TANIUM

2022 INSIGHTS STUDY

# Endpoint security visibility report

## See cyber threats coming

Cybersecurity INSIDERS

TANIUM

## Key findings

Malware (specifically ransomware, trojans, exploit kits, etc.) poses the biggest security threat to organizations (35%). This is followed by human error (24%), insider threats (20%) and zero-day exploits (11%).

Cybersecurity professionals prioritize lack of 24/7 security coverage (38%) and speed of incident response (36%) as the two most critical security challenges.

Reduced employee productivity (44%) and disrupted business activities (38%) are the top-two negative business impacts resulting from a security incident.

The most significant impact of endpoint attacks against organizations is the loss of end user productivity (48%).

INTRODUCTION

# The recent, massive shift to remote work has increased the complexity of securing the endpoint.

The 2022 Endpoint Security Visibility Report reveals real impacts to business when there is a security incident. The report highlights what is and what is not working for securing the endpoint.

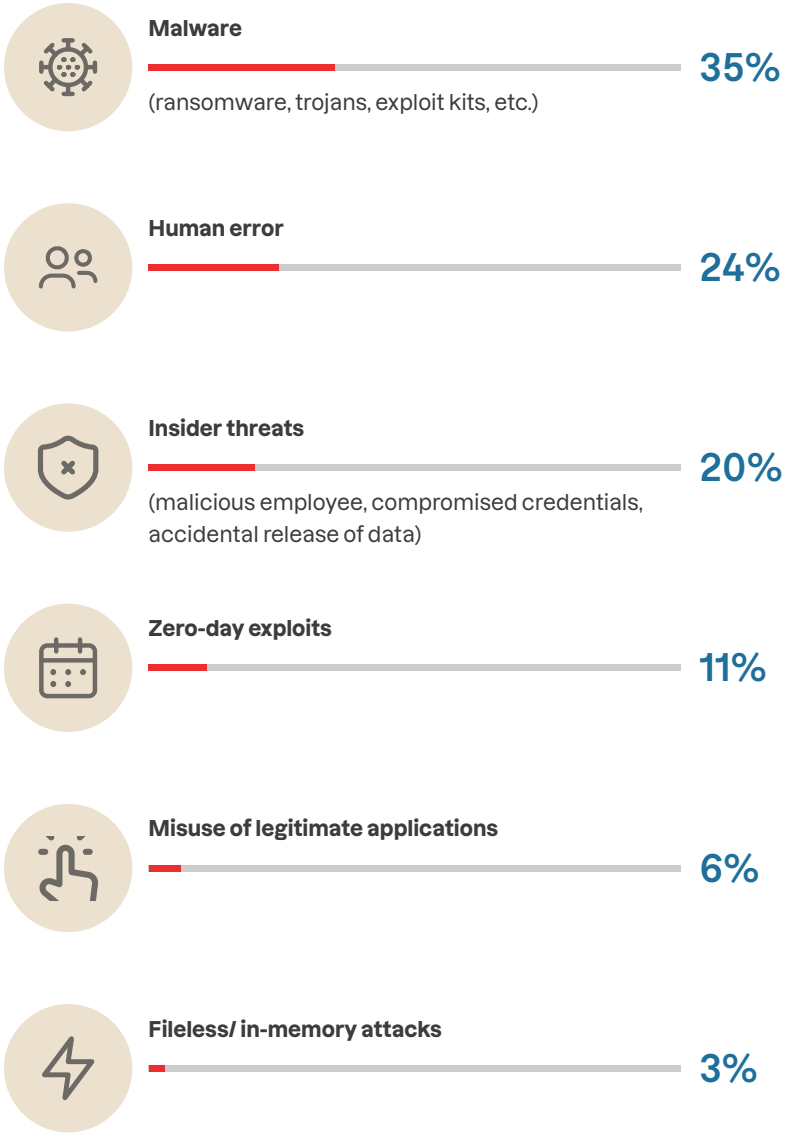
The 2022 Endpoint Security Visibility Report has been produced by Cybersecurity Insiders, the 500,000-member information security community, to explore the latest trends, key challenges, gaps, and solution preferences for endpoint security. We hope you find this report informative and helpful as you continue your efforts in securing your organization.

ENDPOINT SECURITY THREATS

# What poses the biggest security threat to your organization?

The survey reveals that malware (specifically ransomware, trojans, exploit kits, etc.) poses the biggest security threat to organizations (35%). This is followed by human error (24%), insider threats (20%), and zero-day exploits (11%).

To find, isolate, and eradicate threats, IT organizations must have an accurate inventory of their IT estate.

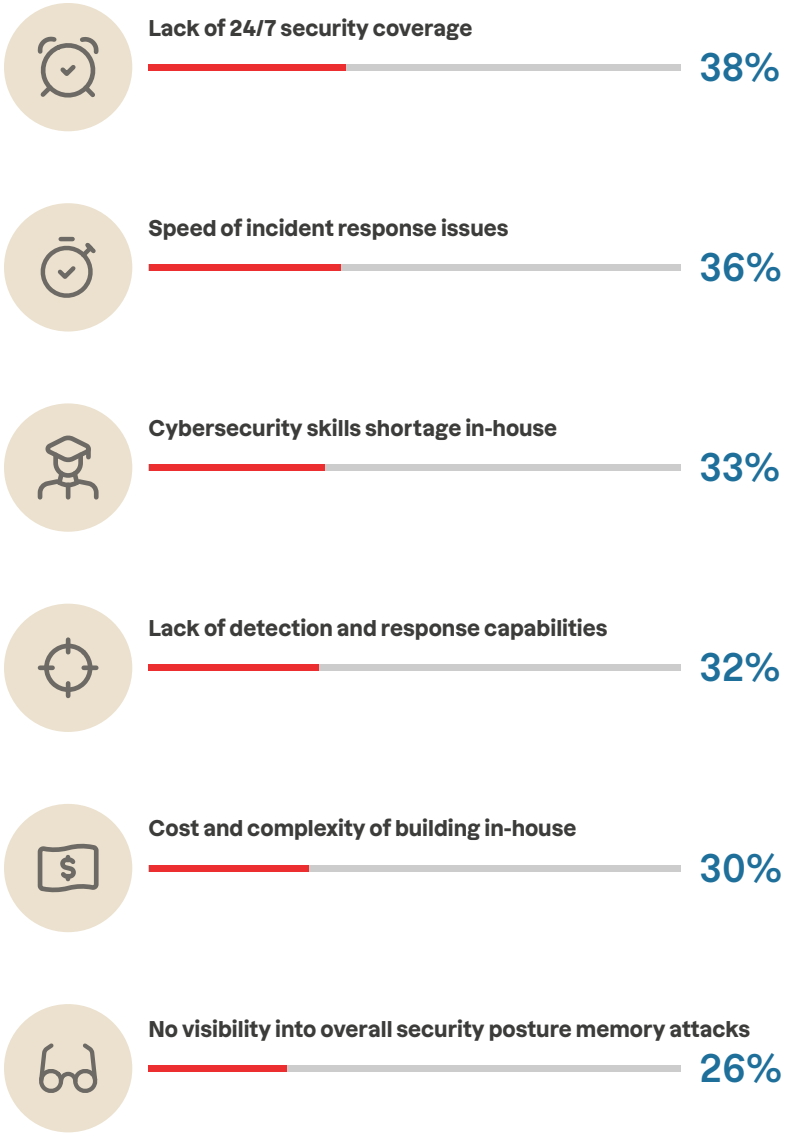



Tanium makes this possible in minutes – not days or weeks – and accounts for devices on premises or in the cloud.

SECURITY OPERATIONS CHALLENGES

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

When asked about the biggest security operations challenges, cybersecurity professionals prioritize lack of 24/7 security coverage (38%) and speed of incident response (36%) as the two most critical security challenges.



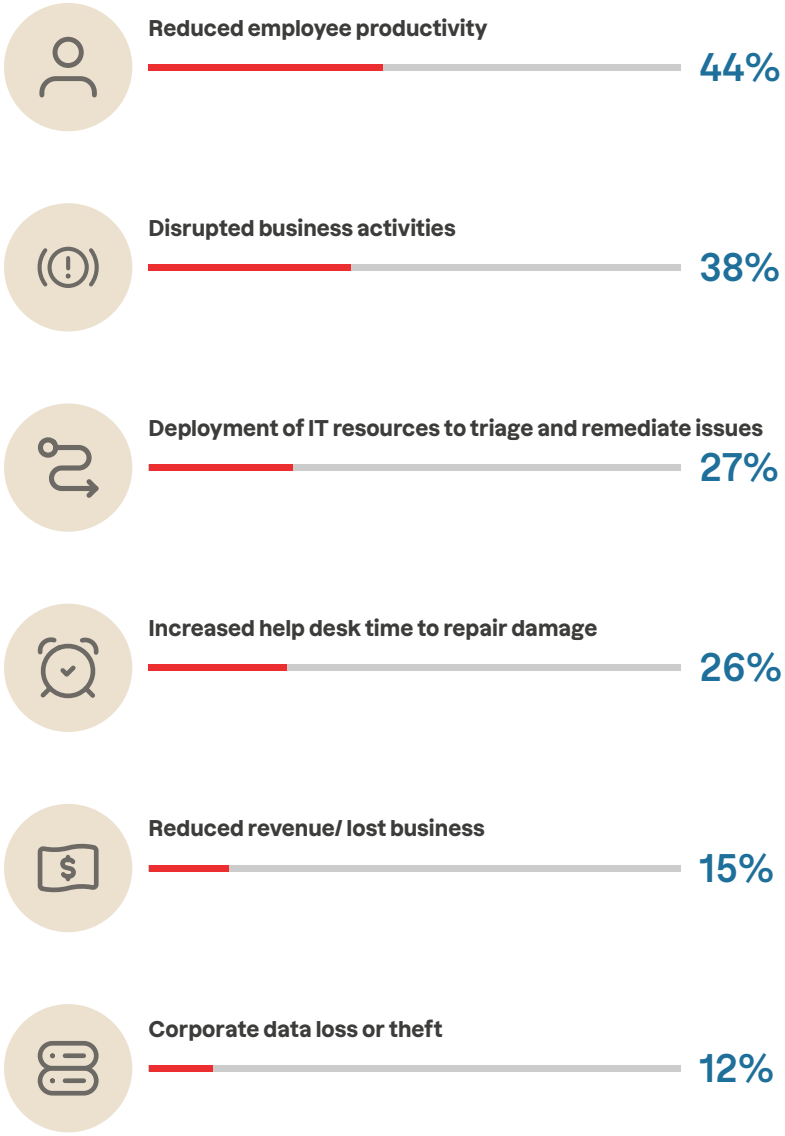

Speed of deployment and provisioning issues 24%
Inability to meet compliance requirements 15%
Lack of customization of correlation rules and reports 14%
Other 8%

Tanium offers real-time security and operational data that helps IT teams see, respond to, and eliminate threats rapidly.

SECURITY INCIDENTS

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

Security incidents have a real-world impact on businesses. Survey respondents most often mentioned reduced employee productivity (44%) and disrupted business activities (38%) as the top-two negative business impacts resulting from a security incident.



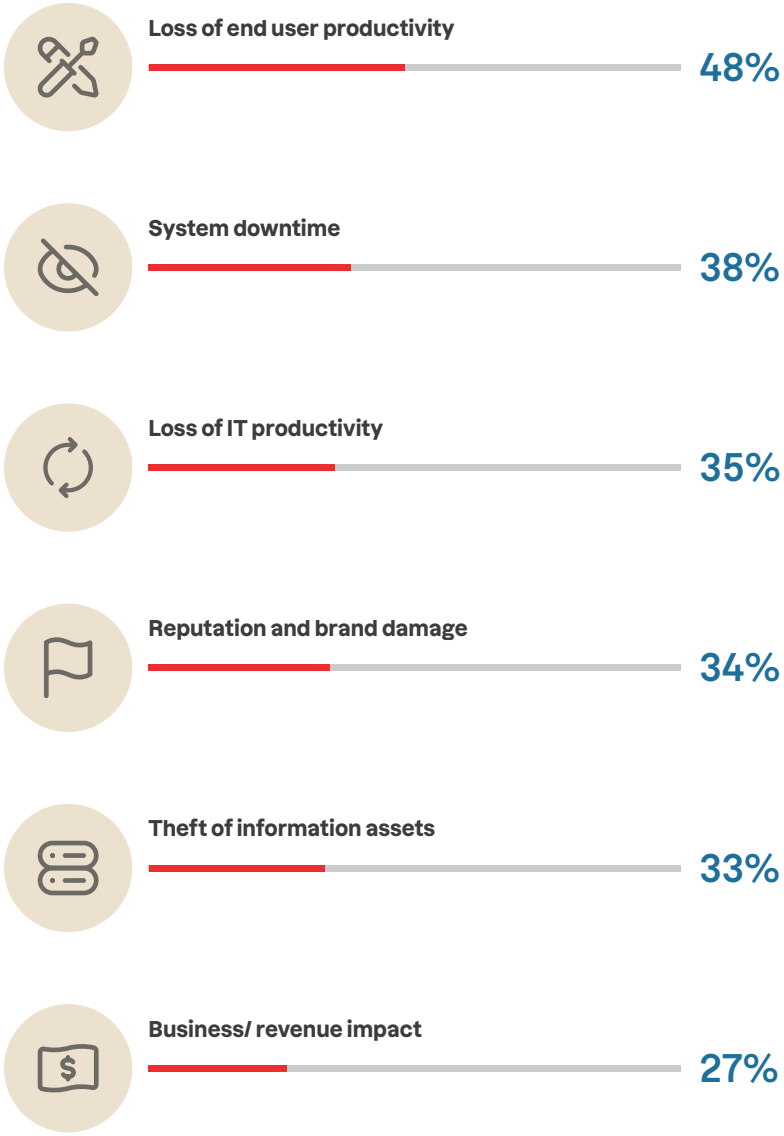

Loss/compromise of intellectual property 9%
Regulatory fines 7%
Lawsuit/legal issues 7%
None 24%
Don't know/unsure 18%

Tanium helps security teams respond faster when incidents occur so disruptions can be minimized and business as usual can resume as quickly as possible.

IMPACT OF ENDPOINT ATTACKS

## What was the most significant impact of endpoint attacks against your organization?

When asked about the most significant impact of endpoint attacks against their organizations, cybersecurity professionals are most concerned about loss of end user productivity (48%).



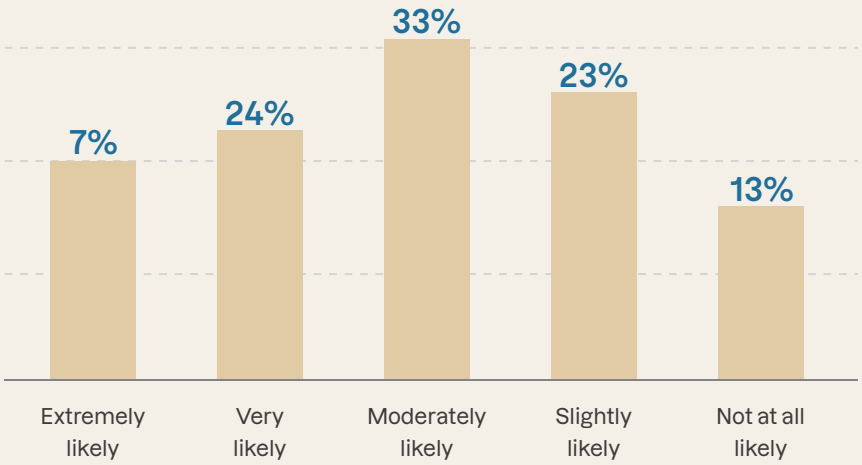

Increased cost 25%
Damage to IT infrastructure 20%
Lawsuits, fines, or regulatory actions 13%
Other 9%

Tanium allows IT teams to manage, inventory, monitor, contextualize, and remediate end user, server, and cloud endpoints with ultimate visibility and control at scale to keep everything up-to-date and secure.

RISK OF FUTURE ATTACKS

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

Cybercrime is growing in prevalence and sophistication, targeting every industry around the world. A majority, 64%, believe it is moderately likely to extremely likely that they will be the victim of a successful cyberattack in the next 12 months. Only 13% believe that a compromise is not at all likely.




# 64%

believe organizations are extremely to moderately likely to become compromised by a successful cyberattack in the next 12 months.

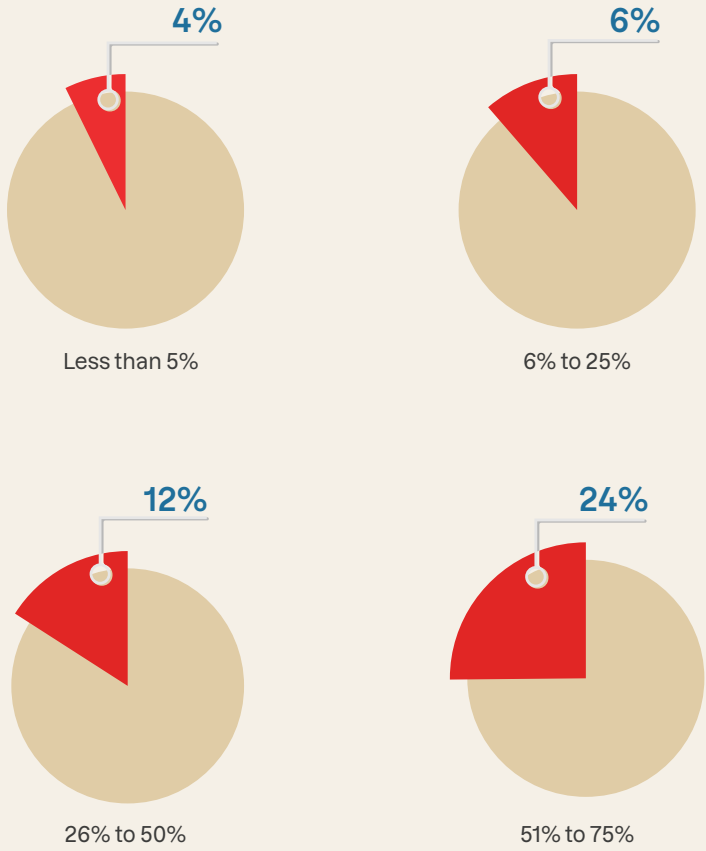
Tanium helps IT teams achieve visibility across endpoints in minutes and locate unmanaged assets on premises or in the cloud.

They can then quickly choose to block unmanaged devices or bring them under management, minimizing security risks.

STOPPING ENDPOINT ATTACKS

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

While nearly half (45%) of cybersecurity professionals believe their existing security posture can stop most endpoint attacks (75% or more), the majority do not.




Tanium allows IT teams to ask questions in plain English to understand the state of their endpoints, examine results, and take action in real time.

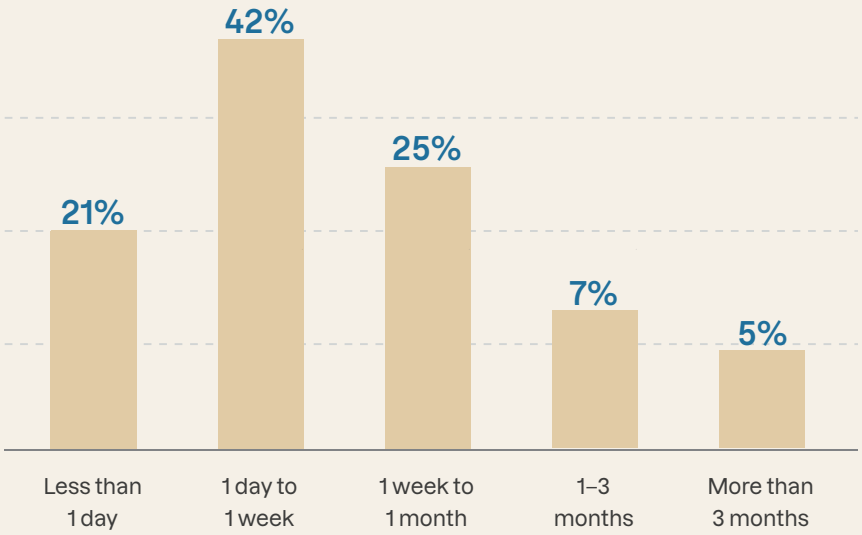
45%

estimate that more than 75% of endpoint attacks can be stopped.

SLOW TO PATCH

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

Organizations are still slow at doing the basics. When asked how long it takes their organization (on average) to roll out a critical security patch, the top answer was between one day and one week (42%). But even in the span of a single day, breaches can wreak havoc.

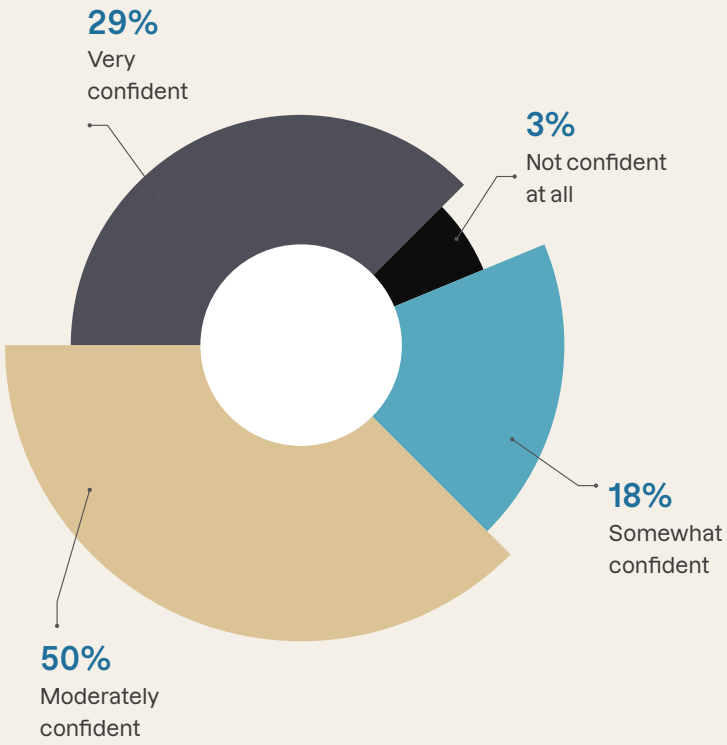



Tanium reduces the time it takes to update endpoints from weeks, days, or hours, down to minutes.

CONFIDENCE IN PATCHES

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

Cybersecurity professionals are, on average, moderately confident in the effectiveness of security patches (50%). Only a third claims to be very confident in patch effectiveness.

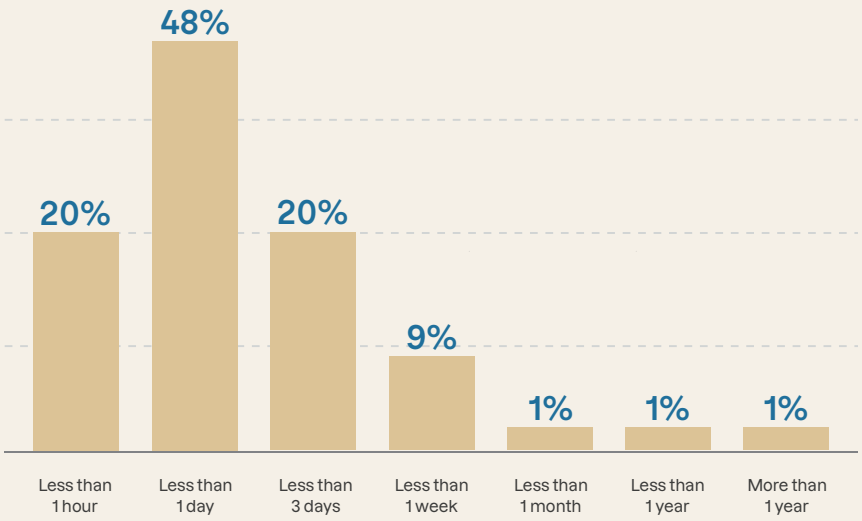



Tanium can increase confidence levels with proactive patching that will substantially reduce security breaches by helping ensure all “doors” are locked.

REMEDIATION TIME

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

A majority of organizations (68%) claim a remediation time of less than a day, following an endpoint attack.



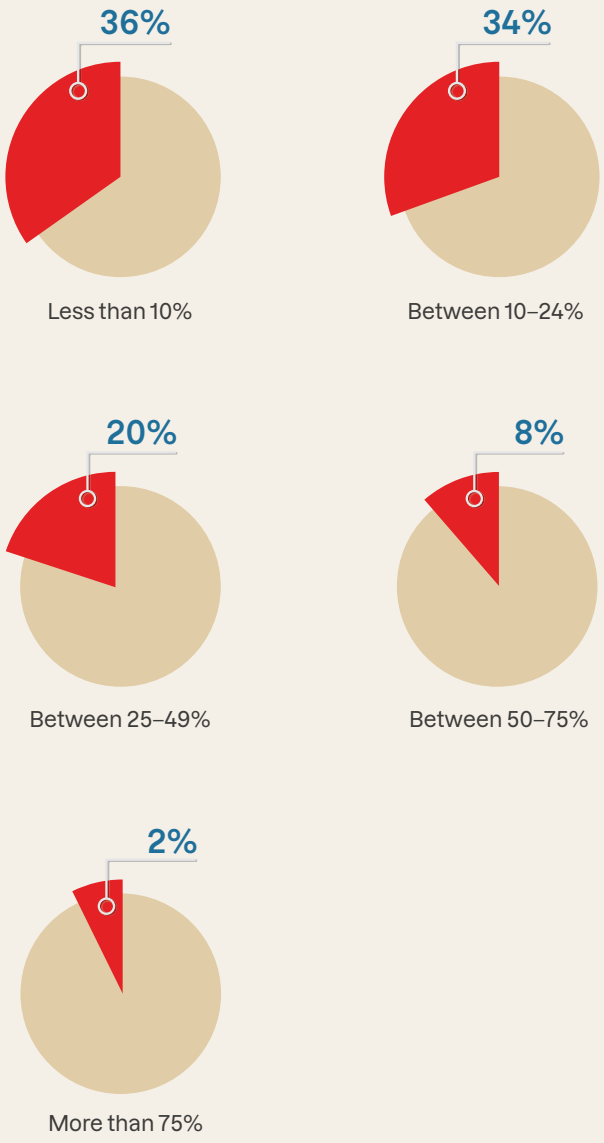

Tanium delivers real-time security and operational data and allows IT teams to see, respond to, and eliminate threats quickly, taking remediation time from hours to minutes.

FALSE POSITIVES

# What percentage of endpoint security alerts do you estimate are false positives?

False positives drain valuable resources and time that could be spent more productively on actual threats.

A majority, 54%, estimate that between 10% and 49% of endpoint security alerts are false positives, with 10% estimating that more than half of alerts are false.

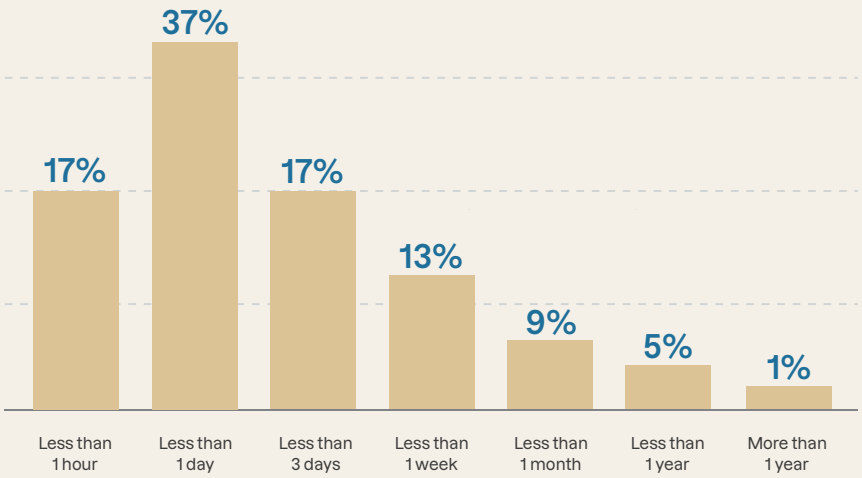



Tanium can accurately investigate, correlate, and then confirm or disprove this alert on any endpoint.

LATERAL MOVEMENT

## How long does it take your organization to ID and track lateral movement?

When asked about the time required to detect lateral movement, 37% of respondents say it takes their organization less than a day to identify and track lateral movement.

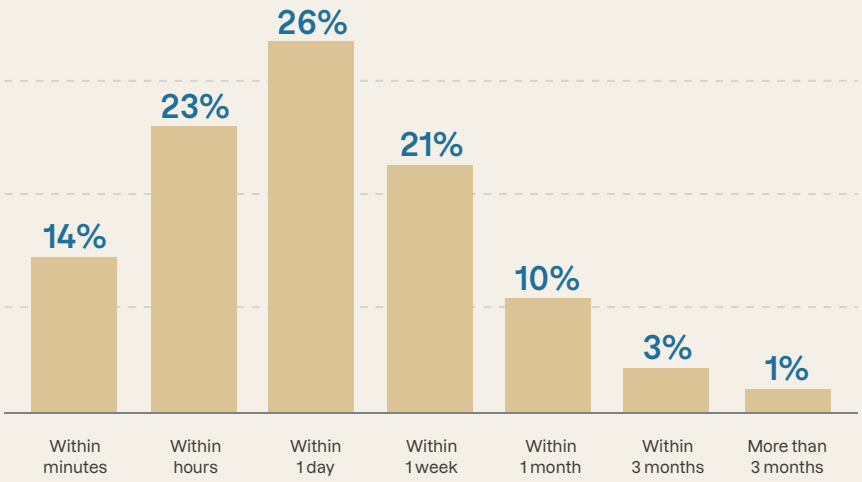



Tanium reduces lateral movement risk with real-time data visualizations that help IT teams prioritize and remediate overly permissive admin rights.

SLOW TO RECOVER

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

With only 26% of surveyed business leaders saying that their organization recovered from a cyberattack within one day (on average), it's clear that many organizations struggle to recover from breaches.




63%

of organizations take between minutes to a day to recover

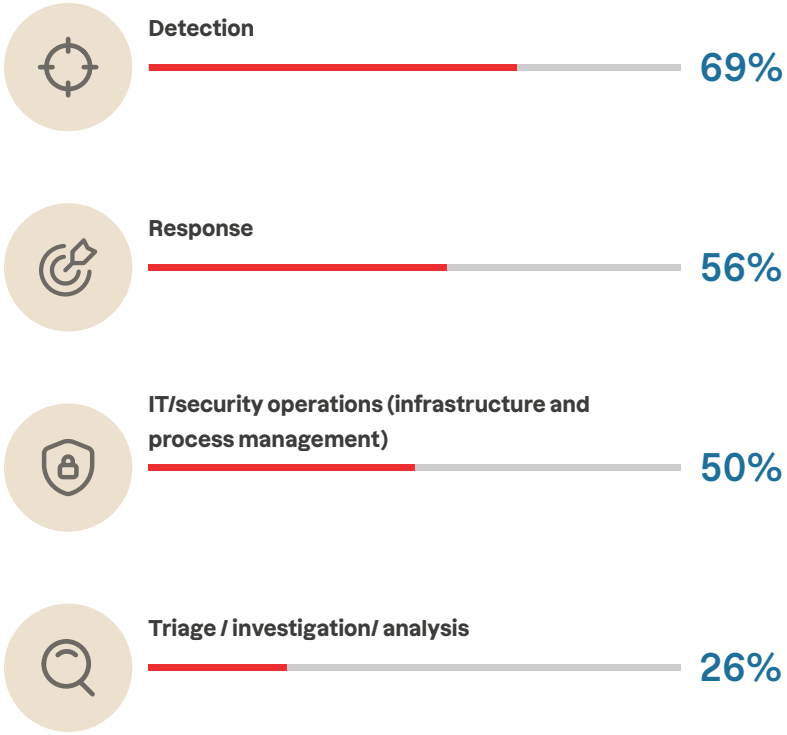
No ability to recover 1%

Tanium's architecture makes it possible to query millions of endpoints in seconds using a single agent, single console, and zero intermediate infrastructure.

ENDPOINT THREAT MANAGEMENT

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

When asked about their priorities for endpoint threat management, most organizations focus on threat detection (69%) over threat response (56%).




From detection and response, to investigation and triage, Tanium has the ability to unite IT operations and security teams by endpoint data and providing real-time visibility into what's happening in the environment.

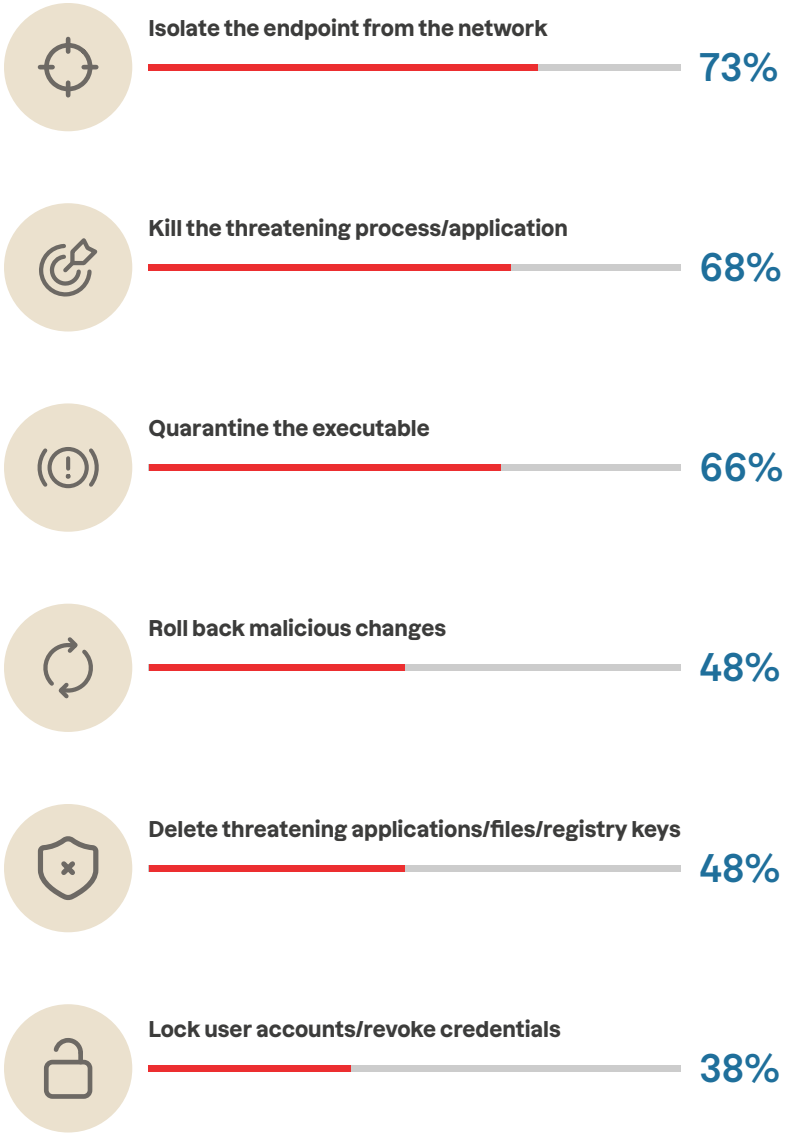
Other 5%

EFFECTIVE RESPONSE CAPABILITIES

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

We asked cybersecurity professionals about the capabilities they consider most critical for effective response to an endpoint attack. Most organizations prioritize isolating the endpoint from the network (73%), followed by killing the threat process or application (68%), and quarantining the executable (66%) as the three most critical capabilities for effective endpoint attack response.

Tanium adapts to incidents, so organizations can fully understand them by using remote forensic investigation on suspicious machines, equipping them to take a wide variety of remedial actions, such as imposing network quarantines, deploying patches, or running custom scripts.

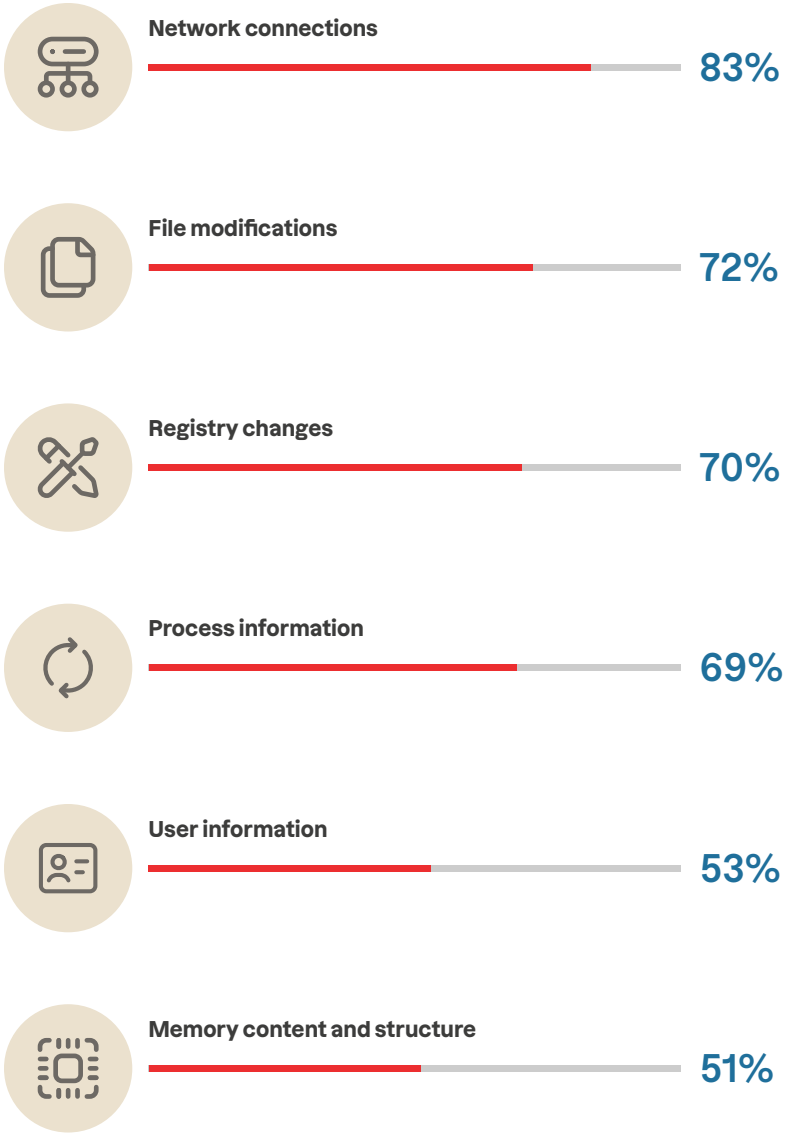



Reimage to known good state 36%
Other 4%

ENDPOINT SECURITY VISIBILITY

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

When asked about the level of visibility organizations expect from an endpoint security solution, the most mentioned priority is visibility into network connections (83%), followed by file modifications (72%).



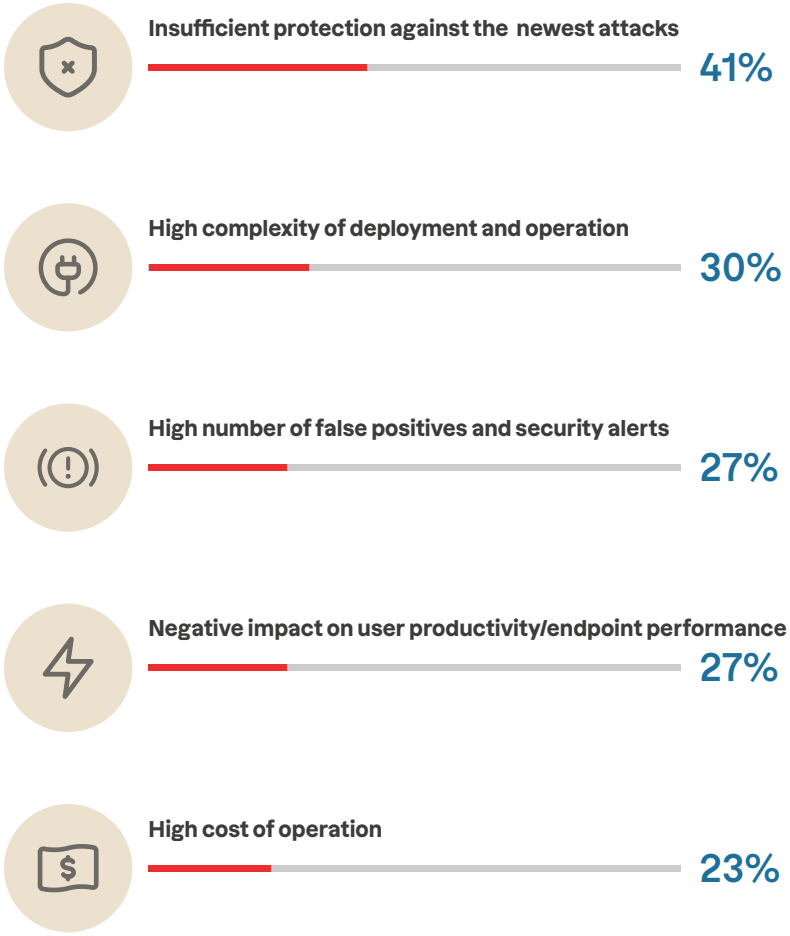

Binary file 41%
Other 3%

Tanium was built from the ground up for deeper and faster visibility, delivering real-time endpoint data to inform critical IT decisions.

ENDPOINT PROTECTION CHALLENGES

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

Survey respondents view insufficient protection against the newest attacks (41%) and high complexity of deployment and operation (30%) as the biggest challenges with their current endpoint protection solution.




No challenges 18%
Other 6%

Tanium allows IT organizations to ask questions about their environment in plain English and see real-time endpoint activity, equipping them with the ability to see cyber threats coming.

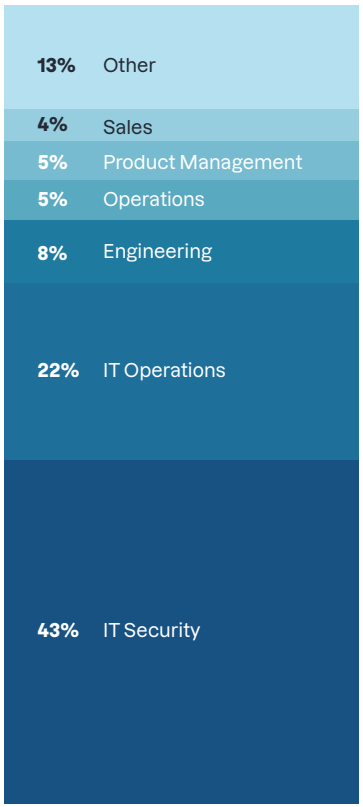
# Demographics

This 2022 Endpoint Security Visibility Report is based on the results of a comprehensive online survey of 345 cybersecurity professionals, conducted in September 2021, to gain deep insight into the latest trends, key challenges, and solutions for endpoint solutions.

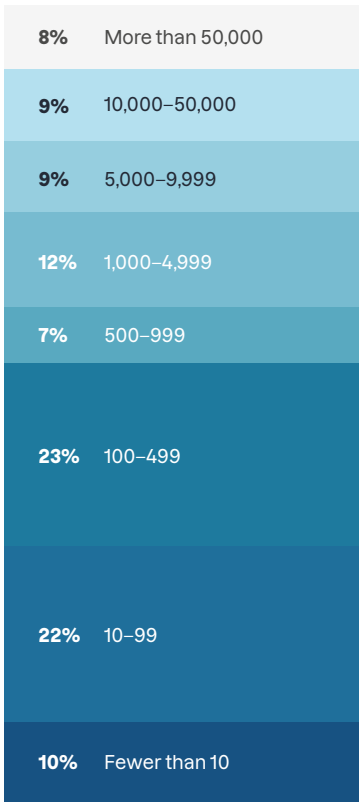
The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross section of organizations of varying sizes across multiple industries.

### Career level

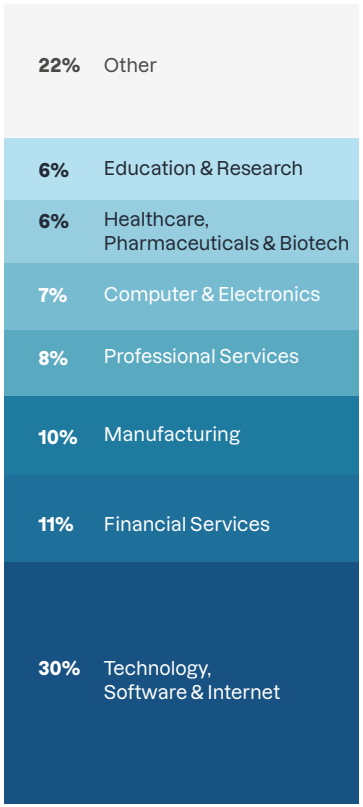

### Department




### Company size




### Industry



Tanium is the platform that organizations trust to gain visibility and control across all endpoints in on-premises, cloud and hybrid environments. Our approach addresses today's increasing IT challenges by delivering accurate, complete and up-to-date endpoint data — giving IT operations, security and risk teams confidence to quickly manage, secure and protect their networks at scale. Tanium's mission is to help see and control every endpoint, everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.