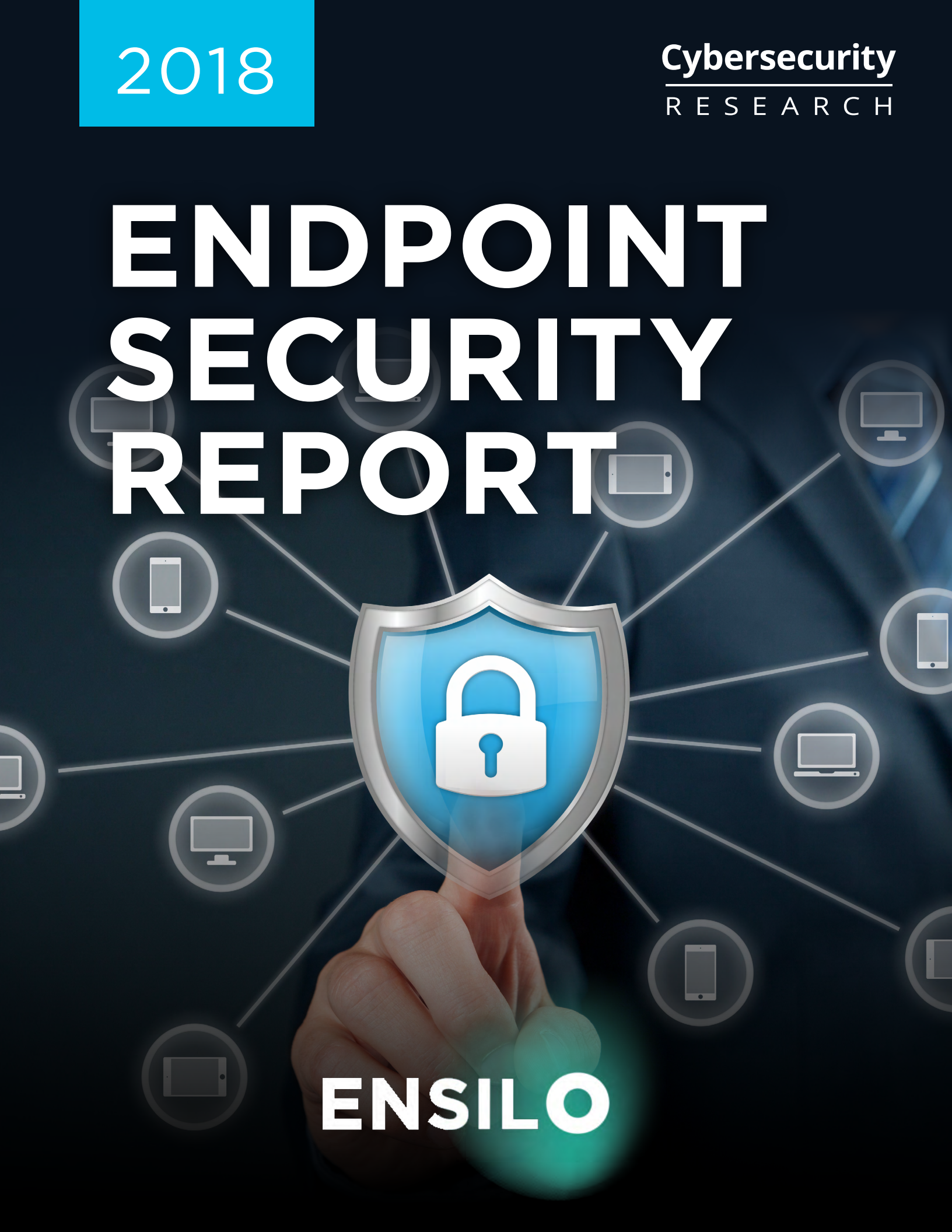
2018

Cybersecurity
RESEARCH

ENDPOINT SECURITY REPORT



ENSILO

INTRODUCTION

The 2018 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 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.

We would like to thank ENSILO for supporting this unique research.

We hope you will enjoy the report.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

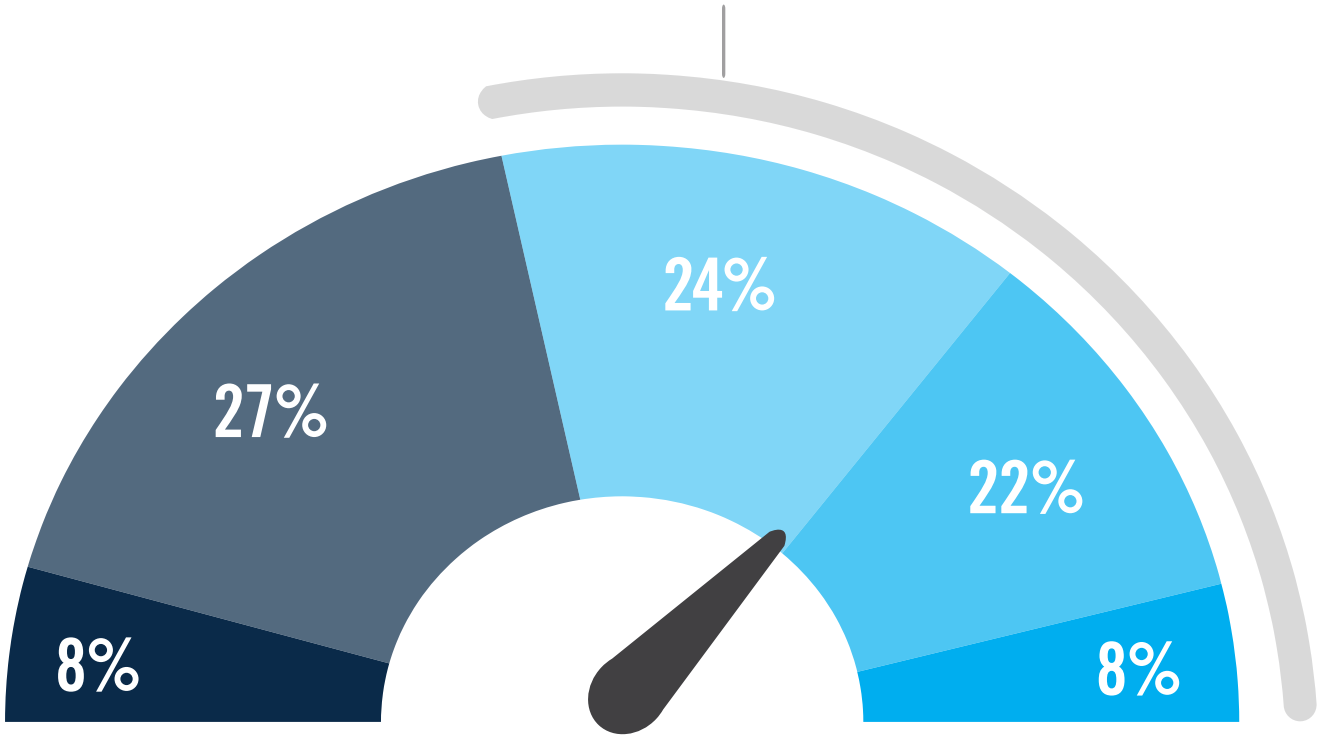
Cybersecurity
INSIDERS

RISK OF FUTURE ATTACKS

A majority of 54% believe it is moderately likely to extremely likely that they will experience successful cyber attacks in the next 12 months. Only 8% 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?

54% Believe it's moderately likely to extremely likely that they will experience successful cyber attacks in the next 12 months.



Don't know 11%

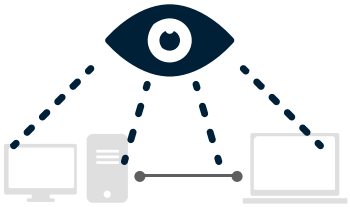
ENDPOINT SECURITY SHORTCOMINGS

The key driver for considering better endpoint security solutions is the inability of existing endpoint security products to stop an increasing number of threats (57%) such as fileless malware, advanced attacks and evasive threats. Lack of threat defense is closely followed by lack of visibility into endpoints (49%).

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

57%

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

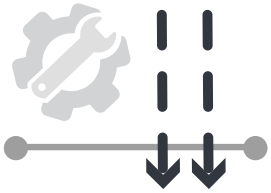


49%

Our team has insufficient visibility into what is happening on endpoints

42%

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



36%

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

Compliance requirements or large fines are mandating the use of continuous monitoring and threat detection 34% | Frequent incident analysis and response events are distracting our team from focusing on the right priorities 25% | Leadership is focused on preventing a public breach and the associated costs, negative headlines, and brand damage 25% | Other 4%

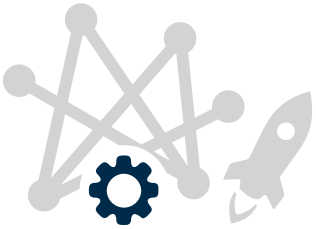
ENDPOINT SECURITY PROBLEMS

Specific challenges with organizations' current endpoint security solutions include insufficient protection against newest attacks (49%), high complexity of deployent and operation (43%), high rates of false positives (31%), and the negative impact of current technologies on user experience (27%).

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

49%

Insufficient protection against the newest attacks

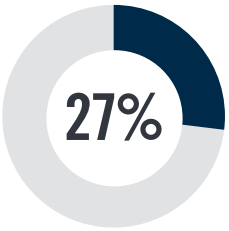


43%

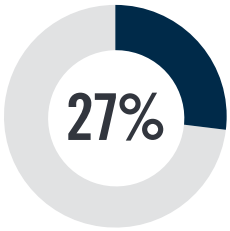
High complexity of deployment and operation

36%

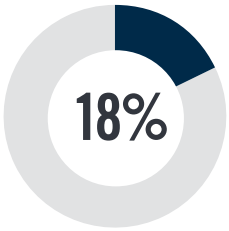
We have good tools and processes in place, but are concerned that threats are still slipping through on endpoints



Negative impact on user productivity/ endpoint performance



High cost of operation



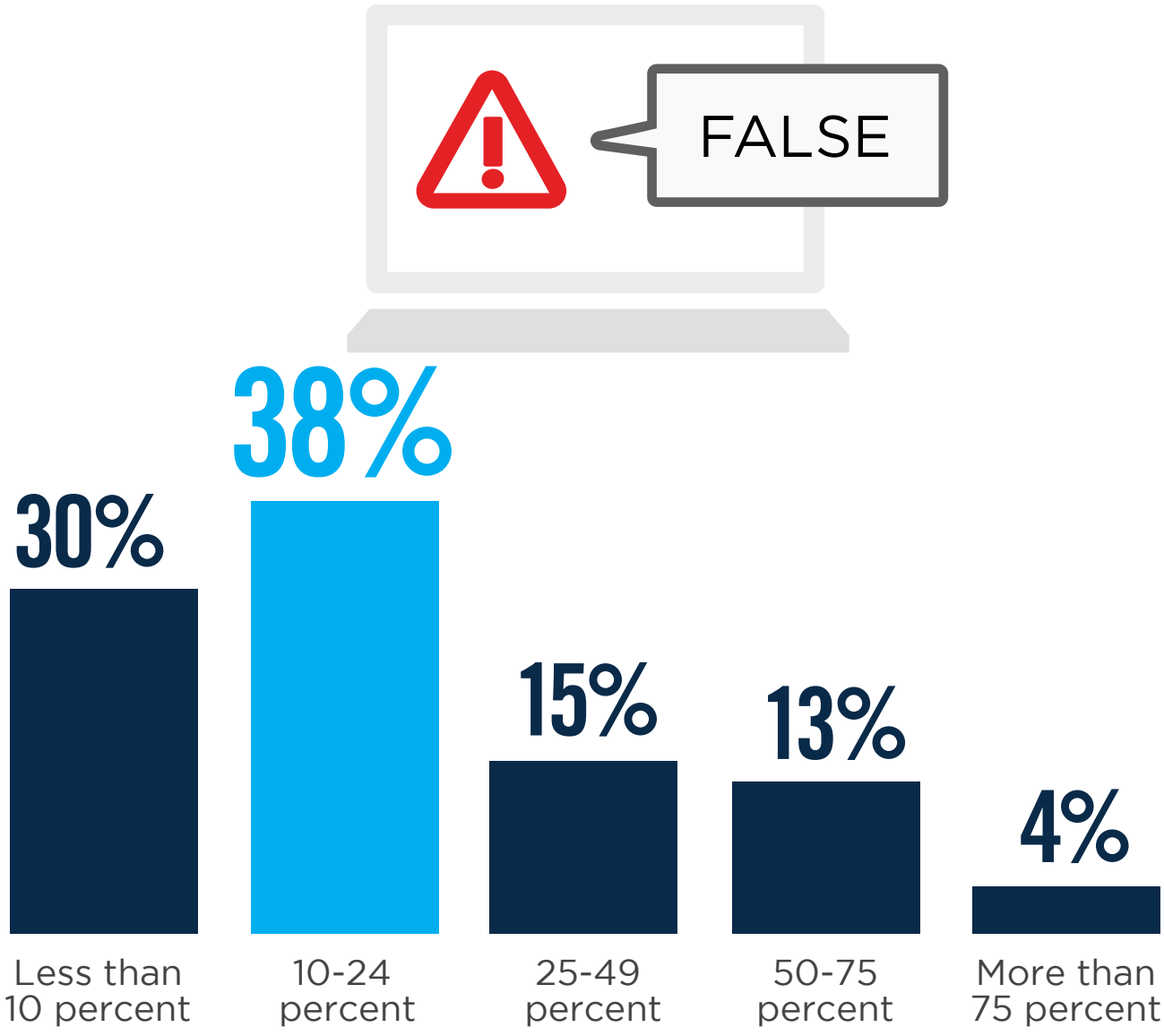
No challenges

Other 4%

FALSE POSITIVES

Highlighted as one of the key endpoint security challenges, a majority of 53% estimate that between 10% and 49% of endpoints security alerts are false positives, with 17% estimating that over 50% of alerts are false positives.

What percentage of endpoint security alerts are false positives?



BIGGEST THREATS

About half of the security threats (48%) that most concern security professionals are endpoint threats, including malware, zero-day attacks, and fileless attacks.

What poses the biggest threat to your organization?

32%

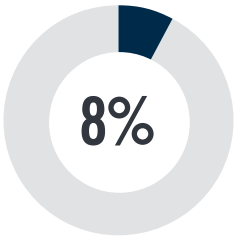
Insider threats
(malicious employee, compromised credentials, accidental release of data)

30%

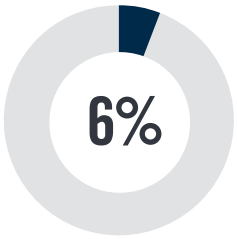
Malware
(ransomware, trojans, exploit kits, etc.)

21%

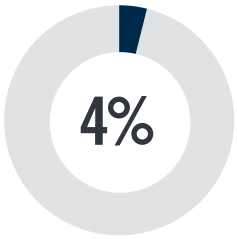
Human error



Zero-day exploits



Misuse of legitimate applications (PowerShell, WMI, MSHTA)

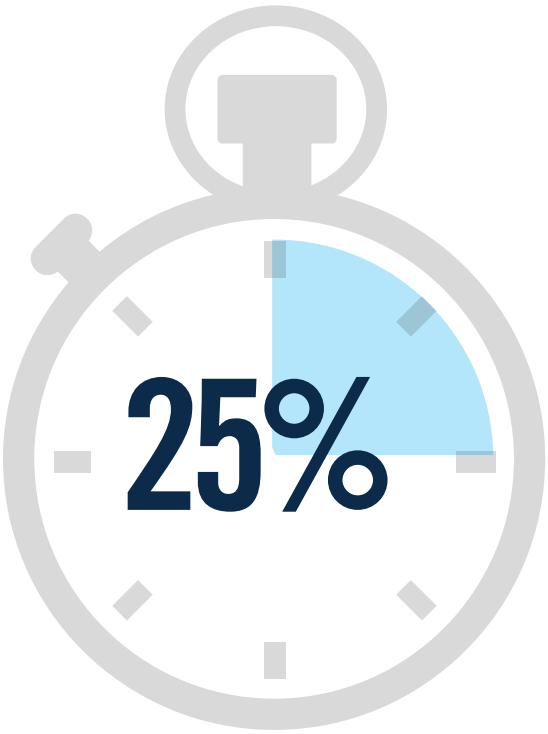


Fileless/in-memory attacks

SLOW TO RECOVER

Asked about their ability to recover from cyber attacks, only 67% of organizations can recover within 1 week (some may not be able to recover at all).

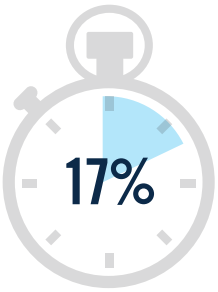
How long did it take your organization to recover from a cyberattack (on average)?



Within one week

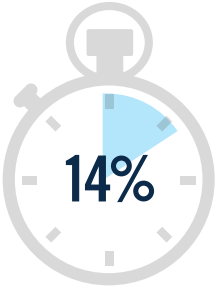
Within minutes

Within 1 month



Within hours

Within 3 months



Within days

> 3 months

No ability to recover 3% | I don't know 11% | Can't disclose 6%

ATTACK IMPACT

The biggest negative impact of endpoint attacks comes from the loss of productivity, both for end users whose work is interrupted (52%) and IT professionals who have to mitigate the attack (40%). System downtime (37%) and Damage to brand and reputation (36%) follow closely.

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

52%

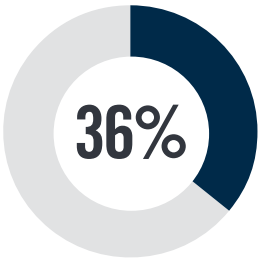
Loss of end user productivity

40%

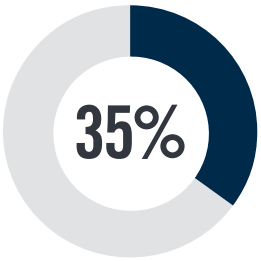
Loss of IT productivity

37%

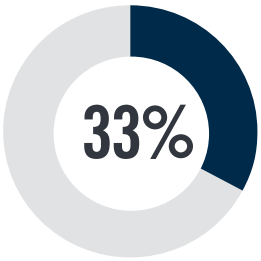
System downtime



Reputation and brand damage



Theft of information assets



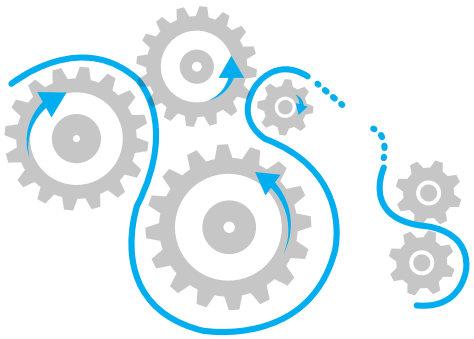
Business/revenue impact

Increased cost 25% | Damage to IT infrastructure 23% | Lawsuits, fines or regulatory actions 13% | Other 8%

IMPACT OF SECURITY INCIDENTS

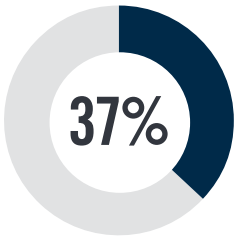
The biggest negative impact of security incidents comes from the loss of productivity, both for employees whose work is interrupted (46%) and IT professionals who have to mitigate the attack (37%).

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

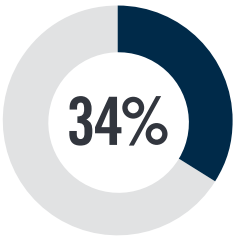


46% Disrupted business activities

36% Reduced employee productivity



Deployment of IT resources to triage and remediate issue



Increased helpdesk time to repair damage

None 20% | Reduced revenue/lost business 20% | Corporate data loss or theft 17% | Loss/compromise of intellectual property 6% | Lawsuit/legal issues 3% | Regulatory fines 3% | Don't know/unsure 20%

ENDPOINT PRIORITIES

When it comes to prioritizing endpoint management capabilities, organziations clearly emphasize detection of endpoint attacks as the top priority. This is followed by IT security operations management to strengthen secuirty posture (55%) and response activities (51%).

What aspect of endpoint threat management is the top priority for your organization?

61%

Detection

55%

IT/Security Operations
(infrastructure and process management)

51%

Response

37%

Triage/Investigation/analysis

ENDPOINT SECURITY CAPABILITIES

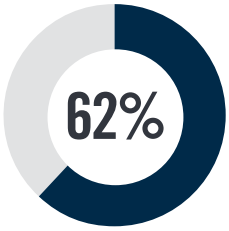
The most important endpoint security capabilities prioritized by organizations is the ability to quickly isolate affected endpoints from the network to prevent or slow the spread of an attack (81%). This is followed by the ability to kill the threatening process or application on the endpoint and quarantining executables (both 74%).

What are the most critical capabilities for effective response to an endpoint attack?

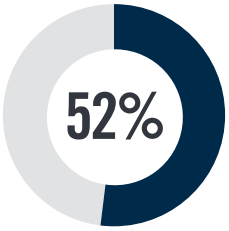
81% Isolate the endpoint from the network

74% Kill the threatening process/application

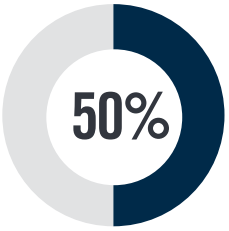
74% Quarantine the executable



Rollback malicious changes



Delete threatening applications/files/ registry keys



Re-image to known good state

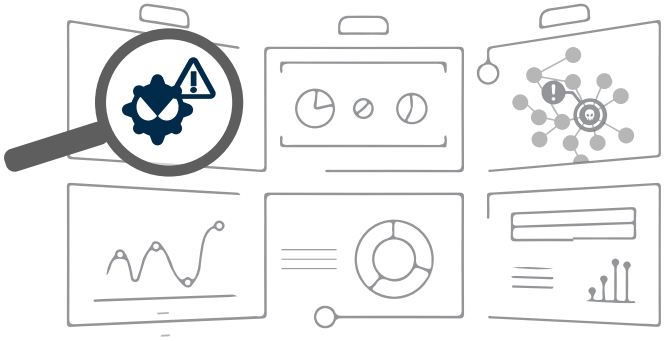
Lock user account / Revoke credentials 33% | Other 2%

CRITICAL EDR CAPABILITIES

Asked about the most critical endpoint detection and response capabilities, organizations emphasize a logical sequence of capabilities starting with automatic detection of suspicious activity (83%), followed by automatic containment of the attack (67%), automatic notification (60%) and threat intelligence integration (60%).

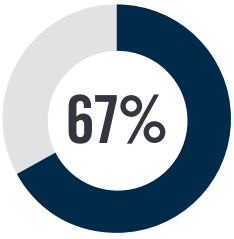
What do you consider the most critical endpoint detection and response capabilities?

83%

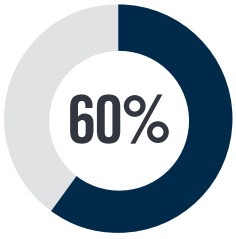


Automatic detection of suspicious activity

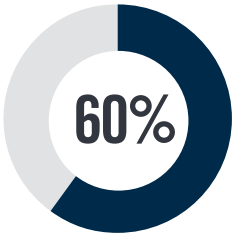
(application access / activity, OS activity, data interaction incl. creation, modification, deletion, transmission, etc., user access)



Automatic containment of attacks



Automatic notification of attacks



Threat intelligence integration

ENDPOINT VISIBILITY

At the device level, IT security professionals look for endpoint visibility into network connections (93%), file modifications (81%), and registry changes (74%).

What level of visibility are you looking for from an endpoint security solution?

93%

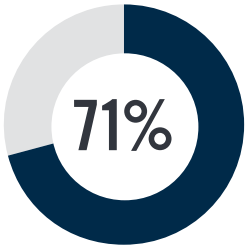
Network connections

81%

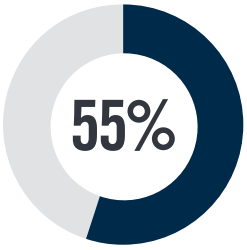
File modifications

74%

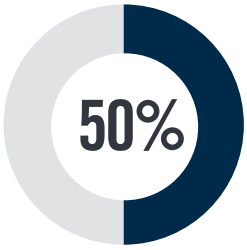
Registry changes



Process information



Memory content and structures

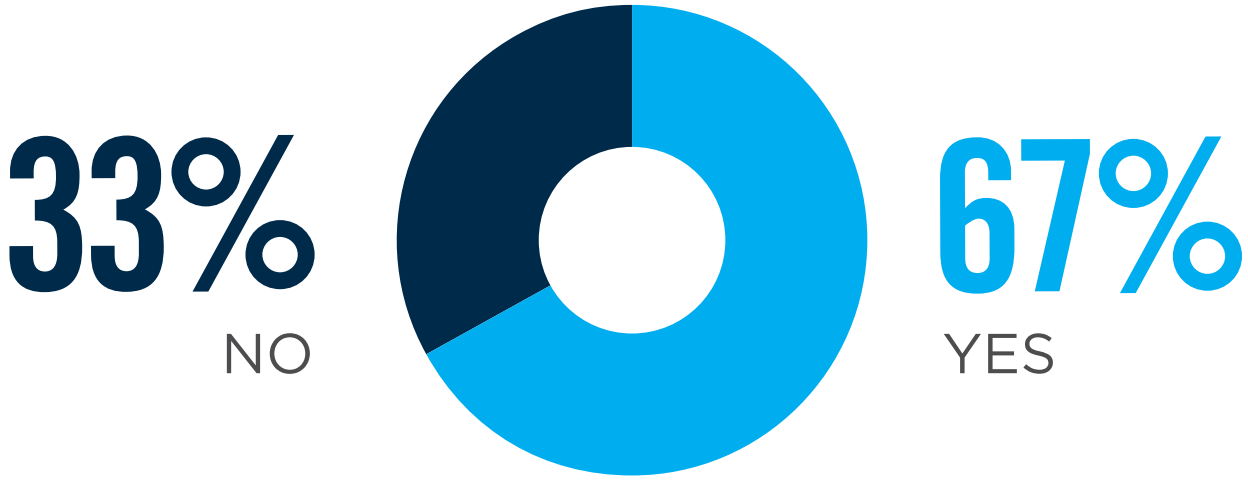


User informatiom

ENDPOINT PROTECTION
CLIENTS VS SERVERS

A majority of 67% confirm they use the same endpoint protection solution on their Windows client endpoints as on their Windows servers.

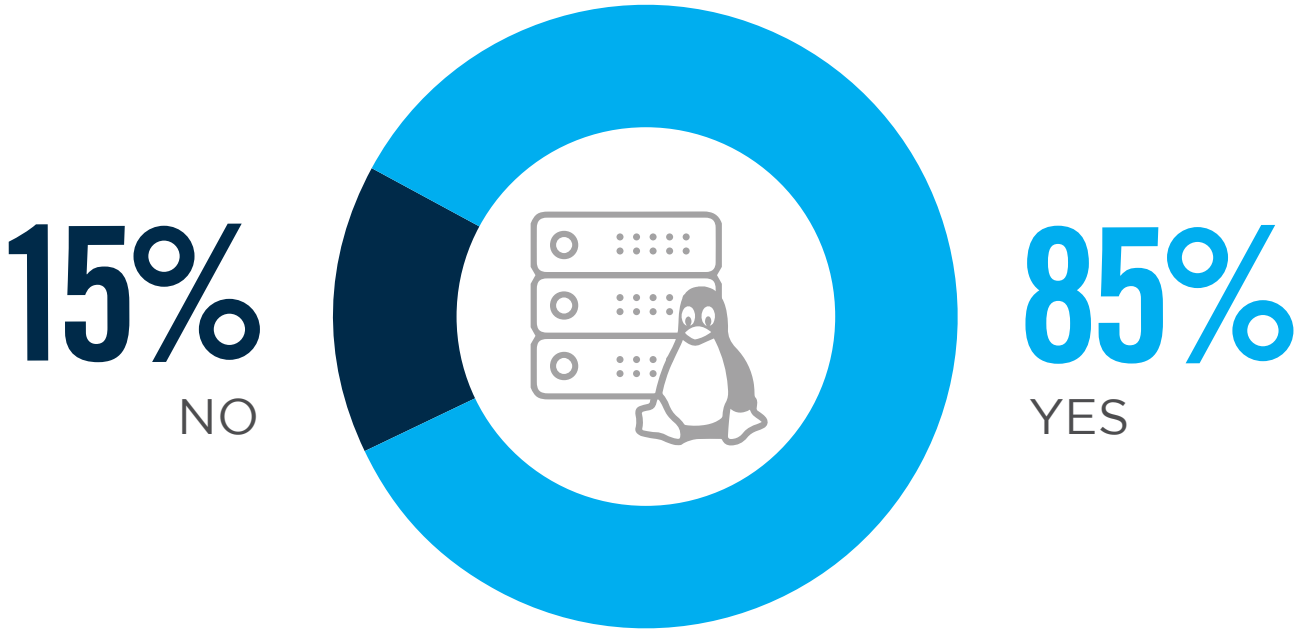
Do you use the same endpoint protection solution on your Windows client endpoints (Win 7, 8, 10) vs. Windows Servers (2008, 2012, 2016)?



ENDPOINT PROTECTION ESSENTIAL FOR LINUX SERVERS

An overwhelming majority of 85% respondents believe endpoint protection is essential for Linux servers.

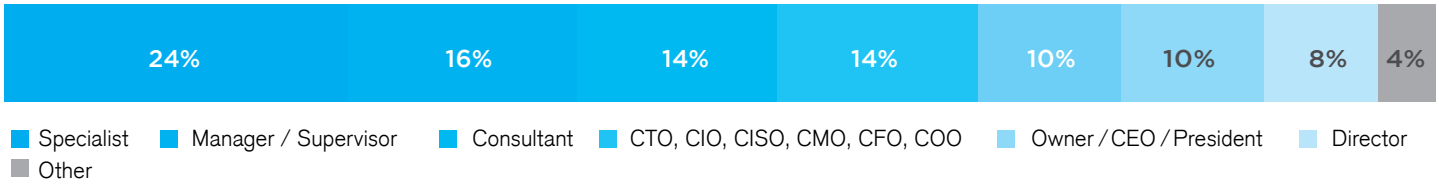
Do you believe endpoint protection is essential for Linux servers?



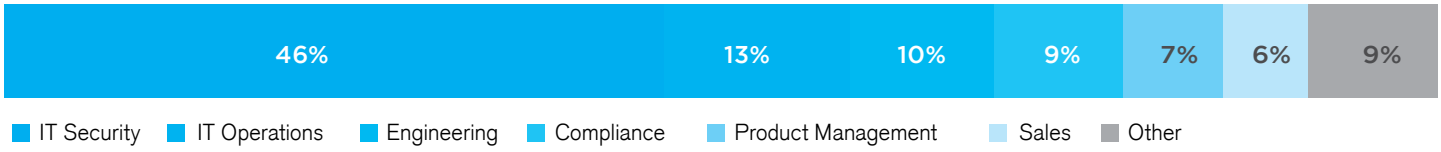
METHODOLOGY & DEMOGRAPHICS

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.

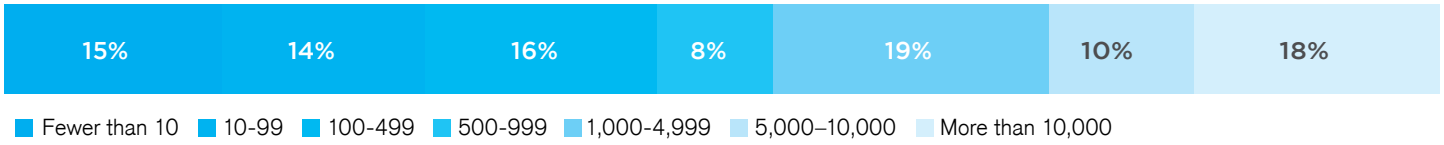
CAREER LEVEL



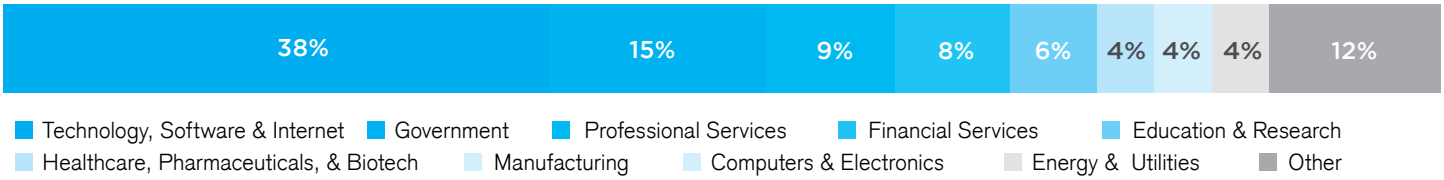
DEPARTMENT



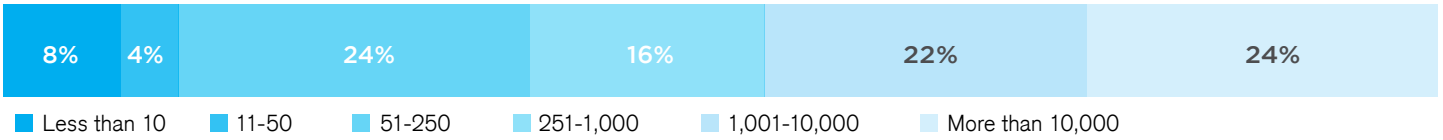
COMPANY SIZE



INDUSTRY



NETWORK-CONNECTED ENDPOINTS SUPPORTED



enSilo comprehensively and automatically secures the endpoint pre- and post-infection in real-time and orchestrates incident response. A single lightweight agent includes next generation antivirus, application communication control, automated endpoint detection and response with real-time blocking, threat hunting, incident response and virtual patching capabilities. With enSilo, organizations can effectively manage malware threats without alert fatigue, excessive dwell time or breach anxiety.

+1 800 413 1782 | sales@ensilo.com

www.ensilo.com