2020

Cybersecurity
RESEARCH

ENDPOINT SECURITY REPORT

Created in partnership with Motorola Solutions, Inc.

MOTOROLA SOLUTIONS

INTRODUCTION

The 2020 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.

Faced with the challenges of defending against new and increasingly sophisticated threats, such as fileless malware, advanced attacks, and evasive threats, a majority of organizations are reporting an increase in endpoint security risk, while feeling insufficiently prepared to tackle new threats with existing endpoint security platforms.

Although next-generation Endpoint Detection and Response (EDR) solutions offer advanced detection, protection, and response capabilities, they can also be complex to deploy and manage. Many organizations, particularly small and mid-sized agencies and businesses, have found that a Managed Security Services Provider (MSSP) often offers the best approach for managing EDR and getting value faster from these solutions.

We would like to thank Motorola Solutions, Inc. for supporting this unique research.

We hope you enjoy this report.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity INSIDERS

Motorola Solutions, Inc. has partnered with Cybersecurity Insiders to produce this report. Cybersecurity Insiders conducted the research through a comprehensive online survey of IT and cybersecurity professionals, ranging from technical executives to senior managers and IT security practitioners, across the spectrum of organization sizes and industries. The results, which were compiled in coordination with Motorola Solutions to highlight key areas, reveal the latest trends in security, what challenges they are facing and what requirements they are prioritizing in solutions. We hope the report insights will guide our customers in their cybersecurity risk and threat management strategy.

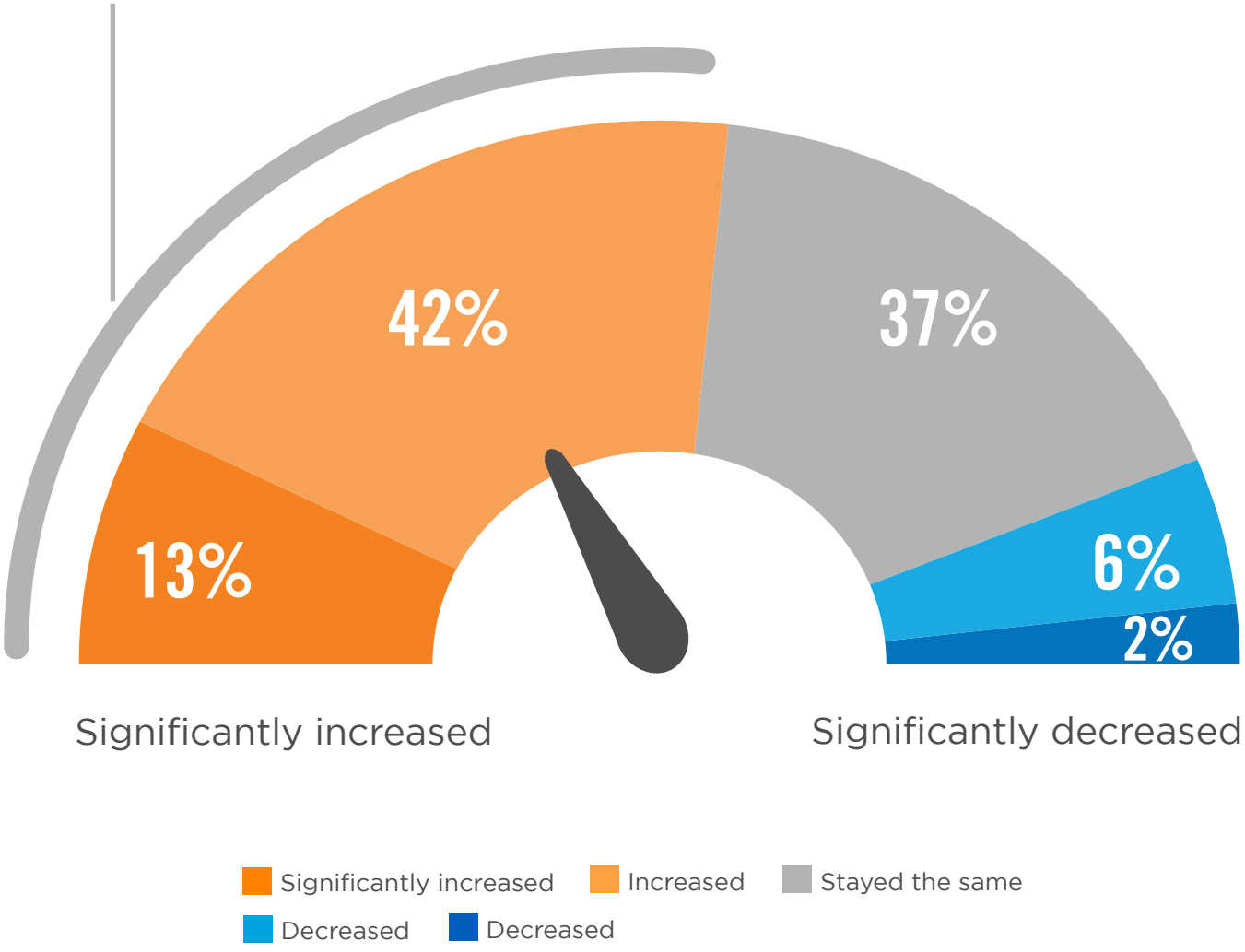
MOTOROLA SOLUTIONS

ENDPOINT SECURITY RISK

Most organizations are reporting an increase or significant increase in endpoint security risk (55%), likely due to the proliferation of new threats. Thirty-seven percent stayed the same, and only 8% observed a decline.

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

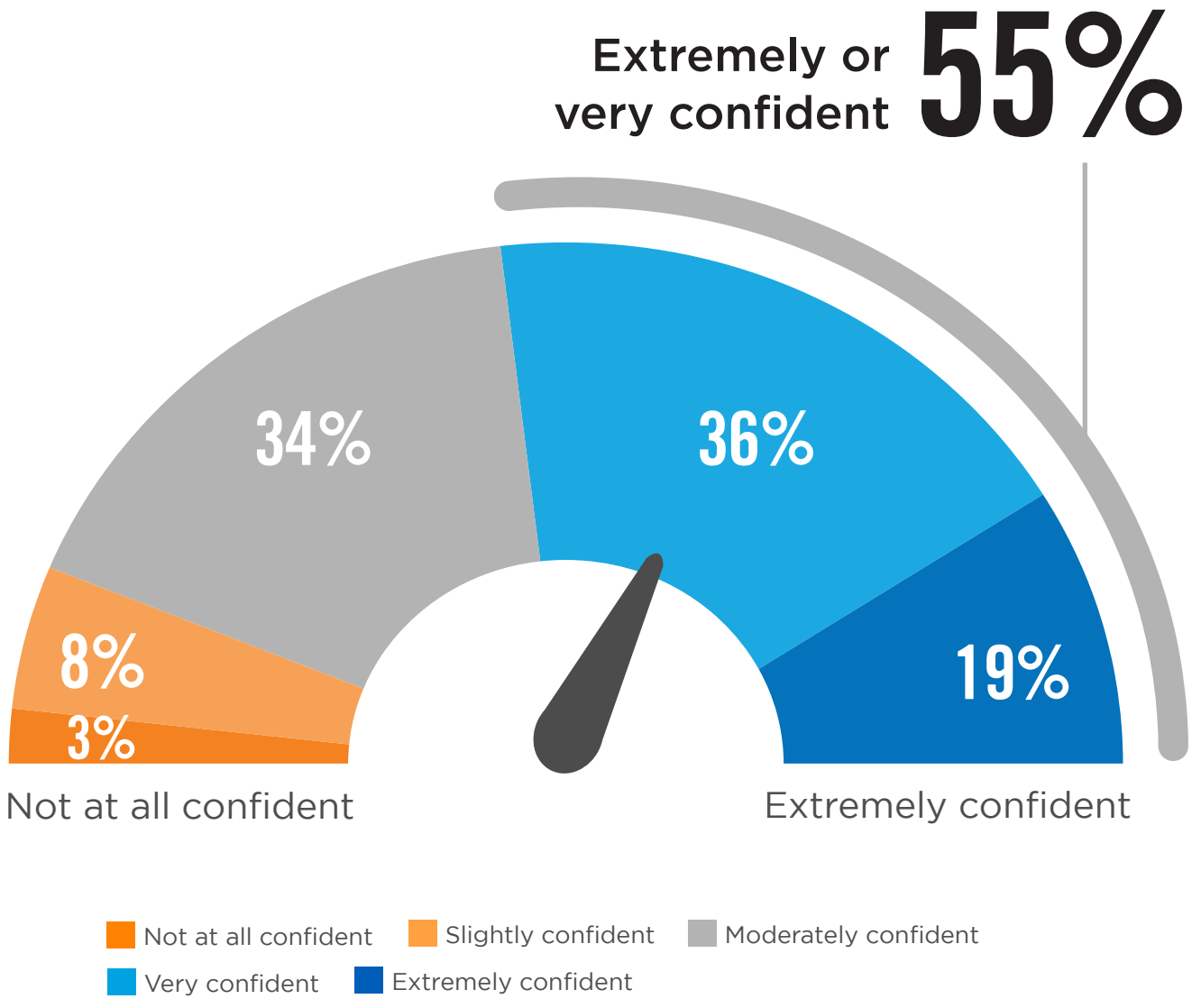
55% See an increase or significant increase in endpoint security risk



CONFIDENCE IN ENDPOINT SECURITY

Just over half of organizations (55%) are very confident or extremely confident in their organization's endpoint security posture.

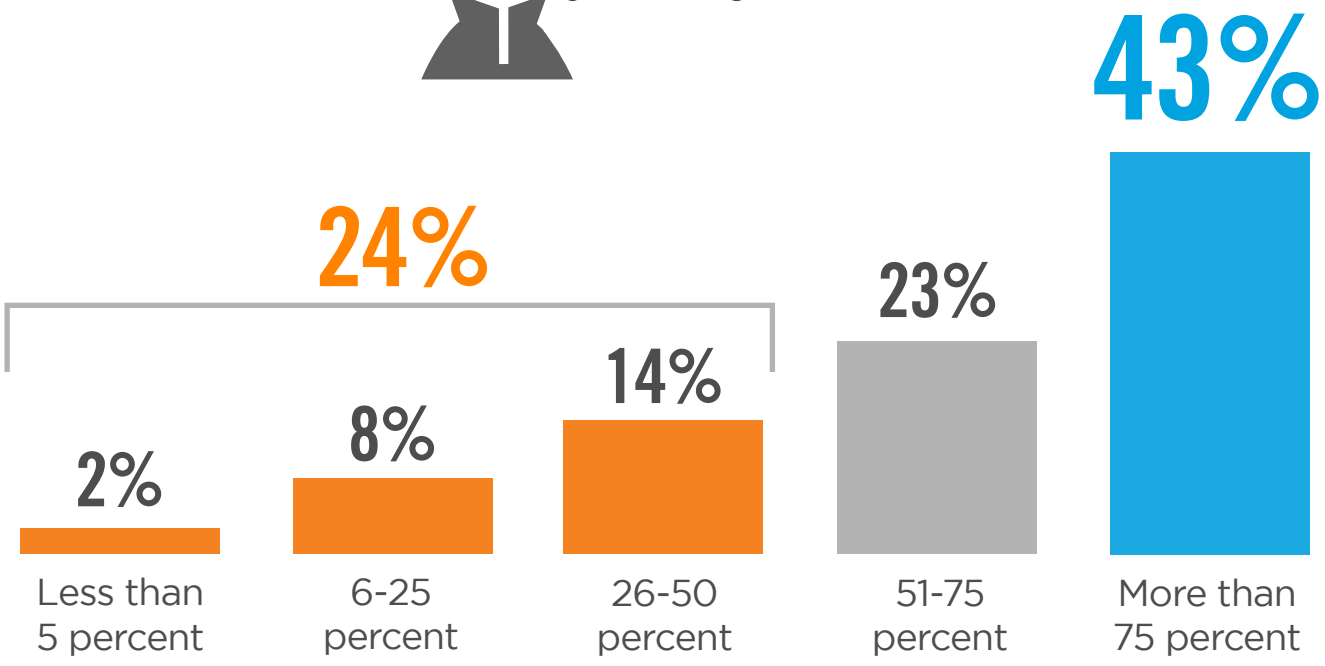
How confident are you in your organization's endpoint security posture?



STOPPING ENDPOINT ATTACKS

Less than half of organizations believe their current endpoint security posture can stop 75% of attacks or more. Twenty-four percent estimate less than 50% of attacks will be stopped.

What percentage of endpoint attacks do you estimate can be stopped under your current security posture (technology, people, process)?

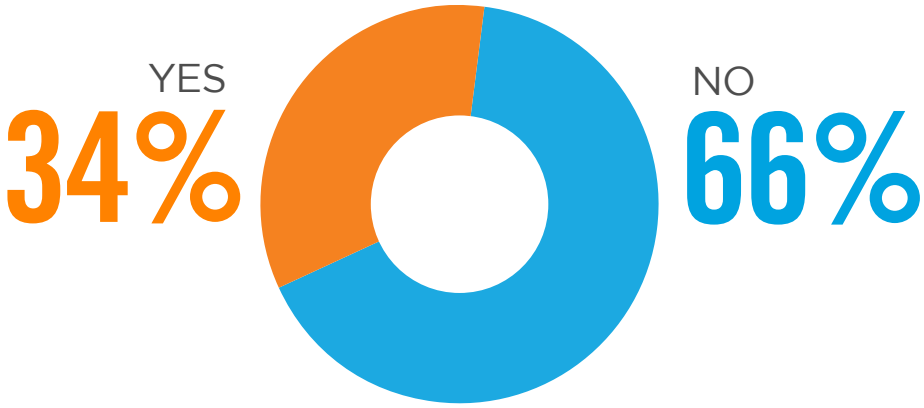


Not sure 10%

SUCCESSFUL ATTACKS

Not surprisingly, 34% of organizations experienced one or more endpoint attacks that successfully compromised data or IT infrastructure. Those who were compromised experienced about 11 compromises in the past 12 months, on average.

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



How many times do you estimate that your organization has been compromised by a cyberattack within the past 12 months?

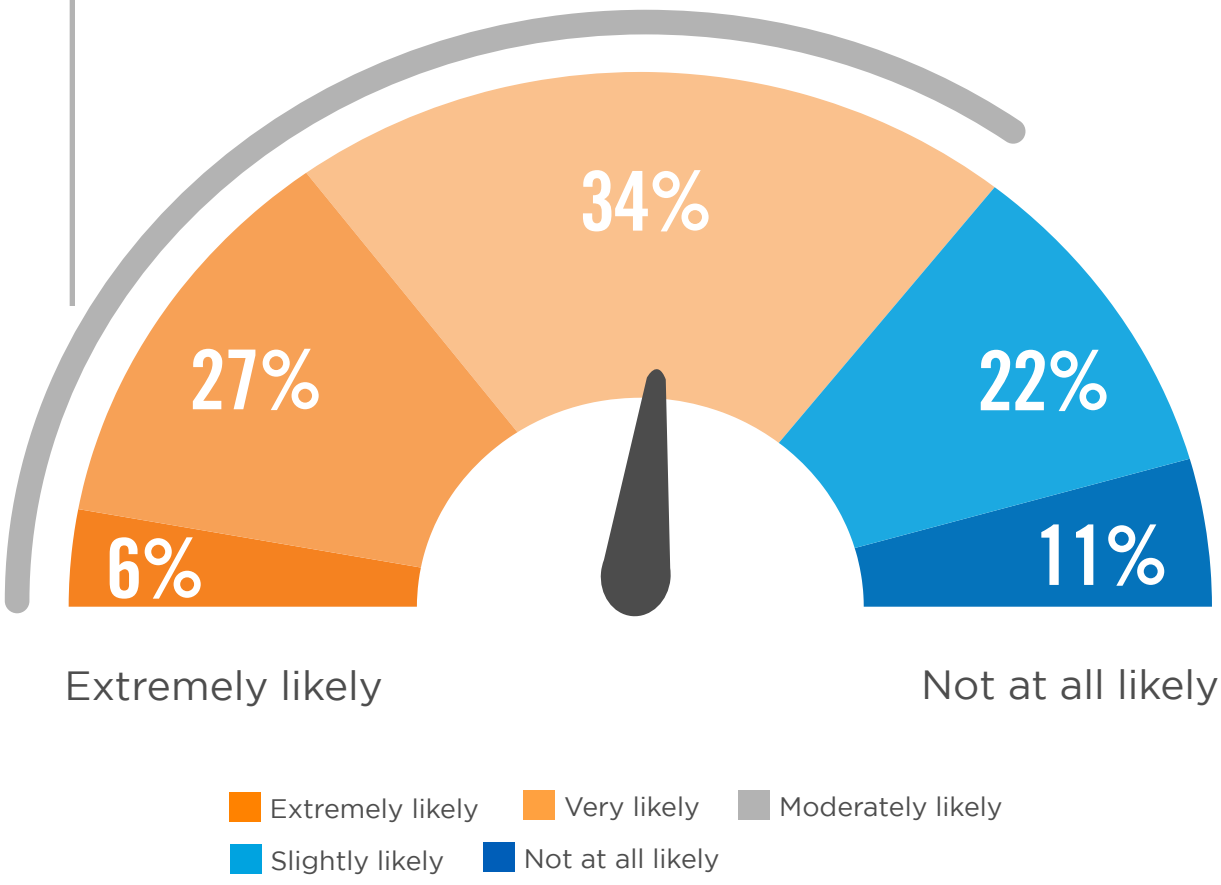
times in
the past year

RISK OF FUTURE ATTACKS

Moreover, a majority of 67% believe it is moderately likely to extremely likely that they will be the victim of a successful cyberattack in the next 12 months. Only 11% believe that a compromise is not at all likely.

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

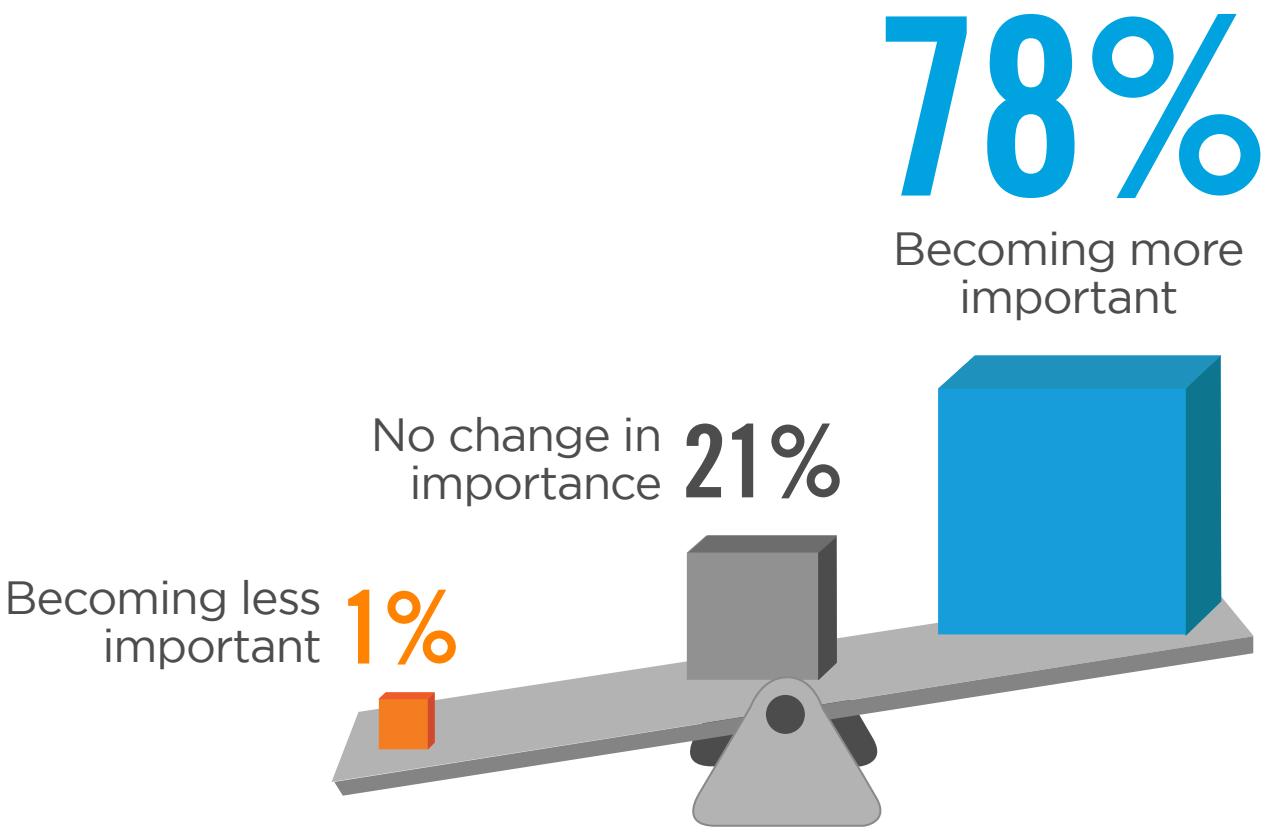
67% **Believe it's moderately likely to extremely likely that they will be impacted by a successful cyberattack in the next 12 months.**



IMPORTANCE OF ENDPOINT SECURITY

As a result of increasing threat pressure and endpoint security risk, 78% see endpoint security becoming more important in the future.

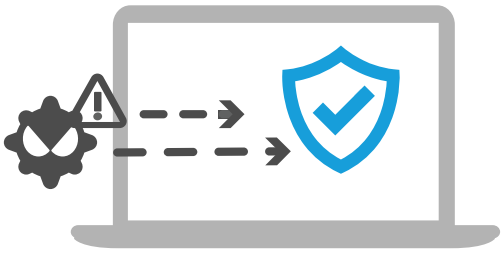
How is the importance of endpoint security changing as part of your organization's overall IT security strategy?



ENDPOINT SECURITY SHORTCOMINGS

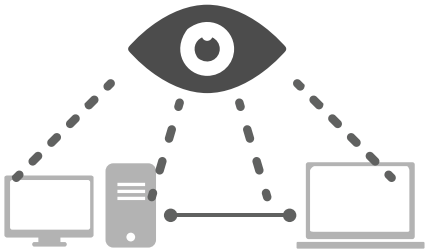
The key driver for considering better endpoint security solutions is the inability of existing endpoint security products to stop an increasing number of threats (49%) such as fileless malware, advanced attacks and evasive threats. Lack of threat defense is closely followed by lack of visibility into endpoints (48%).

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



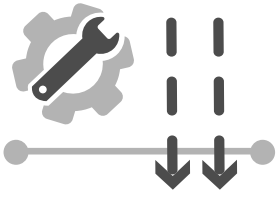
49%

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



48%

Our team has insufficient visibility into what is happening on endpoints



41%

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

35%

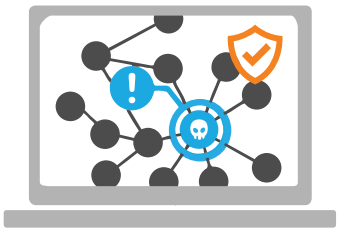
Our team does not have the capacity or expertise to build the solutions needed to respond to increasingly sophisticated threats

Compliance requirements or large fines are mandating the use of continuous monitoring and threat detection 30% | Leadership is focused on preventing a public breach and the associated costs, negative headlines, and brand damage 25% | Frequent incident analysis and response events are distracting our team from focusing on the right priorities 21% | Other 5%

ENDPOINT SECURITY CHALLENGES

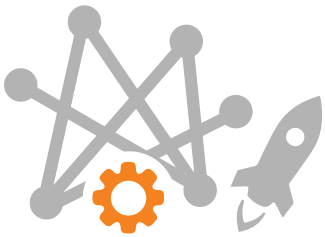
Specific challenges with organizations' current endpoint security solutions include insufficient protection against newest attacks (41%), high complexity of deployment and operation (33%), high rates of false positives (30%), and the negative impact of current technologies on user productivity/ endpoint performance (27%).

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



41%

Insufficient protection against the newest attacks

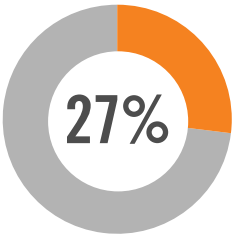


33%

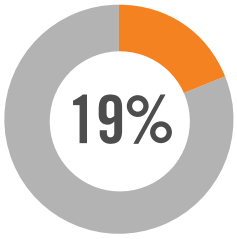
High complexity of deployment and operation

30%

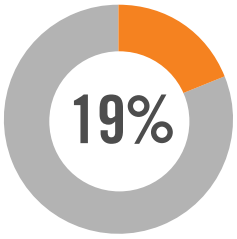
We are experiencing high rates of false positives with current solutions



Negative impact on user productivity/ endpoint performance



High cost of operation



No challenges

Other 4%

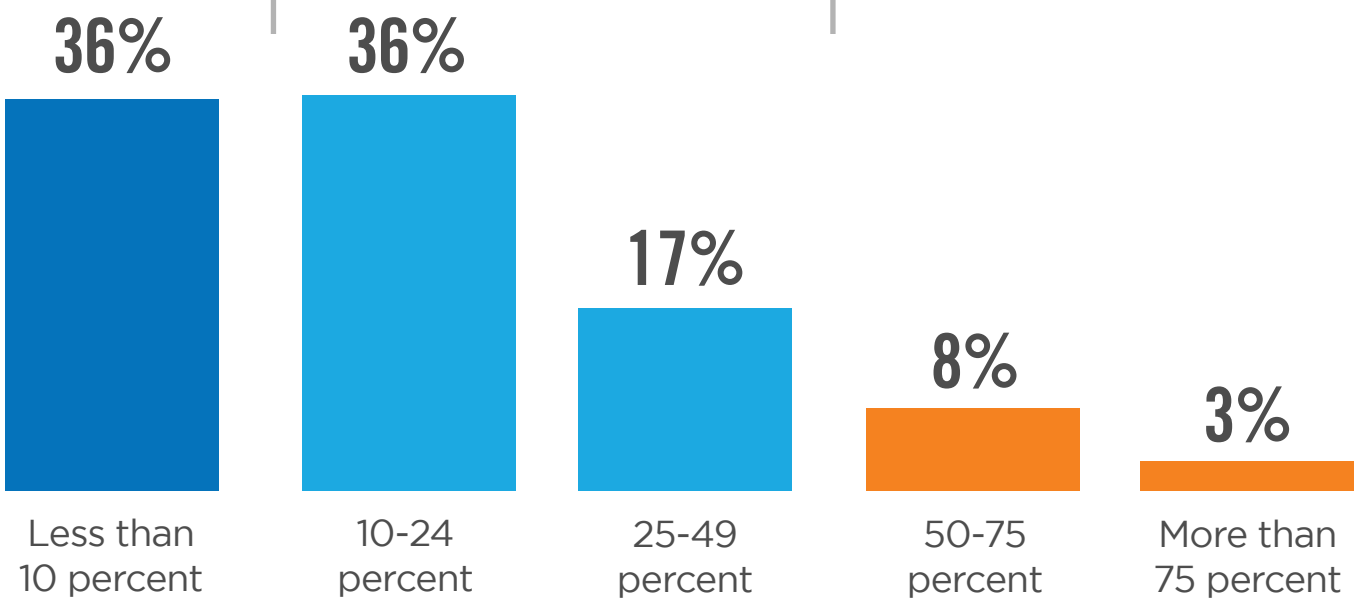
FALSE POSITIVES

Highlighted as one of the key endpoint security challenges, a majority of 53% estimate that between 10% and 49% of endpoint security alerts are false positives, with 11% estimating that over 50% of alerts are false positives.

What percentage of endpoint security alerts are false positives?

53%

Estimate that between 10% and 49% of endpoint security alerts are false positives

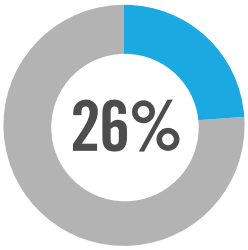


BIGGEST THREATS

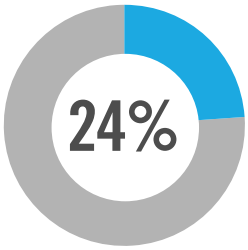
Nearly half of the security threats (43%) that most concern security professionals are endpoint threats, including malware, zero-day attacks, and fileless attacks.

What percentage of endpoint security alerts are false positives?

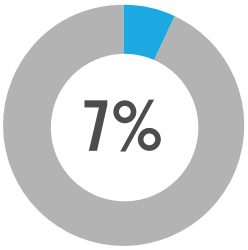
43% **Endpoint threats, including malware, zero-day attacks, and fileless attacks.**



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



Human error



Misuse of legitimate applications
(PowerShell, WMI, MSHTA)

SLOW TO PATCH

Organizations are still slow at doing the basics. Over a third of organizations (42%) take between 1 day and 1 week to roll out critical security patches.

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

42%

Between
1 day and 1 week

19%

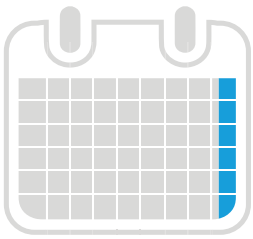
Less than
1 day

25%

Between 1 week
and 1 month

8%

Between
1-3 months



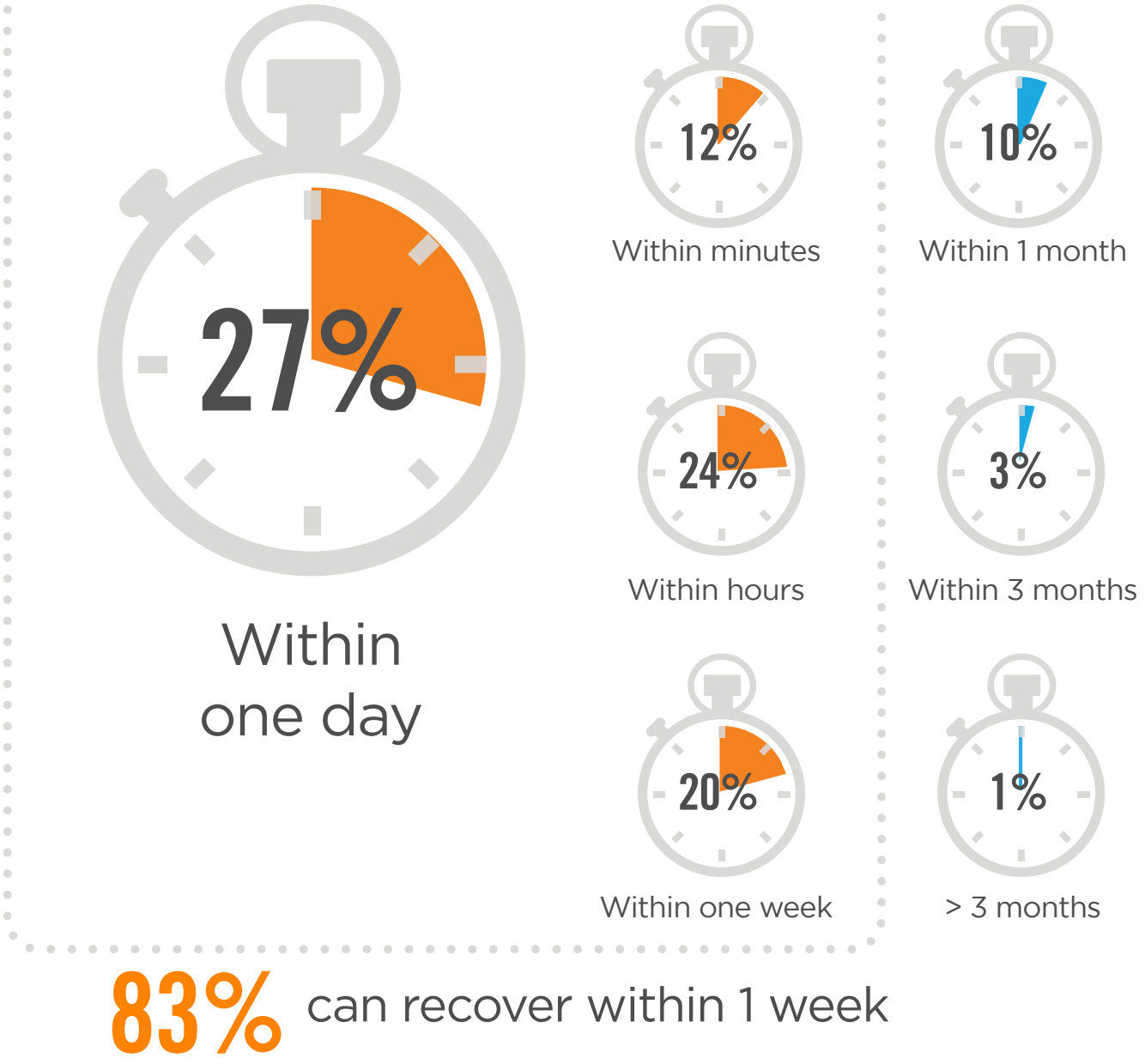
6%

More than
3 months

SLOW TO RECOVER

Asked about their ability to recover from cyber attacks, only 83% of organizations can recover within 1 week (some may not be able to recover at all).

How long did it take your organization to recover from a cyberattack (on average)?



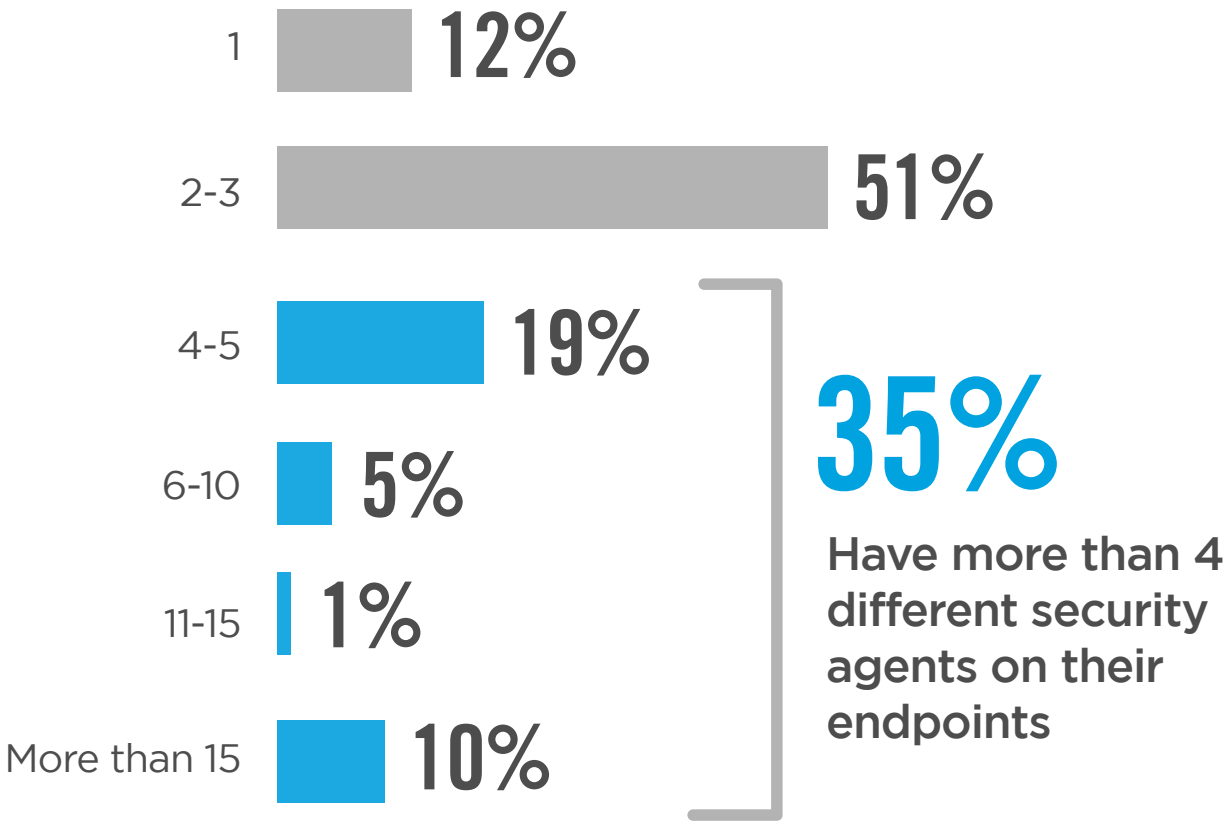
83% can recover within 1 week

No ability to recover 3%

ENDPOINT SECURITY AGENTS

Thirty-five percent of organizations have more than 4 different security agents on their endpoints (some have 15 or more).

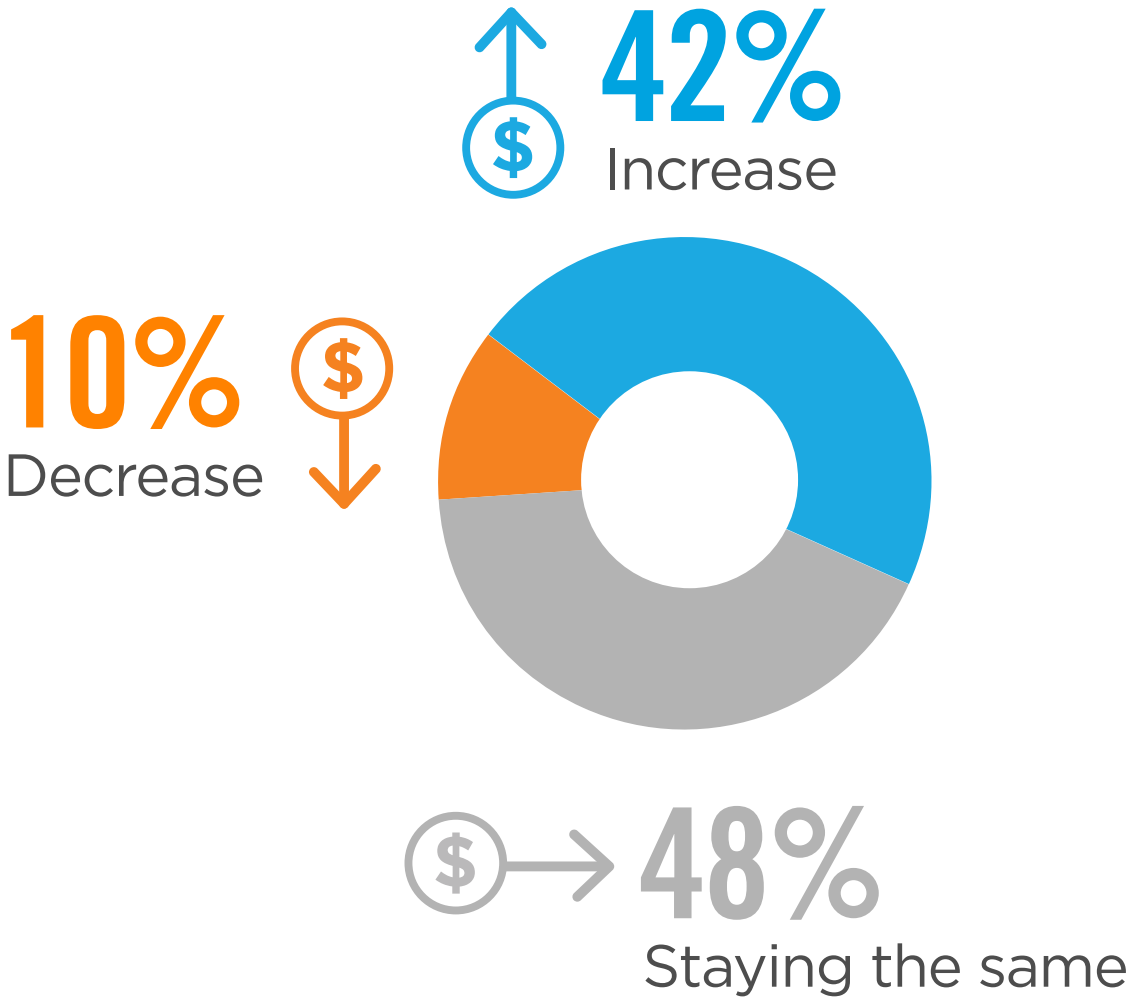
How many security agents/products (e.g. AV, DLP, encryption, EDR) do you have installed on your endpoints (on average)?



ENDPOINT BUDGET TRENDS

Thirty-five percent of organizations have more than 4 different security agents on their endpoints (some have 15 or more).

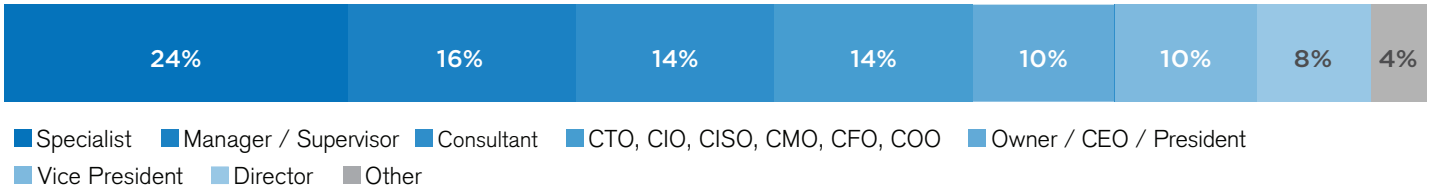
How is your budget for endpoint security changing over the next 12 months?



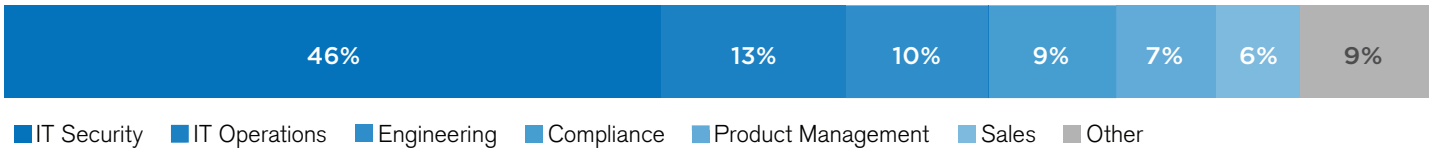
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 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.

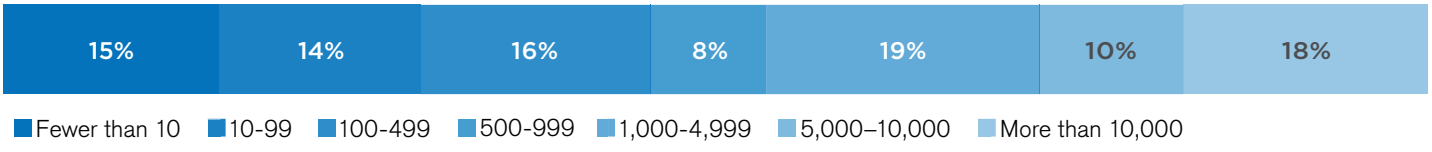
CAREER LEVEL



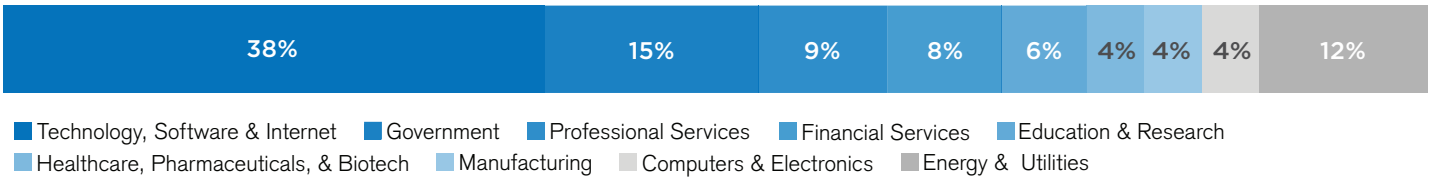
DEPARTMENT



COMPANY SIZE



INDUSTRY



INSTALLED ENDPOINT PRODUCTS

SUPPORTED ENDPOINTS