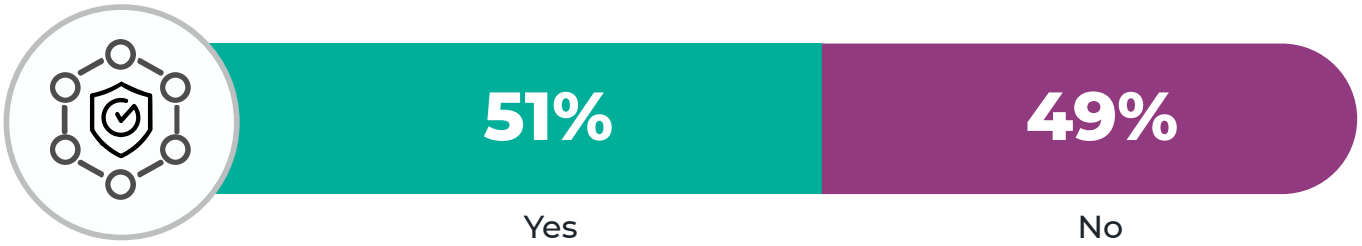
Malware attacks

I don't believe Zero Trust will eliminate threats 16% | I am not sure what Zero Trust is 7% | Other 4%

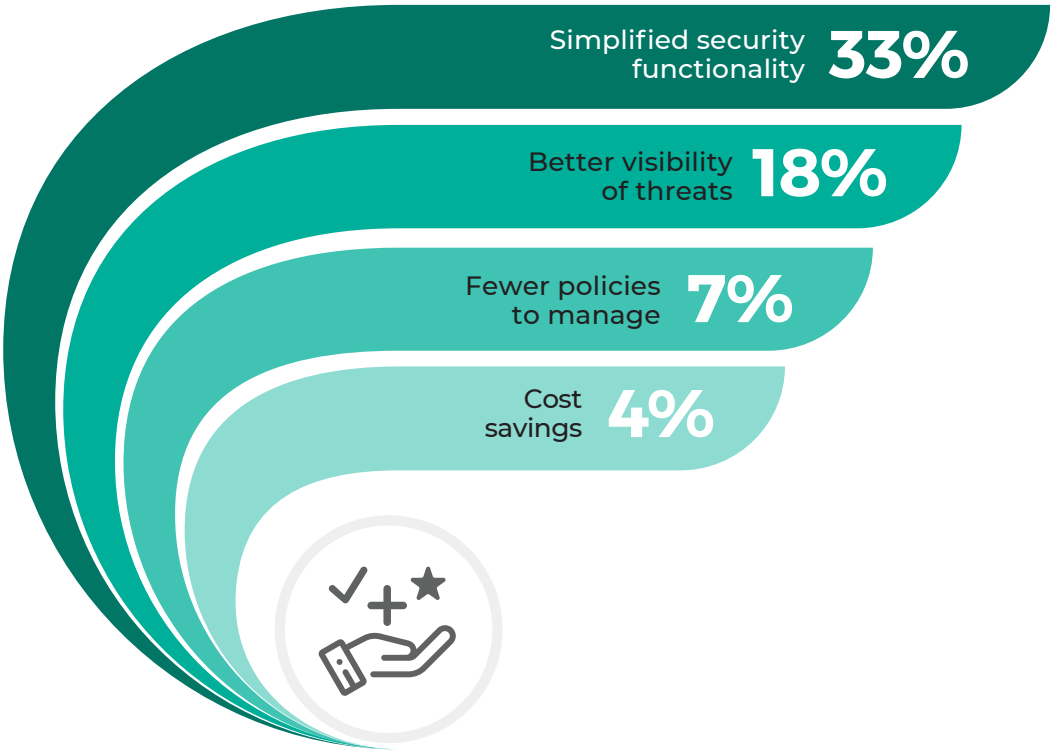
SASE ADOPTION AND BENEFITS

We asked cybersecurity professionals whether their organization adopted (or is planning to adopt) Secure Access Service Edge (SASE). The results are closely split, with a majority of 51% adopting SASE.

Has your organization adopted or does it plan to adopt elements of Security Access Service Edge (SASE)?



What benefits have organizations realized from deploying SASE? Simplified security functionality tops the list of benefits (33%), followed by better visibility into threats (18%) and fewer policies to manage (7%).



We have not adopted SASE 29% | Other 9%

MACHINE LEARNING IN SECURITY

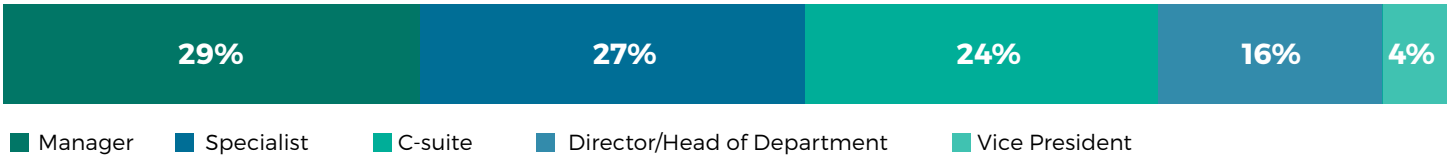
We asked cybersecurity professionals whether their organizations are utilizing machine learning to gain insights about user behavior to inform data security policies. Two-thirds (67%) confirmed that their organization is using or planning to use machine learning in their security stack to adapt to emerging threats and to adapt ATA security to risky user behavior.

Is your organization using or does it plan to use machine learning to apply insights about user behavior to data security policies?

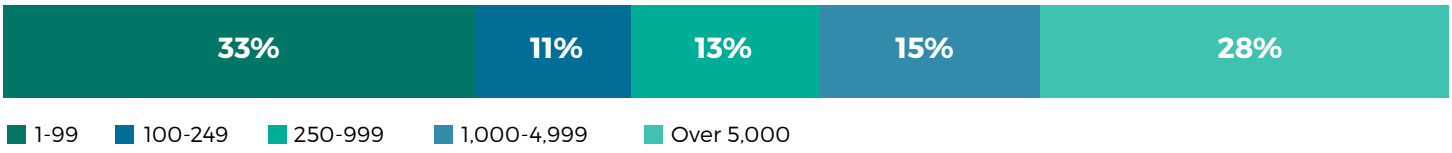
METHODOLOGY & DEMOGRAPHICS

The 2023 State of Security Report is based on a comprehensive survey of 340 cybersecurity professionals from North America conducted in September 2022. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

CAREER LEVEL



COMPANY SIZE



INDUSTRY

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries.

Engage with Forcepoint on Twitter and LinkedIn.

www.forcepoint.com

Cybersecurity INSIDERS

Cybersecurity Insiders is a 500,000+ member online community for information security professionals, bringing together the best minds dedicated to advancing cybersecurity and protecting organizations across all industries, company sizes, and security roles.

We provide cybersecurity marketers with unique marketing opportunities to reach this qualified audience and deliver fact-based, third-party validation thought leadership content, demand-generation programs, and brand visibility in the cybersecurity market.

For more information please visit **www.cybersecurity-insiders.com**

GET THE MEDIA KIT
or contact us for more details at:
info@cybersecurity-insiders.com