2020

ENDPOINT AND IOT ZERO TRUST SECURITY REPORT

Cybersecurity INSIDERS

Research Sponsor

Pulse Secure®

OVERVIEW

The diversity of users, devices, networks, and threats continue to grow as enterprises take advantage of greater workforce mobility, workplace flexibility, and cloud computing opportunities. Not only do organizations need to ensure endpoints are secure and adhering to usage policy, but they must also manage appropriate IoT device access. New Zero Trust security controls can fortify dynamic device discovery, verification, tracking, remediation, and access enforcement. What are the trends and defense mechanisms that IT and security decision-makers should consider to reduce their attack surface and mitigate endpoint and IoT security risks?

The 2020 Zero Trust Endpoint and IoT Security report surveyed more than 325 IT decision-makers ranging from technical executives to IT security practitioners representing a balanced cross-section of organizations of varying sizes to understand key issues, considerations, initiatives, and investments regarding how enterprises are advancing Zero Trust endpoint and IoT security capabilities within their individual organization.

Key findings include:

- 72% of organizations experienced an increase to significant increase in endpoint and IoT security due to workforce mobility and remote workplace flexibility – the top 3 issues being malware, insecure network and remote access and compromised credentials.
- 56% anticipate moderate to extremely likelihood to be compromised by a successful cyberattack originating from endpoints or IoT devices.
- 48% expressed moderate to unlikely means to discover, identify and respond to unknown, unmanaged or insecure devices accessing network and cloud resources.
- 53% plan to increase their near-term endpoint and IoT security expenditures.
- 41% will implement or advance on-premise device security enforcement (NAC), 35% will advance their remote access devices posture checking, and 22% will advance their IoT device identification and monitoring capabilities.

Many thanks to Pulse Secure for supporting this important research project. 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

IMPORTANCE OF ENDPOINT AND IOT SECURITY

An overwhelming majority of organizations (78%) agree that endpoint and IoT security is becoming increasingly important as part of their overall IT security strategy.

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

ENDPOINT AND IOT DEVICE THREATS

Organizations are concerned mostly (78%) with malware remaining the single biggest threat to endpoint and IoT devices. This is followed by insecure network access (61%) and compromised credentials (58%).

What endpoint and IoT device threats is your organization most concerned with?

78%

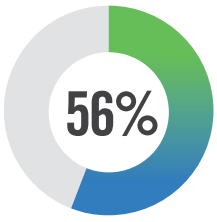
Malware
(e.g., ransomware, trojans, exploit kits, etc.)

61%

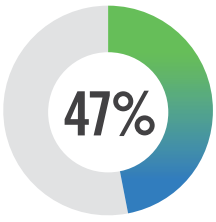
Insecure network access, remote access or data transfer

58%

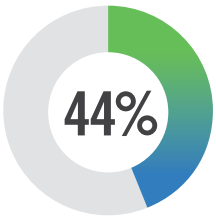
Compromised credentials, weak authentication/ passwords



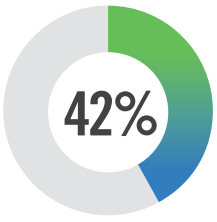
Compromised device



Lack of endpoint compliance, insecure device use
(e.g., poor settings, not updated)



Unknown, unmanaged device



Zero-day exploit

Other 2%

DRIVERS FOR ZERO TRUST CAPABILITIES

When asked about the key drivers for requiring greater security capabilities, 42% of organizations mentioned the inability to efficiently identify, classify and monitor endpoint and IoT devices. This is followed experiencing endpoint security issues despite having tools in place (39%) and by compliance requirements (36%).

What are the key drivers for invoking greater, Zero Trust EDR capabilities?

42%

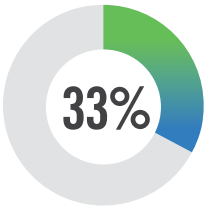
Our team is unable to efficiently identify, classify and monitor endpoint and IoT devices

39%

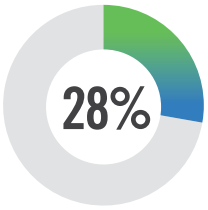
Experiencing endpoint security issues despite tool use

36%

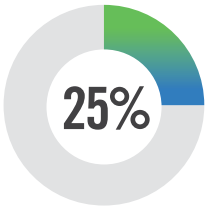
Compliance requirements and penalties are mandating the use of continuous monitoring and threat detection



Our team has insufficient visibility into what is happening on endpoint and IoT devices



IT management initiative to advance zero trust model requiring endpoint verification controls and policy compliance



Existing endpoint detection and response products are failing to stop an increased number of threats

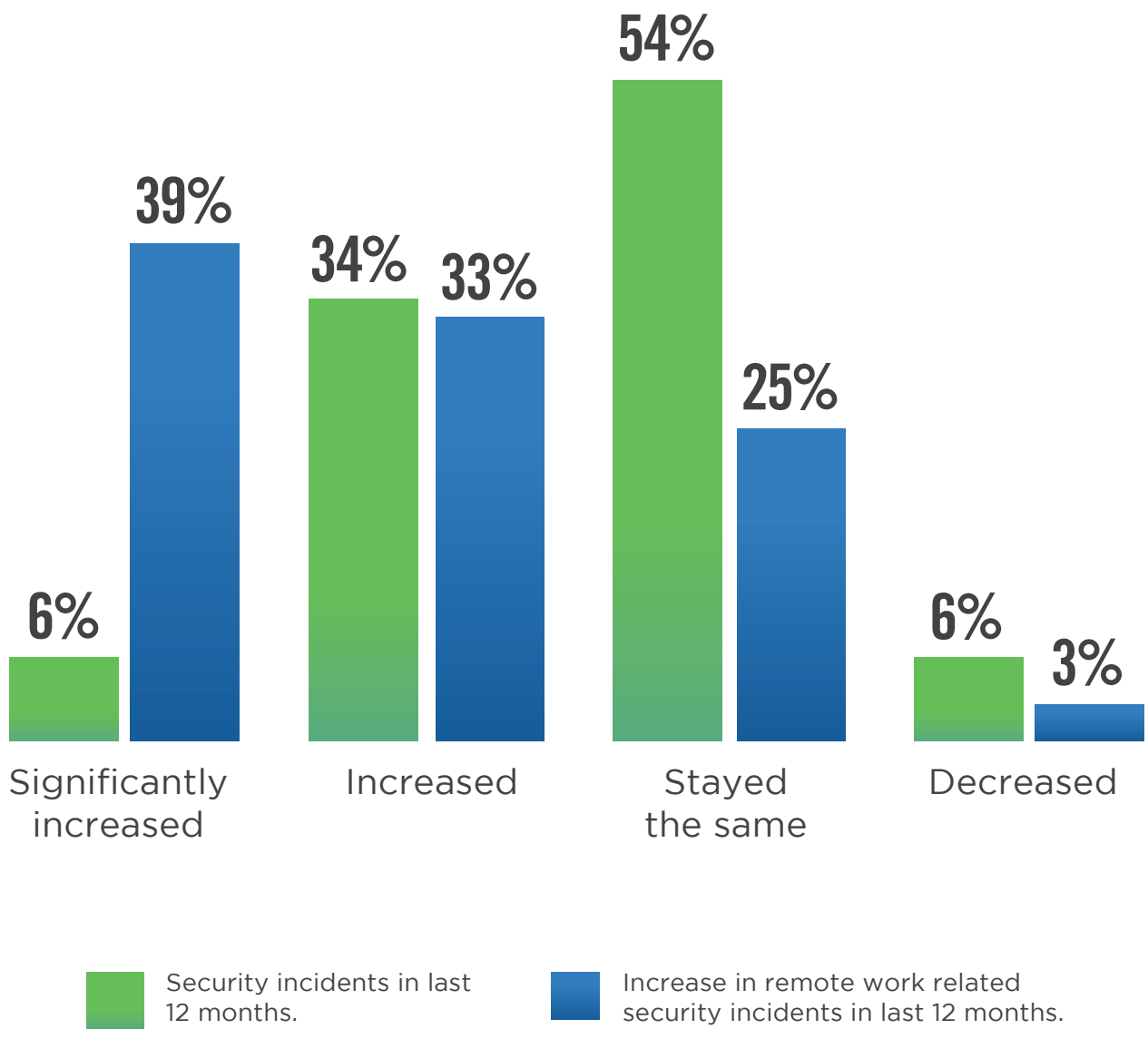
Leadership initiative to prevent a public breach with its associated costs and brand damage 22% | As part of our technology assessment cycles, we are in the process of replacing or expanding endpoint and IoT security tools 19% | Frequent endpoint and IoT security incidents are affecting our team from focusing on the right priorities 17% | Other 2%

EXTENT OF SECURITY INCIDENTS

Forty percent of organizations have experienced an increased or significantly increased number of endpoint and IoT security incidents. Specifically, the increase in remote work has impacted a 72% increase in security issues of the last 12 months.

How have endpoint and IoT security incidents impacted your organization in the last 12 months?

How has the increase in workforce mobility and remote workplace flexibility (i.e., work from home) in your organization resulted in increased endpoint and IoT security issues in the last 12 months?



IMPACT OF SECURITY ISSUES

The most significant negative impact of security issues was a reported loss of user productivity (55%), followed by loss of IT productivity (45%) and system downtime (42%).

What were the most significant impacts of endpoint and IoT security issue(s) in your organization?

55%

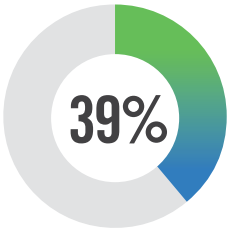
Loss of user productivity

45%

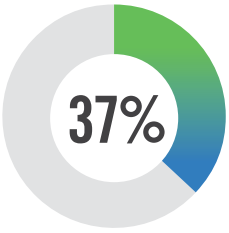
Loss of IT productivity

42%

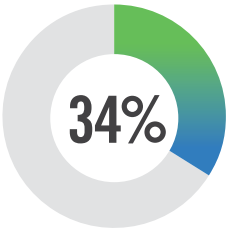
System downtime, compromise



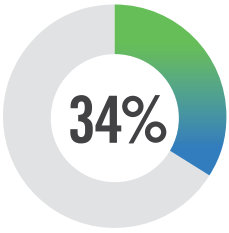
Sensitive data loss or theft



Compliance, fines or legal action



System downtime



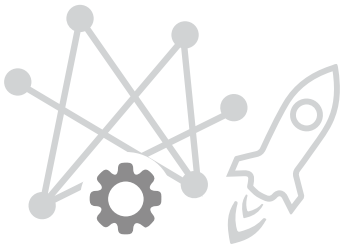
Increased cost

Business revenue impact 29% | Reputation or brand damage 24%

BIGGEST SECURITY CHALLENGES

High complexity of deployment and operations (57%) tops the list of the biggest endpoint and IoT security challenges reported by organizations. This is closely followed by the inability to enforce endpoint and IoT device access/usage policy (43%) and the insufficient protection against the latest threats (40%).

What are the biggest endpoint and IoT security challenges in your organization?



57%

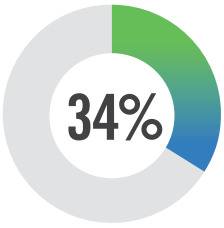
High complexity of deployment and operation

43%

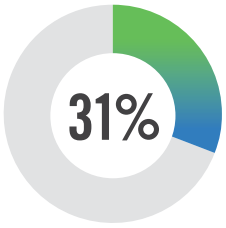
Inability to enforce endpoint and IoT device access/ usage policy

40%

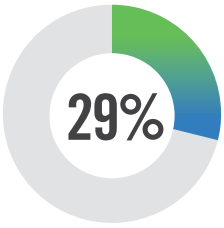
Insufficient protection against the newest threats



High cost of operation



Negative impact on user productivity and endpoint performance



Inability to ensure device security is installed, running and current

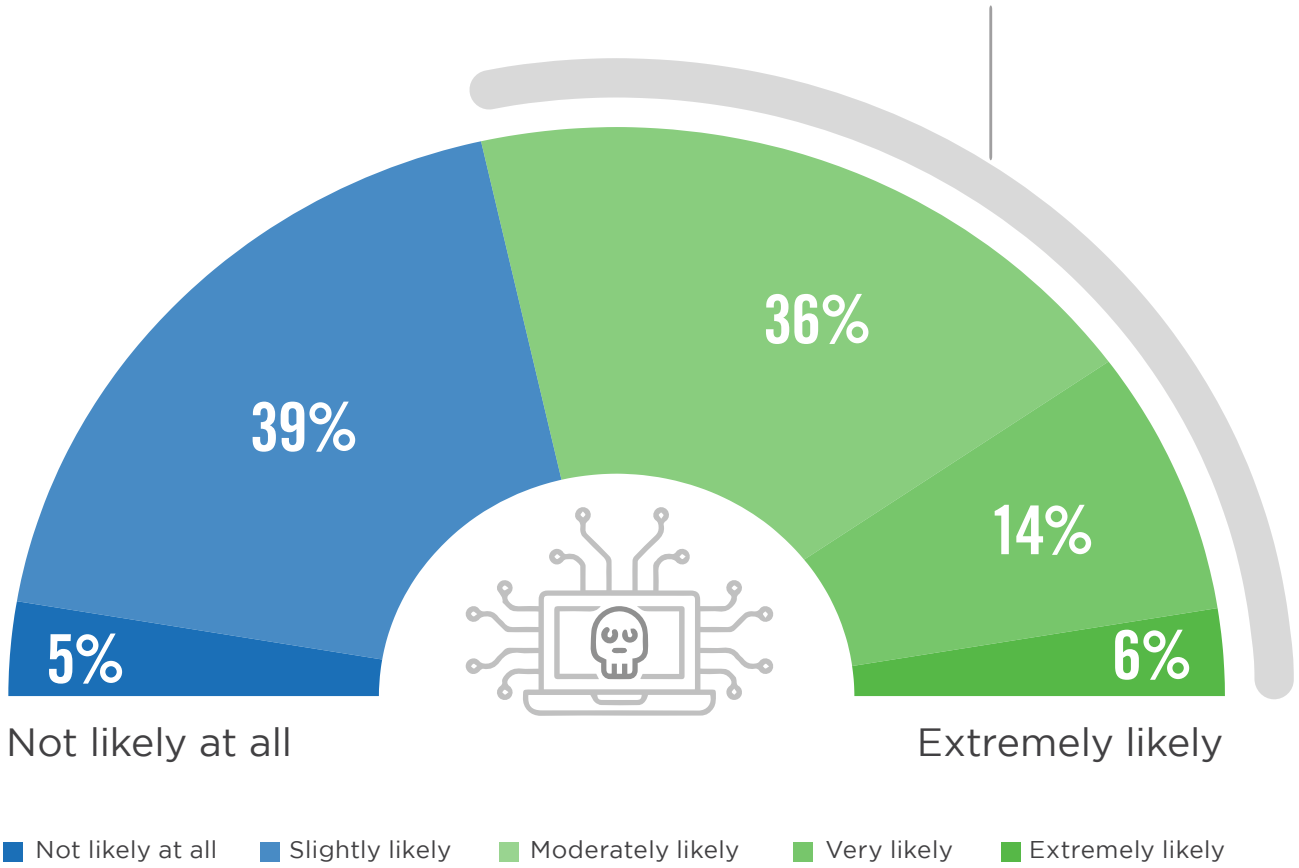
High rate of false positives or inaccuracy of issue 26% | No challenges 9%

LIKELIHOOD OF CYBERATTACK

More than half of organizations in this survey (56%) anticipate a moderate to extremely likelihood to be compromised by a successful cyberattack originating from endpoints or IoT devices.

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

56% Anticipate a moderate to extremely likelihood to be compromised by a successful cyberattack originating from endpoints or IoT devices.

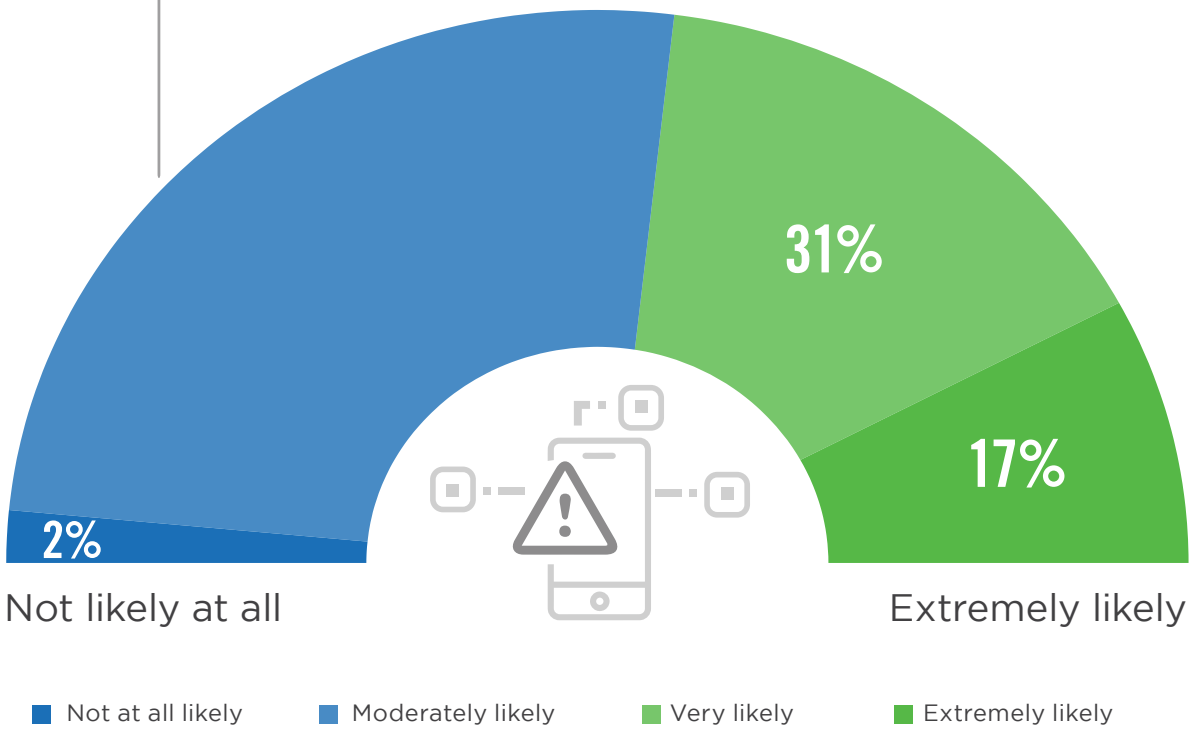


MANAGING RISKY DEVICES

Fifty percent of organizations only have moderate means to discover, identify and respond to unknown, unmanaged or insecure devices that are attempting to access or operate within their networks or cloud infrastructure.

How likely is your organization to discover, identify and respond to unknown, unmanaged or insecure devices attempting to access, accessing or operating within your network or cloud infrastructure?

50% Expressed moderate means to discover, identify and respond to unknown, unmanaged or insecure devices accessing network and cloud resources.



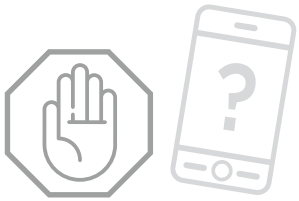
MOST CRITICAL SECURITY CAPABILITIES

When it comes to the most critical capabilities required to mitigate endpoint and IoT security issues, organizations prioritize monitoring endpoint or IoT devices for malicious or anomalous activity (54%). Followed by blocking or isolating unknown or at-risk endpoint and IoT devices (51%), and blocking at-risk endpoint or IoT devices' access to network or cloud resources (46%),

What are your organization's most critical capabilities to mitigate (prevent or respond to) endpoint and IoT security issues?

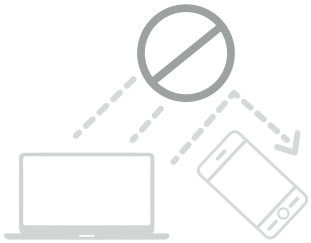
54%

Monitor endpoint or IoT device for malicious or anomalous activity



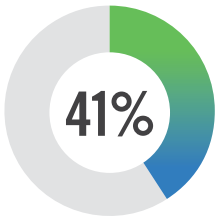
51%

Block or isolate unknown or at-risk endpoint and IoT devices network access

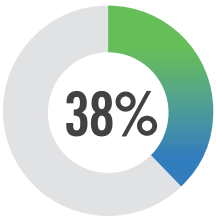


46%

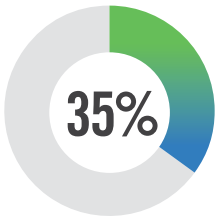
Block at-risk endpoint or IoT device access to network or cloud resources



Enforce endpoint compliance policy prior to access



Segregate network resources and applications



Quarantine the executable

Re-image to known good state 32% | Delete threatening applications, files, registry keys 30% | Notify device owner of policy violation and enable remediation 24%

SECURITY PRIORITIES

When asked about their near-term priorities, organizations are focused on user awareness training (54%), followed by on-premise endpoint and IoT security enforcement (NAC) (41%) and remote access endpoint security posture checks (35%).

What are your organization's near-term, top priorities to reduce endpoint and IoT security issues?

54%

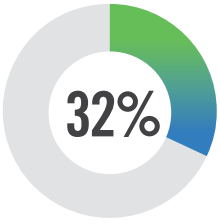
User awareness training

41%

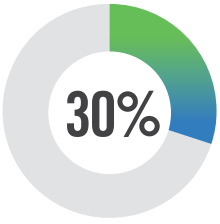
On-premise endpoint and IoT security enforcement (NAC)

35%

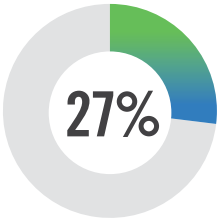
Remote access endpoint security posture check
(prior to network or cloud access)



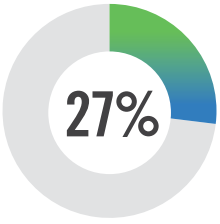
Enhance endpoint security issue triage and attack investigation



Expand endpoint security coverage (e.g., multiple OS, devices, etc.)



User and Entity Behavior Analysis (UEBA)



Enhance integration with other security and IT management solutions

Replace current endpoint security tool 24% | IoT device identification and monitoring 22% | Facilitate endpoint remediation 19% | Attack containment 14% | Enhance network/virtual microsegmentation 11% | Other 7%

SECURITY INVESTMENT

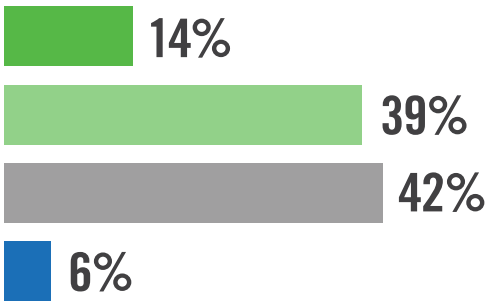
A majority of organizations (53%) anticipate investments in endpoint and IoT security technology to increase or significantly increase. Few expect a decrease (6%).

In the wake of the dramatic shift to working from home, a majority of organizations (61%) is expecting an increase or significant increase of capabilities and investments to secure remote worker access. About a third expect this to stay the same (33%).

To what extent do you anticipate your organization will generally increase investment in endpoint and IoT security technology?

53%

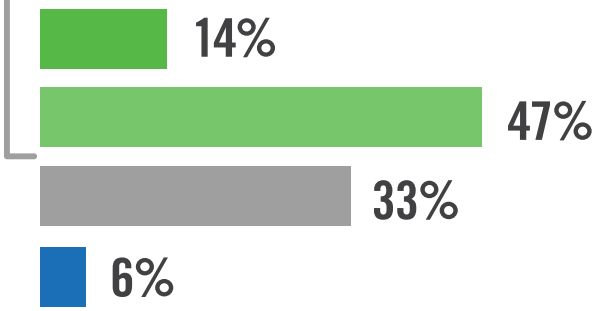
Anticipate investments in endpoint and IoT security technology to increase or significantly increase.



To what extent do you anticipate your organization will increase capabilities and investment to secure remote worker access and endpoint security?

61%

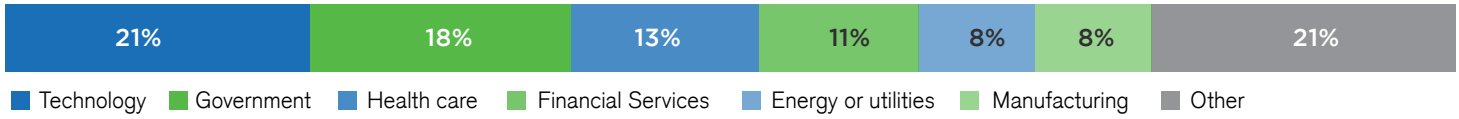
Are expecting an increase or significant increase of capabilities and investments to secure remote worker access.



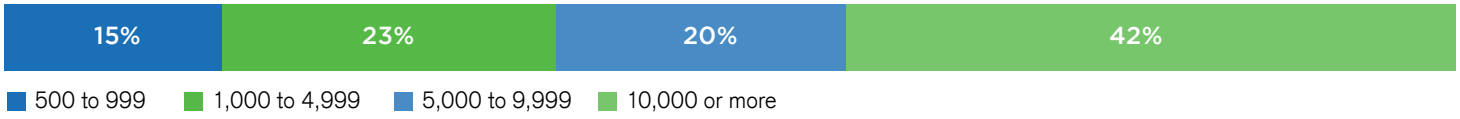
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 327 IT and cybersecurity professionals in the US, conducted in September 2020, to capture current sentiments, issues, solutions, initiatives and investments regarding Zero Trust endpoint and IoT security. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations from financial services, healthcare and technology, to government and energy.

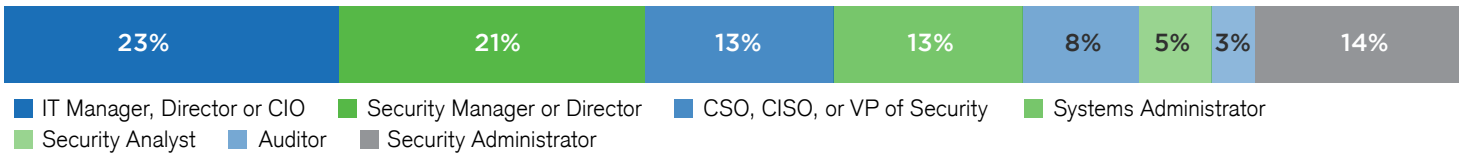
INDUSTRY



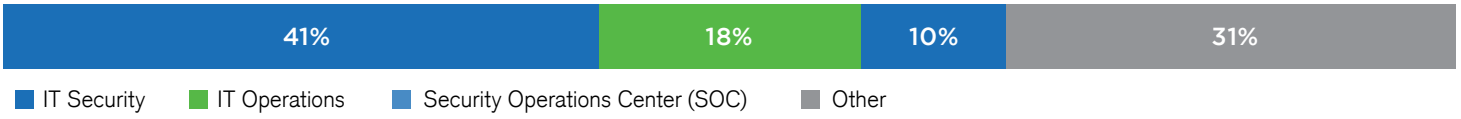
COMPANY SIZE



PRIMARY ROLE



DEPARTMENT



Research Sponsor

Pulse Secure®

Pulse Secure provides easy, comprehensive software-driven Secure Access solutions for people, devices, things and services that improve visibility, protection and productivity for our customers. Our suites and SaaS platform uniquely integrate cloud, mobile, application and network access to enable hybrid IT in a Zero Trust world. Over 24,000 enterprises and service providers across every vertical entrust Pulse Secure to empower their mobile workforce to securely access applications and information in the data center and cloud while ensuring business compliance. Learn more at www.pulsesecure.net