Cybersecurity
INSIDERS

2022

Security Visibility Report

CISCO

INTRODUCTION

As more network traffic from remote users and across data centers, locations, and cloud stacks is encrypted, enterprise IT administrators have increasingly limited visibility into what is happening inside and outside the network. This lack of visibility into security threats is a critical issue for cybersecurity teams, as it degrades the ability to protect systems, identities, applications, and workloads against advanced threats.

This 2022 Security Visibility Report surveyed 278 cybersecurity professionals to reveal the key challenges regarding security visibility, how organizations solve this issue, and the security capabilities organizations prioritize.

Key findings include:

- The biggest visibility challenge for cybersecurity teams is to tell which vulnerabilities are real threats and which will never be exploited by adversaries (41%). This obstacle is closely followed by insufficient visibility into network traffic, especially when that traffic is encrypted (38%).
- The biggest gaps in network visibility are seen in workload traffic (54%), followed by SaaS apps (45%), network-connected devices (42%), and encrypted traffic (35%).

Many thanks to Cisco for supporting this important research project. We hope this report is informative and helpful as you continue your efforts to protect your IT environments.

Thank you,

Holger Schulze

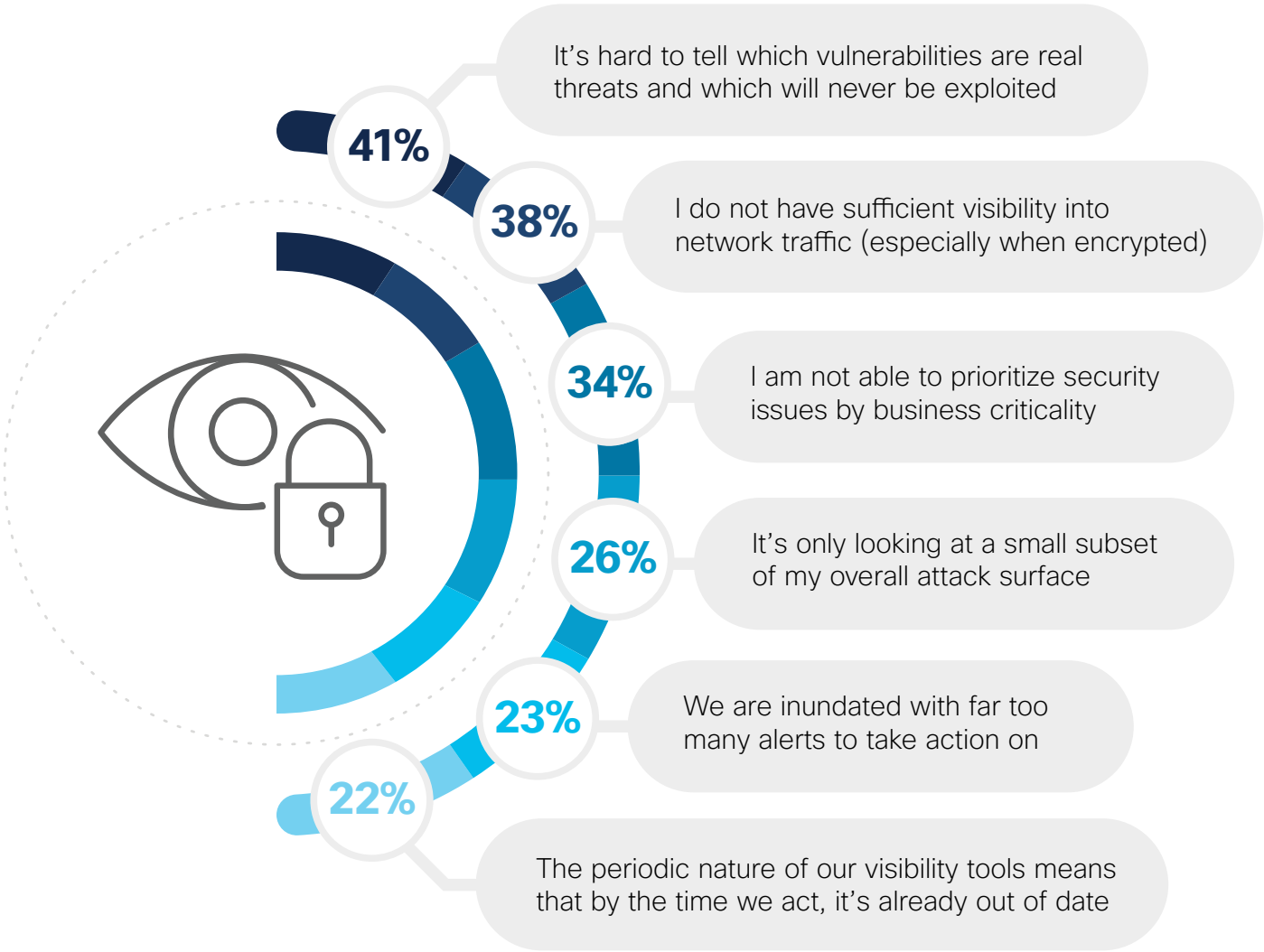
Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

SECURITY VISIBILITY CONCERNS

Limited visibility into security threats is a critical issue for cybersecurity teams, as it hampers the ability to protect systems, identities, applications and workloads. When we asked cybersecurity professionals about their specific concerns with security visibility, the most mentioned challenge is the difficulty to differentiate which vulnerabilities are real threats and which will never be exploited by adversaries (41%). This is closely followed by insufficient visibility into network traffic – especially when that traffic is encrypted (38%) and the inability to prioritize security issues by business criticality (34%).

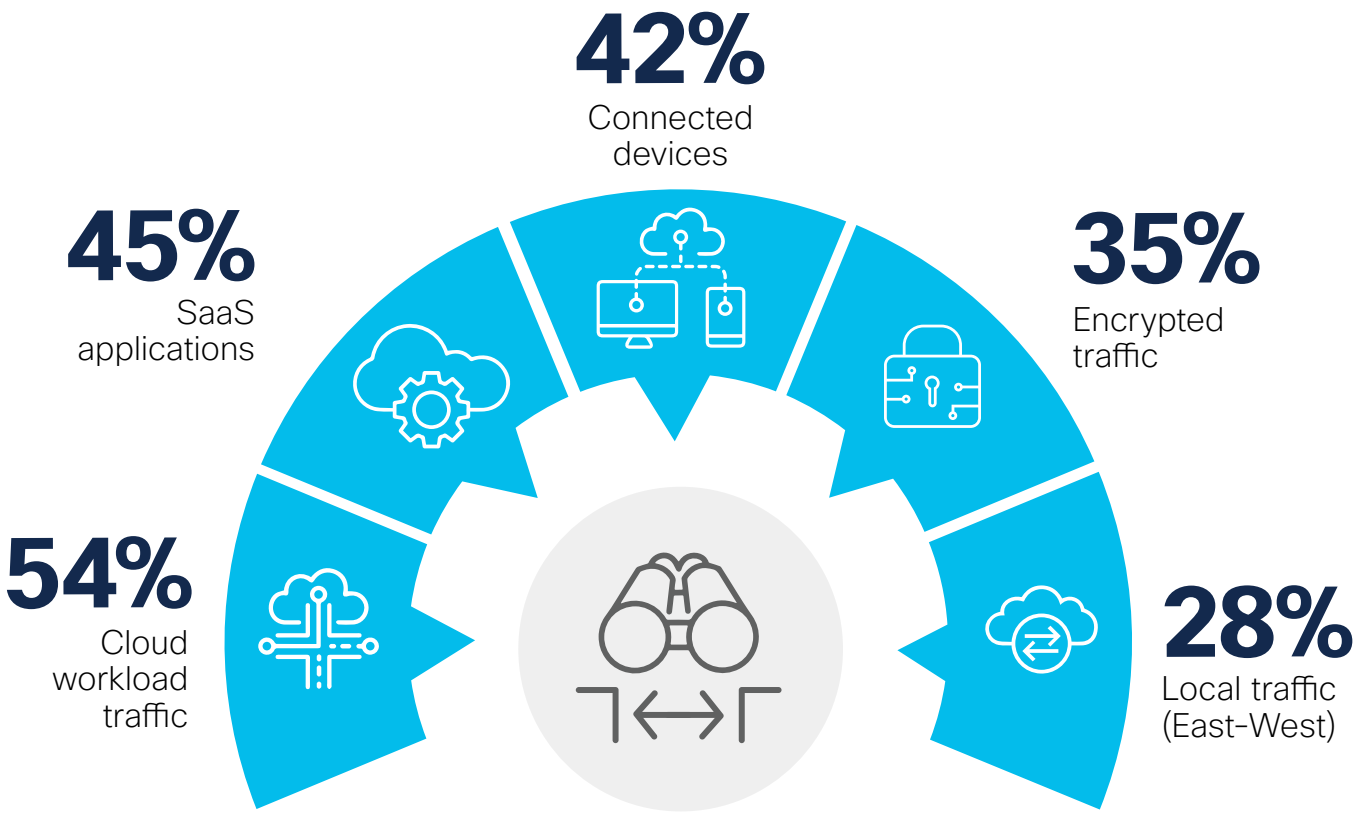
Which of the following concerns do you have about your current security visibility?



NETWORK VISIBILITY GAPS

So where are the biggest gaps in network visibility? Cybersecurity professionals rank workload traffic (54%) as the least visible aspect of networking, followed by SaaS apps (45%), network connected devices (42%), and encrypted traffic (35%).

Where do you have the greatest network visibility gaps?

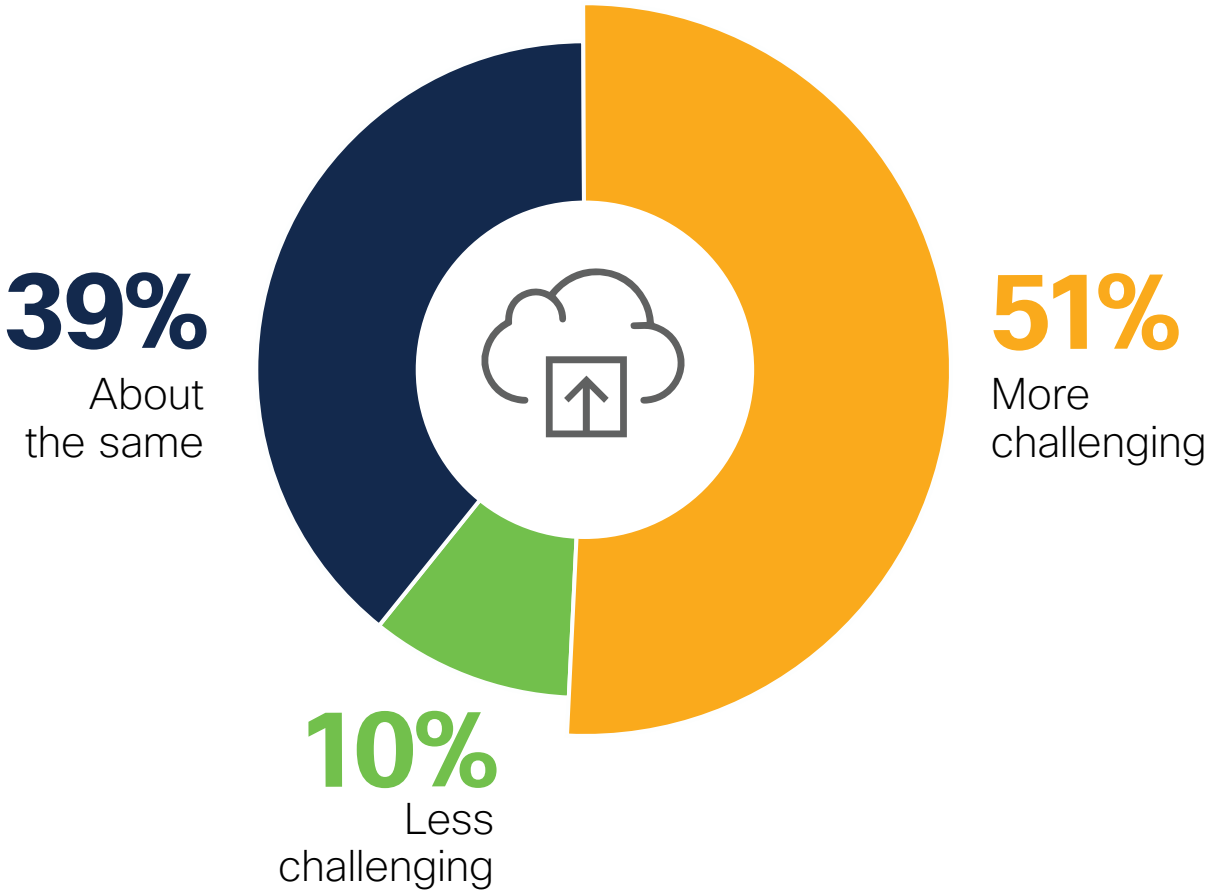


Other 3%

CLOUD VISIBILITY

While the shift to cloud computing delivered significant benefits to organizations, such as improved scalability and ease of deployment, it also created new challenges – network visibility being one of the most critical issues. A majority of cybersecurity professionals (51%) confirm that visibility has become more challenging with the move to the cloud while only 10% see it as less of a challenge.

Has visibility become more challenging with the move to the cloud?



SECURITY CHALLENGES

We asked survey participants what security challenges they are most struggling with. Ransomware (53%) tops the list, following the recent rise in ransomware attacks. he next biggest security challenge is the shift to remote work and the resulting risks (47%), introduced in the wake of the Covid-19 pandemic. Limited visibility into cyber threats (41%) rounds out the top three security challenges experienced by cybersecurity professionals.

What are your biggest security challenges?

53%
Ransomware

47%
Remote workers

41%
Limited visibility

40%
Securing my hybrid on-prem & cloud environment

37%
Inconsistent policy controls

36%
Malware hiding in encrypted traffic

36%
Too many false positives/noise

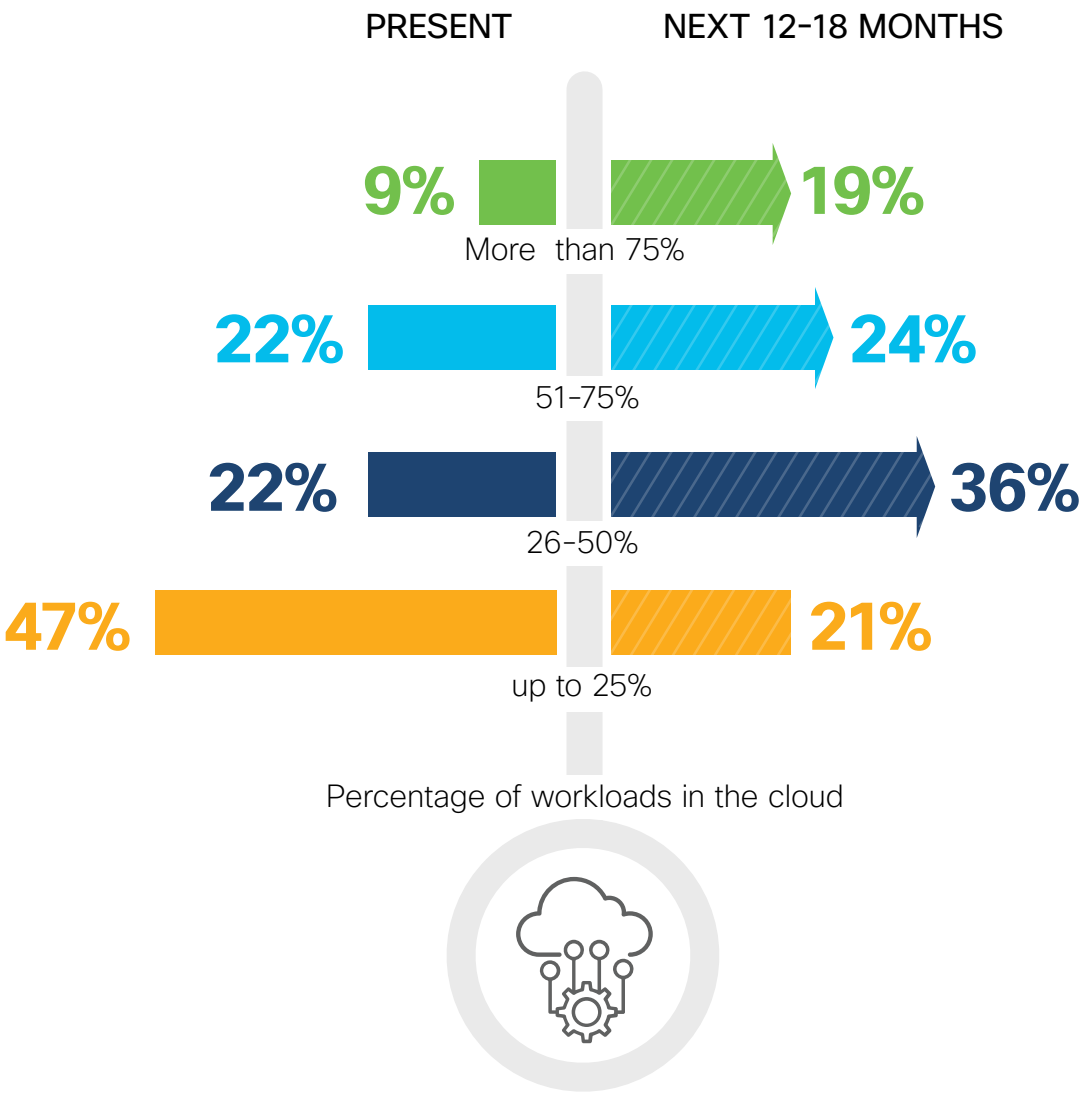
23%
Regaining visibility into that encrypted traffic

Other 1%

CLOUD WORKLOADS

As the shift to cloud continues, a majority of organizations (52%) already have more than a quarter of workloads deployed in the cloud. This is predicted to shift to 79% of organization planning to have more than a quarter of workloads deployed in the cloud in the next 12-18 months.

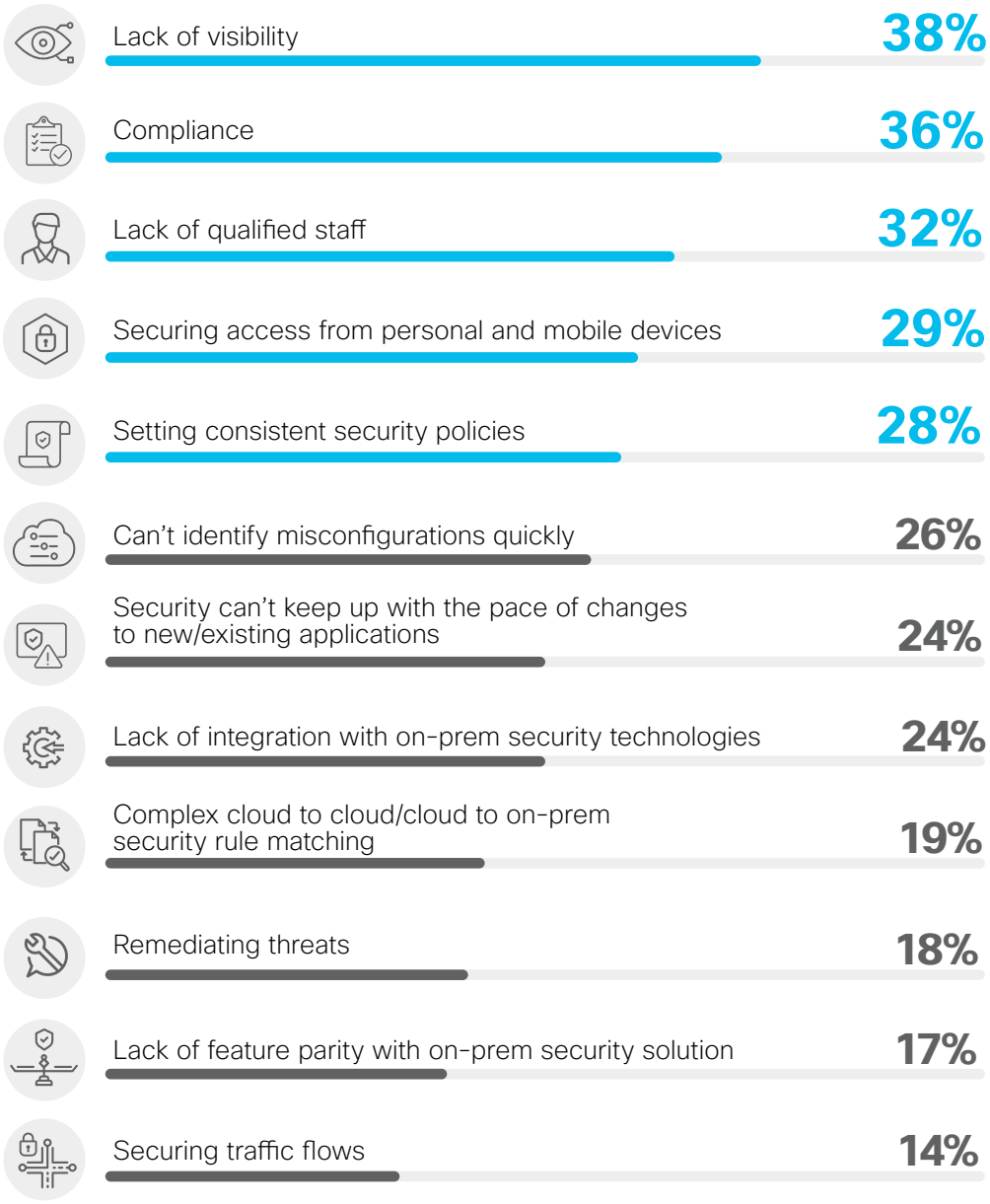
What percentage of your workloads are in the cloud today vs. the next 12-18 months?



CLOUD PROTECTION HEADACHES

Cybersecurity professionals are faced with numerous day-to-day operational challenges when it comes to protecting cloud workloads. Lack of security visibility tops the list (38%), followed by compliance requirements (36%) and the perennial lack of qualified security staff (32%).

What are your biggest operational, day-to-day headaches trying to protect cloud workloads?

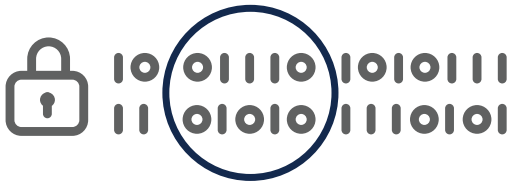


Other 3%

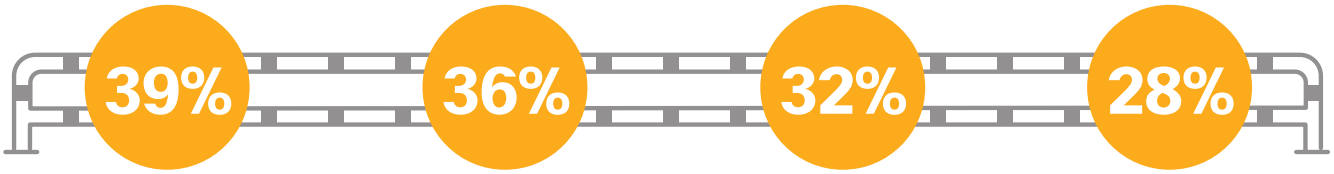
ENCRYPTED TRAFFIC CHALLENGES

Let's drill down on the specific challenges posed by encrypted network traffic. The main challenge that stands out: limited visibility into encrypted traffic (50%). One of the main effects of limited visibility include maintaining compliance with industry mandates (39%). Another major effect is the performance impact on apps and user experience resulting from traffic decryption/ inspection (36%).

What challenges do you have with encrypted traffic in your environment?



50% Limited encrypted traffic visibility



Maintain data privacy/industry compliance (i.e. HIPAA, PCI, Sarbanes-Oxley, GDPR)

SSL traffic decryption/ inspection slows down performance

Adhering to growing data privacy and compliance demands

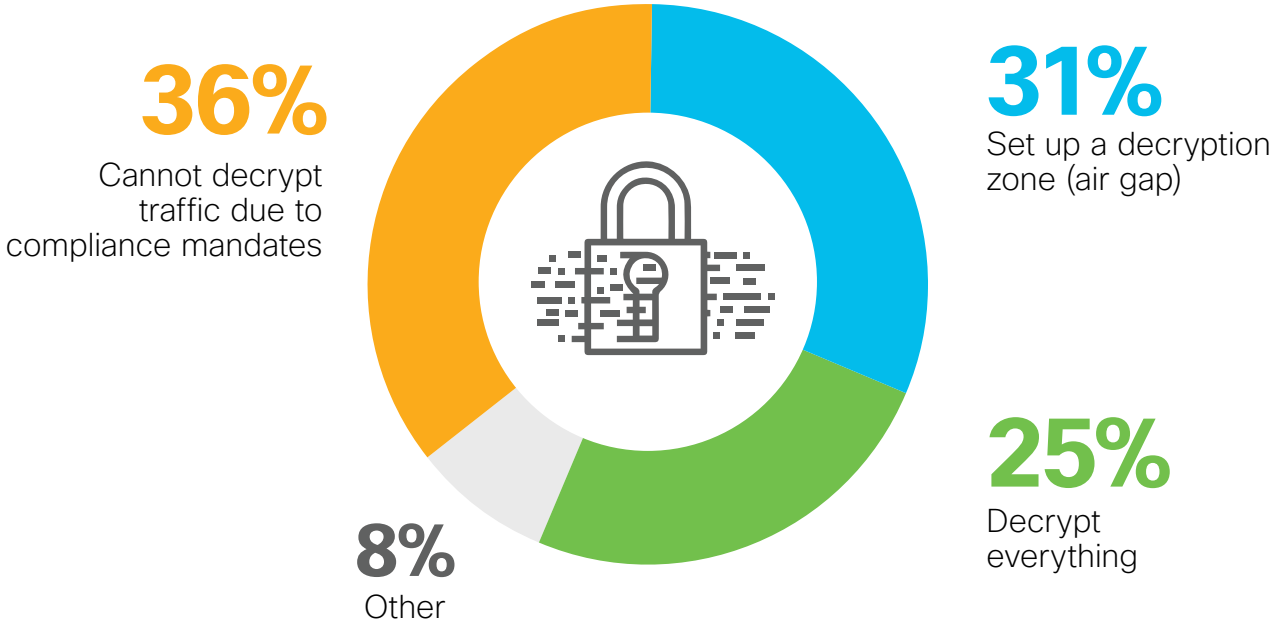
Security analytics/network forensic tools can't detect network breaches/targeted attacks

Data loss from malware hidden in encrypted traffic 24% | Complexity and cost from decentralized SSL decryption (standalone appliance) 22%
No challenges 8% | Other 3%

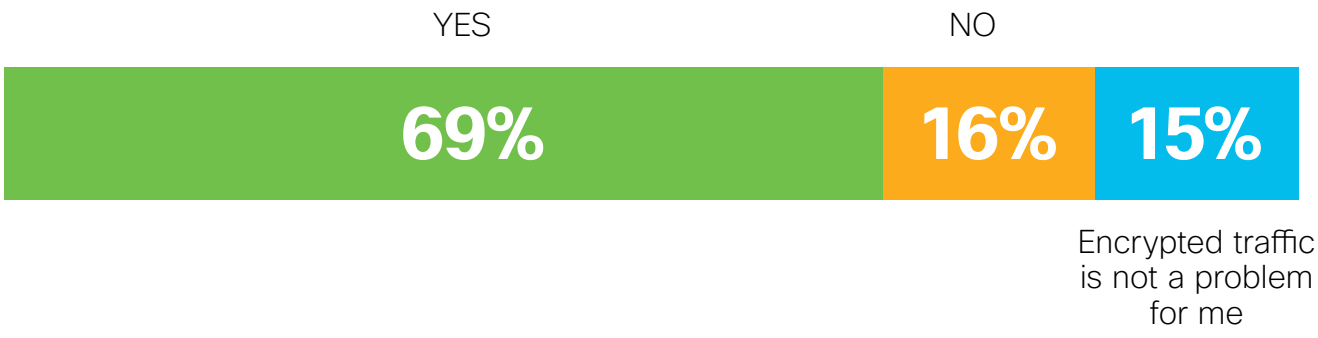
HANDLING ENCRYPTED TRAFFIC

So how do organizations handle the challenges created by encrypted network traffic? Over a third of respondents (36%) cannot decrypt traffic due to compliance mandates, thereby severely limiting their ability to inspect traffic and detect threats. Thirty-one percent set up a decryption zone (air gap) to gain access to data. And a quarter of organizations (25%) attempt to decrypt all traffic. A majority of cybersecurity professionals (69%) would like the ability to have visibility and control of encrypted traffic without requiring decryption.

How do you handle encrypted traffic in your environment?



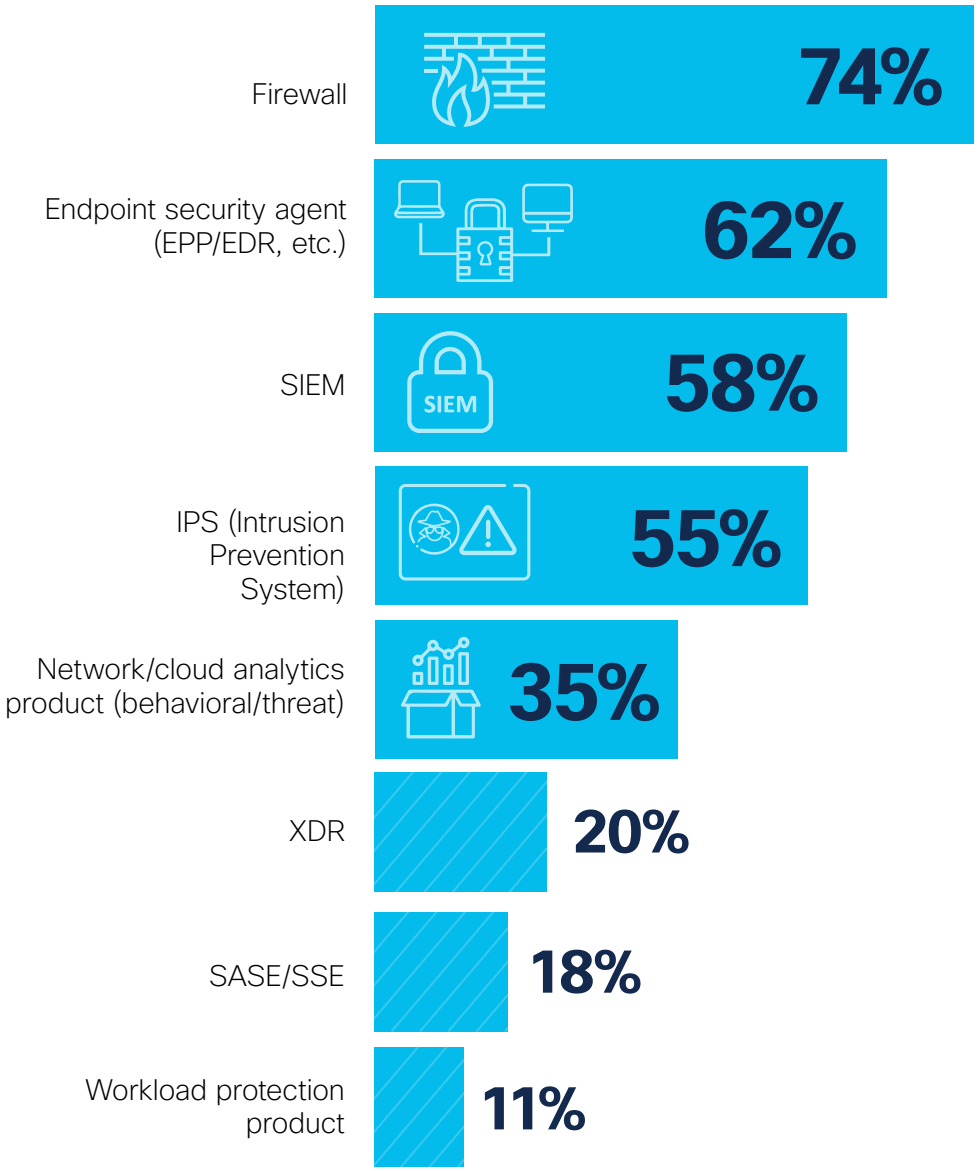
Would you like to have visibility and control of encrypted traffic without requiring decryption?



DEPLOYED SECURITY PRODUCTS

We asked what products organizations have deployed to gain visibility into network traffic. Firewalls top the list (74%), followed by endpoint security agents (62%) and SIEM platforms (58%).

What security products do you have deployed for visibility?

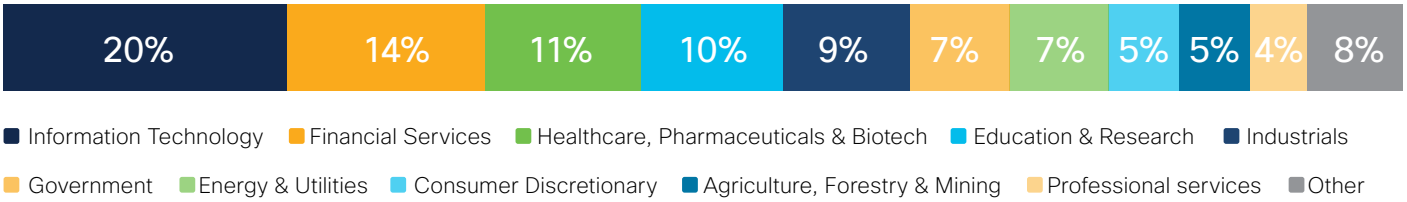


Other 5%

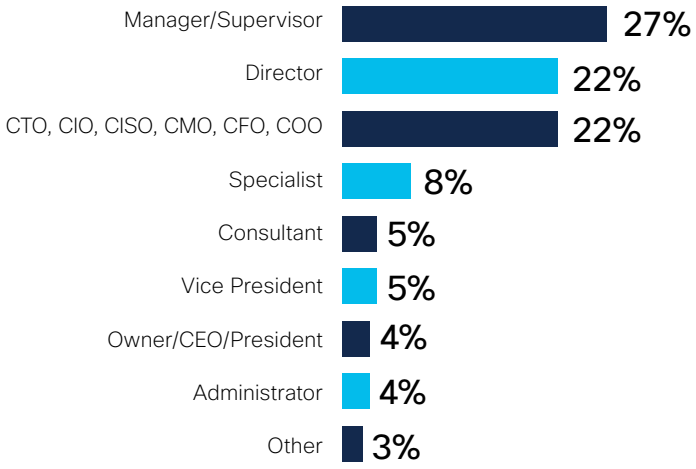
DEMOGRAPHICS

The 2022 Security Visibility Report is based on the results of a comprehensive online global survey of 278 cybersecurity professionals, conducted in July 2022, to gain deep insight into the latest trends, key challenges, and solutions for visibility security. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

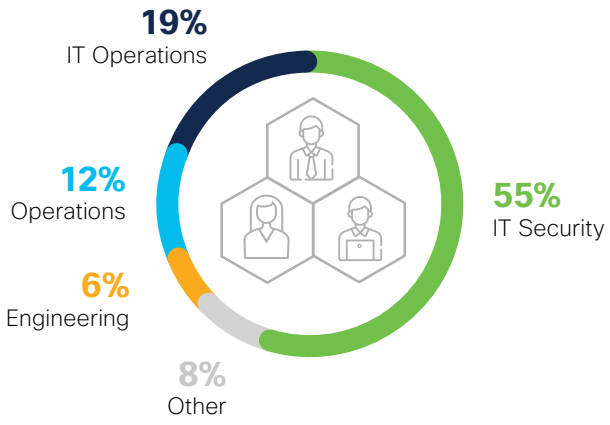
INDUSTRY



COMPANY DEPARTMENT



ROLE POSITION



Cisco has long established itself as the worldwide leader in technology that powers the internet, while building an open, integrated portfolio of cybersecurity solutions along the way. We believe that security solutions should be designed to act as a team. They should learn from each other. They should listen and respond as a coordinated unit. When that happens, security becomes more systematic and effective. Our customers have trusted us for years as both the world's largest provider of IT infrastructure and networking services and the world's largest enterprise cybersecurity business.

Cisco Secure is built on the principle of better security, not more. It delivers a streamlined, customer-centric approach to security that ensures it's easy to deploy, manage, and use – and that it all works together. We're driven by the fact that people and our customers are at the heart of what we do. We understand that customers want to cut through the complexity and noise and feel confident in their security, focusing on outcomes. This requires simplification without being simplistic. Our cloud-native platform is a giant leap forward in that.

We empower the security community with the reliability and confidence that they're safe from threats now and in the future with the Cisco SecureX platform. We help 100 percent of the Fortune 100 companies secure work – wherever it happens – with the broadest, most integrated platform. Learn more about how we simplify experiences, accelerate success, and protect futures at cisco.com/go/secure.

Learn more about Cisco Secure

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