2022

Cybersecurity
INSIDERS

ENDPOINT SECURITY REPORT

adaptiva™

INTRODUCTION

Faced with the challenges of defending against new and increasingly sophisticated threats, organizations are reporting an increase in endpoint security risk, while feeling insufficiently prepared to tackle new threats with existing endpoint security platforms.

The 2022 Endpoint Security Report reveals the latest endpoint security trends and challenges, why and how organizations invest in endpoint security, and the security capabilities companies are prioritizing.

Key findings include:

- 85% of organizations expect a compromising security attack within the next 12 months
- Perennial shortage of cybersecurity skills (44%) is the most reported security operations challenge, followed by the lack of continuous 24x7 security coverage (38%) and slow incident response (37%)
- Each month IT teams spend an average of 36 hours on endpoint security monitoring
- 43% of organizations take at least 1 week to roll out critical patches – 38% take longer than 1 week
- 34% of organizations say they have insufficient visibility into what is happening on the endpoint

Many thanks to Adaptiva for supporting this important research. We hope you find this report informative and helpful as you continue your efforts in protecting your IT environments.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity INSIDERS

BIGGEST THREATS

We asked cybersecurity professionals what they consider the biggest cybersecurity threats to their organization. Malware (including ransomware, trojans, exploit kits, etc.) ranks as the biggest security threat (38%), followed by human error (23%) and zero-day exploits (18%). This confirms related research, highlighting the growing threat from malware, specifically ransomware.

▶ What poses the biggest threat to your organization?

38%

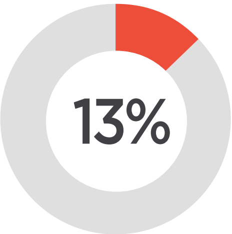
Malware
(ransomware, trojans, exploit kits, etc.)

23%

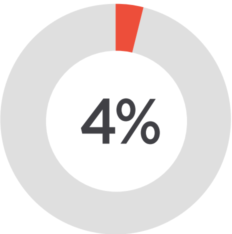
Human error

18%

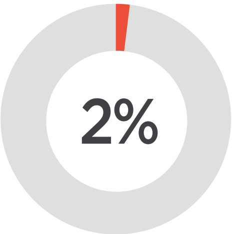
Zero-day exploits



Insider threats
(malicious employee, compromised credentials, accidental release of data)



Misuse of legitimate applications
(PowerShell, WMI, MSHTA)



Fileless/
in-memory attacks

ENDPOINT SECURITY DRIVERS

Organizations' interest in upgrading to next-gen endpoint security solutions is driven by a number of factors. The primary factor is that many installed legacy security products (AV, NGAV, HIPS, EPP, etc.) are failing to stop an increasing number of evolving threats (46%). And even organizations who believe they have solid tools and processes in place are still concerned that threats are slipping through the defenses (41%).

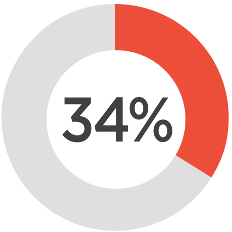
What are the key drivers for considering a next-gen endpoint security solution?

46%

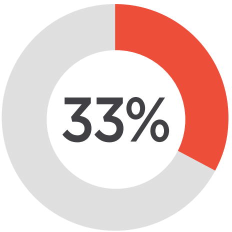
Existing endpoint security products (AV, NGAV, HIPS, EPP, etc.) are failing to stop an increasing number of threats

41%

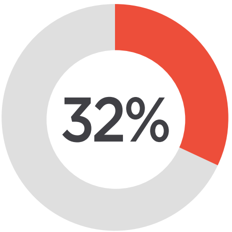
We have good tools and processes in place, but are concerned that threats are still slipping through on endpoints



Our team has insufficient visibility into what is happening on endpoints



Our team does not have the capacity or expertise to build the solutions needed to respond to increasingly sophisticated threats



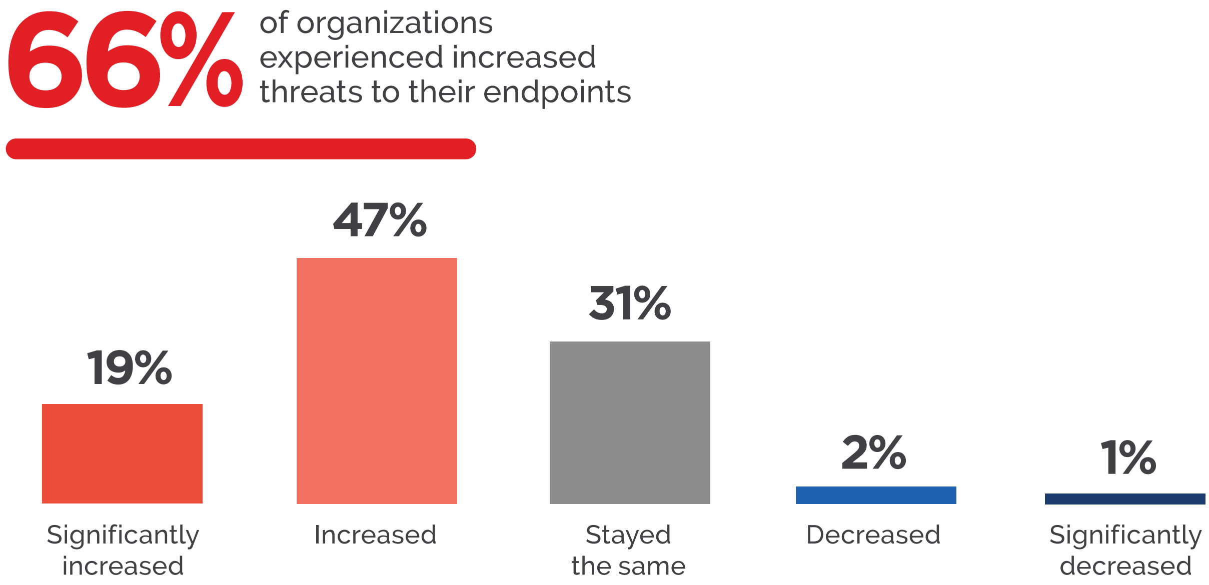
Leadership is focused on preventing a public breach and the associated costs, negative headlines, and brand damage

Compliance requirements or large fines are mandating the use of continuous monitoring and threat detection 22% | Frequent incident analysis and response events are distracting our team from focusing on the right priorities 20% | Other 7%

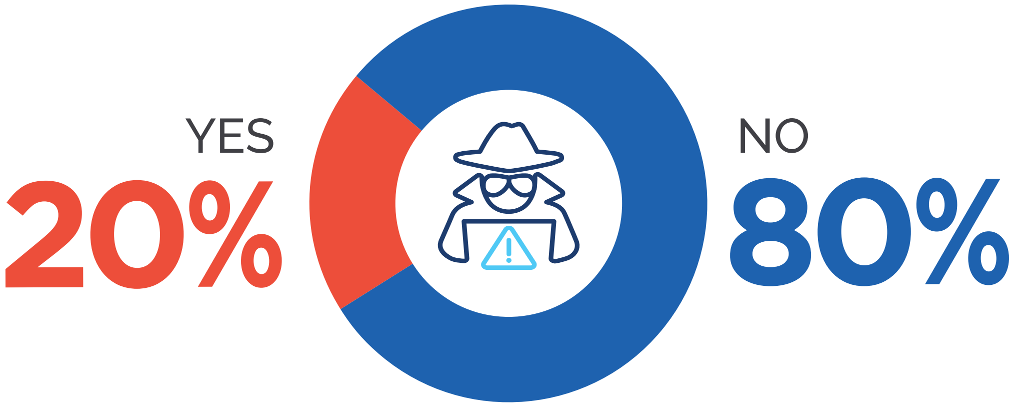
ENDPOINT SECURITY RISK

A majority of organizations experienced an increase of cyber threats to their endpoints (66%). Twenty percent of cybersecurity professionals report that their organization experienced a "successful" endpoint attack in the last 12 months that compromised data assets and/or IT infrastructure. The number of undetected attacks is likely significantly higher.

How has endpoint security risk to your organization changed in the last 12 months?



Has your organization experienced any endpoint attacks in the last 12 months that successfully compromised data assets and/or IT infrastructure?

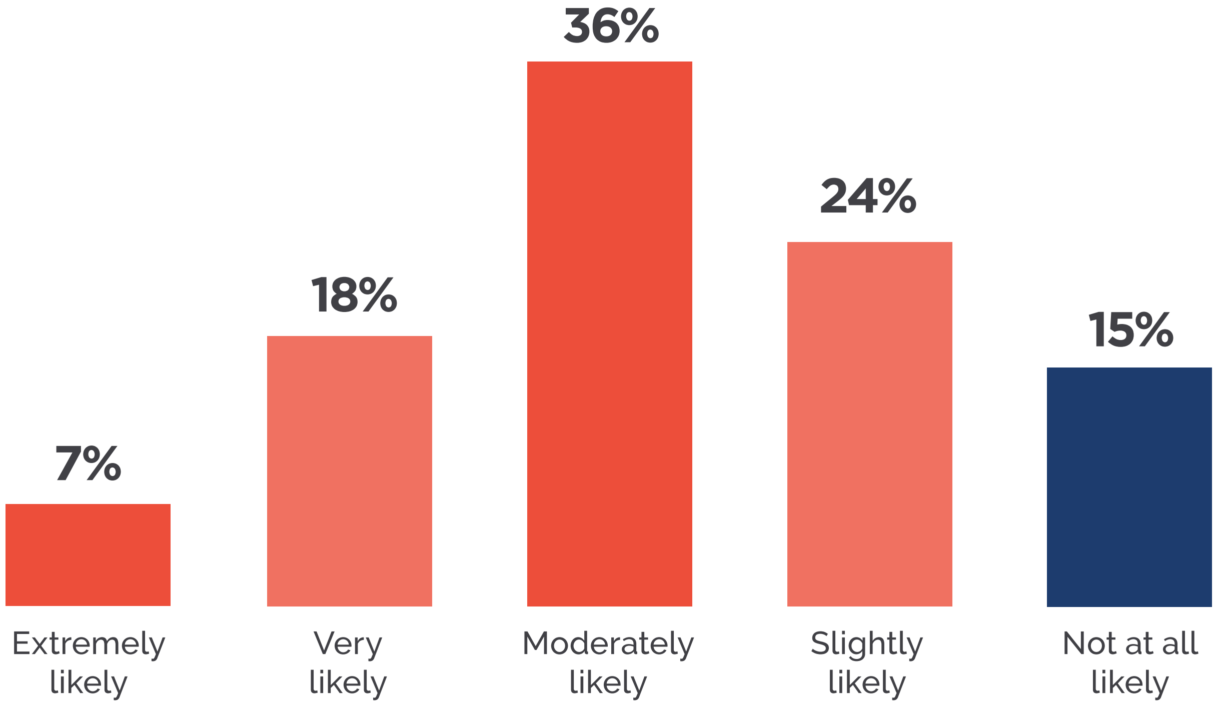


ATTACK RISK

In light of a worsening threat landscape, organizations are quite pragmatic regarding cyber-attacks and realize they are likely being targeted. Over eight out of 10 respondents believe a compromising attack will likely happen in the next 12 months (85%).

What do you believe is the likelihood that your organization will become compromised by a successful cyberattack in the next 12 months?

85% of organizations expect a compromising attack within the next 12 months



ATTACK IMPACT

When asked about the most significant negative impact organizations experienced from endpoint attacks, organizations most frequently list loss of end-user productivity (47%). This is followed by system downtime (40%) and loss of IT productivity (39%).

▶ **What was the most significant impact of endpoint attack(s) against your organization?**

47%

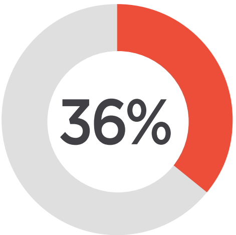
Loss of end-user productivity

40%

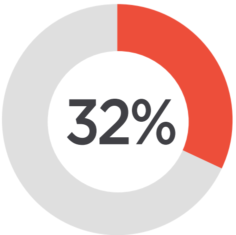
System downtime

39%

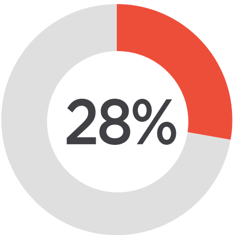
Loss of IT productivity



Reputation and brand damage



Theft of information assets



Business/ revenue impact

PROTECTION CHALLENGES

Respondents report insufficient protection against the newest attacks (35%) as the biggest challenge with their current endpoint protection solution. This is followed by high cost of operation (31%) and negative impact on user productivity and endpoint performance (29%).

What are the biggest challenges with your current endpoint protection solution?

35%

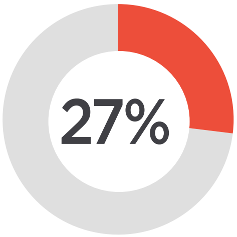
Insufficient protection against the newest attacks

31%

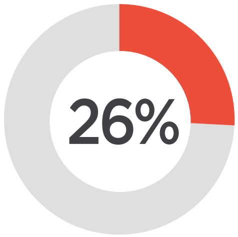
High cost of operation

29%

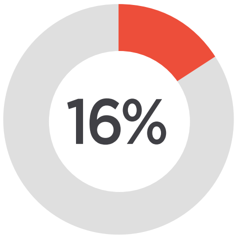
Negative impact on user productivity/ endpoint performance



High complexity of deployment and operation



High number of false positives and security alerts



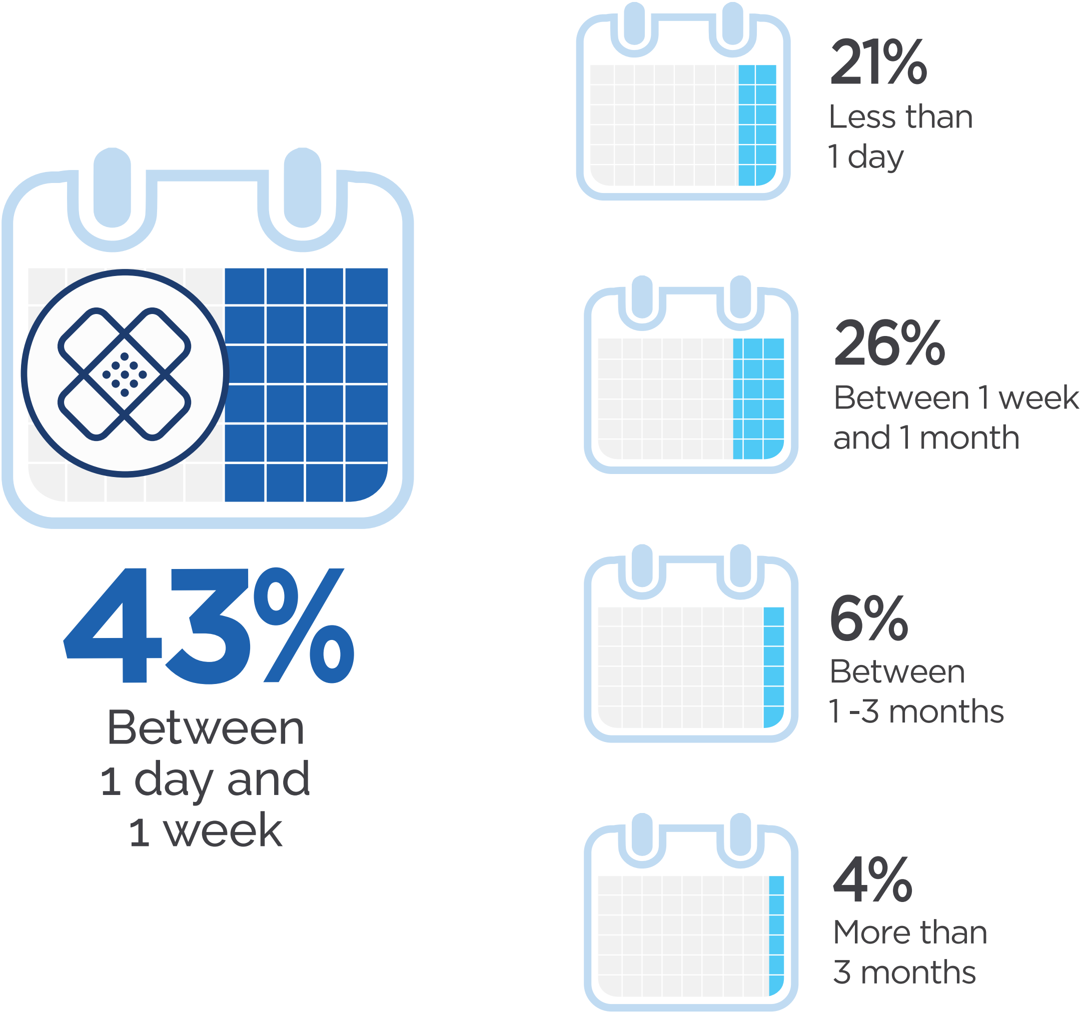
No challenges

Other 6%

SLOW TO PATCH

Many organizations take a long time to roll out critical security patches to reduce known vulnerabilities. Most frequently, organizations take between one day to one week (43%) to apply a patch. Only 21% of organizations address vulnerabilities within a day.

On average, how long does it take your organization to roll out a critical patch?



43%
Between
1 day and
1 week

21%
Less than
1 day

26%
Between 1 week
and 1 month

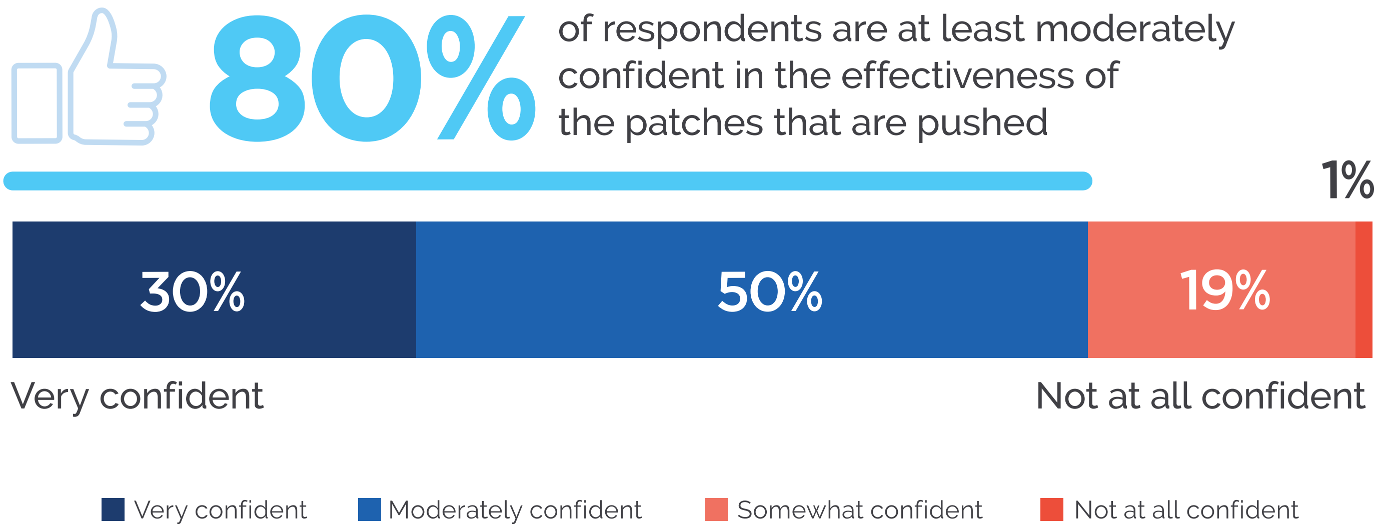
6%
Between
1 -3 months

4%
More than
3 months

CONFIDENCE IN PATCHES

While patches aren't always effective, more than three-quarters of organizations (80%) are moderately to very confident in the effectiveness of the patches that are pushed.

How confident are you in the effectiveness of the patches that are pushed?



MONITORING

Each month IT teams spend an average of 36 hours on endpoint security monitoring.

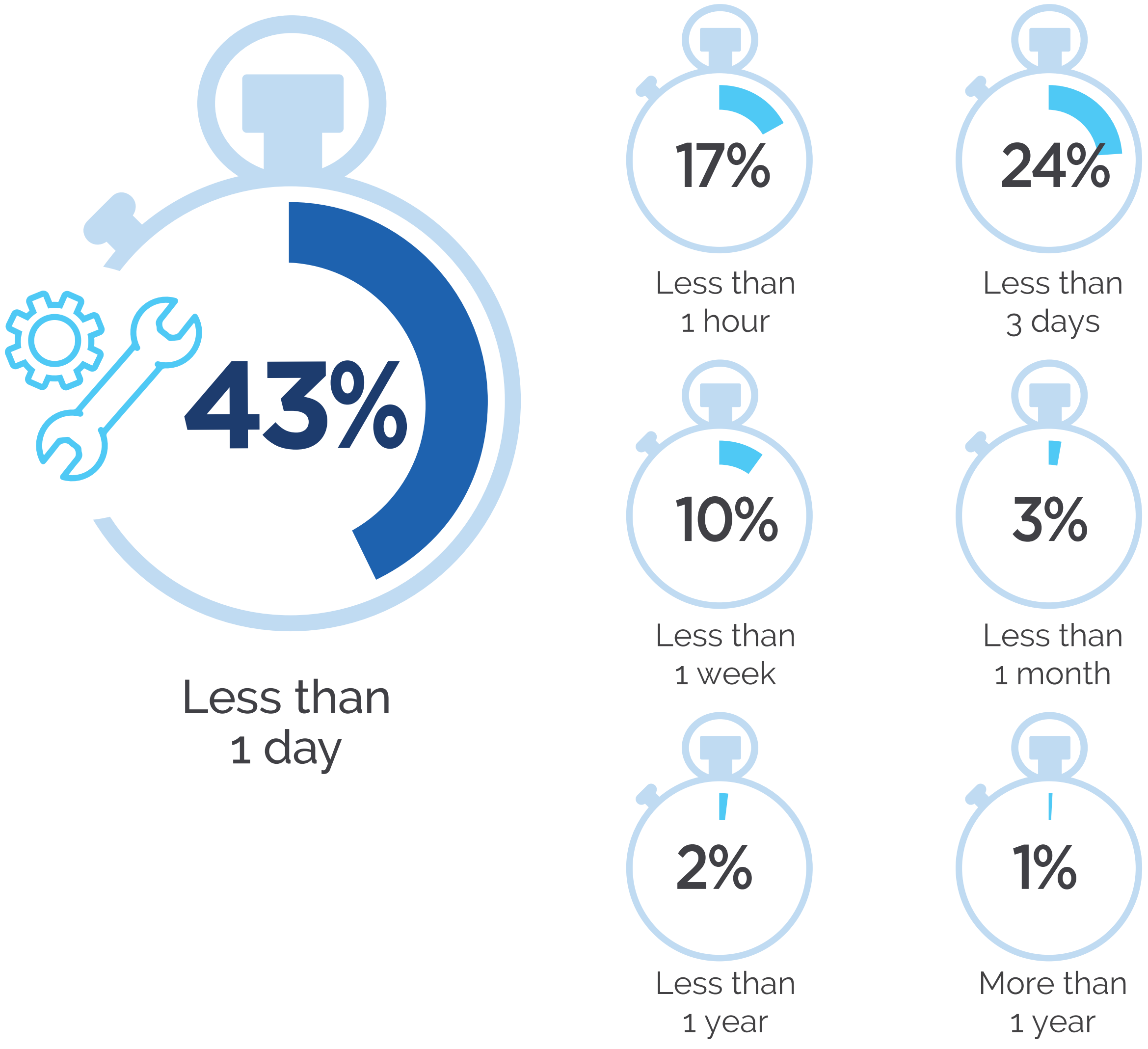
▶ **How many hours is your IT team spending on endpoint security monitoring and log monitoring per month?**

36 hours

REMEDIATION TIME

While 17% take less than an hour to remediate a threat once identified, 43% need up to a day. Forty percent need even longer than that.

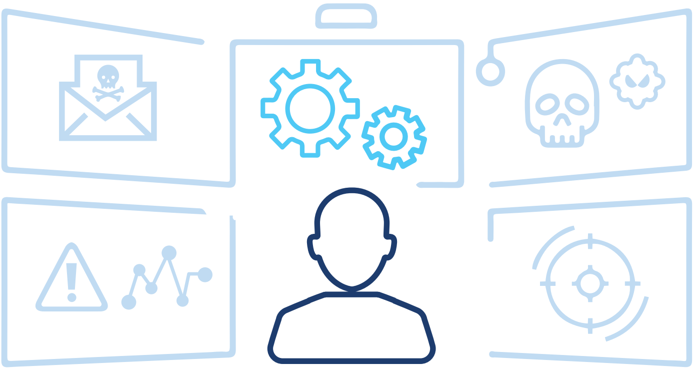
How long does it take your organization to remediate once a threat has been identified?

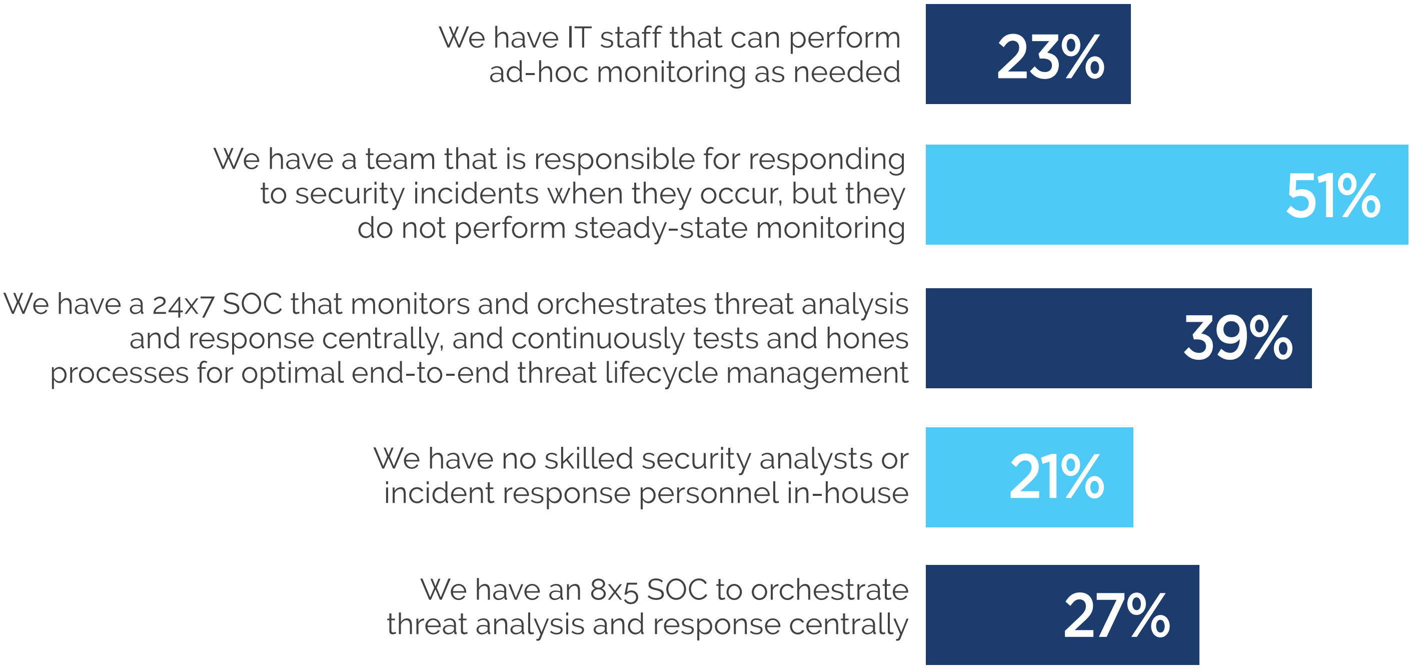


THREAT READINESS

When responding to incoming cybersecurity threats, a fifth of organizations (23%) confirm they can only perform ad-hoc monitoring with IT professionals as the need arises. About half of respondents (51%) say they have dedicated teams in place responsible for responding to security incidents when they occur, but they do not perform steady-state monitoring.

▶ How equipped are your staff and processes to deal with incoming threats?




We have IT staff that can perform ad-hoc monitoring as needed
23%
We have a team that is responsible for responding to security incidents when they occur, but they do not perform steady-state monitoring
51%
We have a 24x7 SOC that monitors and orchestrates threat analysis and response centrally, and continuously tests and hones processes for optimal end-to-end threat lifecycle management
39%
We have no skilled security analysts or incident response personnel in-house
21%
We have an 8x5 SOC to orchestrate threat analysis and response centrally
27%

IMPACT OF SECURITY BREACHES

Security incidents have a real-world impact on businesses. Survey respondents most often mentioned reduced employee productivity (35%) and disrupted business activities (32%) as the top two negative business impacts resulting from a security incident.

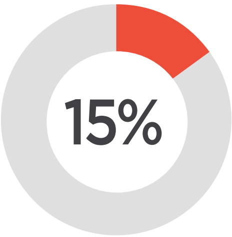
What negative impact have security incidents had on your company in the past 12 months?

35%
Reduced employee productivity

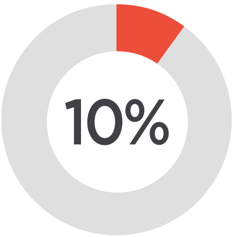
32%
Disrupted business activities

22%
Deployment of IT resources to triage and remediate issue

Increased helpdesk time to repair damage



Reduced revenue/lost business



Corporate data loss or theft

None 30% | Don't know/unsure 16% | Regulatory fines 8% | Lawsuit/legal issues 7% | Loss/compromise of intellectual property 7% | Other 1%

SECURITY OPERATIONS CHALLENGES

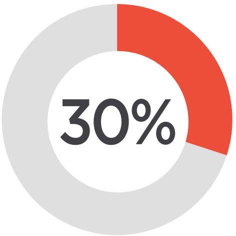
Security professionals report that their biggest operations challenges include the perennial shortage of cybersecurity skills in-house (44%), followed by the lack of continuous 24x7 security coverage (38%) and the lack of incident response speed (37%).

▶ What are the biggest security operations challenges for your IT organization?

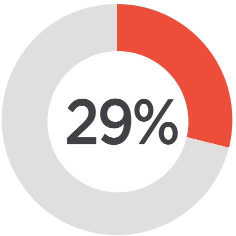
44%
Cybersecurity skills shortage in-house

38%
Lack of 24x7 security coverage

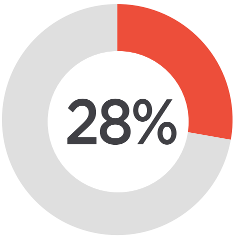
37%
Speed of incident response issues



Cost and complexity of building in-house



No visibility into overall security posture



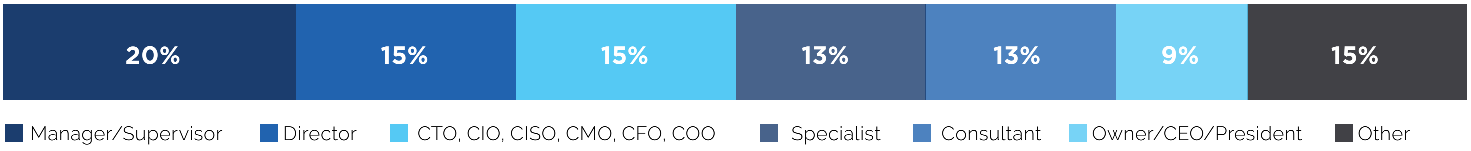
Lack of detection and response capabilities

Speed of deployment and provisioning issues 25% | Lack of customization of correlation rules and reports 17% | Not able to meet compliance requirements 13% | Other 7%

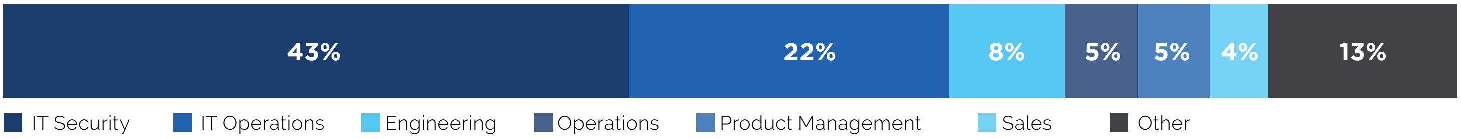
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 345 cybersecurity professionals to gain more insight into the latest trends, key challenges, and solutions for endpoint 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.

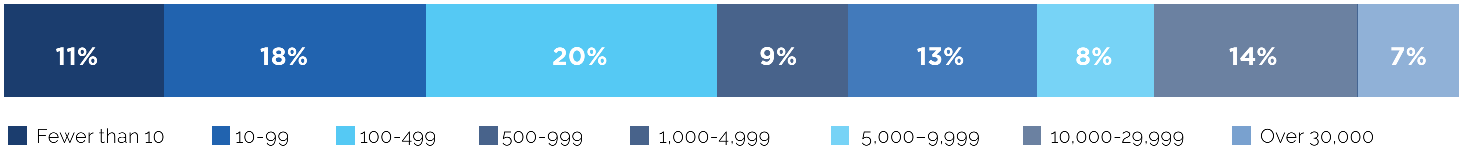
CAREER LEVEL



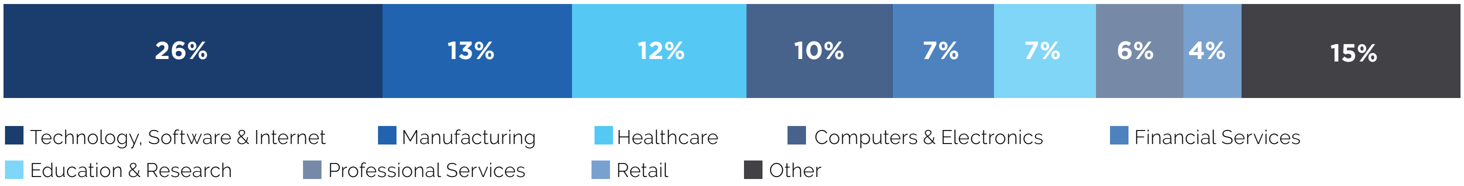
DEPARTMENT



COMPANY SIZE



INDUSTRY



Adaptiva provides unrivaled serverless endpoint management that eliminates the need for a vast IT infrastructure and monitors itself by automating traditionally manual tasks. Leveraging innovative peer-to-peer protocols, the Adaptiva Edge Platform is powered by the surplus capacity of existing devices already on the network – in the office or working from home. This enables IT to continuously deliver software, configurations, and patches to endpoints no matter where they are. The world's largest enterprise organizations and government agencies rely on Adaptiva for best-in-class real-time endpoint visibility and content delivery, as well as automated compliance checks, remediations, and patching without ever throttling the network or the end-user experience. Learn how at **adaptiva.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