INSIDER THREAT

SPOTLIGHT REPORT

Linked in Group Partner

Information Security

PRESENTED BY

ALIEN VAULT

bitglass

CipherPoint

Dtex systems

exabeam

Fasoo Data and Application Security

LIGHTCYBER CLOSING THE BREACH DETECTION GAP

observe it

palerra

Prolifics. Global Technology Solutions Provider

SentinelOne®

TEMASOFT NETWORK SECURITY PRODUCTS

Veriato

INSIDER THREAT SPOTLIGHT REPORT

TABLE OF CONTENTS

OVERVIEW

Highly publicized insider data thefts and security breaches highlight the increasing need for better security practices and solutions to reduce the risks posed by malicious insiders as well as unintentional insiders.

This report is the result of comprehensive crowd-based research in partnership with the 300,000+ member Information Security Community on LinkedIn and Crowd Research Partners to gain more insight into the state of insider threats and solutions to prevent them.

Many thanks to our sponsors for supporting this unique research project:

AlienVault | Bitglass | CipherPoint | Dtex | Exabeam | Fasoo | LightCyber | ObserveIT | Palerra | Prolifics | SentinelOne | Temasoft | Veriato.

Thanks to everyone who participated in the survey.

I hope you will enjoy this report.

Holger Schulze

Holger Schulze
Group Founder
Information Security
Community on LinkedIn

✉ hhschulze@gmail.com

LinkedIn Group Partner
Information Security

KEY SURVEY FINDINGS

1 Seventy-four percent of organizations feel vulnerable to insider threats — a dramatic seven percentage point increase over last year's survey. However, less than half of all organizations (42 percent) have the appropriate controls in place to prevent an insider attack.

2 Inadvertent data breaches (71 percent) top the list of insider threats companies care most about. Negligent data (68 percent) and malicious data (61 percent) breaches come in a close second and third.

3 Privileged users, such as managers with access to sensitive information, pose the biggest insider threat to organizations (60 percent). This is followed by contractors and consultants (57 percent), and regular employees (51 percent).

4 Fifty-six percent of security professionals say insider threats have become more frequent in the last 12 months. Forty-two percent of organization expect a budget increase over the next year — a strong gain of eight percentage points from the previous year.

5 Over 75 percent of organizations estimate insider breach remediation costs could reach $500,000. Twenty-five percent believe the cost exceeds $500,000 and can reach in the millions.

INSIDER THREATS AND VULNERABILITY

TOP INSIDER THREATS

Inadvertent data breaches (71 percent) top the list of insider threats companies care most about. Negligent data (68 percent) and malicious data (61 percent) breaches come in a close second and third.

Q: What type of insider threats are you most concerned about?

71%

Inadvertent data breach/leak

(e.g. careless user causing accidental breach)

68%

Negligent data breach

(e.g. user willfully ignoring policy, but not malicious)

61%

Malicious data breach

(e.g. user willfully causing harm)

6% Not Sure/Other

RISKY USERS

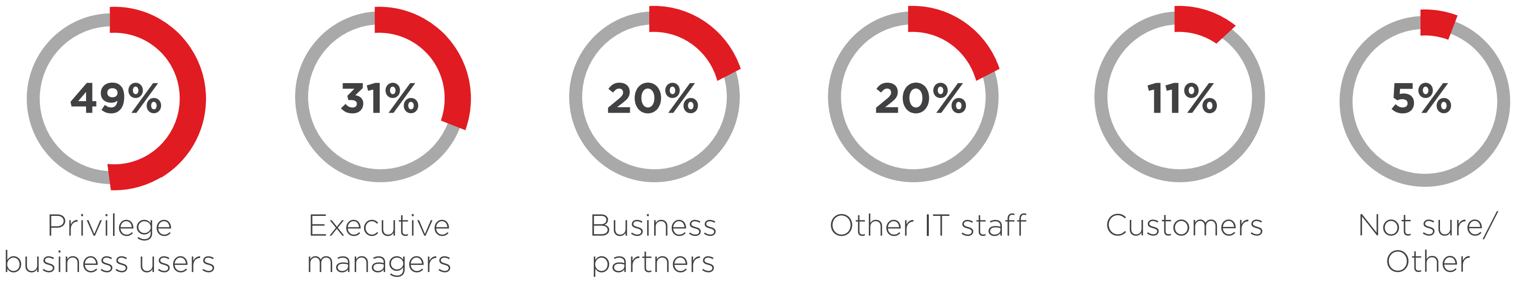
In this year’s survey, privileged IT users, such as administrators with access to sensitive information, pose the biggest insider threat (60 percent). This is followed by contractors and consultants (57 percent), and regular employees (51 percent).

Q: What user groups pose the largest security risk to organizations?

60% Privileged IT Users / Admins

57% Contractors/Consultants Temporary Workers

51% Regular Employees



MOST VULNERABLE APPLICATIONS

Collaboration and communication applications, such as email, are most vulnerable to insider attacks (44 percent), followed by a tie between finance and accounting (39 percent) and cloud storage and file sharing applications such as Dropbox (39 percent). In this year's survey social media channels such as Facebook move to the third spot (34 percent).

Q: In your opinion, what types of applications are most vulnerable to insider attacks?

44% **Collaboration & communication** (email, messaging)

39% Finance & accounting

39% Cloud storage & file sharing apps (DropBox, OneDrive, etc)

34% Social media (Facebook, LinkedIn, Twitter, etc)

Custom business applications 33% | Website 32% | Sales & Marketing (CRM, marketing automation, etc) 26% | Productivity (Office 365, word processing, spreadsheets, etc) 28% | Business intelligence / analytics 27% | HR 25% | IT Operations 24% | Cloud applications 22% | Application development & testing % | Content management 18% | Disaster recovery / storage / archiving 17% | Supply chain management 14% | Project management 9% | Not sure / Other 8%

THREATS COMPANIES CARE MOST ABOUT

Monetizing sensitive data (55 percent), fraud (51 percent) and sabotage (42 percent) are the top motivations for malicious insider threats that companies are most concerned about. Espionage is the least concern, as highlighted by respondents (38 percent).

Q: What motivations for malicious insider threats are you most concerned about?

55% Monetizing sensitive data

51% Fraud

42% Sabotage

39% IP theft

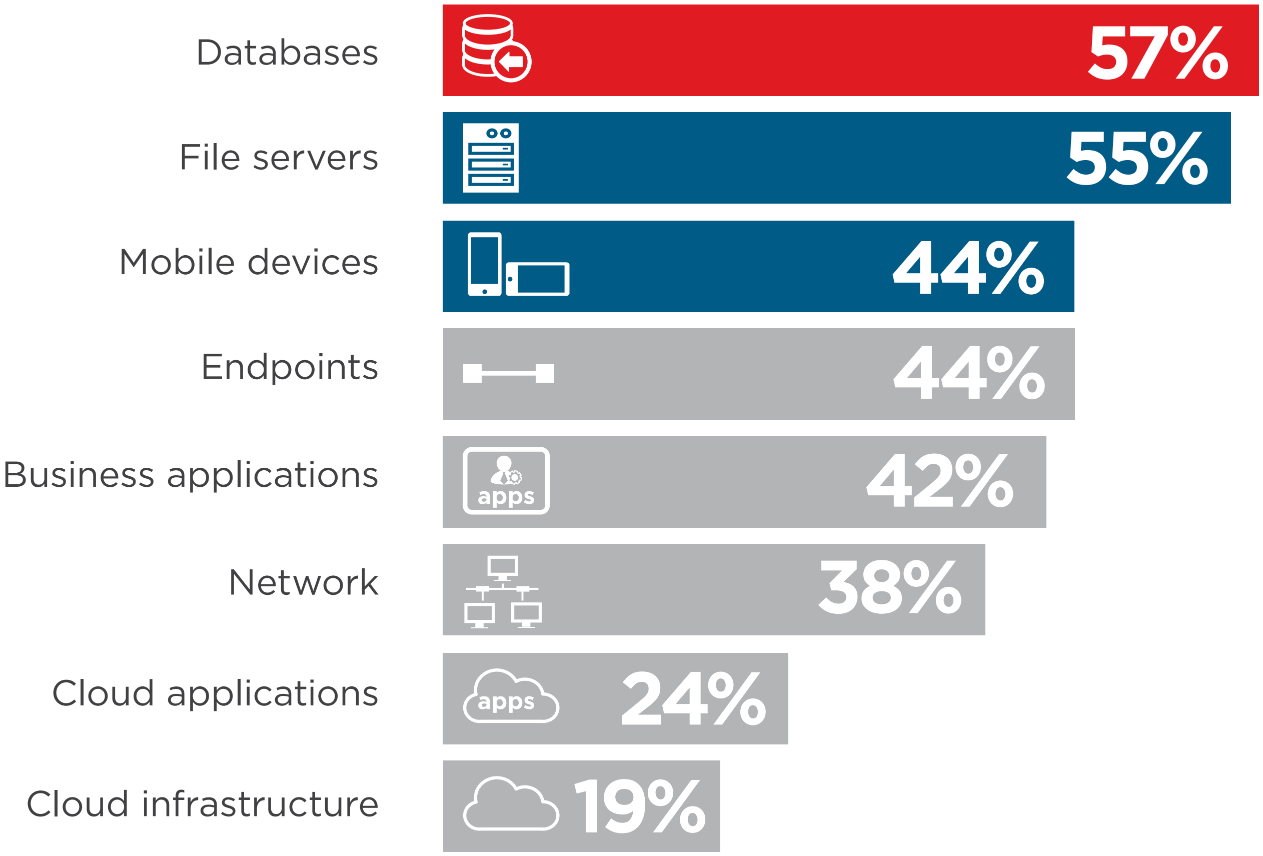
38% Espionage

10% Not sure/Other

IT ASSETS AT RISK

Given the amount of sensitive information that resides in databases, it is no surprise that similar to last year, 57 percent of companies named databases as the most vulnerable asset to an insider attack. File servers (55 percent) and mobile devices (44 percent) were named as the second and third assets that are most vulnerable. Cloud infrastructure was the least vulnerable (19 percent).

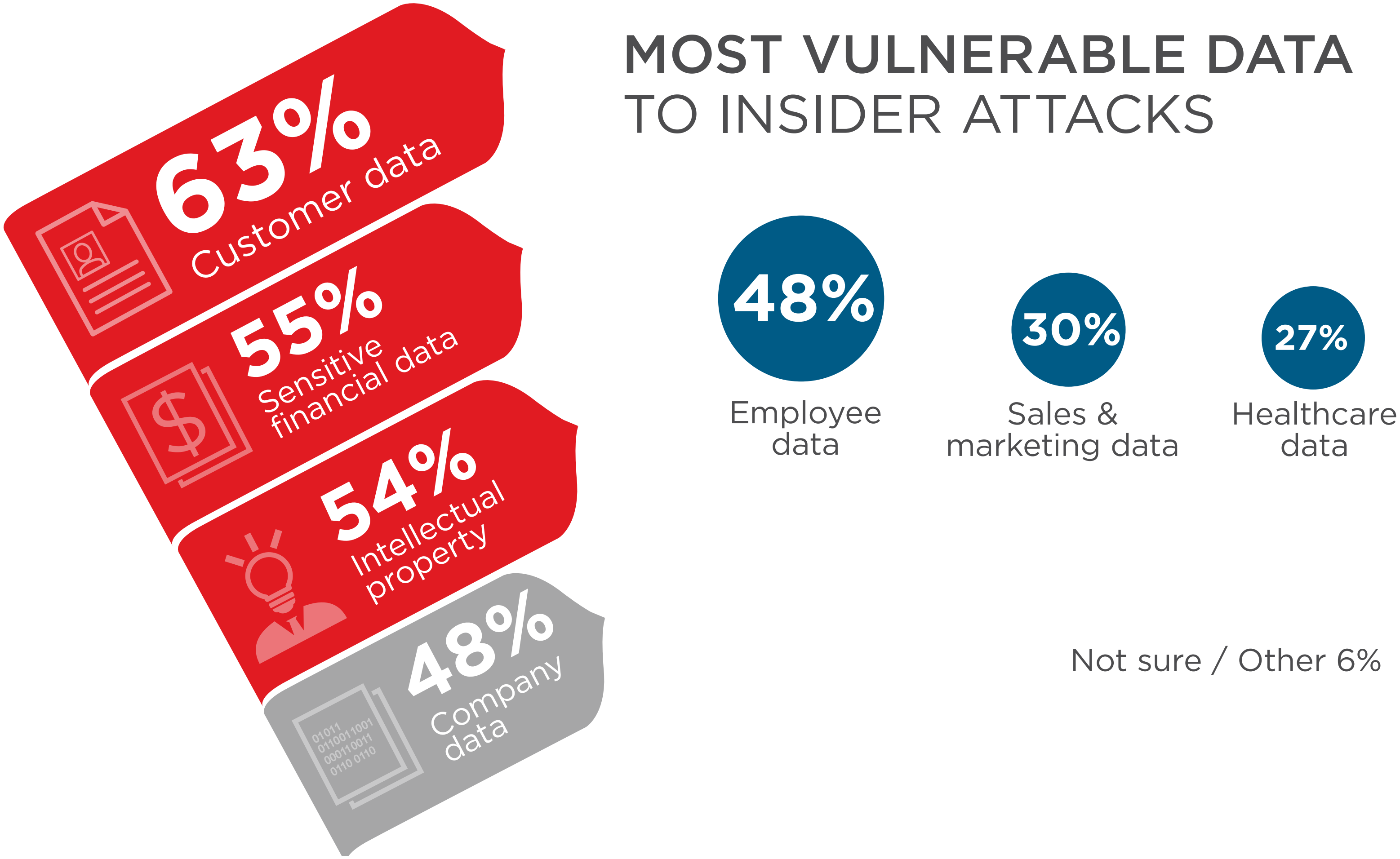
Q: What IT assets are most vulnerable to insider attacks?



DATA MOST VULNERABLE TO INSIDER ATTACKS

As expected, due to its value, customer data is most vulnerable to insider attacks (63 percent) again this year. Financial data (55 percent) and intellectual property (54 percent) marginally switch spots.

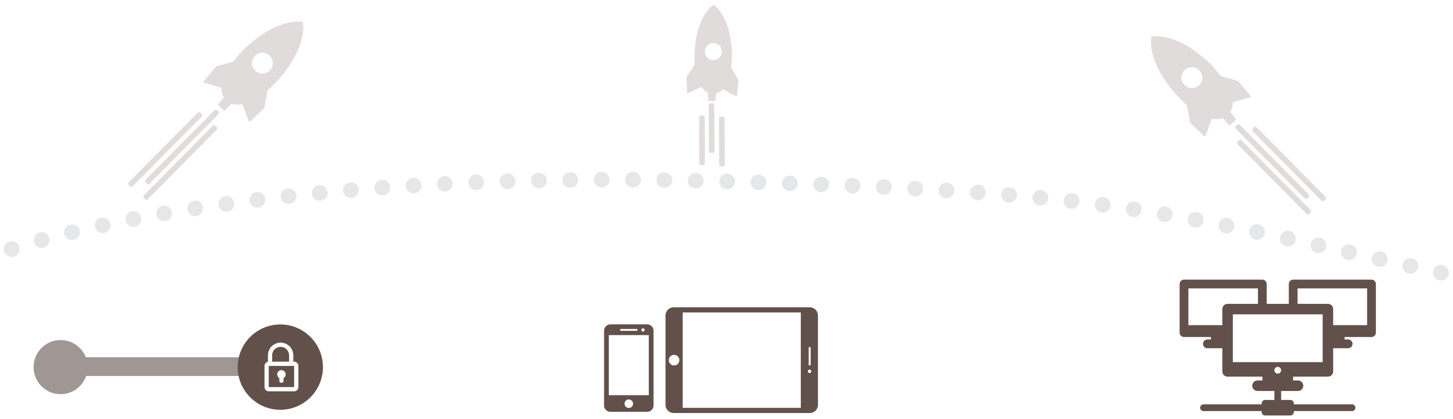
Q: What types of data are most vulnerable to insider attacks?



LAUNCH POINTS FOR INSIDER ATTACKS

Endpoints (57 percent) by far are the most common assets used to launch an insider attack. Cloud infrastructure (20 percent) is the least likely place people use to launch an attack.

Q: What IT assets are most commonly used to launch insider attacks from?



57% Endpoints

36% Mobile devices

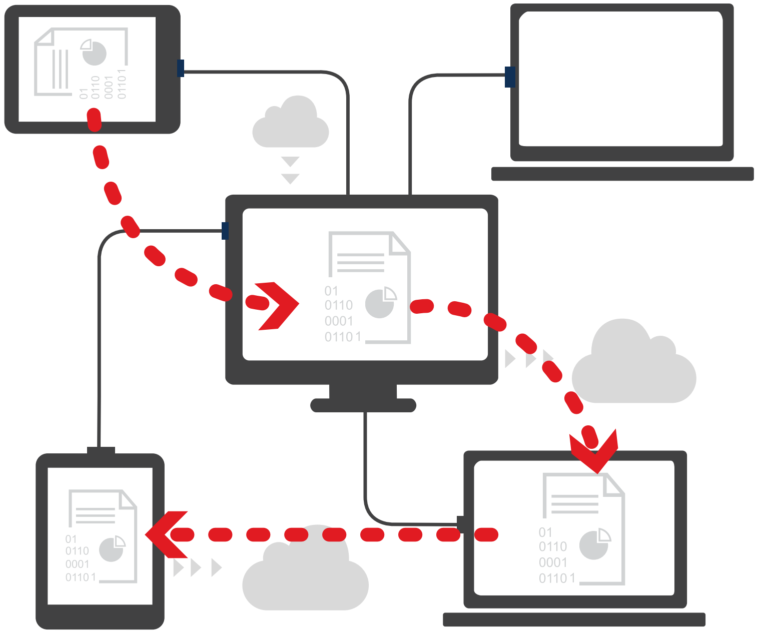
35% Network

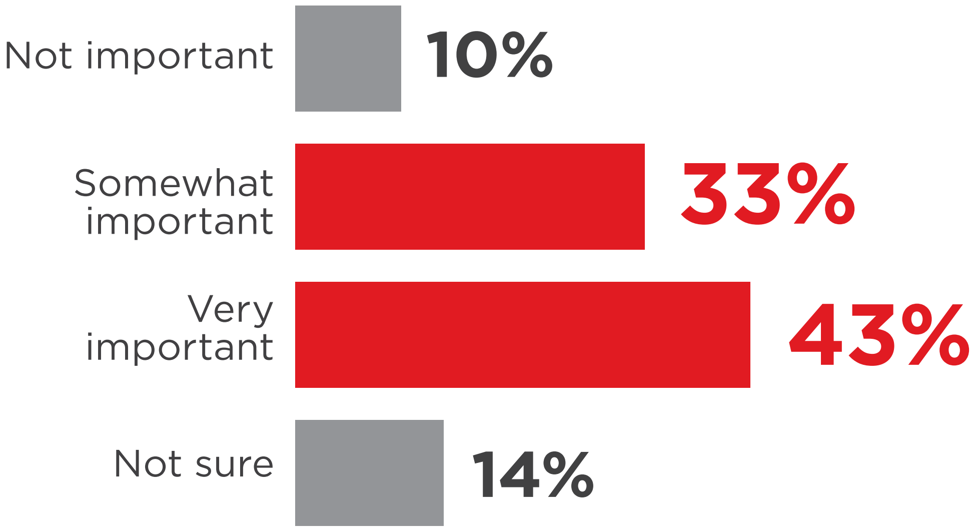
File servers 31% | Business applications 29% | Databases 27% | Cloud infrastructure or applications 20% | Not sure / Other 13%

MONITORING FILE MOVEMENT

File sharing is a popular way to cause a security breach. As a result, 75 percent of organizations feel tracking file movement across the network is a critical component of their data security strategy.

Q: How important is tracking file movement across your network for your data security strategy?

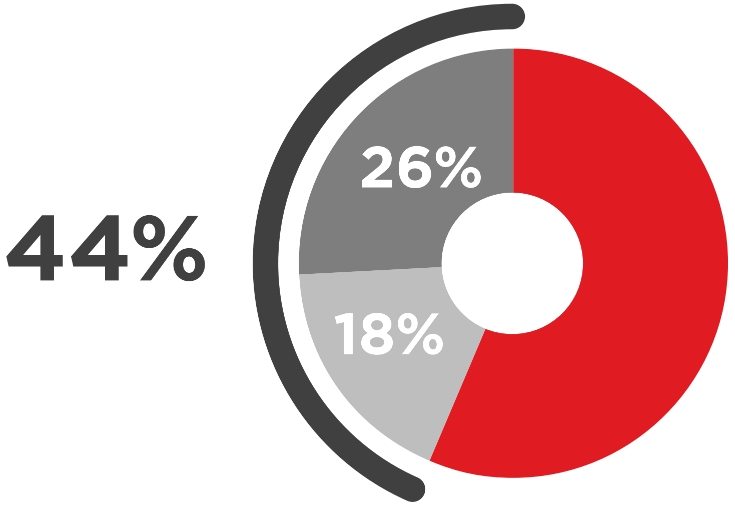




THE RISE OF INSIDER ATTACKS

Almost half of respondents have no idea if their organization experienced an insider attack in the last 12 months (44 percent). However, more people feel that insider attacks have become more frequent in the last 12 months (56 percent). Eighteen percent said they are seeing fewer breaches while 26 percent of respondents were not sure.

Q: Do you think insider attacks have generally become more frequent over the last 12 months?

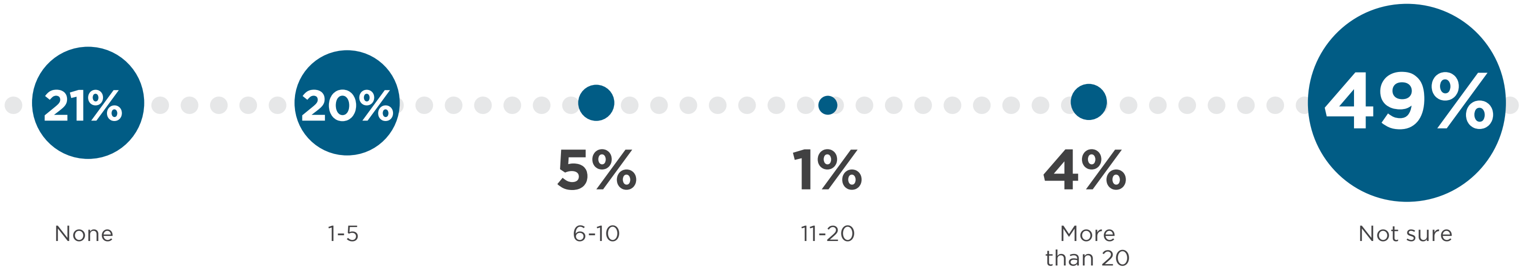


56%

Think insider attacks have become more frequent in the past 12 months.

🟥 Yes ■ No ■ Not sure

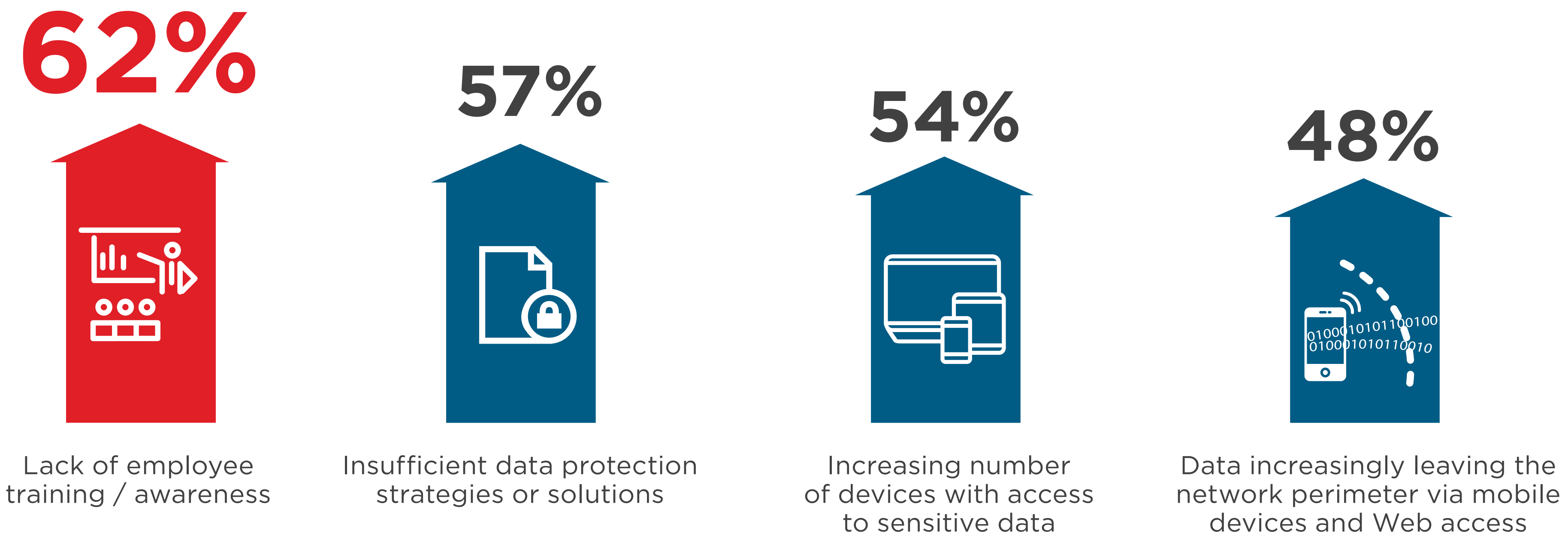
Q: How many insider attacks did your organization experience in the last 12 months?



WHY INSIDER ATTACKS ARE INCREASING

This year, lack of employee training and awareness (62 percent) tops the list as the reason for the rise in insider attacks. Insufficient data protection strategies and solutions (57 percent) and the proliferation of sensitive data moving outside the firewall on mobile devices (54 percent) are again named as sources for why insider threats are on the rise.

Q: What do you believe are the main reasons why insider threats are rising?

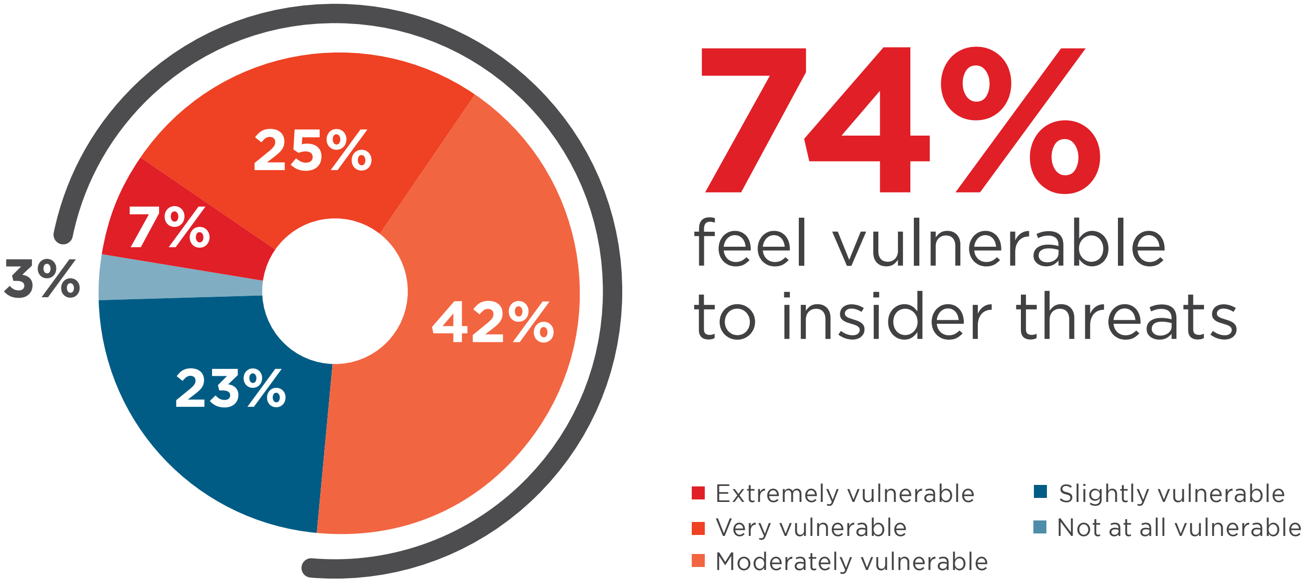


More employees, contactors, partners accessing the network 45% | Increasing amount of sensitive data 37% | Increased public knowledge or visibility of insider threats that were previously undisclosed 29 % | Technology is becoming more complex 27% | Increasing use of cloud apps and infrastructure 27% | Not sure / Other 10%

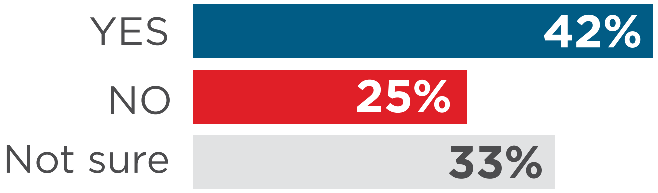
COMPANY VULNERABILITY

Seventy-four percent of organizations feel vulnerable to insider threats - a dramatic seven percentage point increase over last year's survey. Even though 42 percent of companies feel they have appropriate controls to prevent an insider attack, only three percent of companies feel they are not at all vulnerable to an insider attack.

Q: How vulnerable is your organization to insider threats?



74% feel vulnerable to insider threats



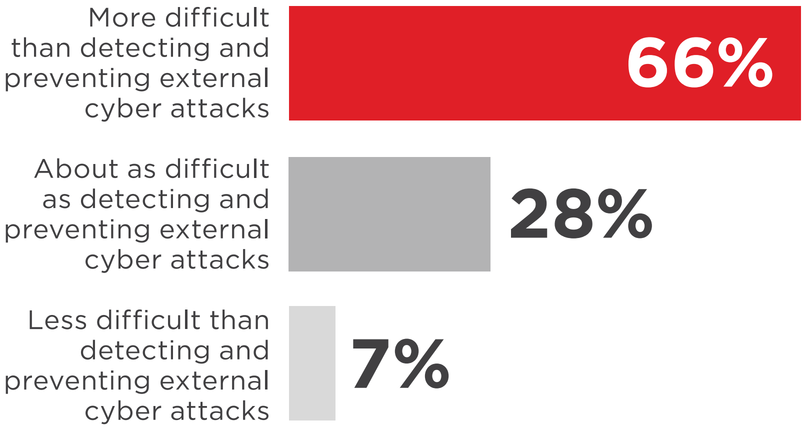
Q: Does your organization have the appropriate controls to prevent an insider attack?

THREAT DETECTION

INTERNAL VERSUS EXTERNAL ATTACKS

Similar to our previous survey, the majority of respondents (66 percent) have a harder time detecting and preventing an insider attack versus an external cyber attack.

Q: How difficult is it to detect and prevent insider attacks compared to external cyber attacks?



The key reasons for the difficulty in detecting and preventing insider attacks are that insiders often already have access to systems and sensitive information (67 percent), the increased use of cloud based applications (53 percent), and the rise in the amount of data that is leaving the protected network perimeter (46 percent).

Q: What makes the detection and prevention of insider attacks increasingly difficult compared to a year ago?

67% Insiders already have credentialed access to the network and services

53% Increased use of applications that can leak data (e.g., Web email, DropBox, social media)

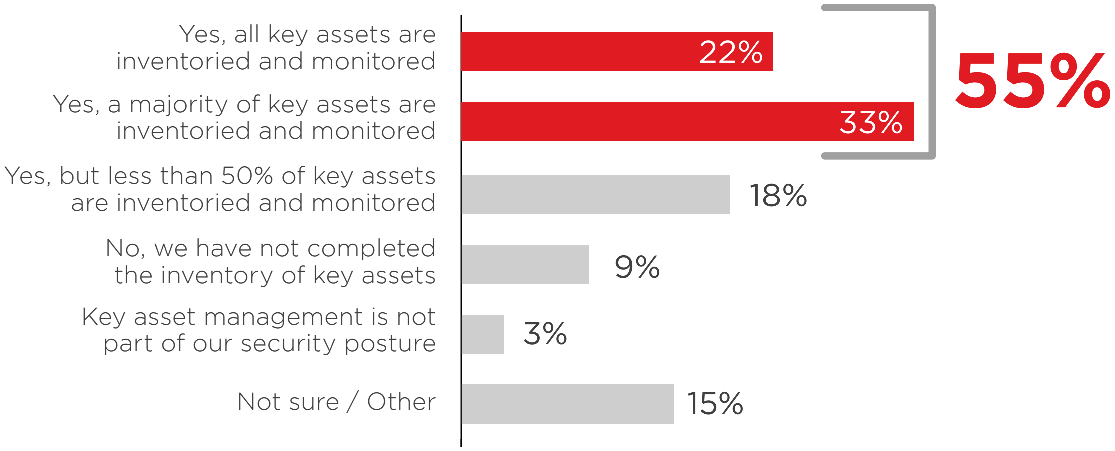
46% Increased amount of data that leaves protected boundary / perimeter

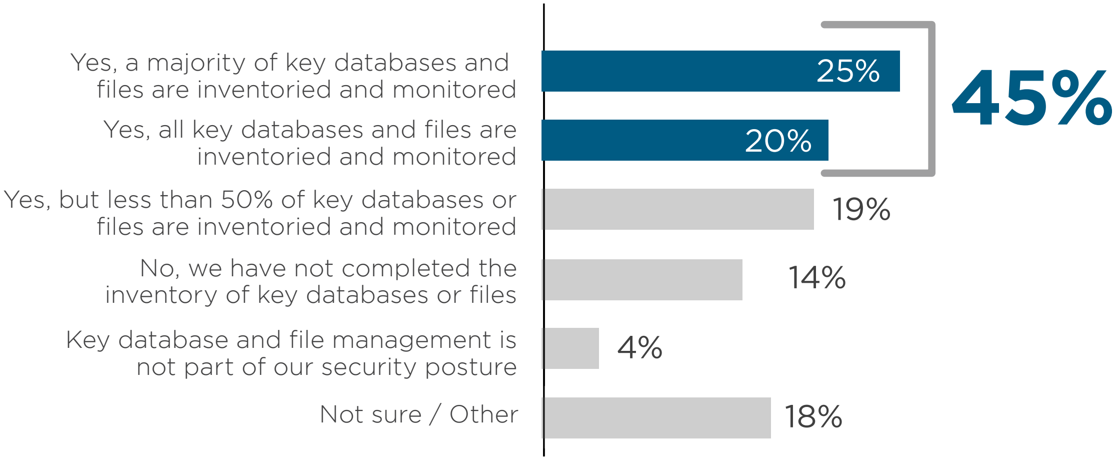
More end user devices capable of theft 33% | Difficulty in detecting rogue devices introduced into the network or systems 32% | Absence of an Information Security Governance Program 31% | Insiders are more sophisticated 28% | Migration of sensitive data to the cloud along with adoption of cloud apps 24% | Not sure / Other 10%

WHAT COMPANIES MONITOR

Q: Do you monitor key assets and system resources?

Fifty-five percent of respondents inventory and monitor all or the majority of their key assets.

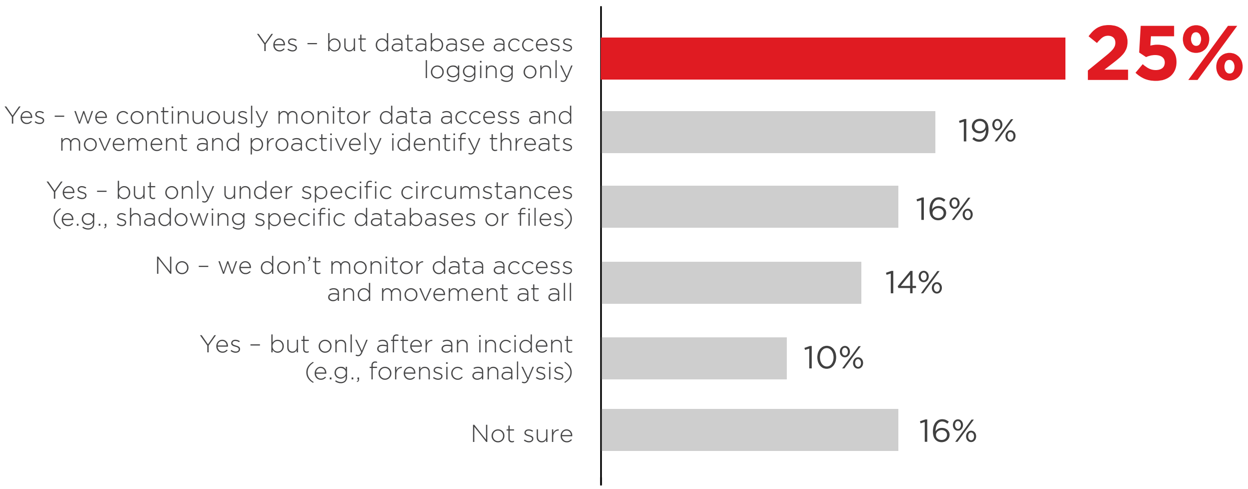




Q: Do you monitor key databases and file transfer activities?

Forty-five percent of companies monitor the majority or all of their databases and file transfer activities.

DATA ACCESS AND USER BEHAVIOR MONITORING

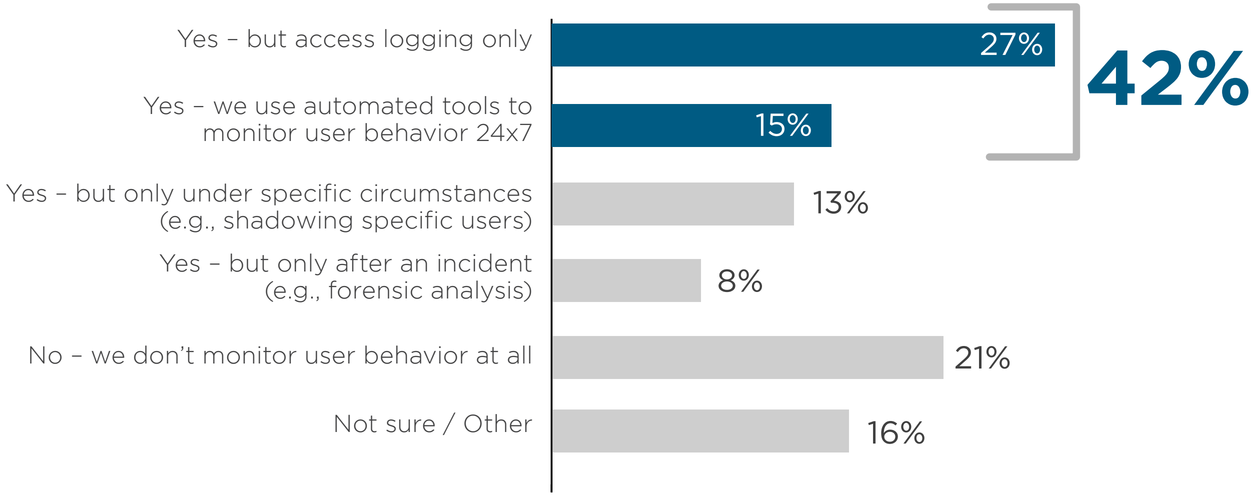


Q: Do you monitor data access and movement?

Most companies are only monitoring database access (25 percent). Only 19 percent of companies are continually monitoring data and network movement. A surprising 14 percent of companies do not monitor at all. Ten percent of companies implement monitoring only after an attack.

Q: Do you monitor user behavior?

Most organizations monitor their user behavior (42 percent). Twenty one percent do not monitor user behavior.

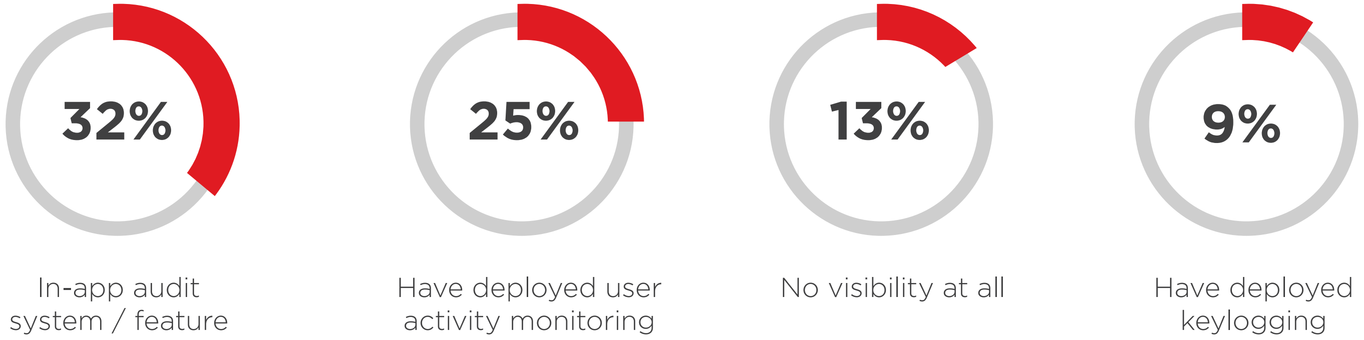


USER BEHAVIOR VISIBILITY

Again this year, most organizations (49 percent) rely on server logs to review user behavior. Only 25 percent have deployed dedicated user activity monitoring solutions. Thirteen percent of respondents have no visibility at all.

Q: What level of visibility do you have into user behavior within core applications?

49% Server Logs

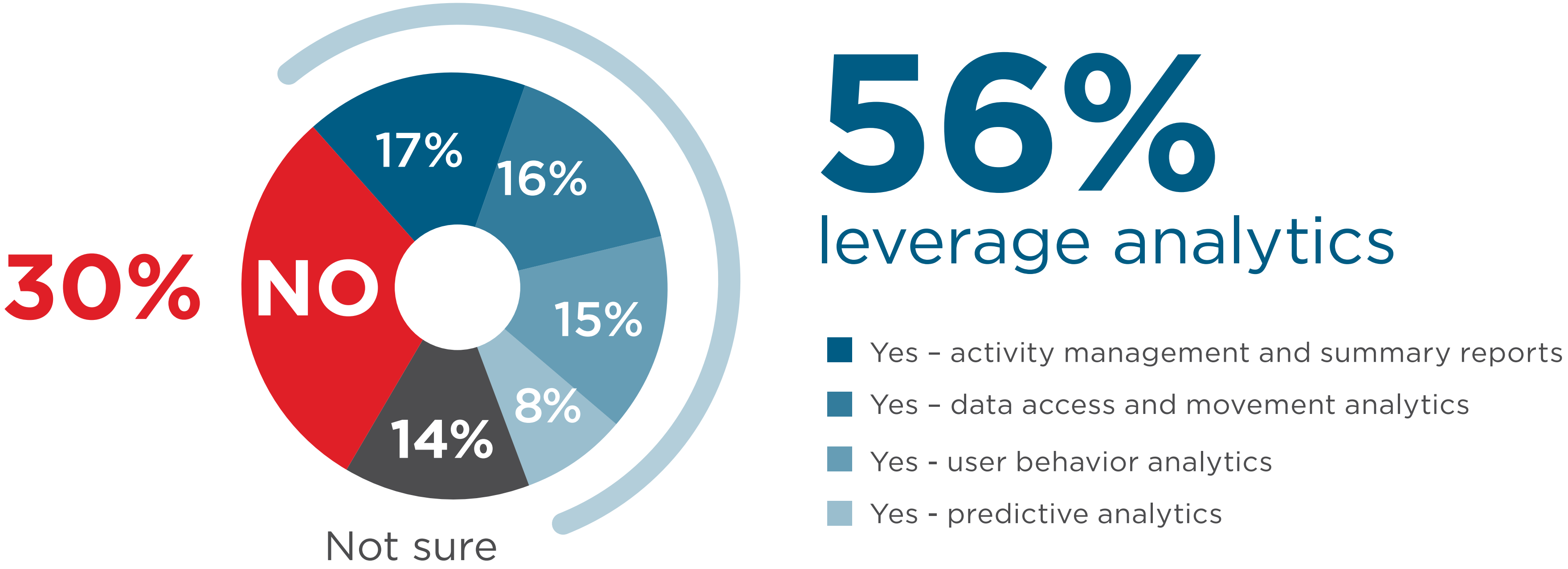


16% Not sure / Other

INSIDER THREAT ANALYTICS

The number of organization that do not leverage insider threat analytics is down 20 percent compared to last year (30 percent this year compared to 50 percent last year). Of the 56 percent of the organizations that are using some type of analytics, only eight percent use predictive analytics.

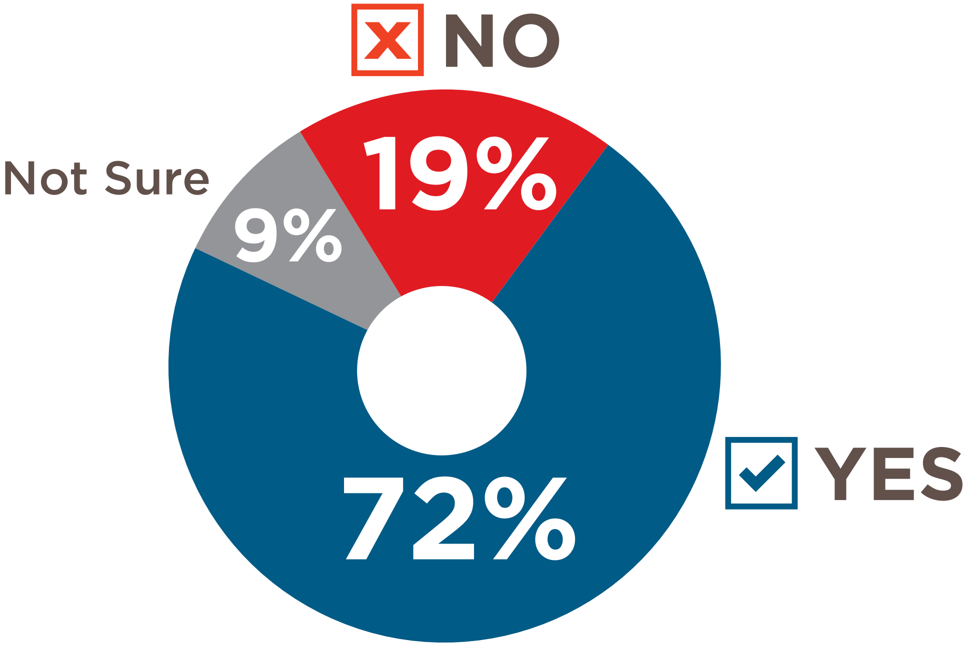
Q: Does your organization leverage analytics to determine insider threats?



TRAINING TO IDENTIFY SECURITY RISKS

Most organizations (72 percent) offer training for their employees on how to identify security risks.

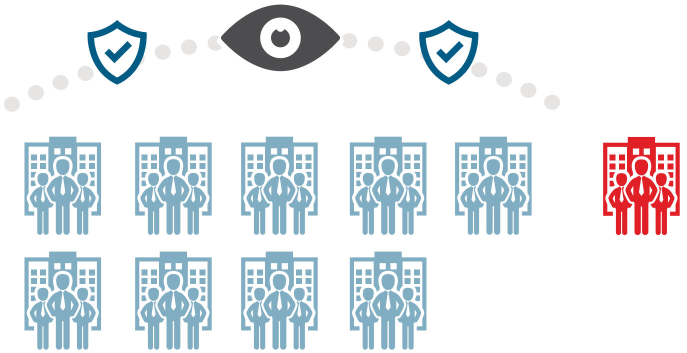
Q: Do you offer training to your employees and staff on how to identify security risks?



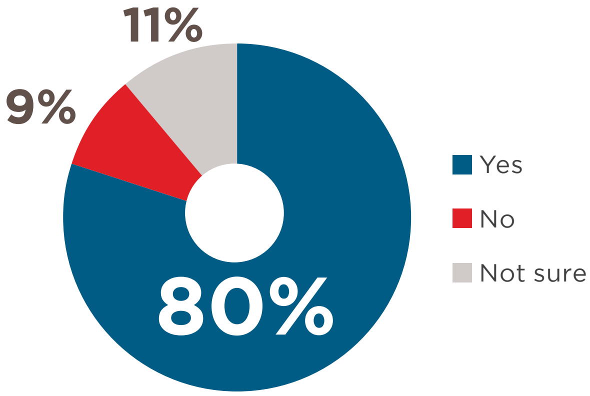
SECURITY TOOLS AND PROCESSES

CONTROLS TO COMBAT INSIDER THREATS

Organizations that proactively implement specific controls to prevent cyber attacks as part of its risk management program outnumber those that do not almost 10:1.



Q: Do you include cyber attacks in your risk management framework?



The controls that these organizations utilize include security perimeter defense tools (76 percent), database and file monitoring tools (67 percent) and security events dashboard (58 percent).

Q: What risk controls are important for managing risk of cyber attack occurrences?

76% Security perimeter defense tools

67% Database and file monitoring tools

58% Security events dashboard

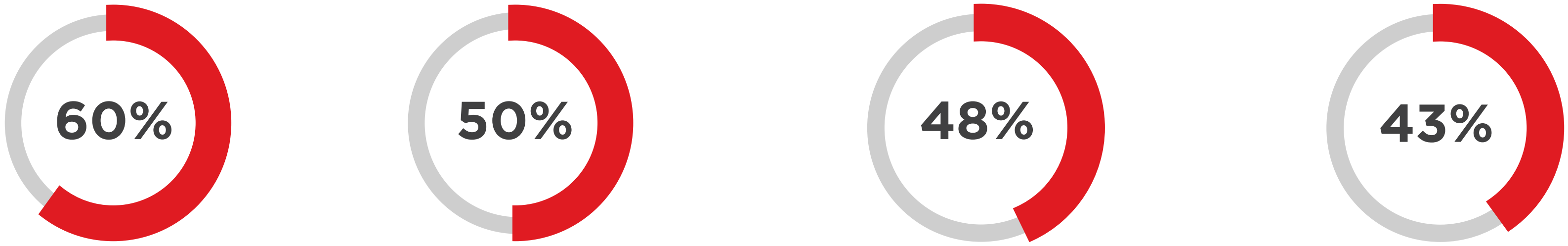
Access violations Key Risk Indicators by database or system 55% | Security event remediation processes 55% | Data loss and corruption Key Risk Indicators 52% | System of Record monitoring 46% | System down time Key Risk Indicators 24% | Not sure / Other 13%

BARRIERS TO BETTER INSIDER THREAT MANAGEMENT

Similar to our last survey, the biggest perceived barrier to better insider threat management is organizational, starting with a lack of training and expertise (60 percent). Rounding out the top three are insufficient budgets (50 percent) and lack of collaboration between departments (48 percent). Notably, lack of collaboration is the barrier with the highest gain since the previous survey, moving up 10 percentage points.

Q: What are the biggest barriers to better insider threat management?

#1 #2 #3 #4



#1 Lack of training & expertise — ⬇ **3% p.p.** from last year

#2 Lack of budget — ⬆ **2% p.p.** from last year

#3 Lack of collaboration between separate departments — ⬆ **10% p.p.** from last year

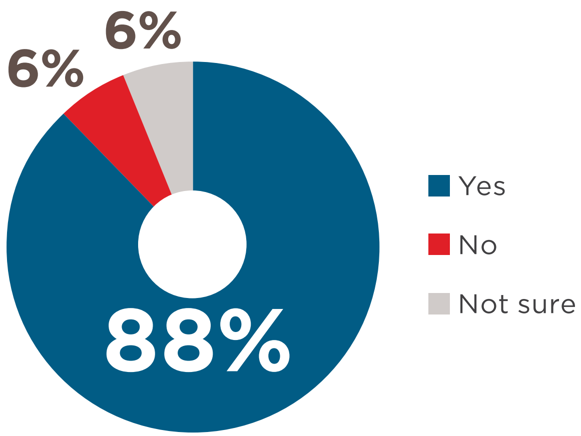
#4 Not a priority — **Stay the same** from last year

Lack of staff 35% | Lack of suitable technology 28% | Not sure / Other 11%

RISK MANAGEMENT FRAMEWORK

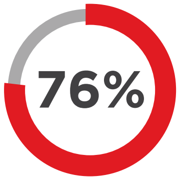
The majority of respondents (88 percent) think integrating security controls with business processes is a must.

Q: Do you think an Information Security Governance Program is required to ensure that security is integrated with an organization's business processes?

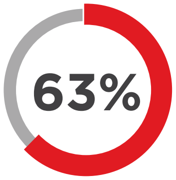


The top three tactics companies use to implement an effective security governance program include: security policies with measured compliance with measured compliance (76 percent), escalation processes to inform board members quarterly on security performance and breaches (63 percent), and a security stewardship organizational structure (61 percent).

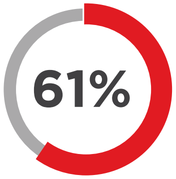
Q: What is required to implement such a program?



Implement Security Policies with measured compliance



Escalation process to inform board members quarterly on security performance and breaches



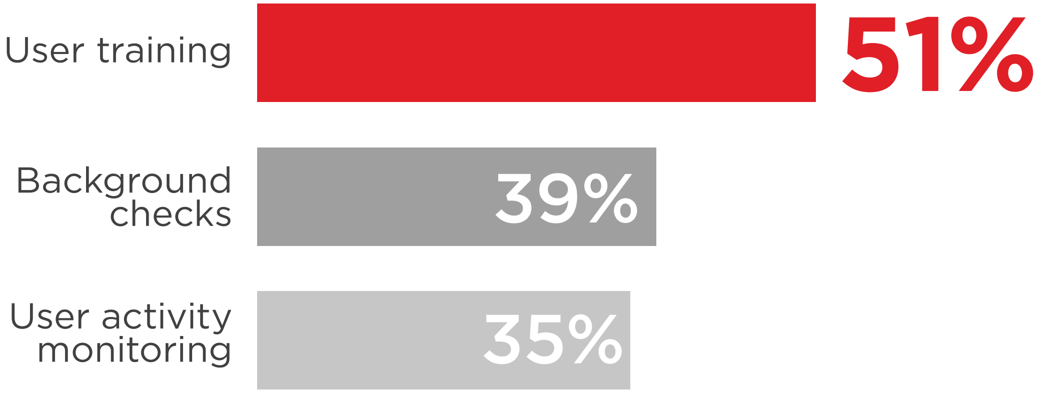
Security Stewardship organizational structure

Oversight mechanism 54% | Performance measurement 40% | Not sure / Other 14%

INSIDER THREAT APPROACH

User training (51 percent), background checks (39 percent) and monitoring user activity (35 percent) top the list of how organizations overcome insider threats.

Q: How does your organization combat insider threats today?



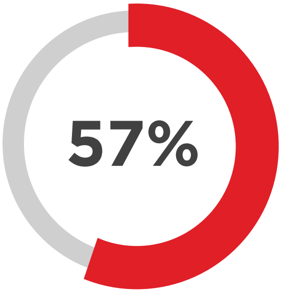
Information Security Governance Program 34% | Database Activity Monitoring 24% | Native security features of underlying OS 22% | Secondary authentication 21% | Specialized 3rd party applications and devices 15% | Custom tools and applications developed in house 11% | Managed Security Service provider 8% | We do not use anything 7% | Not sure/Other 15%

MOST EFFECTIVE TOOLS

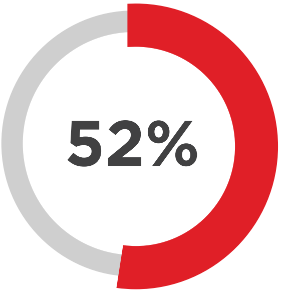
Policies and training (57 percent) are considered the most effective tools in protecting against insider threats. identity and access management (IAM) (52 percent) and encryption of data (at rest, in motion, in use) (50 percent) round out the top three.

Q: What are the most effective security tools and tactics to protect against insider attacks?

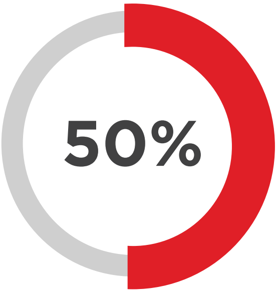
#1 Policies & training



#2 Identity and access management (IAM)



#3 Encryption of data (at rest, in motion, in use)



Data Loss Prevention (DLP) 49% | Security information and event management (SIEM) 46% | User behavior anomaly detection 45% | Intrusion Detection and Prevention (IDS/IPS) 42% | File Activity Monitoring 41% | User monitoring 40% | Endpoint and mobile security 39% | Data Access Monitoring 38% | Multi-factor authentication 38% | Network defenses (firewalls) 37% | Security analytics & intelligence 37% | Sensitive and Private Data Identification 35% | Database Activity Monitoring 34% | Tokenization 19% | Enterprise Digital Rights Management solutions (E-DRM) 17% | Password vault 17% | Cloud Access Security Broker (CASB) 11% | Cloud Security as a Service 10% | Not sure / Other 10%

FOCUS ON DETERRENCE

Most organizations continue to place their insider threat management focus and resources on deterrence tactics (61 percent), followed by detection (49 percent) and analysis and forensics (35 percent).

Q: What aspect(s) of insider threat management does your organization mostly focus on?

61%

Deterrence
(e.g., access controls, encryption, policies, etc.)

49%

Detection
(e.g., monitoring, IDS, etc.)

35%

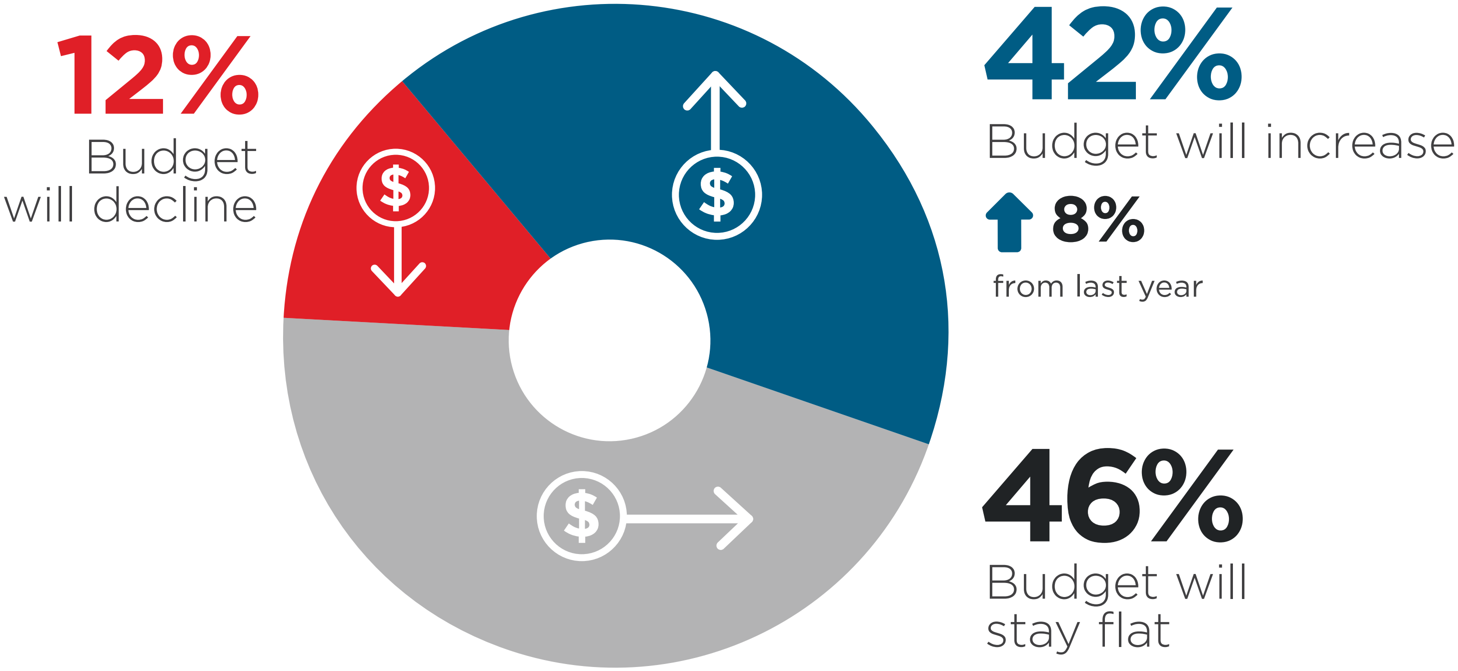
Analysis & Forensics
(e.g., SIEM, etc.)

Deception (e.g., honeypots, etc) 9% | None 7% | Not sure / Other 3%

BUDGET TRENDS

With insider attacks on the rise, 42 percent of organizations expect a budget increase over the next 12 months. This represents a strong gain of eight percentage points from the previous year.

Q: How is your security budget changing over the next 12 months?



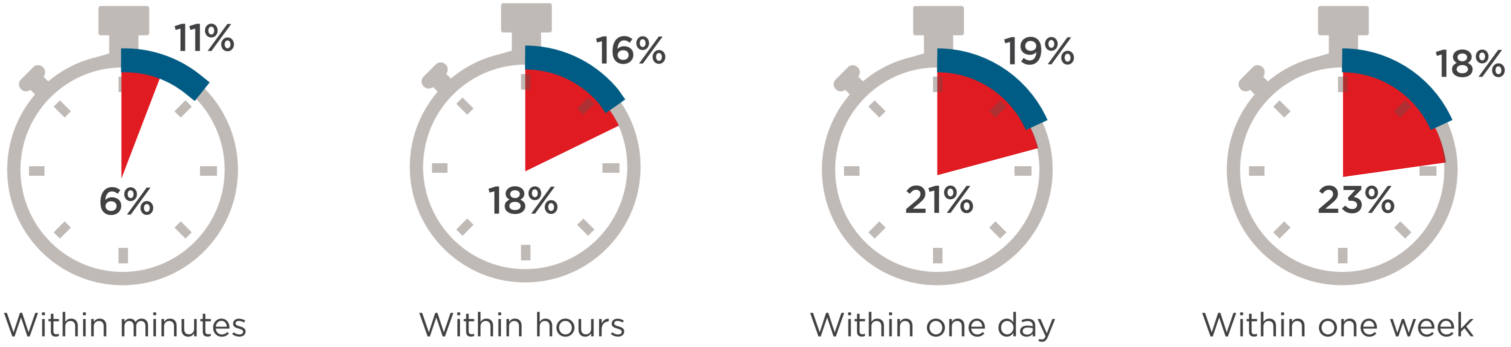
RECOVERY AND REMEDIATION

SPEED OF DETECTION & RECOVERY

Q: How long would it typically take your organization to detect an insider attack?

Year over year companies are getting better at both detecting and recovering from insider attacks. This year most IT professionals feel their organization could detect an insider attack within one day, up six percent year over year.

Within one month 9% | Within three months 7% | Longer than three months 7% | No ability to detect 13%



46% organizations detect an insider attack within the same day or faster

68% organizations recover from an insider attack within a week or less

🟦 Detection time 🟥 Recovery time

Q: How long would it typically take your organization to recover from an insider attack?

Organizations are getting more confident of their ability to recover from an attack. Sixty-eight percent of organizations feel they could recover from an attack within a week - up over 20 percent from last year's survey.

Within one month 15% | Within three months 5% | Longer than three months 9% | No ability to recover 3%

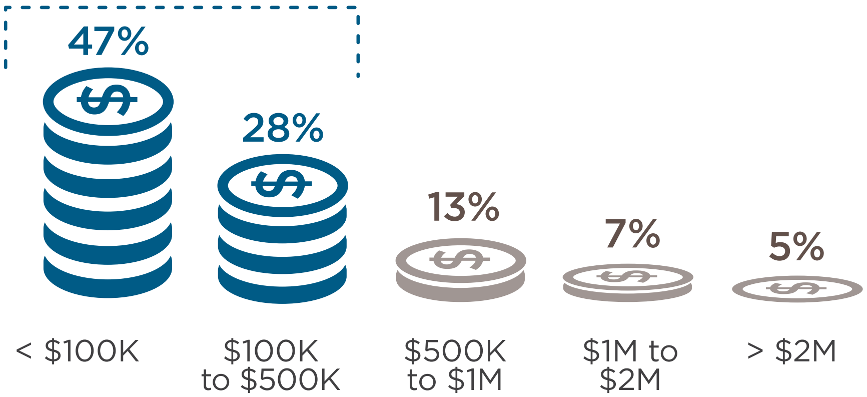
COST OF REMEDIATION

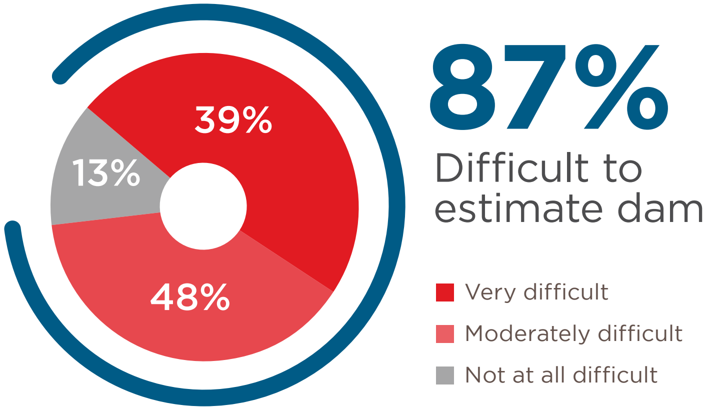
Q: What is the estimated, average cost of remediation after an insider attack?

Insider attacks can be costly to organizations, from immediate economic impact to long term damages in reputation and trust. This year, successful attacks are costing organizations even more money and the damage is getting more difficult to detect.

With over 75 percent of organizations estimating costs could reach a half a million dollars. Of those that are able to estimate the average cost of remediation, 25 percent believe the cost exceeds $500,000 and can reach in the millions.

75%
estimates cleanup costs up to $500K





87%
Difficult to estimate damages

Q: Within your organization, how difficult is it to determine the actual damage of an occurred insider threat?

Eighty seven percent of organizations find it difficult to determine the actual damage of an insider threat. This is 20 percent more than last year.

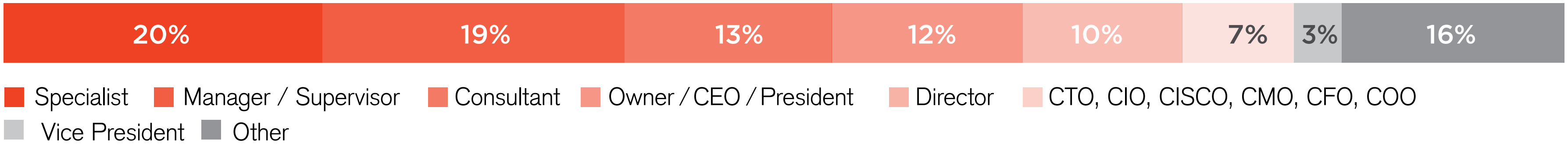
METHODOLOGY AND DEMOGRAPHICS

METHODOLOGY & DEMOGRAPHICS

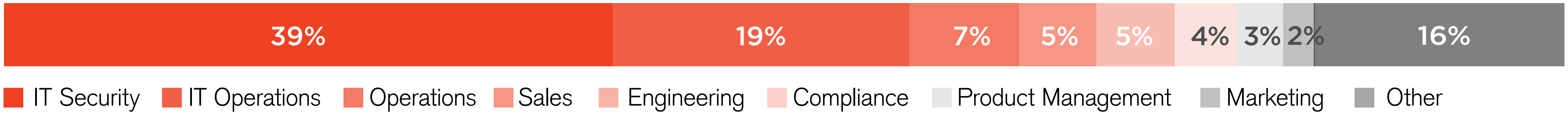
The Insider Threat Spotlight Report is based on the results of a comprehensive survey of over 500 cybersecurity professionals to gain more insight into the state of insider threats and solutions to prevent them.

The respondents range from technical executives to managers and IT security practitioners, and they represent organizations of varying sizes across many industries. Their answers provide a comprehensive perspective on the state of cloud security today.

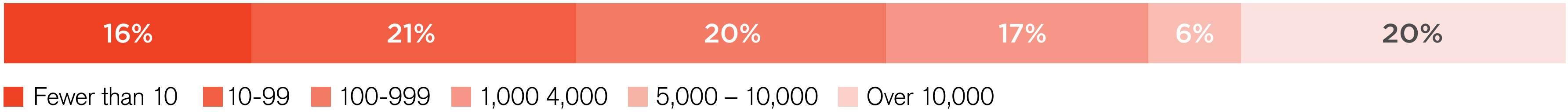
CAREER LEVEL



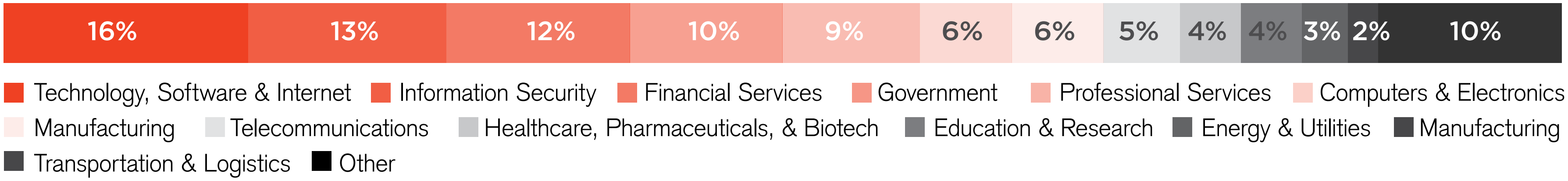
DEPARTMENT



COMPANY SIZE



INDUSTRY



SPONSOR OVERVIEW

SPONSORS

AlienVault | www.alienvault.com

AlienVault has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, AlienVault Unified Security Management, with the power of AlienVault's Open Threat Exchange, the world's largest crowd-sourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams.

If your organization has adopted cloud infrastructure or services, you have a significant amount of valuable data in the cloud – all of which needs to be secured. AlienVault Unified Security Management™ (USM) simplifies cloud security management with a platform of essential tools to achieve complete security visibility and accelerate compliance reporting.

Bitglass | www.bitglass.com

The Bitglass Cloud Access Security Broker (CASB) solution provides end-to-end data protection from the cloud to the device. It deploys in minutes and works with any cloud app on any device.

Bitglass enables enterprises to understand and control usage of cloud apps like Office 365 and Salesforce, and internal apps like Exchange and Sharepoint. Cloud data at rest is protected with encryption and suspicious activity detection. IT security teams can enforce consistent access, sharing, and data leakage prevention policies across multiple cloud services, and protect mobile devices - without MDM.

CipherPoint | www.cipherpoint.com

CipherPoint's ability to restrict content views of unstructured sensitive data up to and including the IT Administrators makes it the foremost leader in Insider Threat Protection. Our platform natively supports content stores both on-prem (SharePoint and File Servers) and in the Cloud (SharePoint Online, OneDrive for Business, and GoogleDocs) for document storage. Via our API, organizations can also extend this patented approach to security to whatever platform they want to secure. We can auto-classify content on the upload, and also provide secure email for data transmissions. Prem, Cloud, or Hybrid, CipherPoint is your solution for today's complex security problems.

SPONSORS

Dtex | www.dtexsystems.com

Dtex provides unique endpoint data with advanced analytics to detect data breaches, insider threats, and outsider infiltration at enterprise scale. Dtex accurately pinpoints threats by combining thousands of patterns of known bad behavior with user behavior analytics. Unlike other vendors, Dtex avoids the lock-and-block methods that can adversely impact user productivity. This ‘trust but verify’ approach recognizes that the endpoint is the new perimeter of the organization.

Exabeam | www.exabeam.com

Exabeam is a security intelligence solution that leverages existing log data to quickly detect modern cyber attacks, prioritize security incidents, and accelerate effective response. As a result, Exabeam not only improves security, but also transforms SOC efficiency and productivity. By operating on existing data and requiring no agents or network taps, Exabeam delivers value immediately.

Fasoo | www.fasoo.com

Fasoo has successfully retained its leadership in the data and application security market by deploying solutions for more than 1,200 organizations enterprise-wide, securing more than 2.5 million users. Fasoo offers a data security framework that enables organizations to have the highest level of protection against data breach threats through a multi-layered architecture of data-centric security and people-centric policies. The framework consists of multiple Fasoo solutions, each of which has value on its own but together they comprise a comprehensive approach to data security.

SPONSORS

LightCyber | www.lightcyber.com

LightCyber is a leading provider of Behavioral Attack Detection solutions that provide accurate and efficient security visibility into attacks that have slipped through the cracks of traditional security controls. The LightCyber Magna™ platform is the first security product to integrate user, network and endpoint context to provide security visibility into a range of attack activity. Founded in 2012 and led by world-class cyber security experts, the company's products have been successfully deployed by top-tier customers around the world in industries including the financial, legal, telecom, government, media and technology sectors.

ObserveIT | www.observeit.com

ObserveIT is the world's leading provider of user activity monitoring software. Founded in 2006, ObserveIT is the only security software company that provides user behavior analytics, alerting and visual forensics to know when users put your business at risk. With ObserveIT, information security teams are able to detect data misuse within core applications, see exactly what's happening in live sessions and act in real time. To do this, ObserveIT provides screen-recording technology to capture all user activity regardless of the environment and converts screenshots into user activity logs that makes it easy to search, analyze, audit and act upon alerts. ObserveIT has more than 1,200 customers in over 70 countries.

Palerra | www.palerra.com

Palerra is a leading Cloud Access Security Broker (CASB), and the pioneer of API-centric CASB solutions that help customers realize the full promise of the cloud. The Palerra LORIC platform secures all data, users, and devices across SaaS, IaaS, and PaaS, whether managed or unmanaged.

LORIC uses intelligent analytics and dynamic decision-making capabilities to enable automated threat prediction, breach discovery, and user behavior analytics across thousands of threat vectors. LORIC also provides provisioning capabilities to securely establish controls, configurations, and baselines for applications. With no hardware, software, or agents, LORIC deploys in under five minutes and scales with cloud services.

SPONSORS

Prolifics | www.prolifics.com

Leading Security organizations understand the importance of integrating security within business processes. However, implementing that effectively can be a challenge. Prolifics applies an innovative approach to help organizations achieve comprehensive Information Security Governance programs, by scanning and validating database access policies, server file movements and other functionalities using pre-built business process workflows.

SentinelOne | sentinelone.com

SentinelOne was founded in 2013 by an elite group of cybersecurity and defense experts who share a clear vision on how to protect against advanced attacks in a post-antivirus era. SentinelOne's next-generation endpoint and server protection stops known and unknown threats using sophisticated machine learning and intelligent automation while providing detailed forensics for further analysis. SentinelOne is PCI-DSS, HIPAA, and AV-TEST-certified so that organizations can replace their antivirus and still meet compliance requirements.

TEMASOFT | temasoft.com

TEMASOFT is a software company committed to becoming a leader in data protection solutions, with over 15 years' experience building security and infrastructure software applications for various partners, including several award-winning products used by thousands of customers worldwide.

Veriato | www.veriato.com

Veriato develops intelligent, powerful monitoring solutions that provide companies with visibility into human behaviors and activities occurring within their firewall. Our products make organizations more secure and productive.

CONTACT US

Want to see your brand featured in the next cybersecurity report?

Contact us to learn more.

✉ info@crowdresearchpartners.com

Visit Crowd Research Partners for more details

Produced by:

Crowd Research Partners

LinkedIn Group Partner
Information Security