2022

Cybersecurity INSIDERS

# STATE OF SECURITY POSTURE REPORT

Balbix®

# OVERVIEW

The 2022 State of Security Posture Report reveals that cybersecurity teams are struggling to measure and improve their security posture as their organizations move to the cloud and as their leadership increasingly expects them to measure cyber risk in monetary terms due to the rise of ransomware and the general impact of cyber attacks to business.

The report has been produced by Cybersecurity Insiders, the 500,000 member online community of information security professionals to explore the latest trends, key challenges, gaps, and solution preferences for cybersecurity operations.

**Key findings include:**

- 62% of organizations are not confident in their security posture. Lack of visibility in their asset inventory and inability to prioritize vulnerabilities based on business risk contribute to this.
- 62% of organizations are not able to quantify their cyber risk in monetary units.
- 83% of organizations do not have a unified view into a cloud and on-premises security posture. This contributes to silos and inefficiencies in security posture management.
- Cybersecurity leaders struggle to communicate their security posture to the board and senior management.

We would like to thank Balbix for supporting this important industry research project.

We hope you find this report informative and helpful as you continue your efforts in securing your organizations against evolving threats and during challenging times.

Thank you,

Holger Schulze

**Holger Schulze**
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

# CONFIDENCE IN SECURITY POSTURE

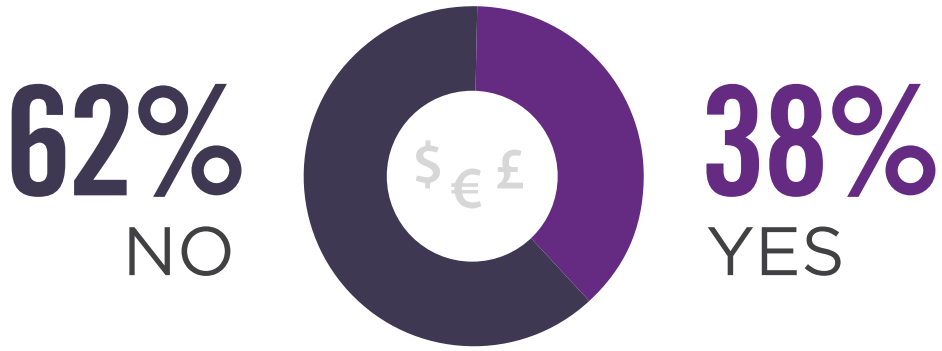
Organizations experience a significant lack of confidence in their security posture. Sixty-two percent say they are, at best, somewhat confident in their security posture.

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

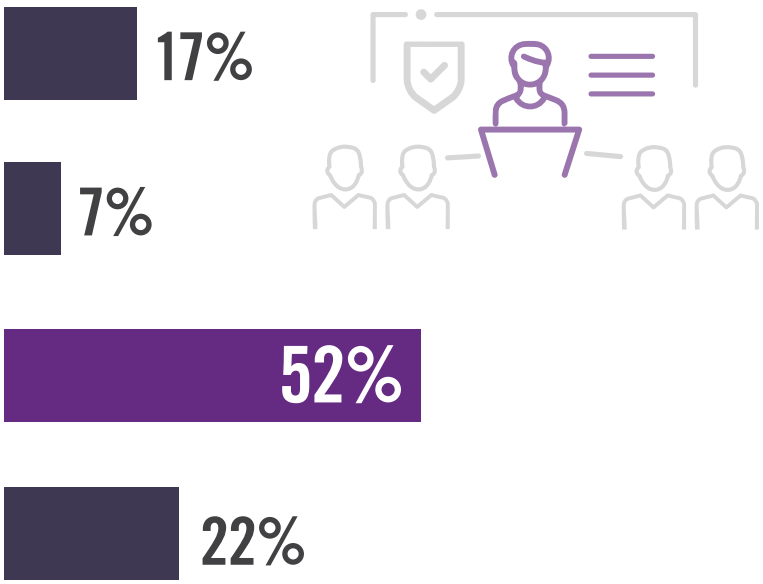
# CYBER RISK IMPACT

Sixty-two percent of organizations are not able to quantify their cyber risk in monetary units, which makes it hard for cybersecurity leaders to get the attention of the board and justify investment in cybersecurity staff and controls. As a result, board presentations are just "okay" for most organizations (52%) and could be better.

**Are you able to quantify your cyber risk in monetary units (dollars, euros, pounds, etc.)?**




**Which of the following most closely characterizes your most recent board or senior management presentation on cybersecurity?**




Other 2%

# BLIND SPOTS IN ASSET INVENTORY

To accurately measure their security posture, organizations need visibility into their asset inventory. Knowing what assets they have is foundational to securing those assets. When asked how they would rate their asset inventory awareness, 58% of organizations are aware of fewer than 75% of the assets on their network.

Eighty-three percent of organizations confirm they have at least 50% asset coverage; that is, they know roughly how many assets they have but with only spotty coverage for business criticality and categorization for each asset. This is a significant issue because without an accurate and up-to-date inventory, organizations will struggle to improve security posture.

**Which of the following best describes your organization's handle on asset inventory?**

**> 75% asset coverage**
We know exactly how many assets we have with business criticality and categorization for all of them.

42%

**50-75% asset coverage**
We know roughly how many assets we have but have spotty coverage for business criticality and categorization.

41%

**25-50% asset coverage**
We have a general idea of the number of assets on our network but are unable to accurately categorize or determine their business criticality.

15%

**< 25% asset coverage**
We do not have any real processes around asset inventory in our organization.

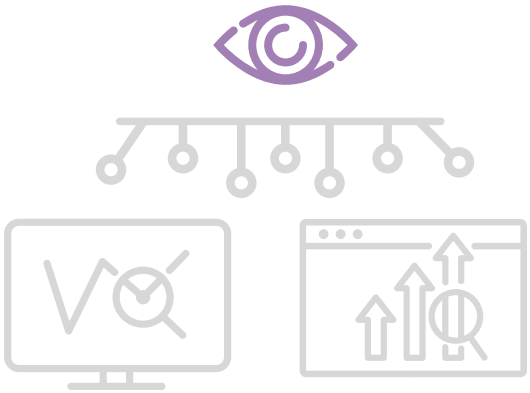
2%

**58%**
**of organizations confirm they have 75% asset coverage**

# INADEQUATE VISIBILITY IS AN ISSUE

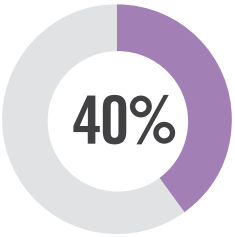
Only half of organizations report that they have sufficient visibility into cyber risks. While 65% report they have continuous visibility, lack of prioritization and resources to patch in a timely manner is inhibiting the effectiveness of vulnerability programs.

**Do you have holistic security visibility across your business?**

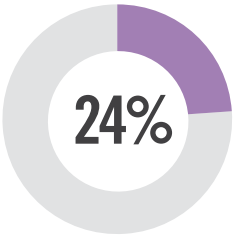


**50%**

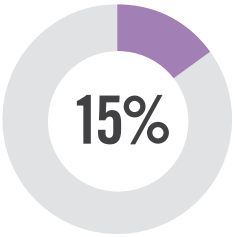
have analytics in place across a number of systems to identify patterns and anomalies




Have analytics in place across all data to detect basic violations




Use detailed mapping and implementation of patterns and anomalies across wide ranging data sources




We have analytics across all systems to identify behavioral patterns and anomalies

# RISK AREAS

We asked what risk areas organizations have continuous visibility into. Sixty-eight percent list unpatched systems, followed by identity and access management (59%), and phishing, web, and ransomware (52%). It is alarming that organizations report low visibility into risk areas such as asset inventory (49%), password issues (48%), and malicious insiders (23%).

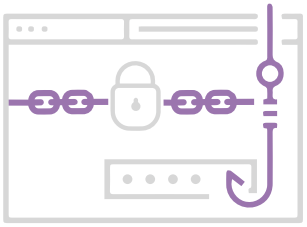
**Which of the following risk areas do you have continuous visibility into?**

**68%**

Unpatched systems

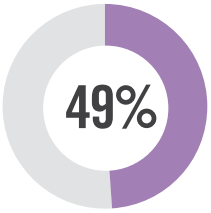
**59%**

Identity and access management

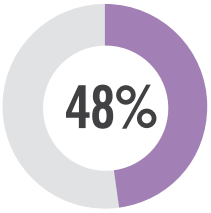


**52%**

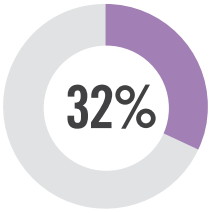
Phishing, web, and ransomware



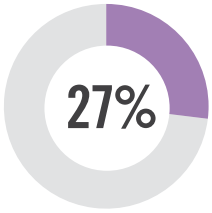

Asset inventory




Password issues




Denial of service attacks



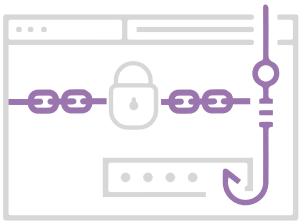

Misconfigurations

Encryption issues 25% | Flat networks 23% | Malicious insiders 23% | Other 3%

# BIGGEST SECURITY THREATS

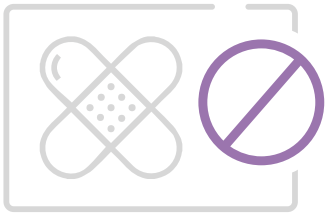
When asked about the biggest security threats facing organizations, 86% are most concerned about phishing and ransomware attacks. This is followed by vulnerabilities created by unpatched systems (54%) and misconfigurations (45%).

**Which of the following areas do you believe are driving the most risk to your organization?**



**86%**

Phishing, web, and ransomware

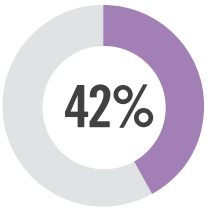


**54%**

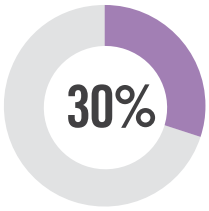
Unpatched systems


**45%**

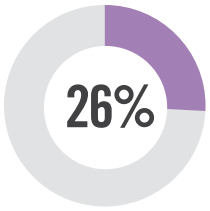
Misconfigurations



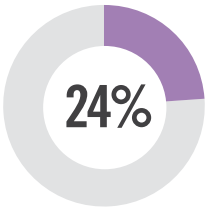

Identity and access management




Password issues




Malicious insiders



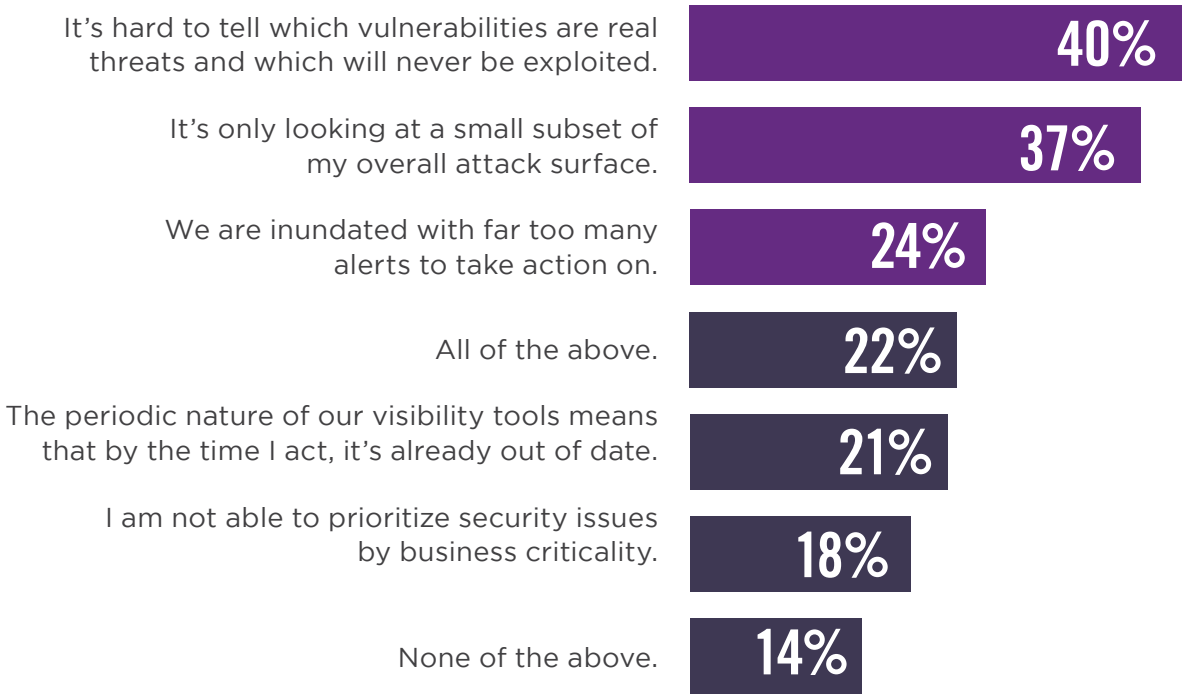

Asset inventory

Denial of service attacks 21% | Flat networks 20% | Encryption issues 20% | Other 3%

# VULNERABILITY PRIORITIZATION

The inability to prioritize vulnerabilities continues to inhibit the effectiveness of vulnerability management programs. Forty percent of organizations find it hard to tell which vulnerabilities are real threats and which ones will never be exploited. Thirty-seven percent are only looking at a small subset of the overall attack surface. Twenty-four percent feel inundated with far too many alerts to take action on.

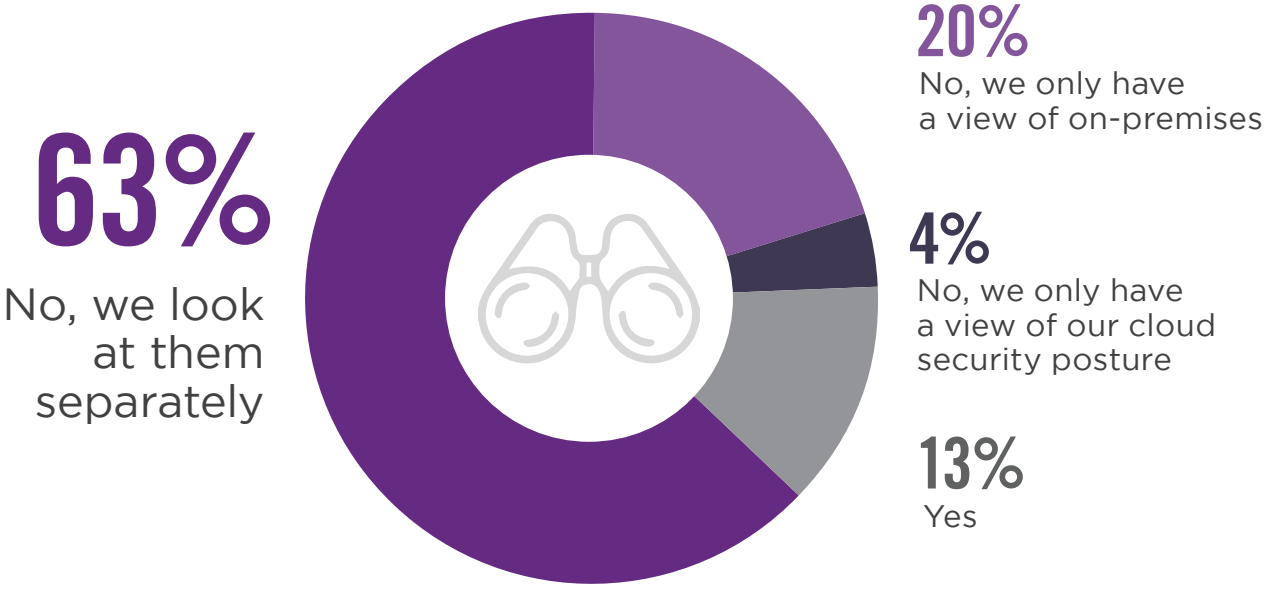
**Which of the following are concerns that you have about your current security visibility?**



# CLOUD SECURITY CONFIDENCE

Most organizations (63%) confirm they are lacking a unified view into their cloud and on-premises security posture.

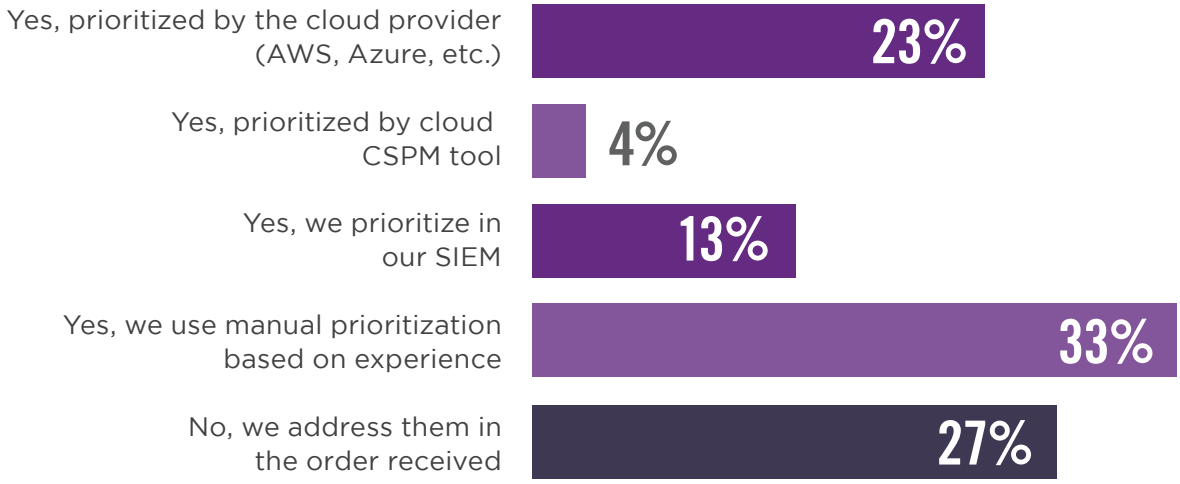
**Do you have a unified view into your security posture across cloud infrastructure and on-premises infrastructure?**



# CLOUD SECURITY PRIORITIES

It's no different in the cloud where 60% of organizations are manually prioritizing alerts or not at all.

**When it comes to your cloud security posture, do you have a way of prioritizing alerts and cyber risks for remediation? How do you prioritize alerts?**

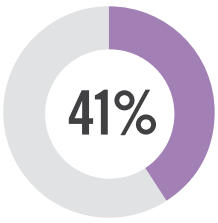



# SECURITY METRICS

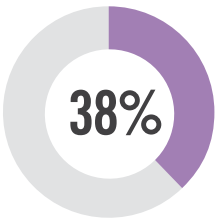
It is important that organizations prioritize the right metrics to gauge cybersecurity posture. Patch management metrics are the most mentioned cybersecurity metrics collected by organizations (66%), followed by vulnerability metrics (41%).

**Which of the following are the most important cybersecurity posture management metrics for your organization?**

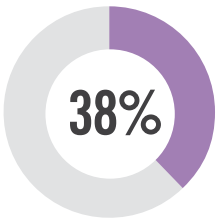
**66%** Patch management coverage/compliance/ cadence



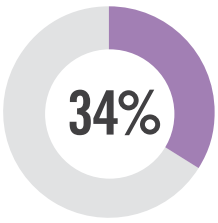

Number of low/ medium/high severity vulnerabilities




Percentage of systems complying with configuration standards



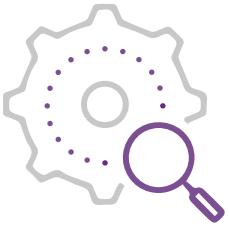

Performance on vulnerability remediation SLAs for high criticality assets




Attack surface discovery coverage as a percentage

Assets with poor or no cybersecurity visibility 31% | Mean time to remediate vulnerable systems 31% | Vulnerability scanning coverage as a percentage 28% | Cyber risk in monetary units (e.g., Dollars, Euros, Pounds, Yen, etc.) for each asset and for groups of assets 24% | Mean time to inventory (all assets on the network) 17% | Assets with deep cybersecurity visibility 14%

# ADDRESSING SECURITY POSTURE CHALLENGES



## ASSET DISCOVERY AND MANAGEMENT

Though security leaders have some security tools in place, it is challenging to sift through all the data and alerts to identify critical vulnerabilities. As a result, they constantly worry about unseen cyber risks and vulnerabilities. Organizations need to unify all the data generated by their IT and cybersecurity tools – such as CMDB, firewalls, vulnerability tools, EDR, SIEM, MDM systems, Active Directory, IoT/OT management systems, cloud infrastructure APIs etc. to get an organized view into their asset inventory and attack surface.

**Most of the respondents are not accounting for 25% or more of assets in their inventory.** This creates huge blind spots in security posture and serious risks. Enterprises must have a continuous, real-time view of their inventory that includes all devices, apps, and services. This means managed and unmanaged infrastructure, on-prem and cloud, and fixed and mobile. They should also have intel on how devices are being used.

## RISK VISIBILITY

**Infosec teams need visibility into all the devices and applications on their network, as well as the hundreds of attack vectors they are susceptible to.** This visibility should be continuous, as periodic scans go quickly out of date. Lastly, infosec teams should have visibility into the severity of vulnerabilities to know if they are real threats or just noise.

## CLOUD SECURITY POSTURE MANAGEMENT

**Sixty-three percent of organizations view their cloud and on-premises assets through separate dashboards and 20% only have a view of their on-prem assets.** Organizations need to merge cloud and on-premises visibility into one view, eliminating the need for security practitioners to look through multiple dashboards and allow them to work more productively.

## QUANTIFYING BREACH RISK

**Sixty-two percent of respondents are not able to calculate their breach risk in monetary terms.** As a result, it is challenging to catch the attention of the board and enable them to make the right decisions when it comes to security investments. Calculating cyber risk in monetary terms provides a common language that organizations - from security engineers and IT admins to the CISO, CFO, and CIO - can use to prioritize projects and spending and track the effectiveness of their overall cybersecurity program.

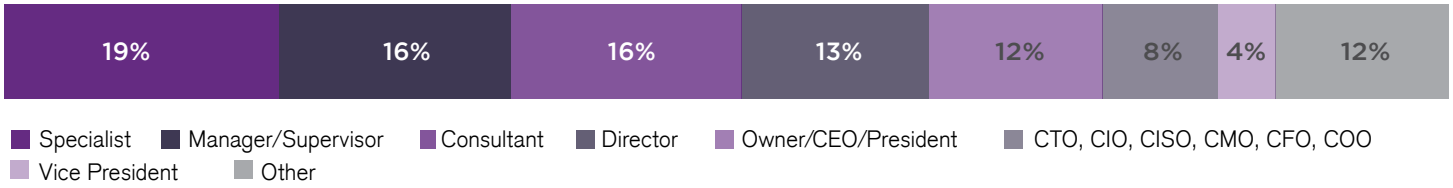
## COMMUNICATING TO THE BOARD

**Fifty-two percent of cybersecurity leaders are settling for "okay" board presentations when they could be nailing it.** Effective board-level presentations start with quantifiable risk metrics and intuitive visualizations. They should focus on business objectives and help stakeholders understand where the company is regarding cyber risk, where it should be, and how it can get there.

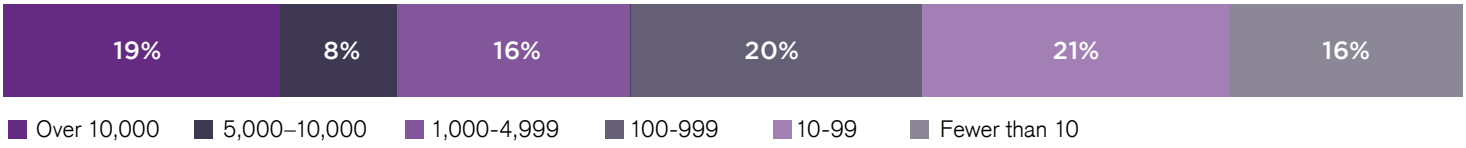
# METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 297 IT and cybersecurity professionals in the US, conducted in October 2021, to explore the latest trends, key challenges, gaps, and solution preferences for cybersecurity operations. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

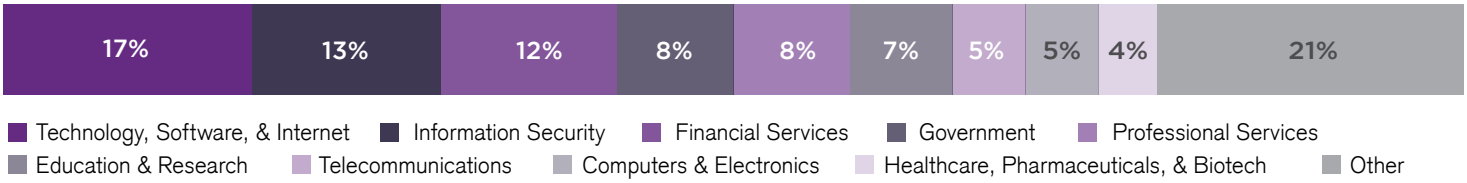
## CAREER LEVEL



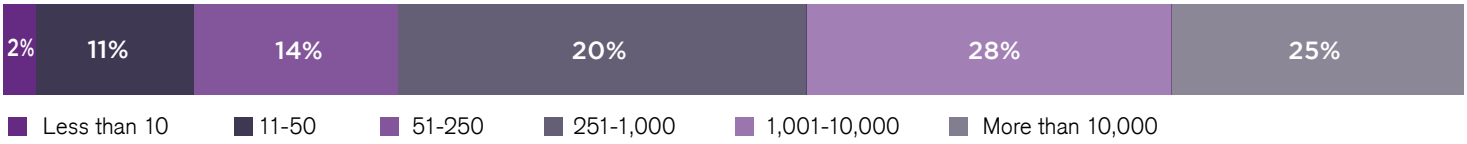

## COMPANY SIZE



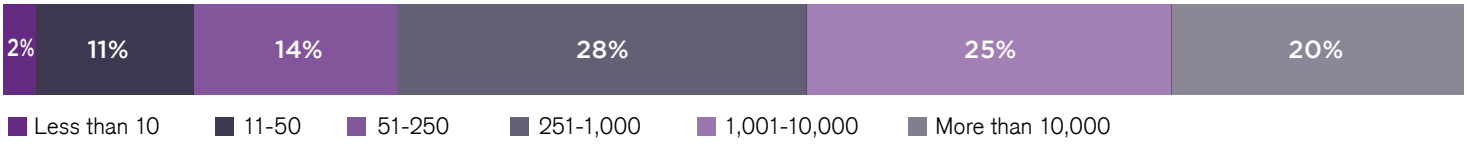

## INDUSTRY




## NETWORK-CONNECTED ENDPOINTS




## DATA COLLECTION TOOLS



Balbix provides the world's leading platform for cybersecurity posture automation. Using Balbix, organizations can discover, prioritize, and mitigate unseen risks and vulnerabilities at high velocity with seamless data collection and petabyte-scale analysis capabilities.

Balbix is deployed and operational within hours, and helps to decrease breach risk immediately. With Balbix, organizations can:

- **Unify all their cybersecurity data**
  Balbix continuously discovers and monitors your devices, apps, and users across 100+ attack vectors by analyzing the data from existing cybersecurity tools (and optionally via the Balbix sensors) and provides a single, comprehensive, and organized view of the asset inventory.

- **Evaluate vulnerabilities and risk items, then prioritize based on business criticality**
  The Balbix platform uses specialized AI to predict likely breach scenarios, prioritize vulnerabilities to fix, and prescribe necessary risk mitigation actions. Balbix denominates risk metrics in monetary terms which enables everyone involved to have a common language and make better decisions faster.

- **Enable stakeholders to own their cyber risk and critical mitigation tasks**
  Balbix provides risk dashboards and reports to enable organizations to gamify cyber risk reduction and demonstrate the value of their security program to senior leadership and the board.

www.balbix.com