2019

Cybersecurity
INSIDERS

INSIDER THREAT REPORT

FORTINET

INTRODUCTION

Many of today's most damaging security threats are not the result of malicious outsiders or malware, but instead originate from trusted insiders—whether malicious or negligent—who have access to sensitive data and systems.

The 2019 Insider Threat Report reveals the latest trends and challenges facing organizations, how IT and security professionals are dealing with risky insiders, and how organizations are preparing to better protect their critical data and IT infrastructure.

Key findings include:

- 68% of organizations feel moderately to extremely vulnerable to insider attacks.
- 68% of organizations confirm insider attacks are becoming more frequent.
- 56% believe detecting insider attacks has become significantly to somewhat harder since migrating to the cloud.
- 62% think that privileged IT users pose the biggest insider security risk to organizations.

The survey data shows insider threats continue to pose serious risks to organizations. It also illustrates that most still have significant work to do in designing and building effective insider threat programs, including user entity and behavior analytics (UEBA).

This 2019 Insider Threat Report has been produced by Cybersecurity Insiders, the 400,000-member community for information security professionals, to explore how organizations are responding to the evolving security threats in the cloud.

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

We hope you'll find this report informative and helpful as you continue your efforts in protecting your IT environments against insider threats.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

TYPES OF INSIDER THREATS

The term "Insider Threat" is often associated with malicious employees intending to directly harm the company through theft or sabotage. In truth, negligent employees or contractors can unintentionally pose an equally high risk of security breaches and leaks by accident.

In this year's survey, companies are somewhat more worried about inadvertent insider breaches (71%), negligent data breaches (65%), and malicious intent by bad actors (60%) than they are about compromised accounts/machines (9%).

What type of insider threats are you most concerned about?

71%

Inadvertent data breach/ leak

(e.g., careless user causing accidental breach)

65%

Negligent data breach

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

60%

Malicious data breach

(e.g., user willfully causing harm)

Compromised accounts/machines (e.g., user system taken over without knowledge) 9% | Other 3%

MOTIVATIONS FOR INSIDER ATTACKS

To understand malicious insider threats, it is important to look at the underlying motivations of insiders. Our survey panel considers fraud (55%) and monetary gain (49%) the biggest factors that drive malicious insiders, followed by theft of intellectual property (44%). The ideal insider threat solution captures threats from all of these vectors, including financial, personal, and professional stressors as indicators that a person is at risk or already an active insider threat.

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

55%

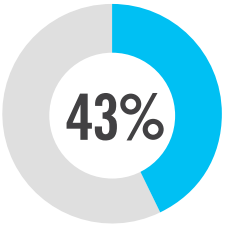
Fraud

49%

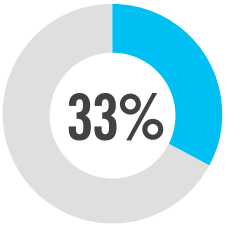
Monetary gain

44%

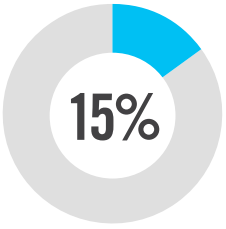
IP theft



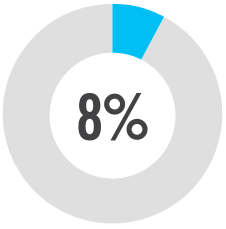
Sabotage



Espionage



Professional benefit



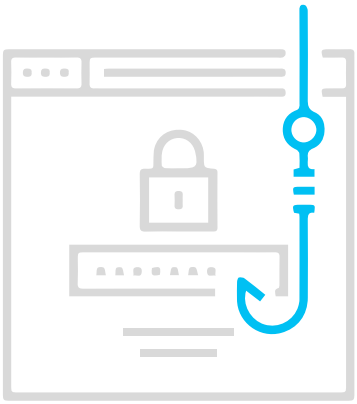
To cause reputation damage

Not sure/other 8%

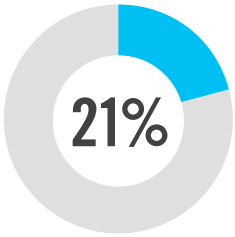
ACCIDENTAL INSIDERS

Cybersecurity experts view phishing attempts (38%) as the biggest vulnerability for accidental insider threats. Phishing attacks trick employees into sharing sensitive company information by posing as a legitimate business or trusted contact, and they often contain malware attachments or hyperlinks to compromised websites.

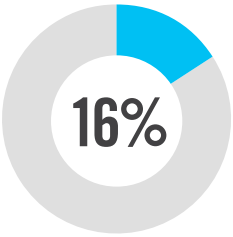
What are the most common accidental insider threats you are most concerned about?



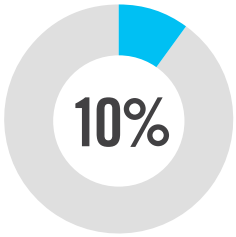
38% Phishing attacks



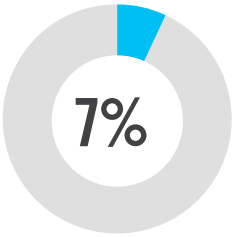
Spear phishing



Poor passwords



Orphaned accounts



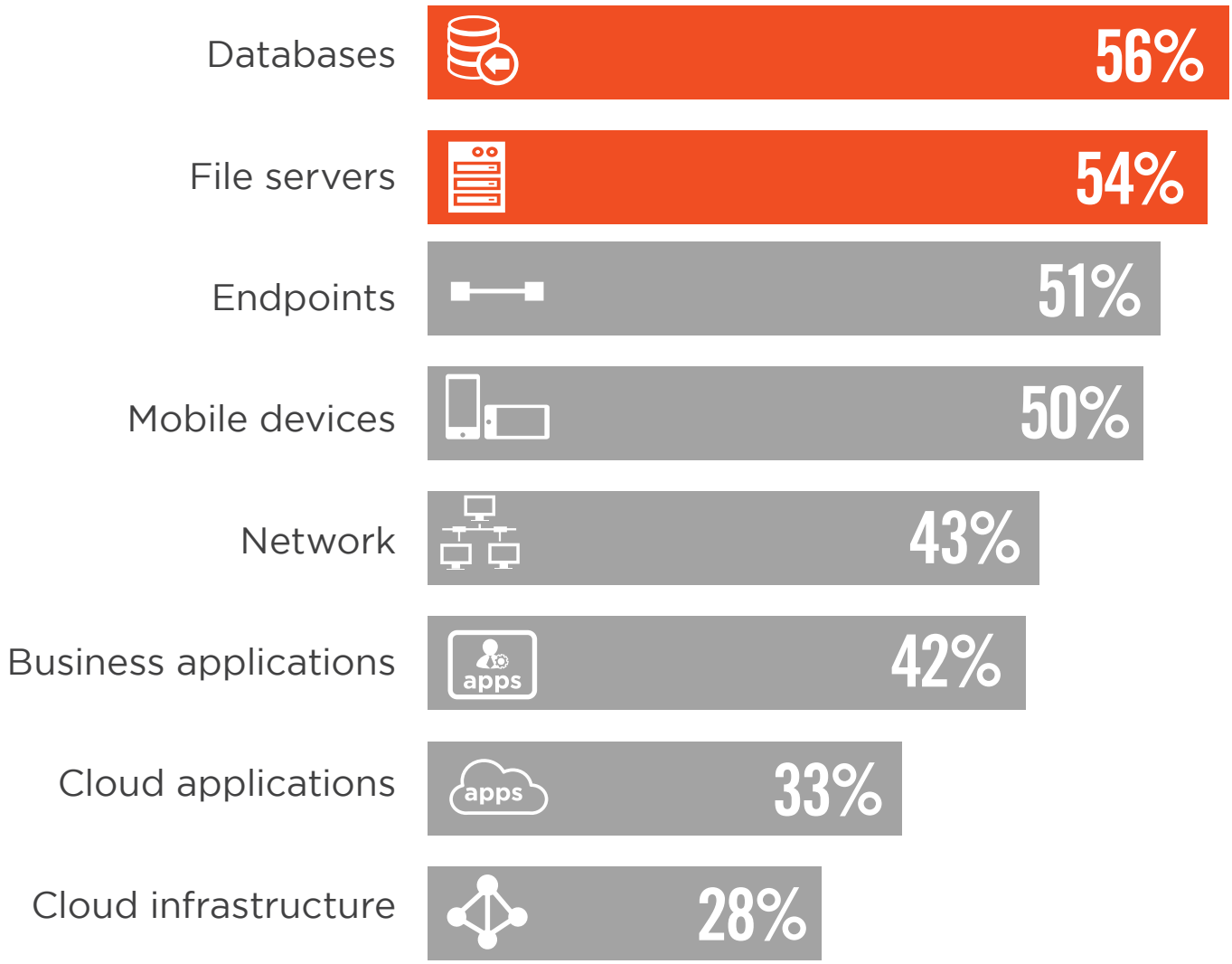
Browsing suspicious sites

Other 8%

IT ASSETS AT RISK

Cyber criminals see a greater opportunity in targeting where corporate data is located in volume. Databases (56%) and corporate file servers (54%) pose the highest risk, followed by endpoints (51%) and mobile devices (50%).

What IT assets are most vulnerable to insider attacks?



Not sure/other 5%

RISKY INSIDERS

Protecting organizations against cyber threats becomes significantly more challenging when the threats come from within the organization—from trusted and authorized users. It can be difficult to determine when users are simply fulfilling their job responsibilities or actually doing something malicious or negligent.

The survey indicates that privileged IT users (62%) pose the biggest insider security risk to organizations, followed by contractors, regular employees, and privileged business users (all tying at 50%).

What type(s) of insiders pose the biggest security risk to organizations?

62% Privileged IT users/admins

50% Contractors/ service providers/ temporary workers

50% Regular employees

50% Privileged business users/executives

Other IT staff 23% | Executive managers 20% | Customers/clients 14% | Business partners 14% | Interns 3% | Other 3%

DEPARTMENTS AT RISK

Organizations in our survey consider their finance departments (41%), support/customer success (35%), and research and development (33%) as the highest risk of insider threats.

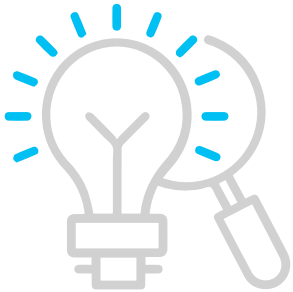
Which departments or groups within your organization present the biggest risk for insider threats?

41%

Finance

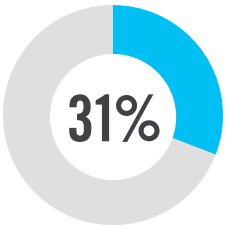
35%

Support/ customer success

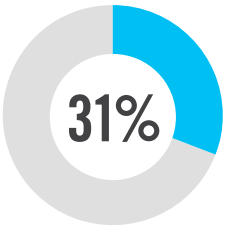


33%

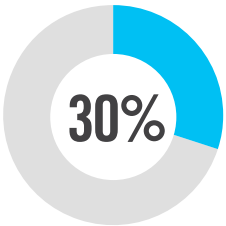
Research and development



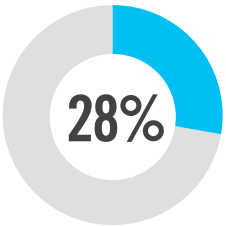
Board of directors/ executive management team



Sales



General administration



Human resources

Marketing 25% | IT 19% | Operations 13% | Legal 13% | Other 8%

MOST VULNERABLE DATA

Data is a core strategic asset and some types of data are more valuable than others as a target of insider attacks. This year, customer data (62%) takes the top spot as the data most vulnerable to insider attacks, followed by intellectual property (56%) and financial data (52%).

What types of data are most vulnerable to insider attacks?

62%

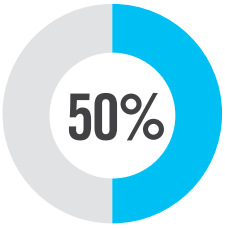
Customer data

56%

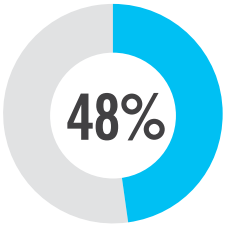
Intellectual property

52%

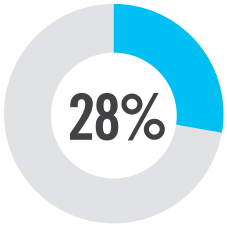
Financial data



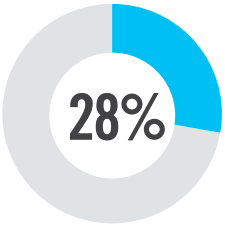
Employee data



Company data



Sales and marketing data



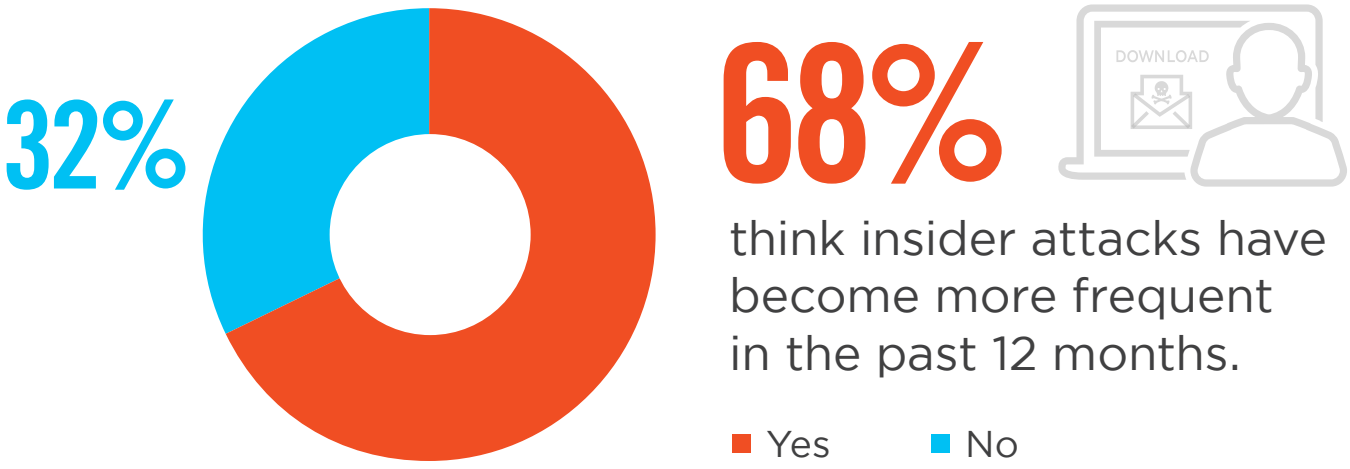
Healthcare data

Not sure/other 4%

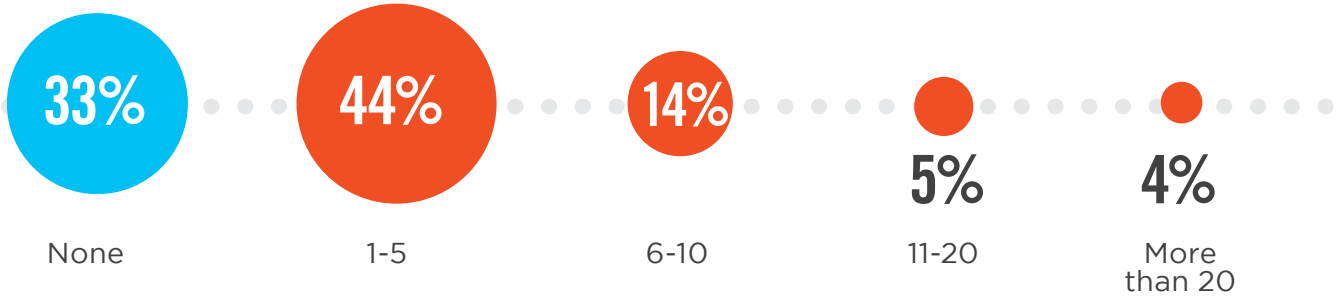
RISE OF INSIDER ATTACKS

A significant majority of organizations (68%) observed that insider attacks have become more frequent over the last 12 months. In fact, 67% have experienced one or more insider attacks within the last 12 months.

Have insider attacks become more or less frequent over the last 12 months?



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

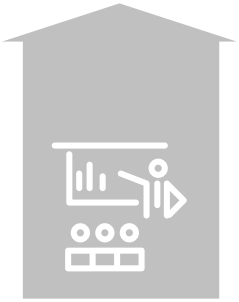


CONTRIBUTING FACTORS

Fifty-four percent believe the most critical factor enabling insider attacks is the lack of employee awareness and training. Another key factor is insufficient data protection strategies or solutions (50%) and the proliferation of devices with access to sensitive data (49%).

What do you believe are the main reasons behind insider attacks?

54%

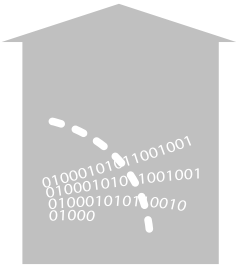


Lack of employee training/ awareness

50%

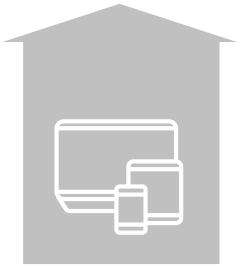
Insufficient data protection strategies or solutions

49%

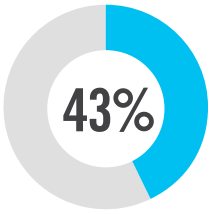


Data increasingly leaving the network perimeter via mobile devices and web access

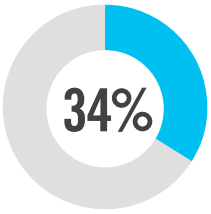
49%



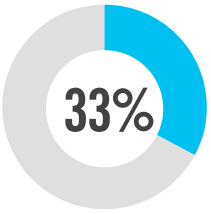
Increasing number of devices with access to sensitive data



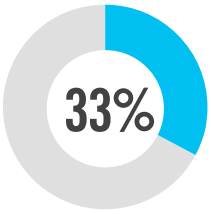
More employees, contractors, partners accessing the network



Increasing amount of sensitive data



Technology is becoming more complex



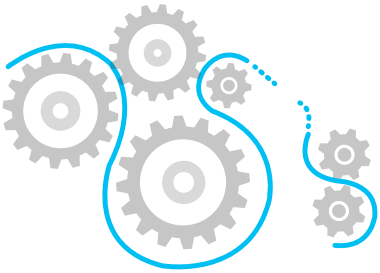
Increasing use of cloud apps and infrastructure

Increased public knowledge or visibility of insider threats that were previously undisclosed 23% | Too many users with excessive access privileges 17% | More frustrated employees/contractors 10% | Not sure/other 9%

INSIDER THREAT IMPACT

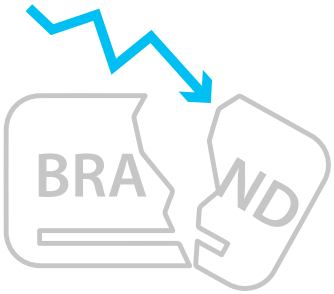
Insider threats have a range of impacts on organizations, ranging from operational disruption (61%) and brand damage (43%) to loss of critical data (43%) as the top three impacts.

What impact have insider threats had on your organization?



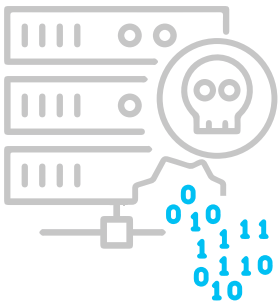
61%

Operational disruption or outage



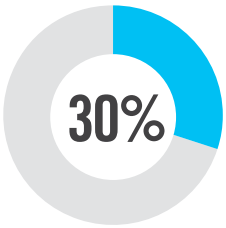
43%

Brand damage

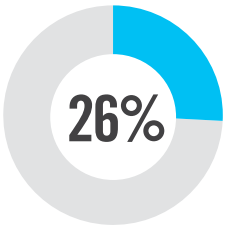


43%

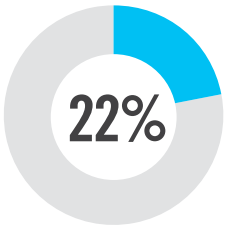
Loss of critical data



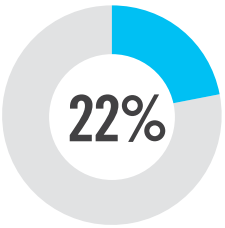
Loss in competitive edge



Expenditure remediating successful intrusions



Loss in market valuation



Legal liabilities

Loss in revenue 17% | No impact 13%

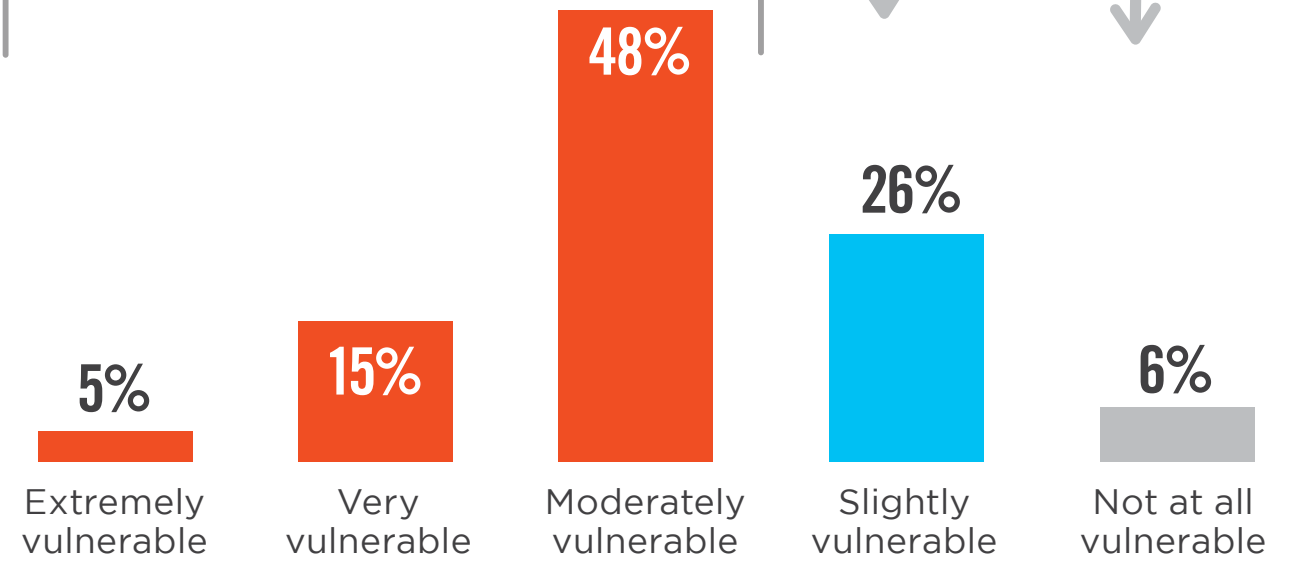
INSIDER VULNERABILITY

We asked cybersecurity professionals to assess their organization's vulnerability to insider threats. An overwhelming 68% of organizations feel moderately to extremely vulnerable. Only 6% say they are not at all vulnerable to an insider attack. Insider threats present another layer of complexity for IT professionals to manage.

How vulnerable is your organization to insider threats?

68%

feel extremely to moderately vulnerable to insider attacks.

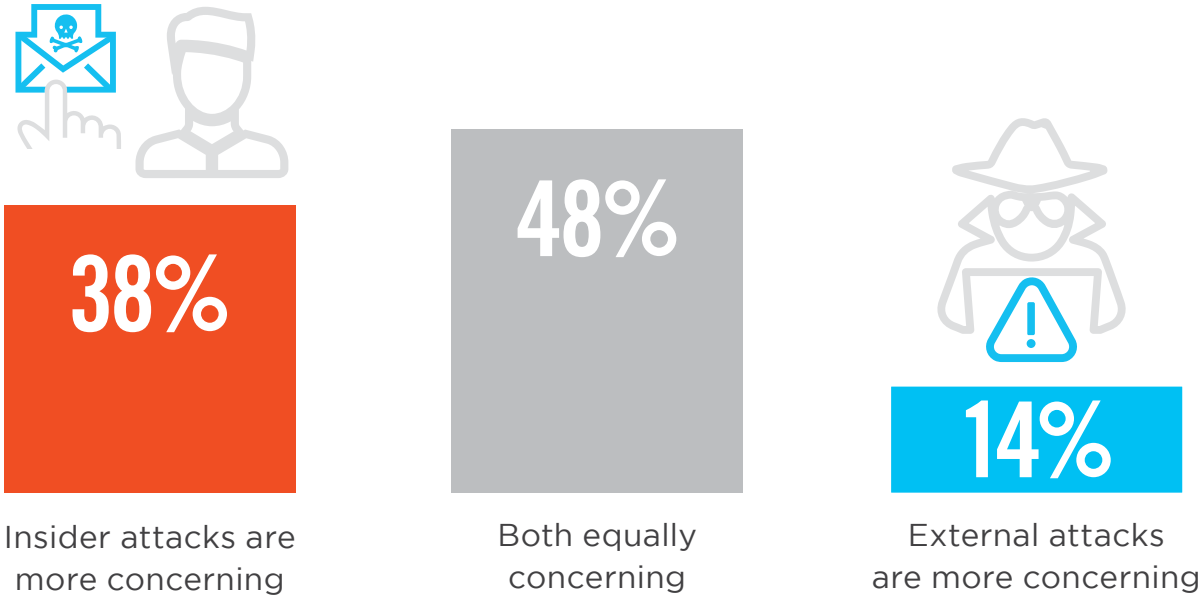


INSIDER ATTACKS OR EXTERNAL ATTACKS

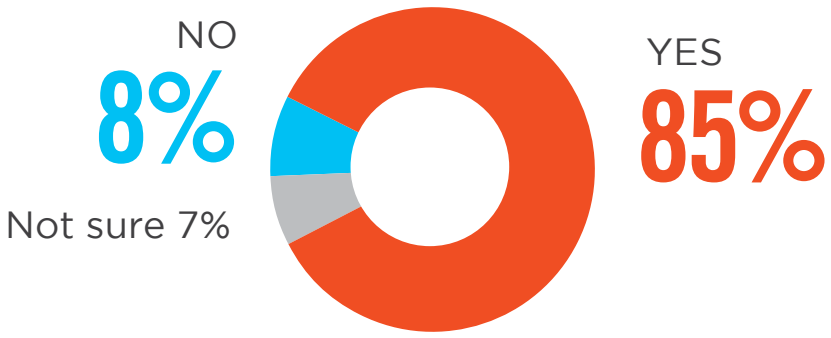
While all attack sources pose threats, organizations are significantly more concerned about attacks originating from inside the organization (38%). This is largely due to the difficulty in detecting insider attacks and the potential damage knowledgeable insiders with admin credentials can create. Only 14% consider external attacks more concerning.

That 85% of organizations in our survey include insider attacks in their risk management framework is further reflection of the importance placed on managing insider threats.

Which is more concerning for you, insider attacks or external attacks?



Do you include insider attacks in your risk management framework?



DETECTION AND PREVENTION

Because insiders often have elevated access privileges to sensitive data and applications, it becomes increasingly difficult to detect malicious activity (60%). Combined with more data leaving the traditional network perimeter (48%) and the proliferation of data-sharing apps (47%), the conditions for successful insider attacks are becoming more difficult to control.

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

60%

Insiders already have credentialed access to the network and services

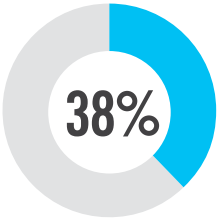
48%

Increased amount of data that leaves protected boundary/perimeter

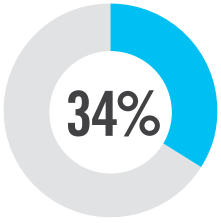
47%

Increased use of applications that can leak data

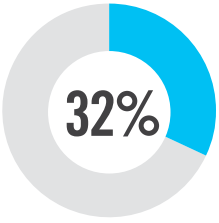
(e.g., web email, Dropbox, social media)



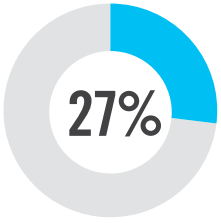
More end-user devices capable of theft



Migration of sensitive data to the cloud along with adoption of cloud apps



Insiders are more sophisticated



Difficulty in detecting rogue devices introduced into the network or systems

Absence of an information security governance program 23% | Not sure/other 7%

INSIDER THREAT PROGRAM DRIVERS

The creation of formal insider threat programs is typically driven by an information security governance program (47%), regulatory compliance (45%), and proactive security team initiative (45%), rather than a response to insider incidents.

What is the primary driver of your insider threat program?

47%

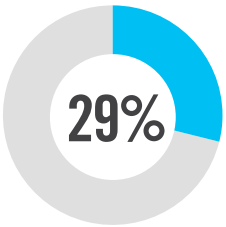
Information security governance program

45%

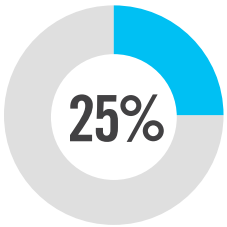
Regulatory compliance

45%

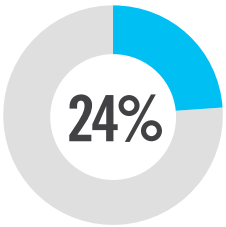
Proactive security team initiative



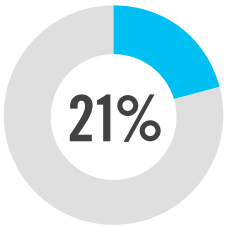
Proactive IT team initiative



Suspected incident



Previously confirmed incident



Directive from the executive management team

Directive from the board of directors 18% | We do not have an insider threat program 16% | Incident(s) that impacted peers or relevant industry 11% | Other 2%

PROGRAM IMPLEMENTATION

Security governance programs require a solid foundation of policies to be effective. Of highest priority are programs that align security policies and measure compliance (73%), enforce security stewardship across the organizational structure (64%), and implement escalation processes to inform board members on security performance (58%).

What is required to implement a security governance program?

73%

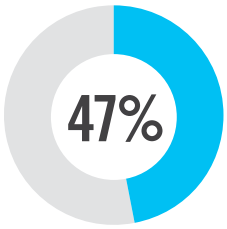
Implement security policies with measured compliance

64%

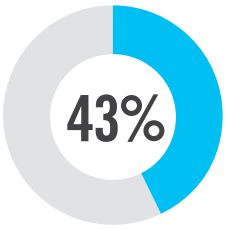
Security stewardship organizational structure

58%

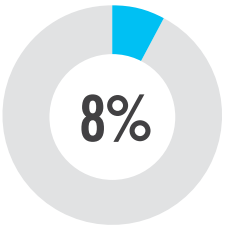
Escalation process to inform board members quarterly on security performance and breaches



Oversight mechanism



Performance measurement



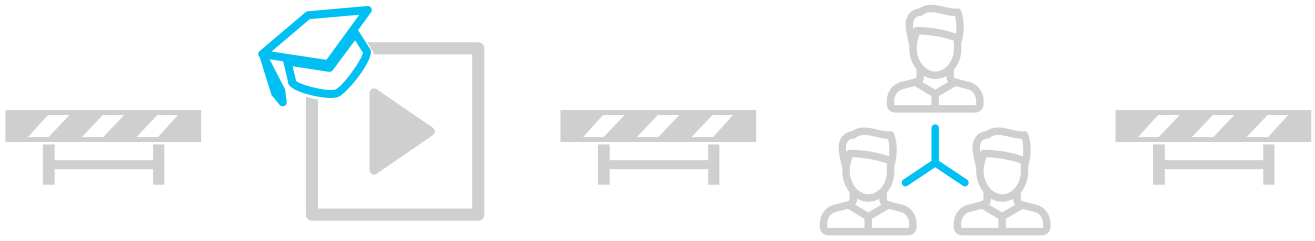
Right tools

Not sure/other 9%

BARRIERS TO INSIDER THREAT MANAGEMENT

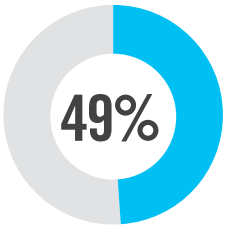
Lack of training and expertise and lack of collaboration among departments (tied with 56%) remain the key barriers to better insider threat management. Other important barriers include lack of budget (49%) and lack of staff (37%).

What are the biggest barriers to better insider threat management?

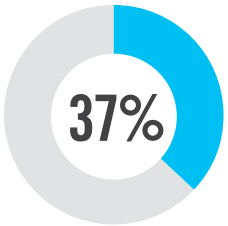


56%
Lack of training and expertise

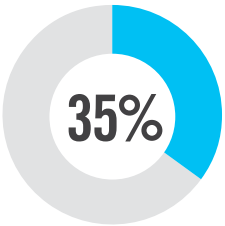
56%
Lack of collaboration between separate departments



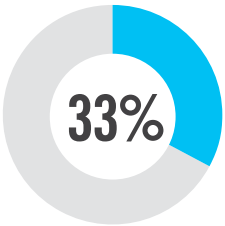
Lack of budget



Lack of staff



Lack of tools/ suitable technology



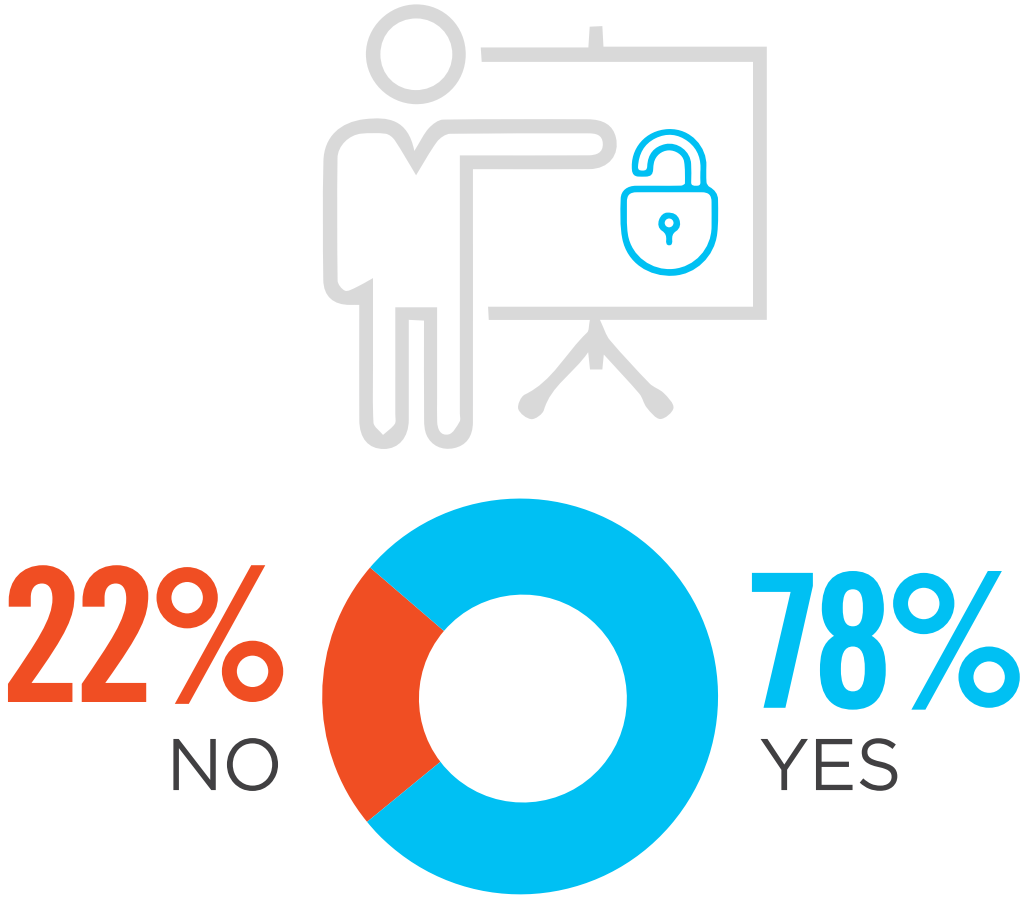
Not a priority

Privacy concerns 4% | Not sure/other 7%

EMPLOYEE TRAINING

A majority of 78% provides security training to employees as part of their insider risk management programs, yet this was cited as a key barrier to better insider threat management.

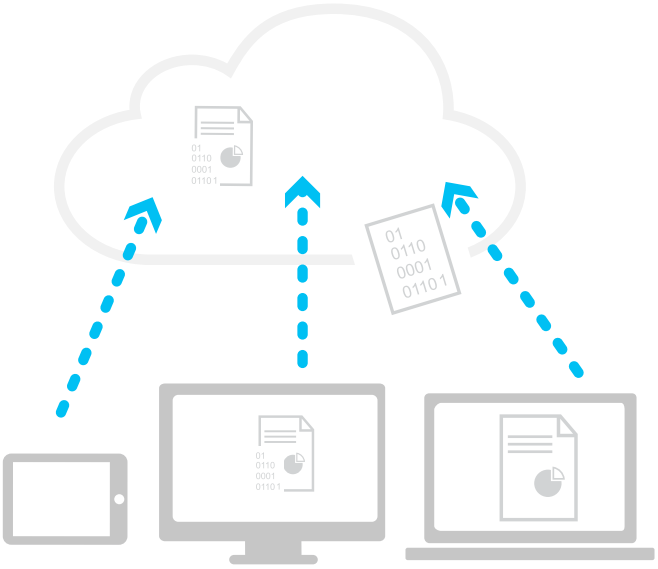
Do you offer training to your employees and staff on how to minimize insider security risks?



INSIDER ATTACKS IN THE CLOUD

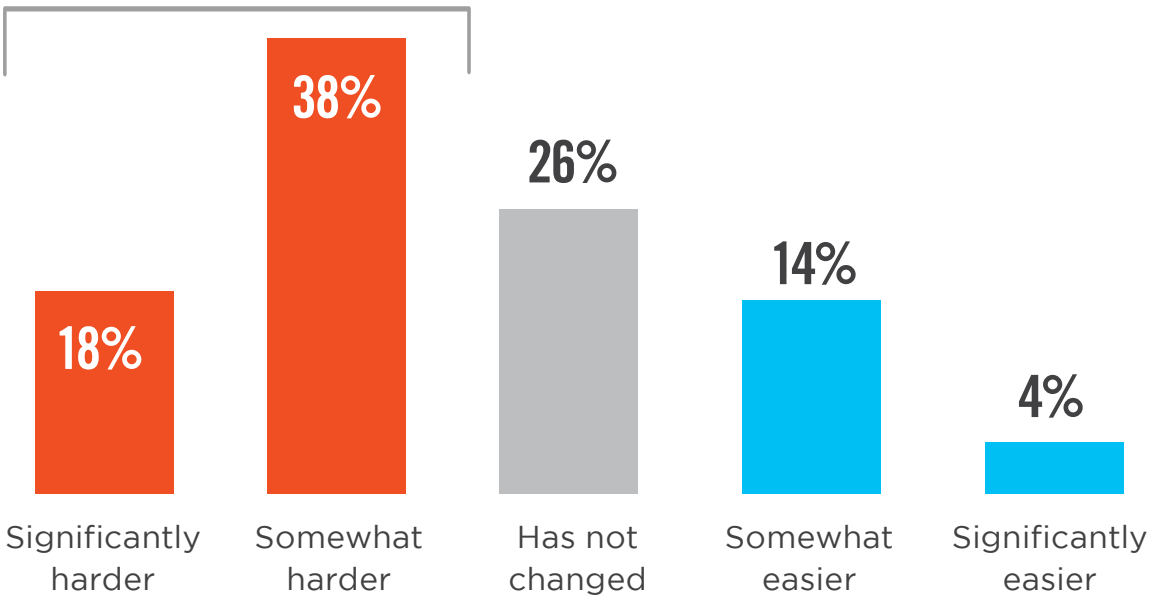
The shift to cloud computing is making the detection of insider attacks more difficult, as confirmed by 56% of cybersecurity professionals.

Since migrating to the cloud, how has detecting insider attacks changed?



56%

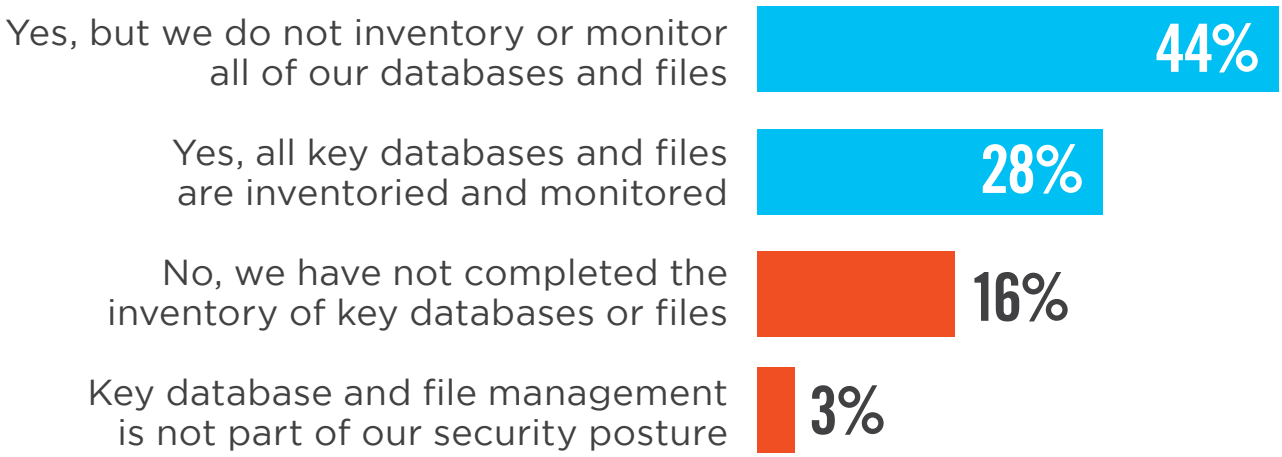
believe that detecting insider attacks has become significantly to somewhat harder.



DATABASE AND FILE TRANSFER MONITORING

Nearly three-quarters of organizations have vulnerabilities with their database monitoring and inventory and thus are unable to detect unusual activities associated with them that might be precipitated with insider threats.

Do you monitor key databases and file transfer activities?

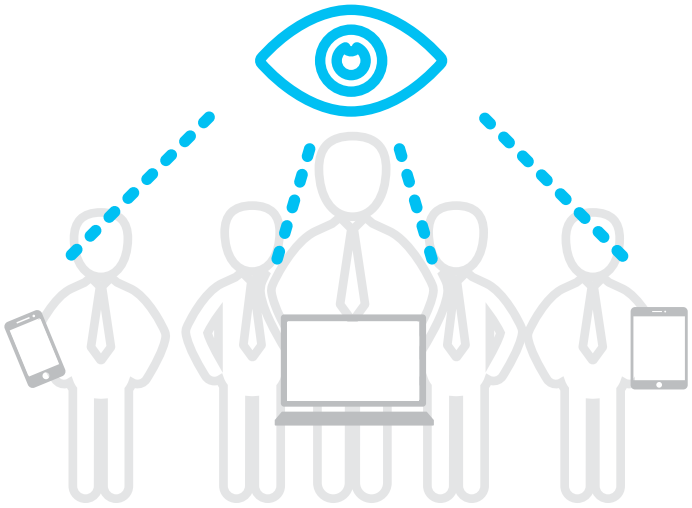


Not sure/other 10%

USER BEHAVIOR MONITORING

The increasing volume of insider threats has caused cybersecurity professionals to take more proactive steps and deploy user and entity behavior analytics (UEBA) tools to detect, classify, and alert anomalous behavior. Nearly three-quarters of organizations lack end-to-end user behavior monitoring that includes both access logging and automated user behavior monitoring. Even more concerning, 25% of organizations do not monitor user behavior at all or only after an incident.

Do you monitor user behavior?



35%
YES, but access logging only

27%
YES, we use automated tools to monitor user behavior 24x7

13%
YES, but only under specific circumstances
(e.g., shadowing specific users)

17%
NO, we don't monitor user behavior at all

8%
YES, but only after an incident
(e.g., forensic analysis)

VISIBILITY INTO USER BEHAVIOR

Full visibility that monitors activity proactively is critical for effective insider threat mitigation: Only slightly more than one-third of organizations actively monitor user behavior. Those who rely on server logs put their organizations at risk, which is reactive and incurs valuable manual labor to aggregate and reconcile.

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

43%

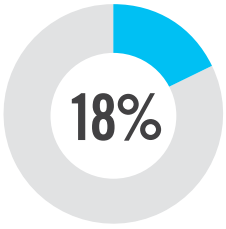
Rely on server logs

34%

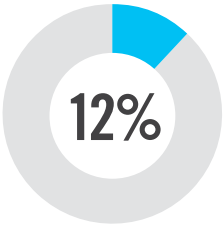
Deployed user activity monitoring

32%

In-app audit system/feature



No visibility at all



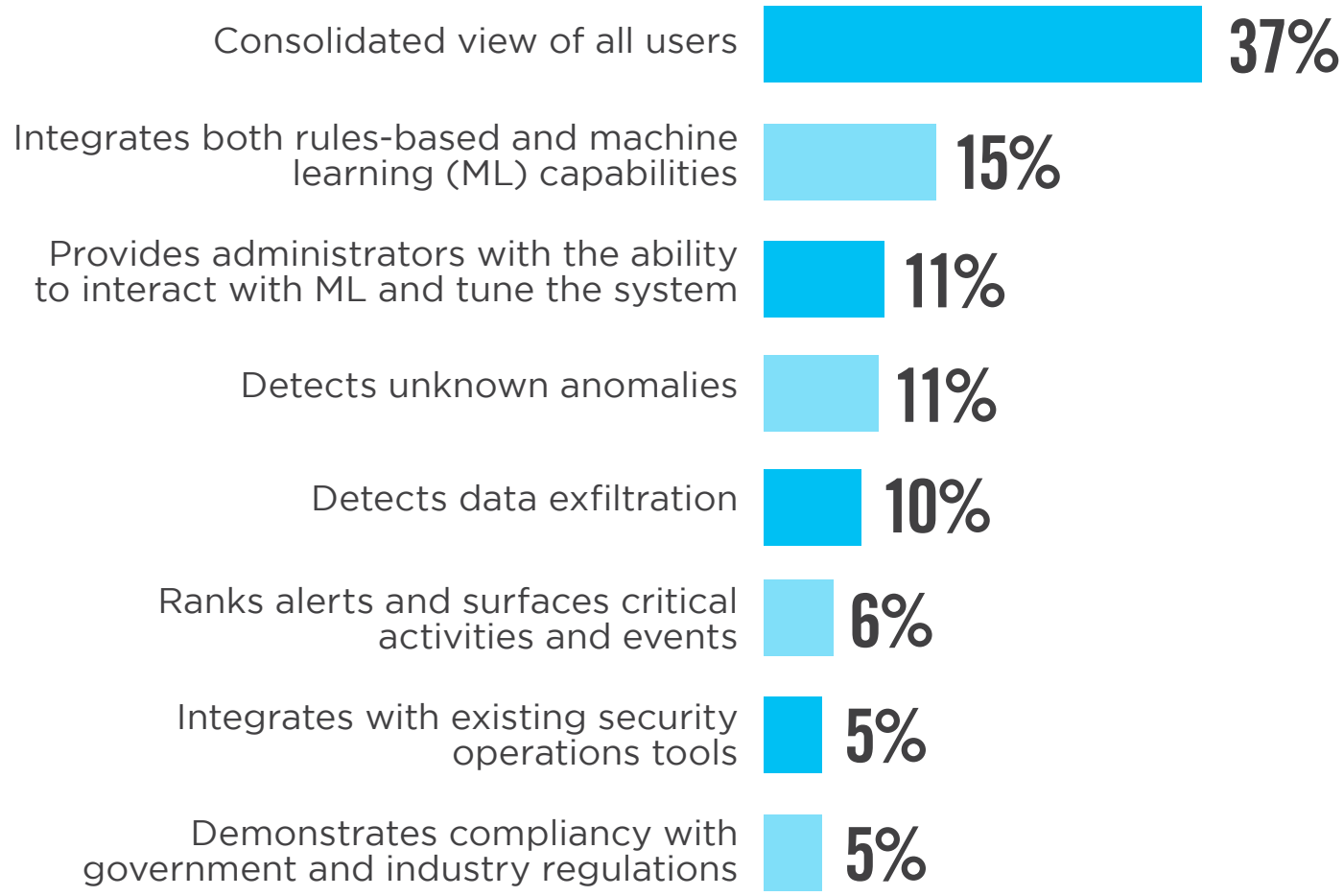
Have deployed keylogging

Not sure/other 14%

IMPORTANT CAPABILITIES

When asked to rank insider threat capabilities in terms of importance, organizations selected a consolidated view of all users as the single highest priority capability. They are aware of security blind spots and want to eliminate them.

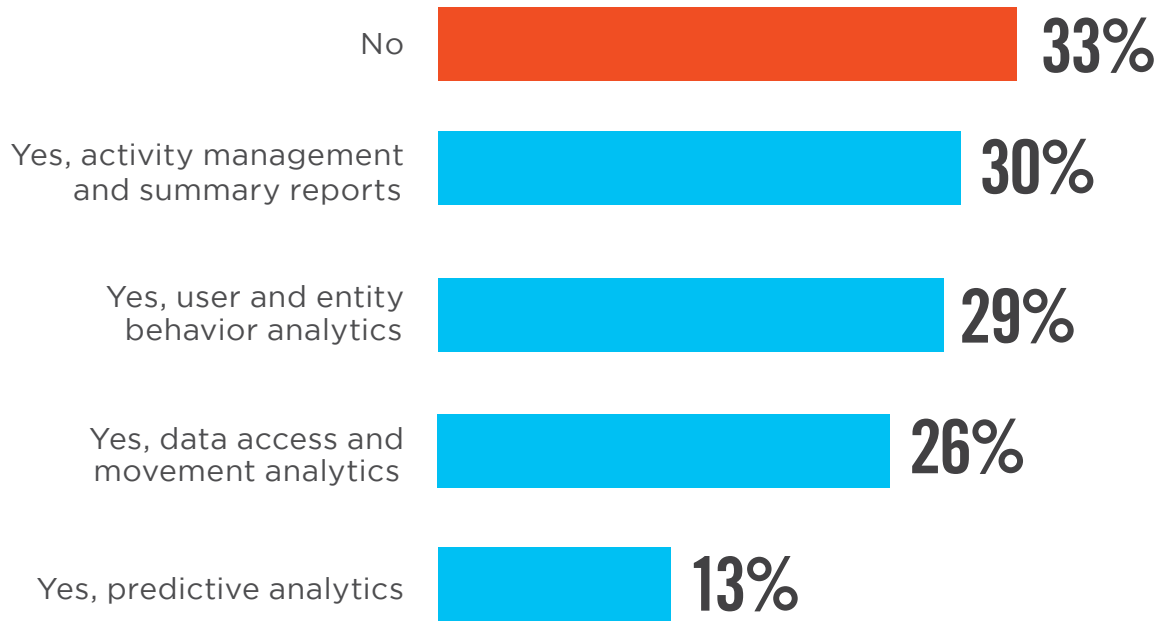
Rank the following insider threat capabilities in terms of importance



INSIDER THREAT ANALYTICS

A majority of organizations utilize some form of analytics to determine insider threats, including activity management and summary reports (30%), user and entity behavior analytics (UEBA) (29%), and data access and movement analytics (26%). One-third still don't leverage analytics to determine insider threats.

Does your organization leverage analytics to determine insider threats?

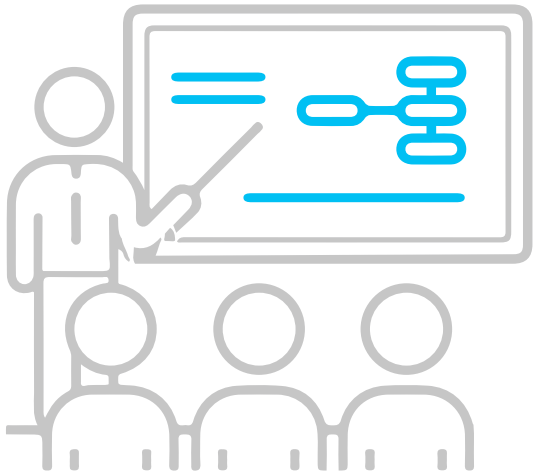


Not sure 11%

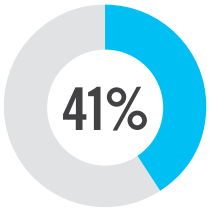
COMBATING INSIDER THREATS

The most utilized tactic in combating insider threats is user training (50%) because it addresses both inadvertent insider threats and the human factor of recognizing insider attacks by the unusual and suspicious behavior often exhibited by malicious insiders. This is followed by dedicated information security governance programs to systematically address insider threats (41%) and user activity monitoring (37%).

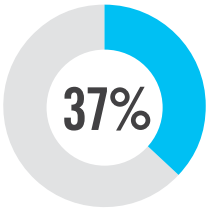
How does your organization combat insider threats today?



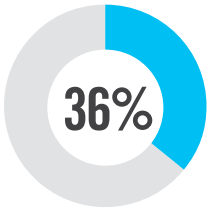
50%
User training



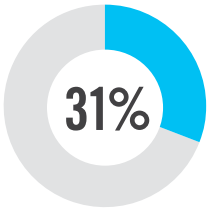
Information security governance program



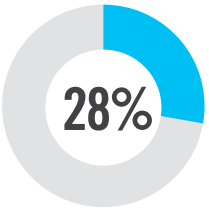
User activity monitoring



Background checks



Database activity monitoring



Secondary authentication

Specialized third-party applications and devices 20% | Native security features of underlying OS 19% | Managed security service provider 15% | Custom tools and applications developed in-house 13% | We do not use anything 4% Not sure/other 10%

MOST EFFECTIVE TOOLS AND TACTICS

The three most effective security tools and tactics deployed by organizations to protect against insider threats are data loss prevention (DLP) (54%), identity and access management (IAM) (52%), and policies and training (49%). Nearly half (46%) of organizations utilize user and entity behavior analytics (UEBA) and security information and event management (SIEM) to strengthen their insider threat programs.

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

54%

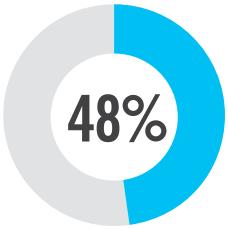
Data loss prevention (DLP)

52%

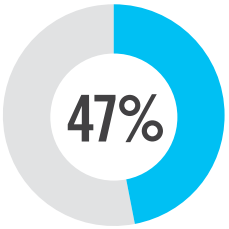
Identity and access management (IAM)

49%

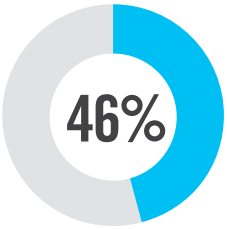
Policies and training



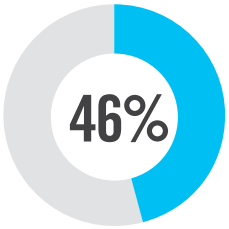
Encryption of data (at rest, in motion, in use)



Multi-factor authentication



user and entity behavior analytics (UEBA)



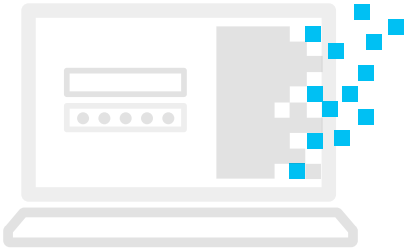
Security information and event management (SIEM)

Data access monitoring 40% | File activity monitoring 40% | Endpoint and mobile security 39% | Security analytics and intelligence 39% | Intrusion detection and prevention (IDS/IPS) 37% | Sensitive and private data identification/classification 36% | Network defenses (firewalls) 35% | User monitoring 33% | Database activity monitoring 33% | Password vault/privileged account vault 23% | Enterprise digital rights management solutions (E-DRM) 20% | Cloud access security broker (CASB) 18% | Tokenization 17% | Cloud security as a service 16% | Internal audits 9% | Network monitoring 8% | Whistleblowers 6% | Not sure/other 9%

FOCUS ON DETERRENCE

While all methods of countering insider threats are important, organizations are shifting their focus towards deterrence and detection of internal threats. These two are at the top of the list (61%), followed by analysis and post-breach forensics (46%) and deception (11%).

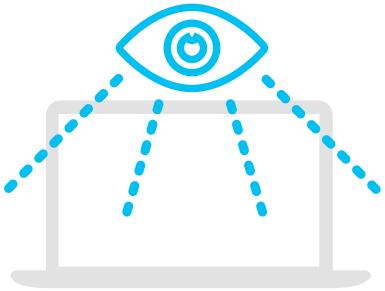
What aspect(s) of insider threat management does your organization mostly focus on?



61%

Deterrence

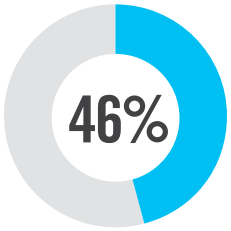
(e.g., access controls, encryption, policies, etc.)



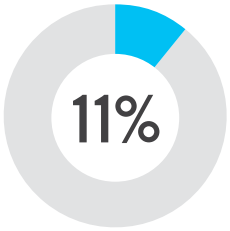
61%

Detection

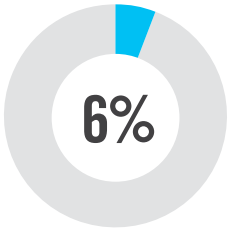
(e.g., user monitoring, IDS, etc.)



Analysis and post-breach forensics (e.g., SIEM, log analysis, etc.)



Deception (e.g., honeypots, decoys, etc.)



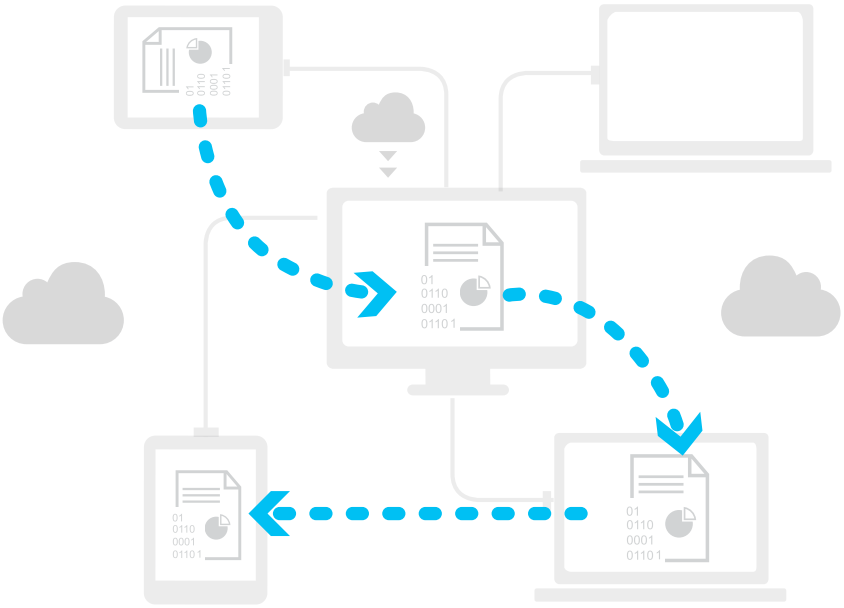
None

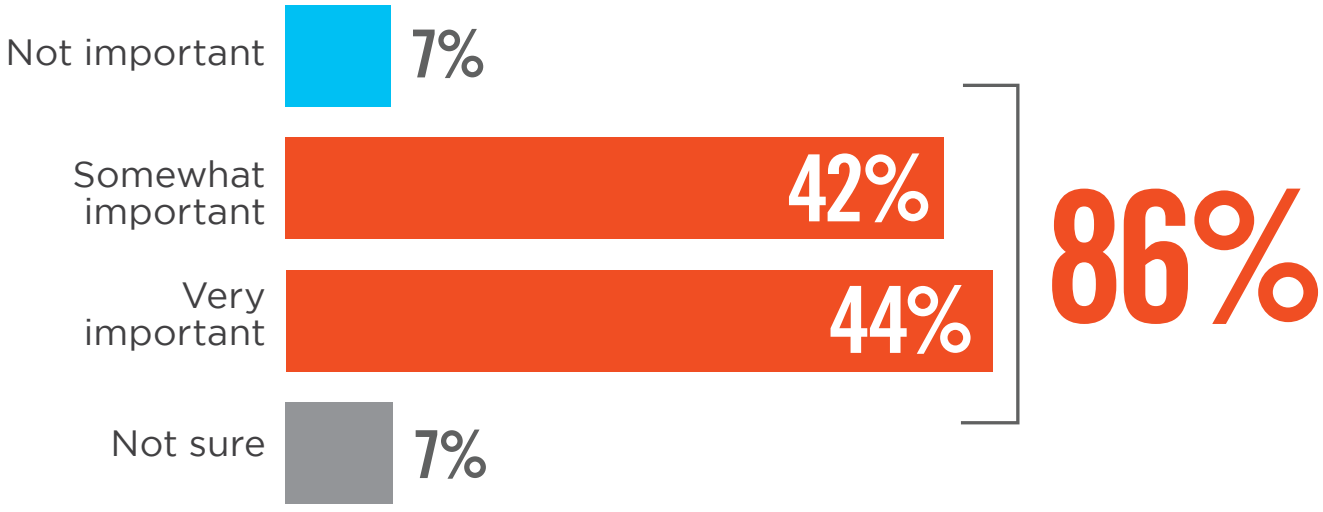
Other 2%

FILE TRACKING

Tracking the movement of sensitive files across the network is somewhat important to very important to 86% of organizations.

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

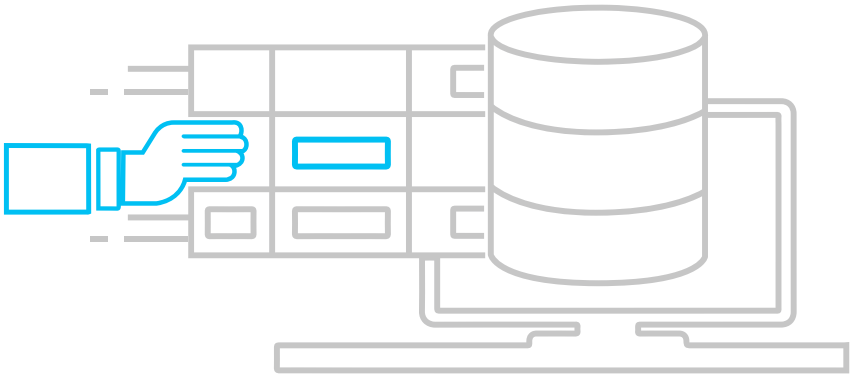


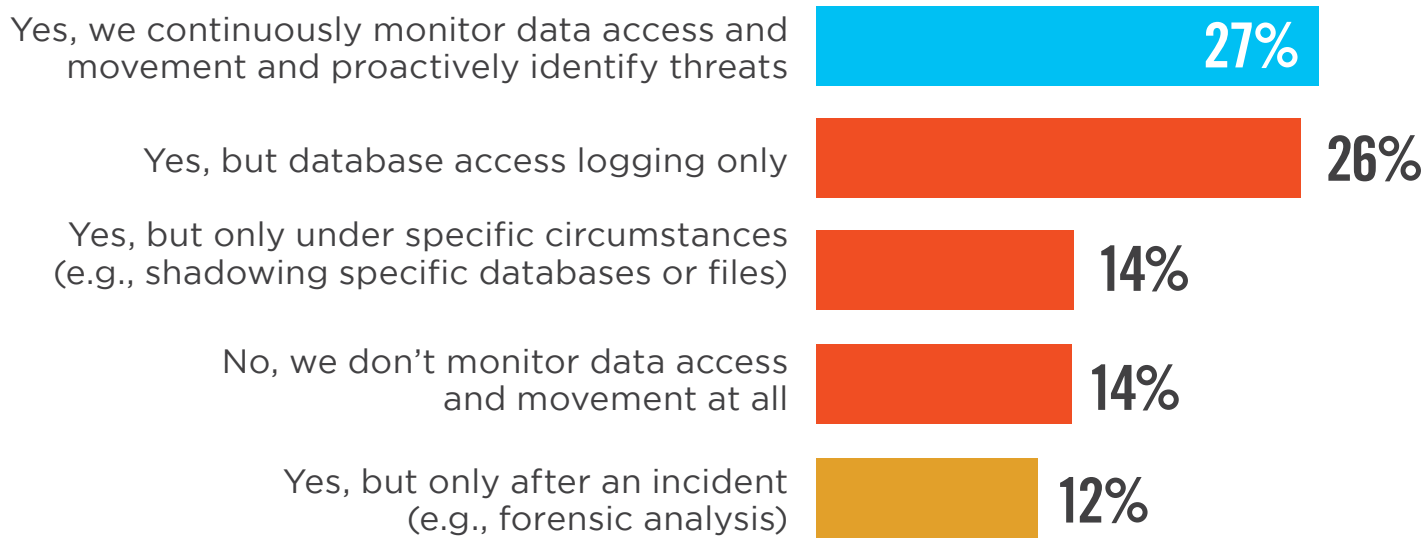


DATA ACCESS MONITORING

More than 7 in 10 of organizations do not conduct end-to-end monitoring of data access and movement. Failing to do so creates risk and exposure to insider threats.

Do you monitor data access and movement?



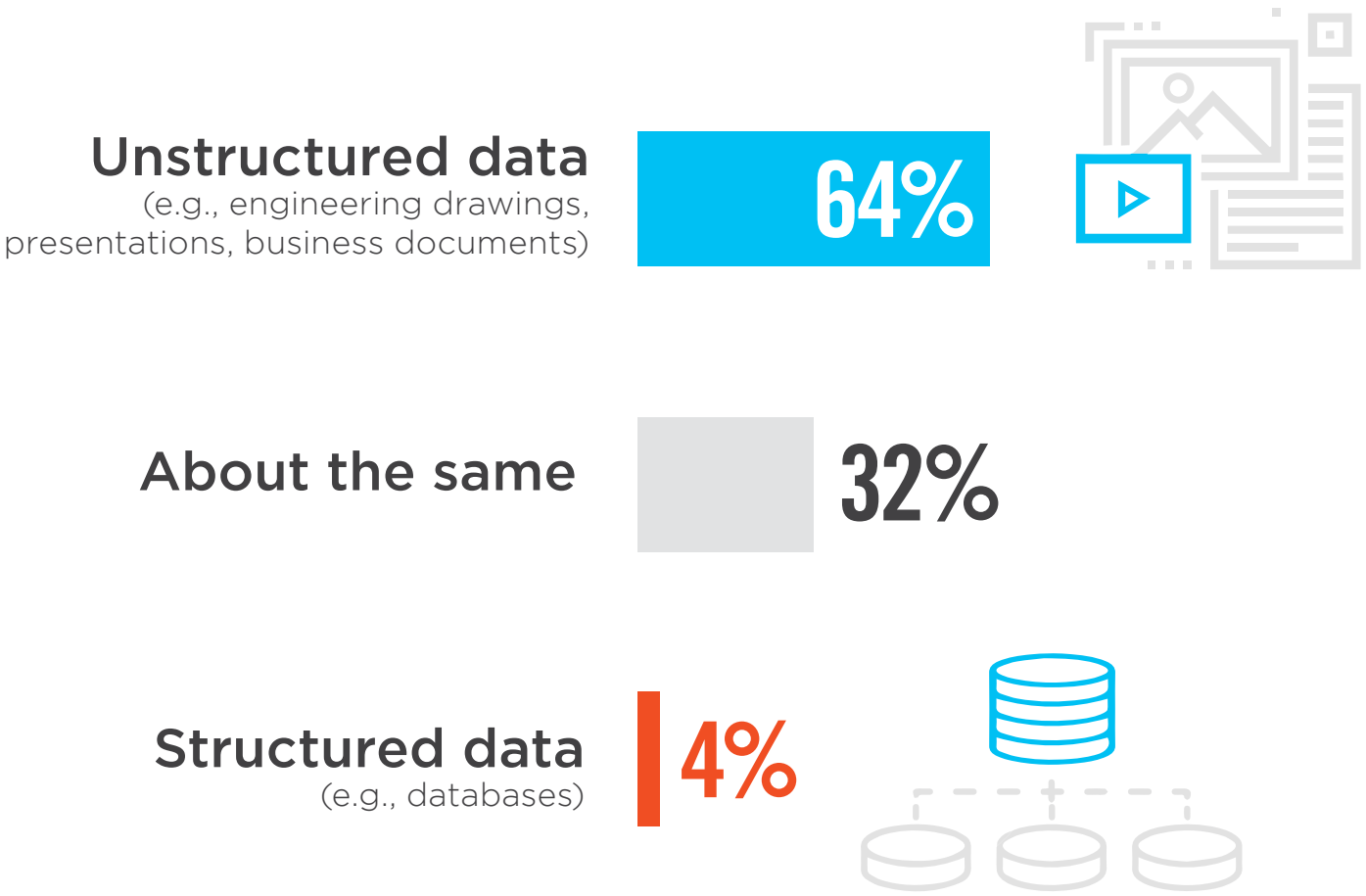


Not sure 7%

PROTECTING INFORMATION

Between the different types of data, organizations find it significantly more difficult to protect unstructured data such as documents, spreadsheets, presentation files, and engineering drawings (64%) than protecting structured data (4%) such as database records.

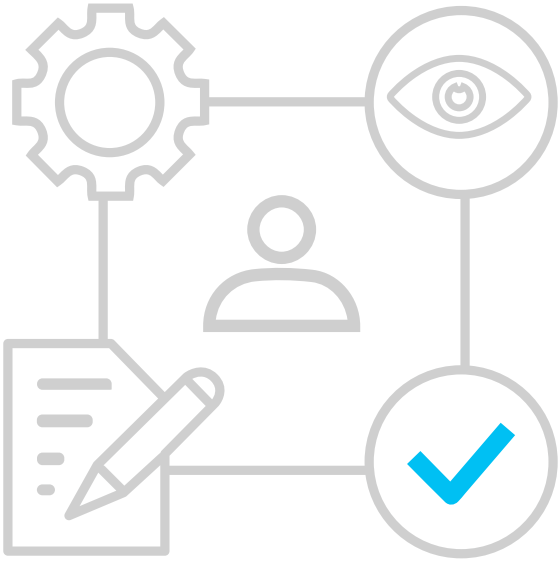
What information type is more difficult to protect against insider threat activities?



SECURITY MONITORING

When asked whether organizations have a formal process in place to monitor and ensure that employees and contractors adhere to security controls and policies, a majority either have already implemented technologies and processes (45%) or are in the process of implementing them (32%).

Do you have a formal process in place to monitor and ensure that employees and contractors adhere to security controls and policies?

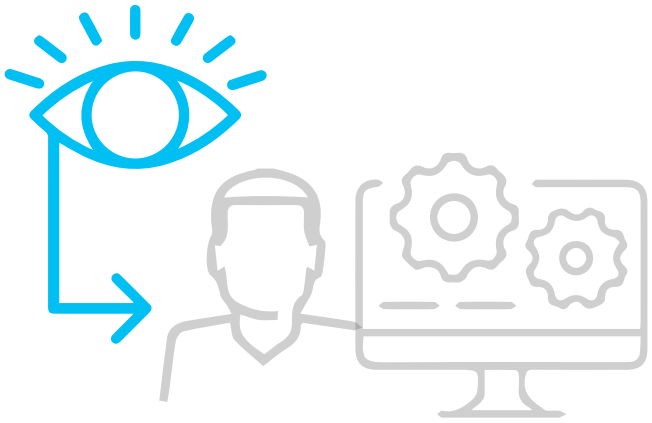


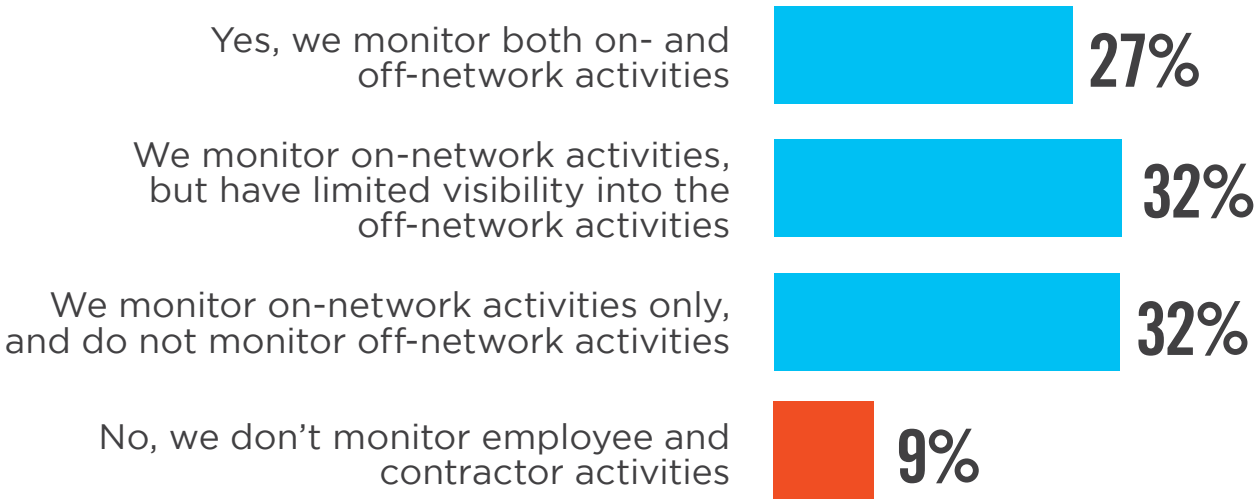
45%	We have implemented technologies and processes that are used to monitor employee and contractor activities to ensure policy adherence.
32%	We are in the process of implementing technologies and processes for monitoring the activities of employees and contractors to ensure policy adherence.
23%	We currently do not have technologies and processes for monitoring employee and contractor activities.

MONITORING EMPLOYEES AND CONTRACTORS

Only 27% of respondents have a comprehensive monitoring of activities—both on- and off-network.

Do you monitor employees' and contractors' on- and off-network activities?

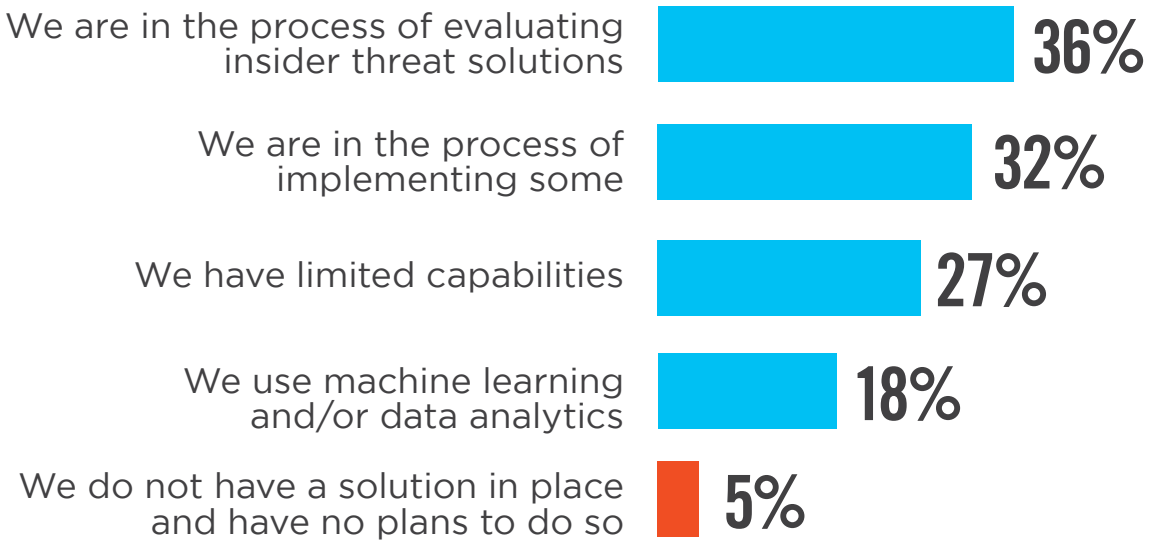




INSIDER THREAT SOLUTIONS

When asked about insider threat solutions, a majority of organizations are still evaluating solutions (36%) or actively implementing them (32%). Only a small fraction (5%) say they have no solutions in place and no plans to implement them.

In what ways are you currently using insider threat capabilities?



USER PRIVACY CONCERNS

Seven out of 10 organizations are concerned about user privacy when monitoring for insider threats. At the same time, more than 4 in 10 indicate they do not have the insider threat tools to ensure compliance with the EU's General Data Protection Regulation (GDPR) and other regulations.

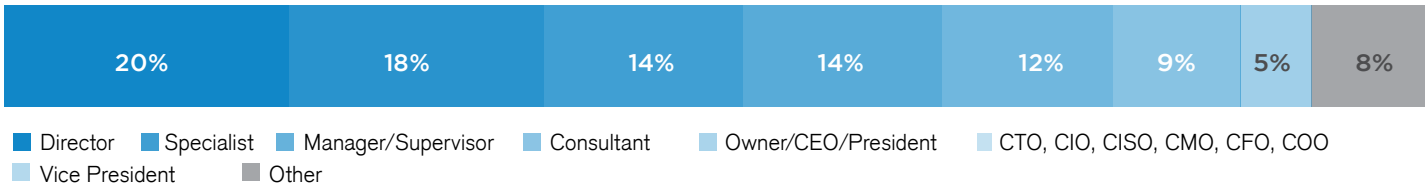
Is user privacy a concern when monitoring insider threats?

Do you believe your tools have the privacy capabilities to ensure compliance to GDPR and other regulations when monitoring insider threats?

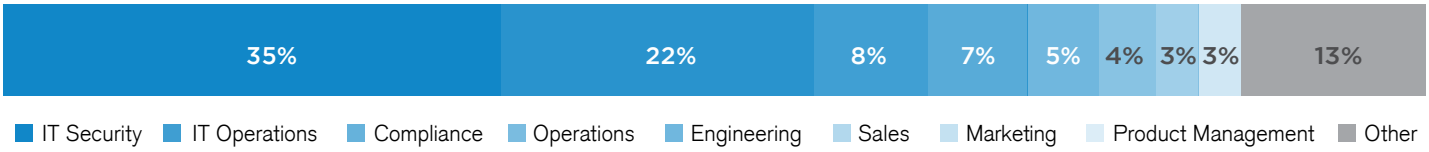
METHODOLOGY AND DEMOGRAPHICS

This Insider Threat Report is based on the results of a comprehensive online survey of cybersecurity professionals, conducted in September of 2019 to gain deep insight into the latest trends, key challenges, and solutions for insider threat management. 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.

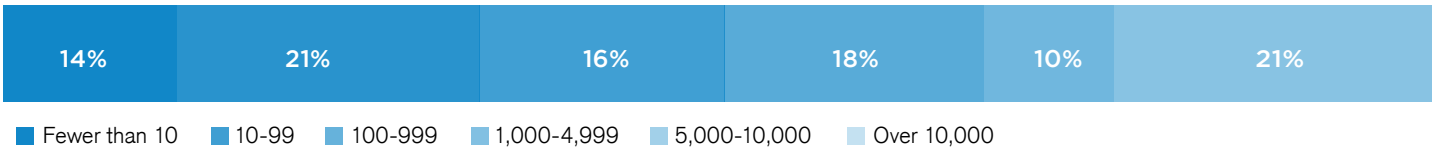
CAREER LEVEL



DEPARTMENT



COMPANY SIZE



IT SECURITY TEAM SIZE

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security features without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide, and more than 415,000 customers trust Fortinet to protect their businesses.

Learn more at **www.fortinet.com**,
the Fortinet Blog, or FortiGuard Labs.