2021

Cybersecurity
INSIDERS

INSIDER THREAT REPORT

GURUCUL

INTRODUCTION

Insider threats continue to rise in the new normal of widespread work-from-home and economic uncertainty.

As organizations adapt to the new normal, it is important to reflect on what drives the increasing risk of insider threats and how the situation is worsened with more employees working from home than ever before, using new applications and tools, and relying on cloud apps.

The 2021 Insider Threat Report reveals the latest trends and challenges facing organizations in this new environment. The report explores how IT and cybersecurity professionals deal with risky insiders and how organizations are preparing to protect their critical data and IT infrastructure better.

Key findings include:

- Virtually all organizations feel vulnerable to insider attacks (98%)
- A majority of organizations (85%) consider unified visibility and control across all apps, devices, web destinations, on-premises resources, and infrastructure extremely to moderately important
- 82% of organizations find it difficult to determine the actual damage of an insider attack
- 49% of organizations can't detect insider threats or can only detect them after the data has left the organization
- Only 11% of organizations consider their monitoring, detecting, and response to insider threats extremely effective

This 2021 Insider Threat Report has been produced by Cybersecurity Insiders, the 500,000-member community for information security professionals to explore how organizations respond to the evolving security threats in the cloud. We would like to thank Gurucul for supporting this unique research.

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

Thank you,

Holger Schulze

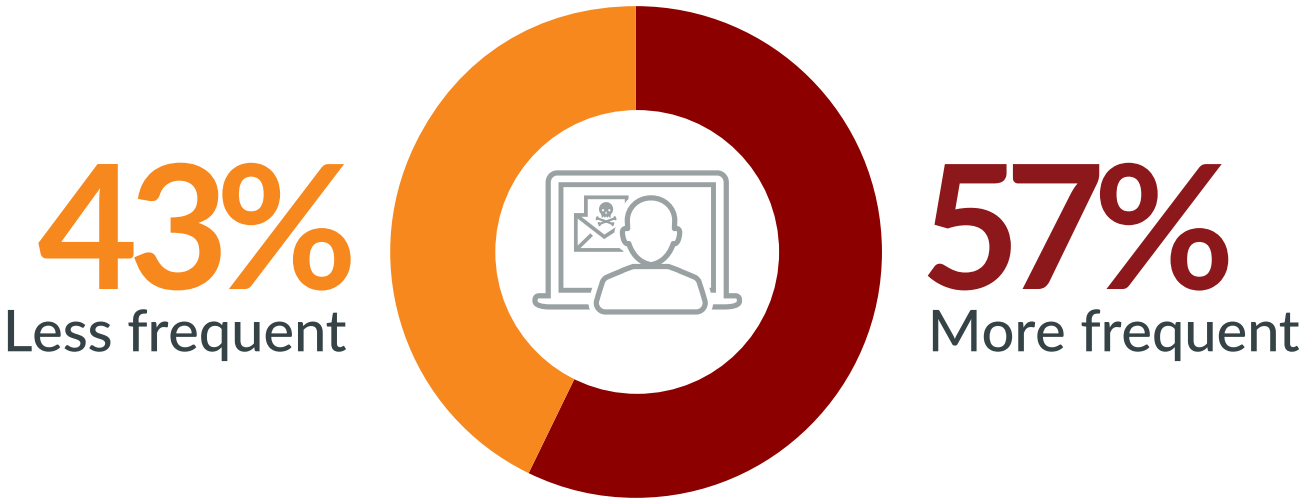
Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

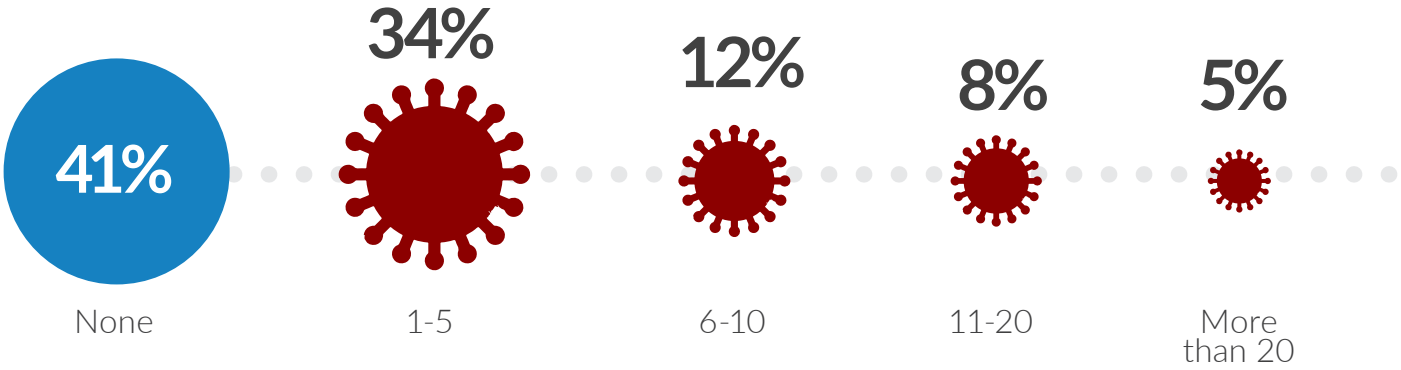
RISE OF INSIDER ATTACKS

Compared to last year, 68% of organizations observed that insider attacks had become more frequent over the last 12 months. This year, 57% indicated an increase in attack frequency indicating that organizations are getting better at predicting a breach. In fact, 59% 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?



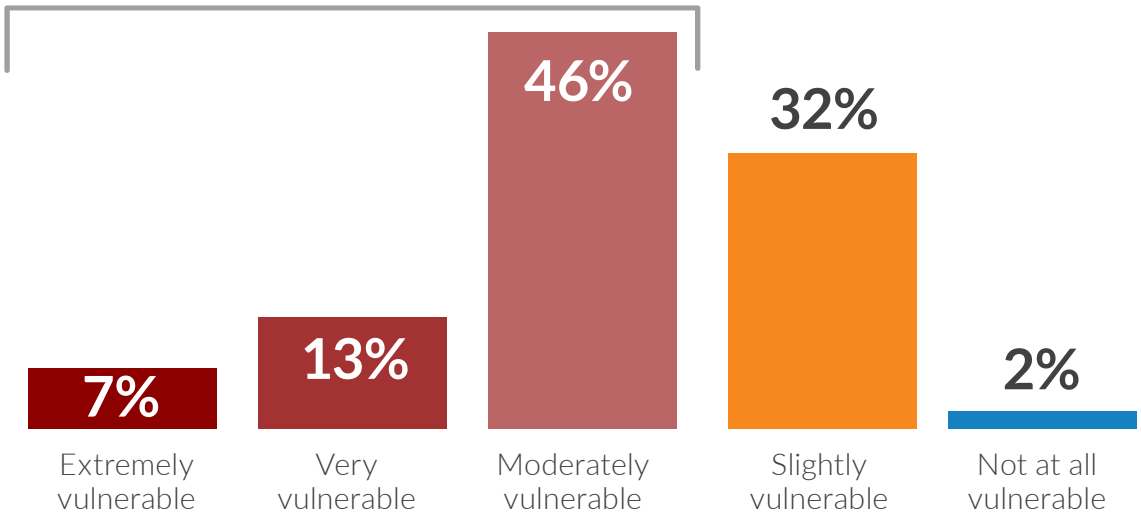
INSIDER VULNERABILITY

We asked cybersecurity professionals to assess their organization's vulnerability to insider threats. An overwhelming 66% of organizations feel moderately to extremely vulnerable. Only 2% say they are not at all vulnerable to an insider attack.

How vulnerable is your organization to insider threats?

66%

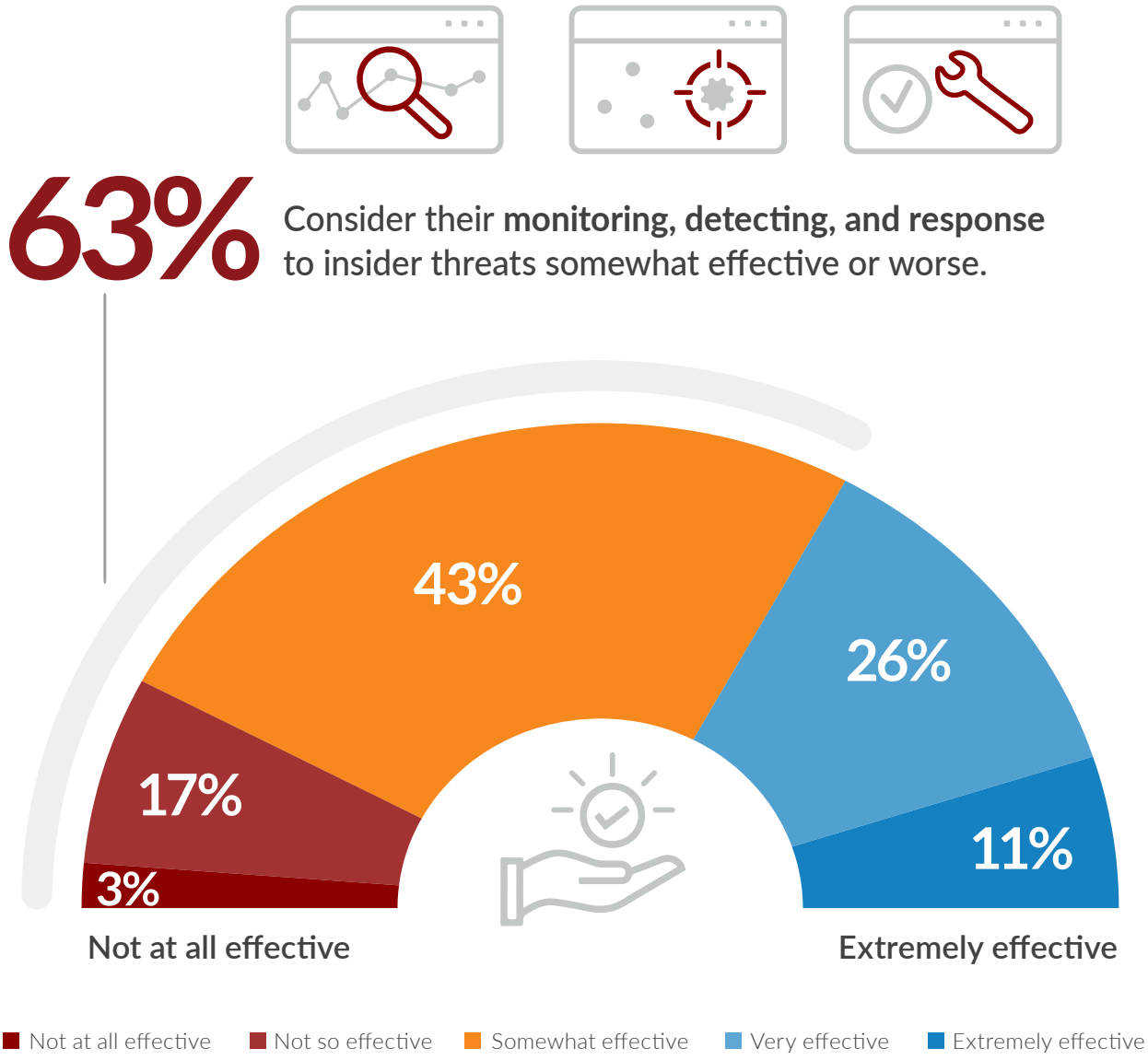
Feel extremely to moderately vulnerable to insider attacks.



INSIDER THREAT DISCOVERY AND RESPONSE

A majority of organizations consider themselves only somewhat effective or worse (63%) when it comes to monitoring, detecting, and responding to insider threats. Only 37% of organizations consider themselves very to extremely effective when it comes to monitoring, detecting, and responding to insider threats.

How would you characterize the effectiveness of your organization to monitor, detect, and respond to insider threats?



INTERNAL VS. EXTERNAL ATTACKS

When comparing internal attacks to external cybersecurity attacks, 50% of respondents confirm that internal attacks are more difficult to detect and prevent than external cyber attacks. Since insiders have approved access privileges, it can be challenging to distinguish legitimate use cases from malicious attacks.

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

50%

More difficult than detecting and preventing external cyber attacks

40%

About as difficult as detecting and preventing external cyber attacks

10%

Less difficult than detecting and preventing external cyber attacks

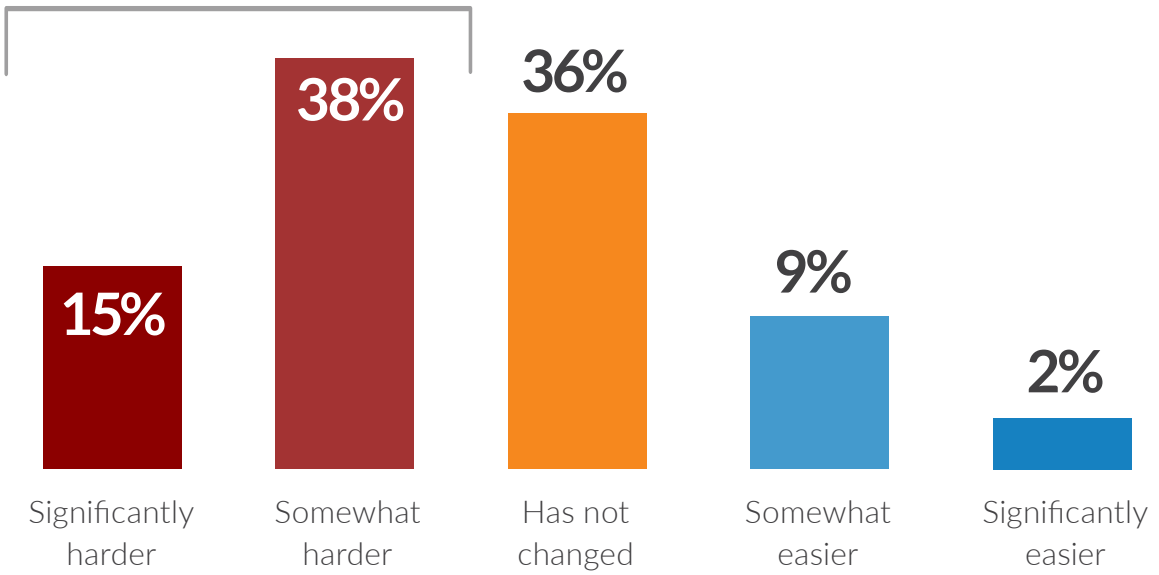
INSIDER ATTACKS IN THE CLOUD

Another factor that is making detection of insider attacks more difficult is the shift toward cloud computing, as confirmed by 53% of cybersecurity professionals.

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

53%

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

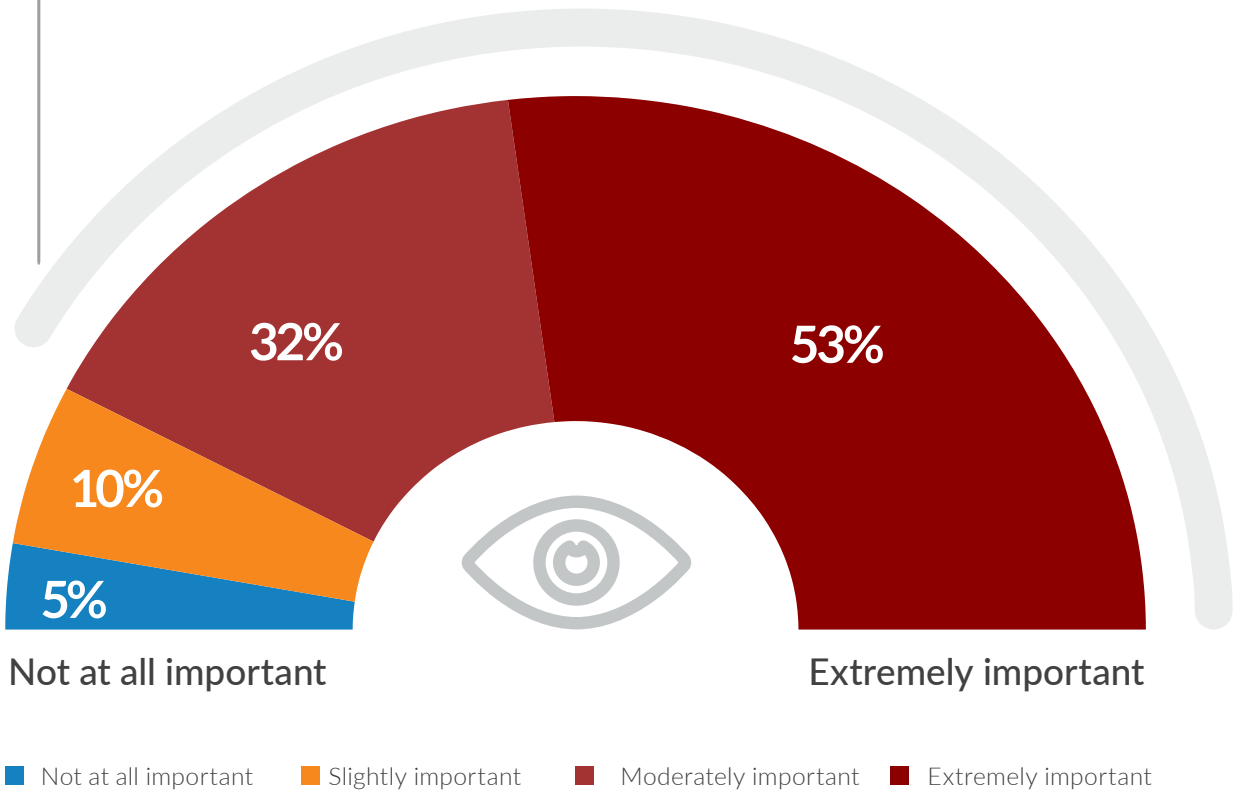


IMPORTANCE OF UNIFIED VISIBILITY

Visibility and control are paramount in preventing an insider threat. Almost all organizations (85%) consider unified visibility and control across all apps, devices, web destinations, on-premises resources, and infrastructure moderately to extremely important.

How important is unified visibility and control across all apps, devices, web destinations, on-premises resources, and infrastructure when it comes to insider threats?

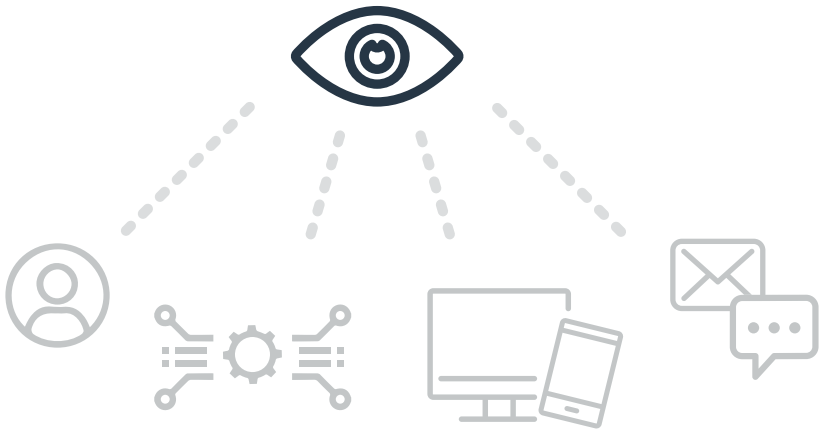
85% Consider unified visibility and control across all apps, devices, web destinations, on-premises resources, and infrastructure moderately to extremely important.

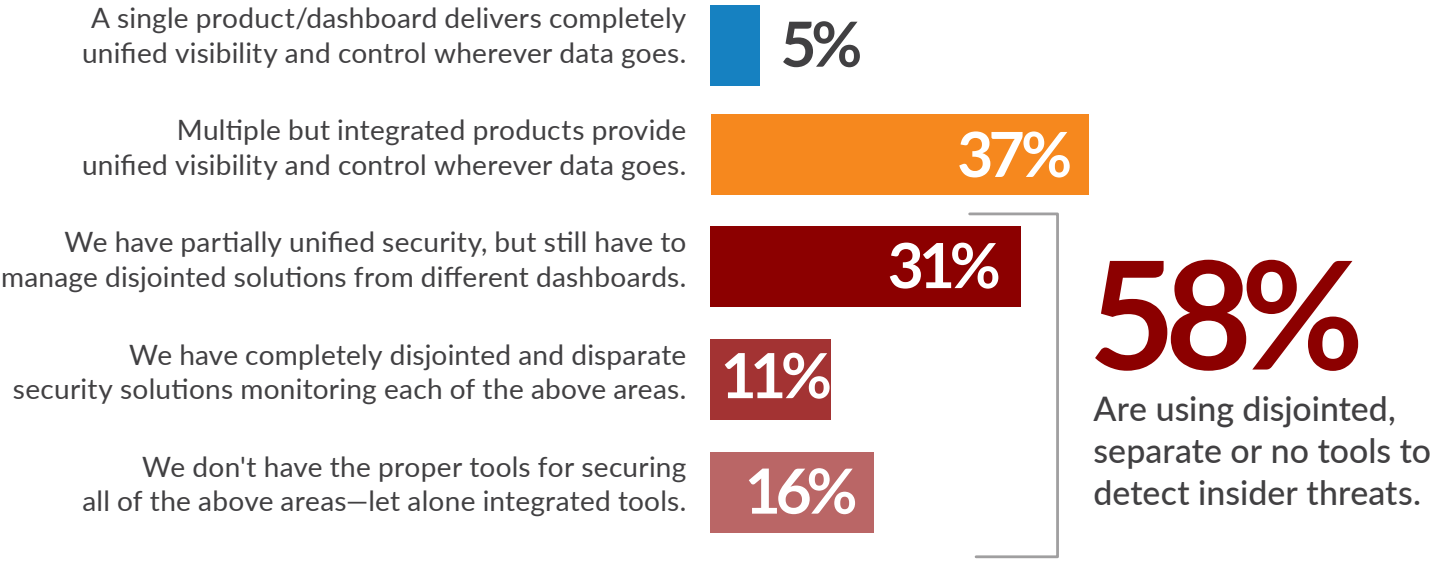


STATE OF UNIFIED VISIBILITY

Thirty-seven percent of organizations deploy multiple but integrated products to provide unified visibility and control. However, most organizations (58%) are using disjointed, separate, or no tools and struggling to detect insider threats.

What level of unified visibility and control do you currently have across all apps, devices, web destinations, on-premises resources, and infrastructure to detect insider threats?

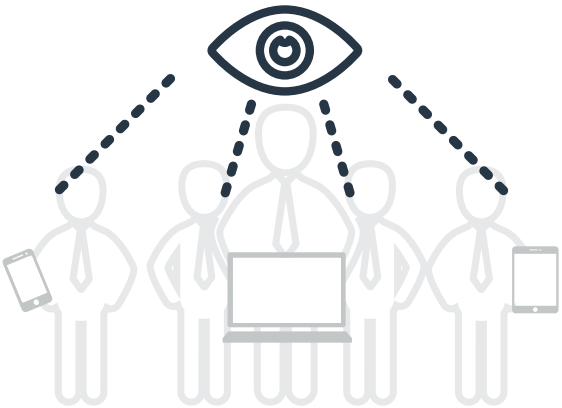


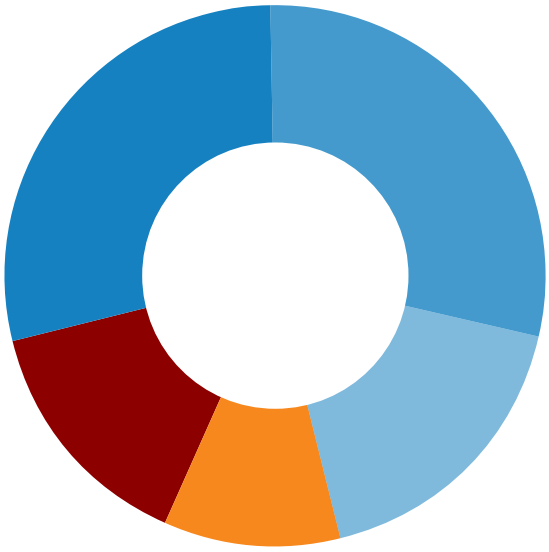


USER BEHAVIOR MONITORING

The continued threat of insider threats have caused cybersecurity professionals to take more action and deploy User Behavior Analytics (UBA) tools to help detect, classify, and alert anomalous behavior. More than 80% of organizations monitor user behavior in one way or another. The most common appoach to monitoring user behavior is access logging only (28%) and automated tools to monitor user behavior (28%).

Do you monitor user behavior?





28%
YES, but access logging only

28%
YES, we use automated tools to monitor user behavior 24x7

17%
YES, but only under specific circumstances
(e.g., shadowing specific users)

14%
NO, we don't monitor user behavior at all

10%
YES, but only after an incident
(e.g., forensic analysis)

Other 3%

VISIBILITY INTO USER BEHAVIOR

When asked about visibility into user activity, organizations continue to rely on server logs to track user behavior (40%), followed by User and Entity Behavior Analytics (UEBA) (30%), and in-app audit features (28%).

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

40%

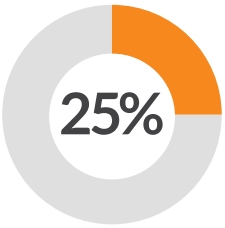
Rely on server logs

30%

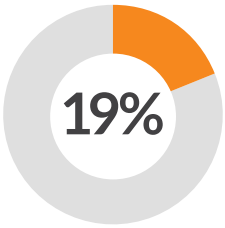
Have deployed User & Entity Behavior Analytics (UEBA)

28%

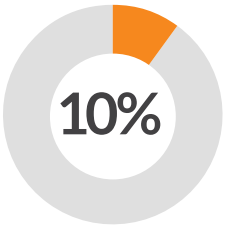
In-app audit system/feature



Visibility into files and data accessed



Actions taken on files



Have deployed keylogging

Not sure/other 19%

ANOMALOUS BEHAVIOR DETECTION

The level of visibility that organizations have to detect anomalous behavior on privileged accounts is high (61%), followed by service accounts (41%) and document repositories (40%). In contrast, visibility into cloud applications is low (28%), and even lower visibility into IoT and SCADA devices (7%).

Are you able to detect anomalous behavior of any of the following?

61%

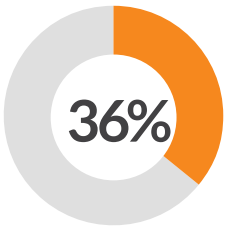
Privileged accounts

41%

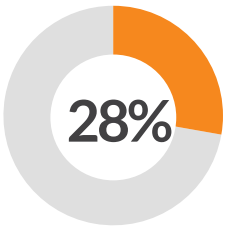
Service accounts

40%

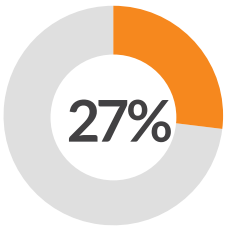
Documents/ document repositories



Systems and devices



Cloud applications and infrastructure



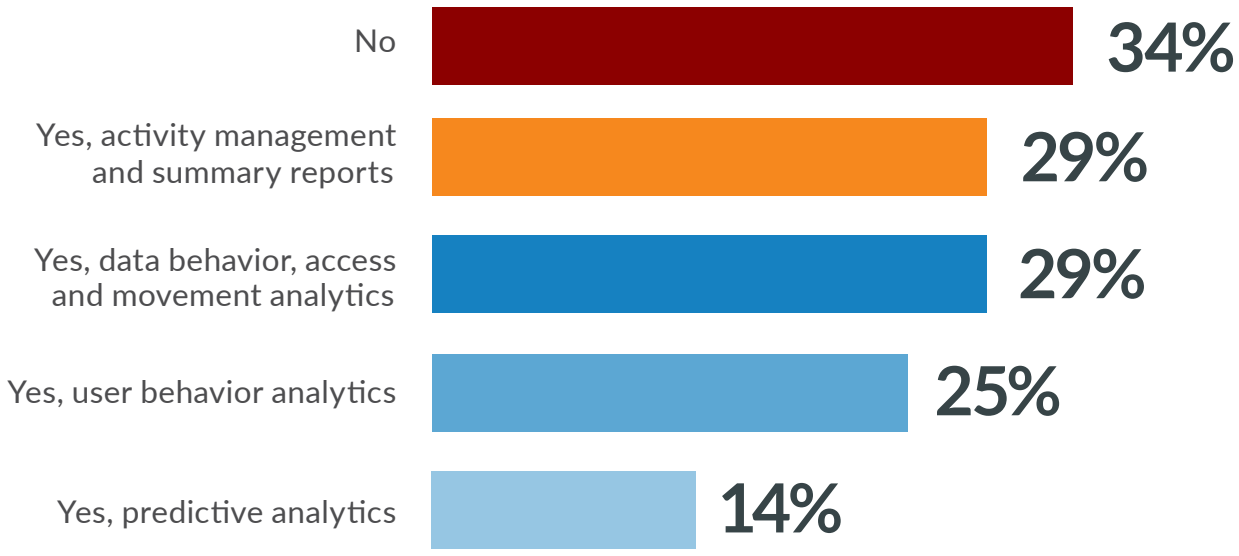
NetFlow/ packet data

Web/shadow IT 22% | IoT and SCADA devices 7% | Other 7%

INSIDER THREAT ANALYTICS

Of the organizations utilizing analytics to determine insider threats, the top two spots are tied at 29%: activity management and summary reports, and data behavior, access and movement analytics. Running a close third is user behavior analytics at 25%.

Does your organization leverage analytics to determine insider threats?

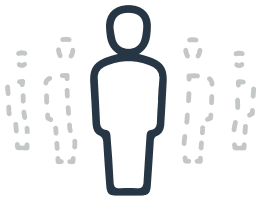


Not sure 16%

SIEM HURDLES

In this year's survey, there hasn't been a significant change regarding the hurdles preventing organizations from maximizing SIEM. Not enough resources is still the biggest challenge (33%), followed by false positives (29%), and problems to detect unknown threats (17%).

What is your biggest hurdle in maximizing the value of your SIEM?



33%

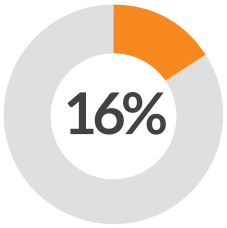
Not enough resources

29%

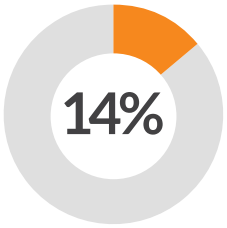
Too many false positives

17%

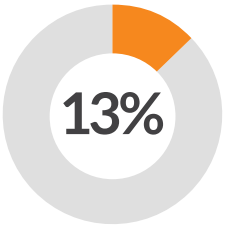
Can't detect unknown threats



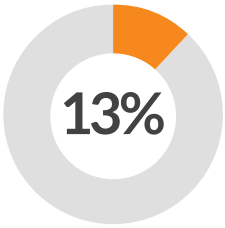
Not using SIEM



Challenges integrating it with cloud security tools



Not logging the right data



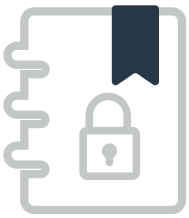
Can't import all the data needed

Inability to prioritize risk 12% | Not sure 5%

DLP CHALLENGES

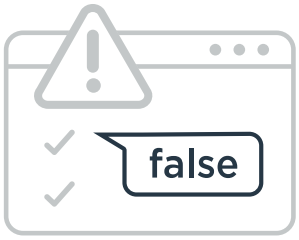
When it comes to utilizing Data Leakage Protection (DLP), organizations continue to face a variety of challenges, most prominently the difficulty to keep policies up to date at the rate of business needs (30%). For this year's report, too many false positives (28% versus 23%) and limited data/file visibility (22% versus 23%) are swapping places as the next two biggest hurdles, compared to last year.

What challenges do you face with DLP?



30%

Difficult to keep policies up to date at the rate of business needs

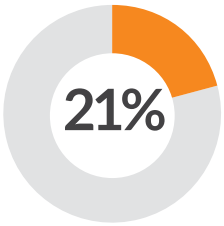


28%

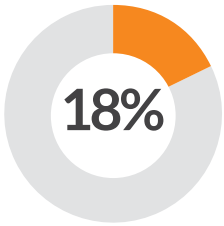
Too many false positives

22%

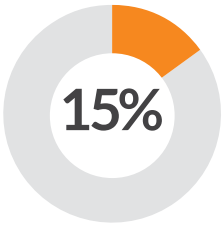
We have limited data/file visibility



Policies impede on employee productivity and collaboration



Policy creation is manual and complex



Solutions fail to detect relevant data and files

Not enough pre-built data patterns in solutions 6% | Not sure 5%

FOCUS ON DETERRENCE

Organizations are focused on deterrence (63%) and detection of internal threats (48%) as their primary focus for mitigating insider threats; analysis and post breach forensics (37%) follow.

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

63%

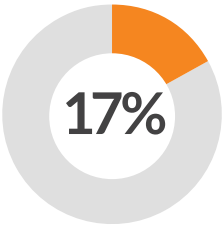
Deterrence
(e.g., access controls, encryption, policies, etc.)

48%

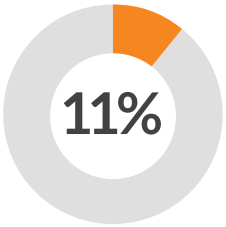
Detection
(e.g., user monitoring, IDS, etc.)

37%

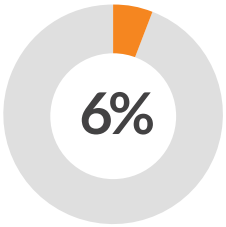
Analysis & post breach forensics
(e.g., SIEM, log analysis, etc.)



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



Prediction
(e.g., User and Entity Behavior Analytics)



None

Other 3%

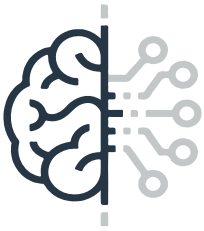
INSIDER THREAT SOLUTIONS

Forty-two percent of organizations have limited capabilities to defend against insider threats. Of the organizations that are defending against insider threats, 26% are using artificial intelligence and machine learning, followed by big data analytics (24%).

In what ways are you currently using insider threat capabilities?

42%

We have limited capabilities

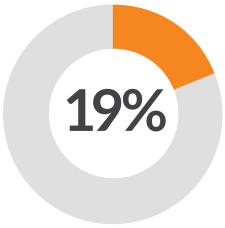


26%

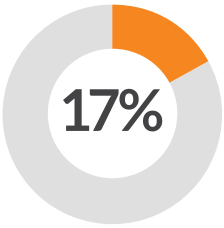
We use artificial intelligence and machine learning

24%

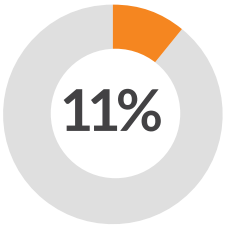
We use big data security analytics



We are currently implementing solutions we have evaluated



We are in the process of evaluating insider threat solutions



We do not have a solution in place but plan to implement one

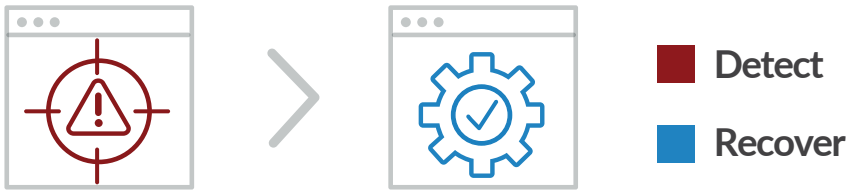
The SecOps team identifies threats with a manual process 5% | We do not have a solution in place and have no plans to do so 4%

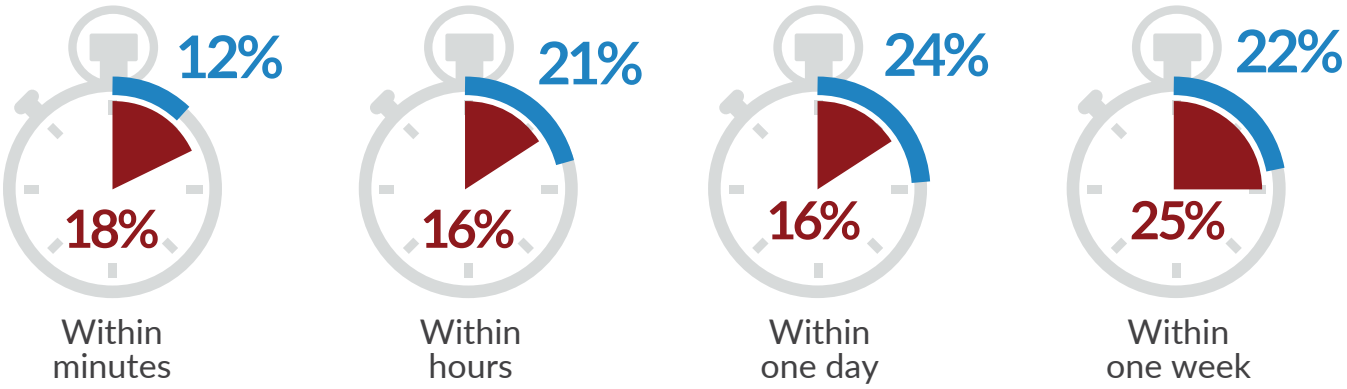
DETECTION AND RECOVERY

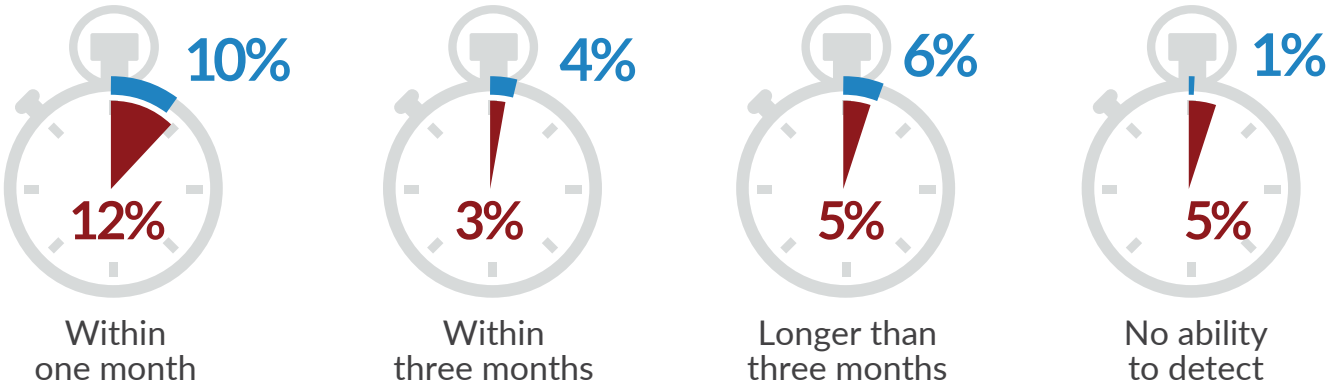
Half the respondents claim they can detect insider threats within the same day (50%), 18% even within minutes of an attack. Twenty-five percent can detect an insider attack within a week and 12% within a month. Only 5% report they have no ability to detect an insider attack.

Most organizations say they could recover from an attack within a day (57%). Extend that to a week and the percentage of organizations that can recover jumps to 79%. Only one percent of companies believe they would never fully recover from a successful insider attack.

How long would it typically take your organization to detect and recover from an insider attack?



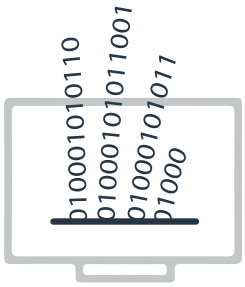




SPEED OF REMEDIATION

Given the impact that insider threats have on an organization, it is surprising that nearly a fifth (18%) still cannot detect insider threats. Thirty-one percent can only remediate after data loss occurred – when the business impact is much larger.

How quickly can you remediate Insider Threats?



31%

After the data has left my organization

27%

In real-time

24%

Before data exfiltration

18%

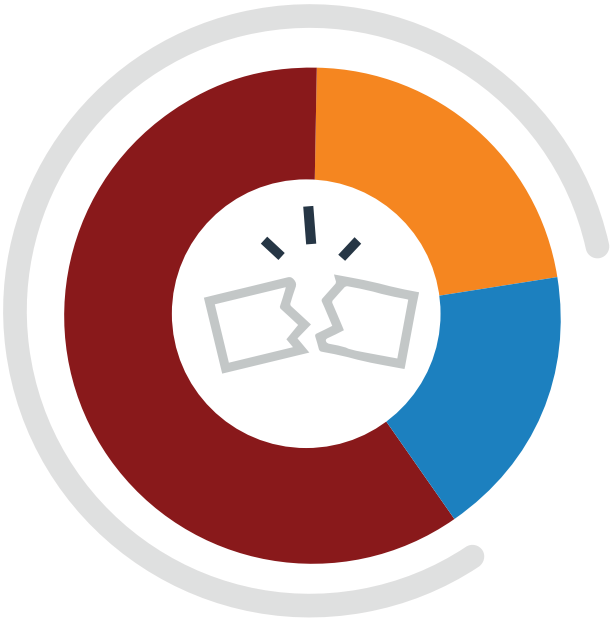
Can't detect insider threats

DAMAGES FROM INSIDER ATTACKS

Eighty-two percent of companies find it moderately to very difficult to determine the damage incurred by insider attacks. Only about one in five companies (18%) have found a way to better understand insider damage.

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

82% Of organizations find it moderately difficult to very difficult to determine the actual damage of an insider attack.



60% Moderately difficult

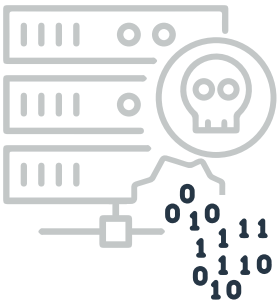
22% Very difficult

18% Not difficult

INSIDER THREAT IMPACT

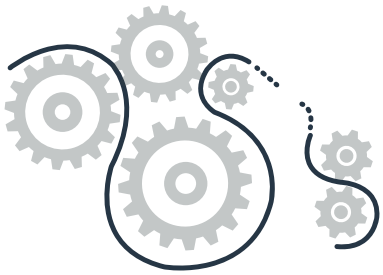
There is a wide variety of ways insider threats impact an organization. This year, loss of critical data tops the list (40%). While operational disruptions continues to be one of the top three challenges, there has been a significant decrease in the share of companies that feel the impact on their ability to operate successfully since last year (54% to 33%).

What impact have insider threats had on your organization?



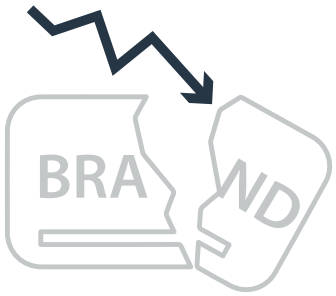
40%

Loss of critical data



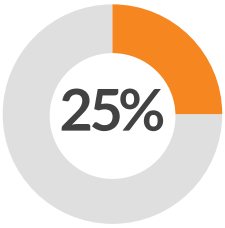
33%

Operational disruption or outage

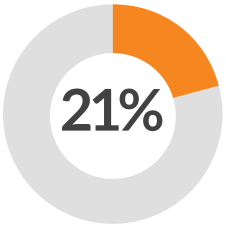


26%

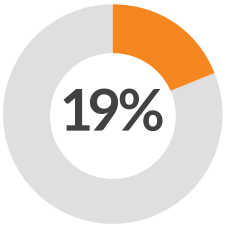
Brand damage



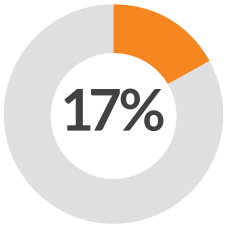
No impact



Legal liabilities



Expenditure remediating successful intrusions



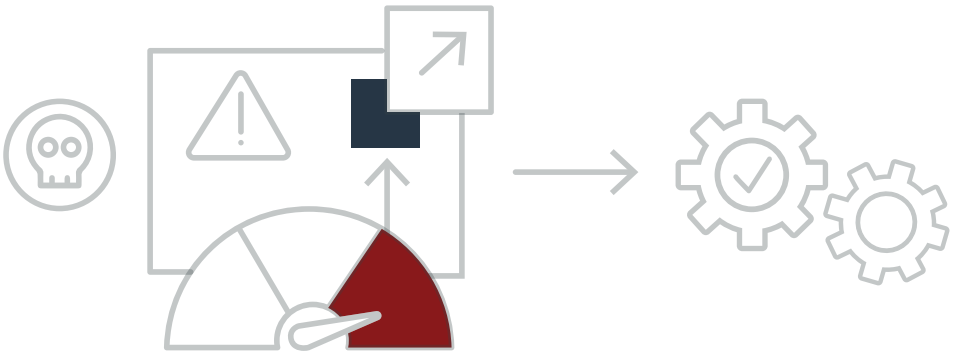
Loss in competitive edge

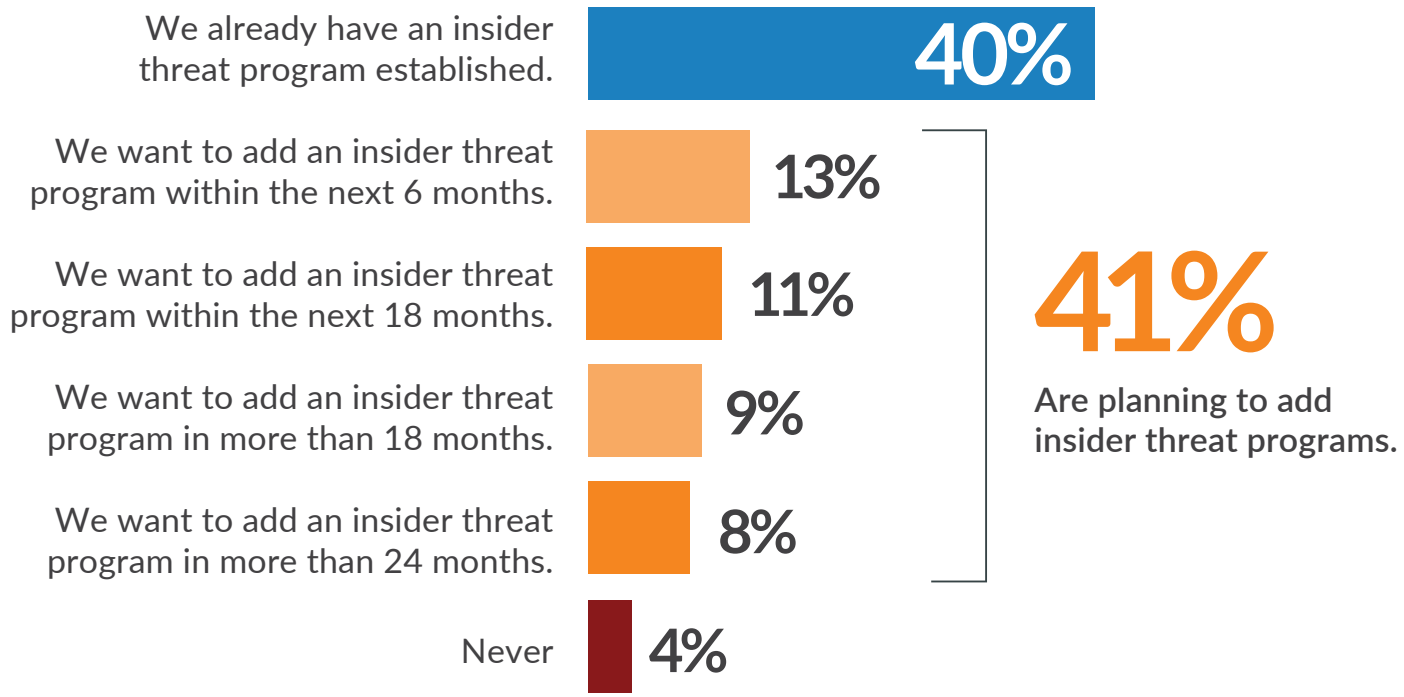
Loss in revenue 15% | Non-compliance with regulations 14% | Loss in market valuation 10%

INSIDER THREAT PROGRAM

Considering the rising risk of insider threats, it is no surprise that 40% of organizations already have an insider threat program in place. Another 41% are planning to add insider threat programs.

Do you have an insider threat program or plan to establish one?





Not sure 15%

METHODOLOGY & DEMOGRAPHICS

This Insider Threat Report is based on the results of a comprehensive online survey of hundreds of cybersecurity professionals, conducted in January 2021, 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

Consultant | Manager/Supervisor | Specialist | Director | Owner/CEO/President | Vice President | CTO, CIO, CISO, CMO, CFO, COO | Other

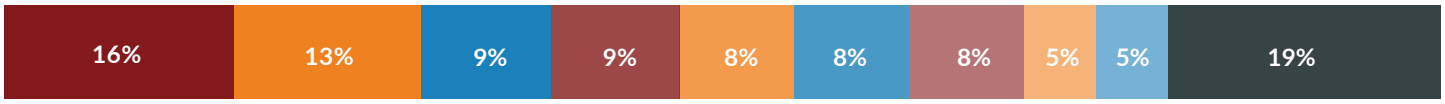
DEPARTMENT

IT Security | IT Operations | Compliance | Engineering | Operations | Sales | Other

COMPANY SIZE

Fewer than 10 | 10-99 | 100-999 | 1,000-4,999 | 5,000-10,000 | Over 10,000

INDUSTRY



Technology, Software & Internet | Education & Research | Financial Services | Healthcare, Pharmaceutical & Biotech | Manufacturing | Professional Services | Information Security | Computers & Electronics | Government | Other

IT SECURITY TEAM SIZE

No dedicated resources | 1 dedicated security resource | 2–5 security resources | More than 5 security resources | Security resources are outsourced | Other

Gurucul is a global cyber security and fraud analytics company that is changing the way organizations protect their most valuable assets, data, and information from insider and external threats both on-premises and in the cloud. Gurucul's real-time Unified Security and Risk Analytics Platform combines machine learning behavior profiling with predictive risk-scoring algorithms to predict, prevent, and detect breaches.

Gurucul technology is used by Global 1000 companies and government agencies to fight cyber fraud, IP theft, insider threat, and account compromise as well as for log aggregation, compliance, and risk based security orchestration and automation for real-time extended detection and response. The company is based in Los Angeles.

To learn more, visit **gurucul.com**

and follow us on LinkedIn and Twitter.