



Rubrik Zero Labs

THE STATE OF DATA SECURITY

A DISTRIBUTED CRISIS

EXECUTIVE SUMMARY:

ESCAPING THE SILENT CRISIS

The transition from exclusively on-premises business IT to hybrid on-premises/cloud environments is among the most important events in the history of business computing.

IT HAS INCREASED SCALABILITY, FLEXIBILITY, AND INNOVATION OPPORTUNITIES.

Often it has become essential for corporate workflows and inter-corporate collaborations.

No wonder

90%

of IT leaders say they are managing distributed hybrid environments.

But as the following data from Rubrik telemetry and Wakefield Research shows, hybrid environments have also created unprecedented hazards:



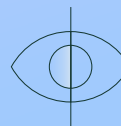
IT leaders report challenges in securing data systemwide, say they lack visibility, and can't establish centralized control.



Ninety percent of survey respondents say they've been attacked. Almost one-fifth say they're getting attacked at a rate that averages to every other week. And those are the ones they know about.



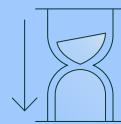
Malicious actors know this, and they are exploiting hybrid cloud systems relentlessly.



Bad actors are changing their techniques, from malware to social engineering and identity-based strategies. Identity attacks may now account for nearly 80% of all attacks.



Attacks are coming over at least 10 vectors, far more than in the past.




The reason? It works. Successful attacks are on the rise, and time from entry to command and control of sensitive data is dropping fast.

As a result

86%

OF COMPANIES SURVEYED REPORT PAYING A RANSOM WHEN FACING EXTORTION DEMANDS.

Nearly three-quarters say attackers were able to access and harm their data.



THESE HAZARDS ARE BECOMING A CRISIS, AND NO ONE IS TALKING ABOUT IT

probably because few have a good plan. Instead, they slowly move to the cloud, say they're counting on cloud providers to fix the issue, or simply ignore it and call it a cost of business.

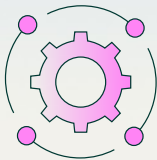
It doesn't have to be like this.

COMPANIES MUST

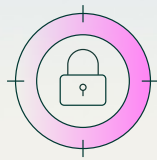


BY THINKING LIKE THEM

Threat actors want to find and control the most valuable data, so they can stop operations. If they can do it, companies can too.



It begins with a focus on regaining control, through system awareness, then a plan of protection, defense, and recovery that prioritizes sensitive data and continuous operations.



Sensitive data can be located and classified in categories such as personal information, financial details, and technical capabilities. This identifies targets before threat actors get there, asserting knowledge and control in the cloud.



A process of continuous backup and restoration should become part of the security process, as rigorously in the cloud as on premises.

DATA AND METHODOLOGY

Rubrik Zero Labs is committed to providing practical, unbiased intelligence aimed at helping organizations reduce their data security risk. In pursuit of this goal, we have included information from three main sources.

01

RUBRIK TELEMETRY

We employed Rubrik telemetry to gain insights into the typical organization's data environment and associated risks

02

WAKEFIELD RESEARCH

Perspectives from 1,600+ IT and security leaders through Wakefield Research

03

CONTRIBUTING ORGANIZATIONS

Research from respected cybersecurity organizations and institutions

RUBRIK TELEMETRY

We employed Rubrik telemetry to gain insights into the typical organization's data environment and associated risks.

It's based on two sources:

BACKUP DATA

is cloud, SaaS, and on-premises data that we've backed up from customer environments.



PRODUCTION DATA

is cloud, SaaS, and production data that Rubrik actively monitors, so organizations can make decisions about how they manage risk in their environments.

NUMBER OF CLOUD FILES SECURED:

Data covers January 1, 2024 through December 31, 2024

5.8 BILLION

total files across cloud and SaaS environments in production

175+ MILLION

sensitive files classified across all managed cloud and
SaaS environments

WAKEFIELD RESEARCH

1,600+

IT and security leaders

10

countries

50%+

CIO or CISOs

50%

CIO or CISOs

1,625

at companies with at least 500 employees
across 10 countries (Australia, France, Germany,
India, Italy, Japan, Netherlands, Singapore, United
Kingdom and the United States); in three regions
(Americas, APAC and EMEA)

50%

Directors / VPs

CONTRIBUTING ORGANIZATIONS

In order to provide a more well-rounded and impartial point of view, Rubrik has also incorporated crucial information from diverse organizations offering distinct perspectives.

WE USED:



CrowdStrike cloud and identity-based analytics around intrusions and breakout times.



Microsoft identity-based analytics and frequency of attacks data.



Allied Market Research cloud adoption information.

DATA SPRAWL IN THE CLOUD ERA

Locating and securing data has been a challenge since the first networked computer.

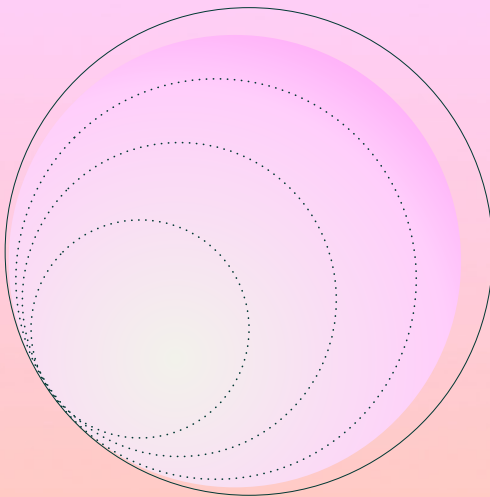
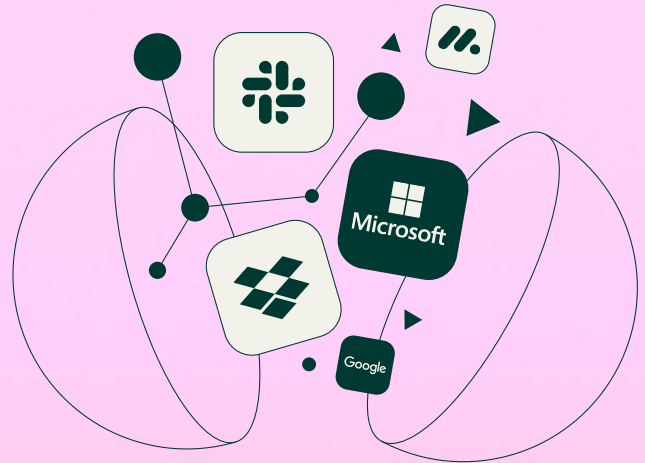


Before, data was in the corporate data center or on people's computers, initially on desks and then on desks and laptops, connected to a single network. Today, data sprawls across many types of devices, relying on many networks to access the corporate jewels, now residing on premises and in the cloud.

**AT SOME POINT,
THE CHANGE
IN SCALE AND
COMPLEXITY
MEANS THAT IT
PROFESSIONALS
ARE IN A NEW
WORLD.**

Over the last couple of decades, business has demanded the benefits that come with using cloud and SaaS services. And with good reason!

MOST OF OUR LIVES ARE EASIER WITH THE CLOUD.



89%

Organizations are continuing to increase their utilization of cloud and SaaS services and hybrid and multi-cloud strategies are becoming the norm, with 89% of organizations utilizing multiple cloud platforms, according to Allied Market Research.¹

IN ADDITION, OUR SURVEY RESULTS SHOWED:

89%



of IT and security leaders said they are managing hybrid cloud environments.
(Wakefield)

50%



of all IT and security leaders reported that they're managing mostly cloud and SaaS-based workloads vs. on-premises workloads.
(Wakefield)

92%



of IT and security leaders surveyed said they are using anywhere between 2 and 5 cloud and SaaS platforms for data storage, applications, and services.
(Wakefield)

66%

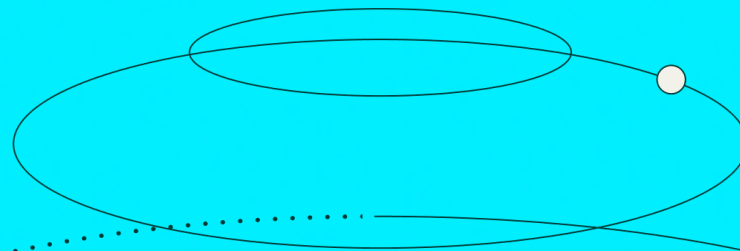


of IT and security leaders surveyed said they are planning to shift toward using more cloud and SaaS-based services over the next year while 31% will maintain their ratio of hybrid cloud and on-premise environments.
(Wakefield)

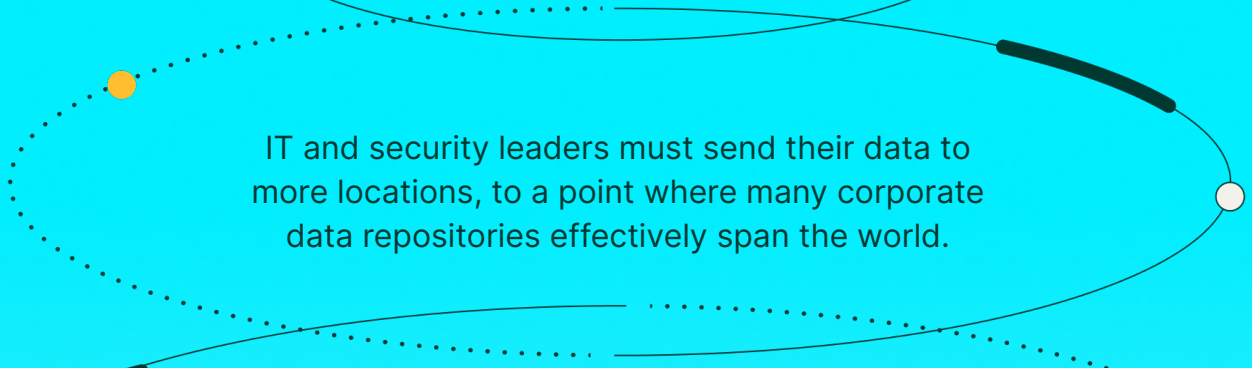
¹<https://www.alliedmarketresearch.com/cloud-native-applications-market-A210373>

DATA COMPLEXITY IN THE CLOUD ERA

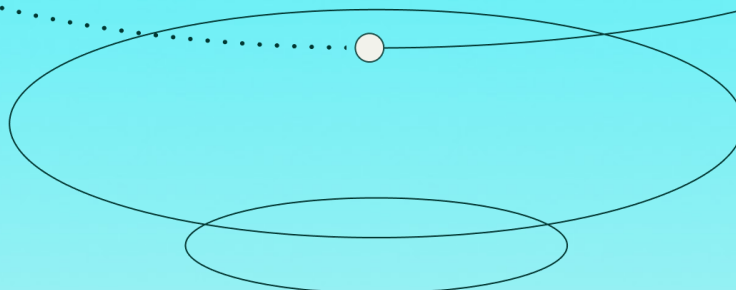
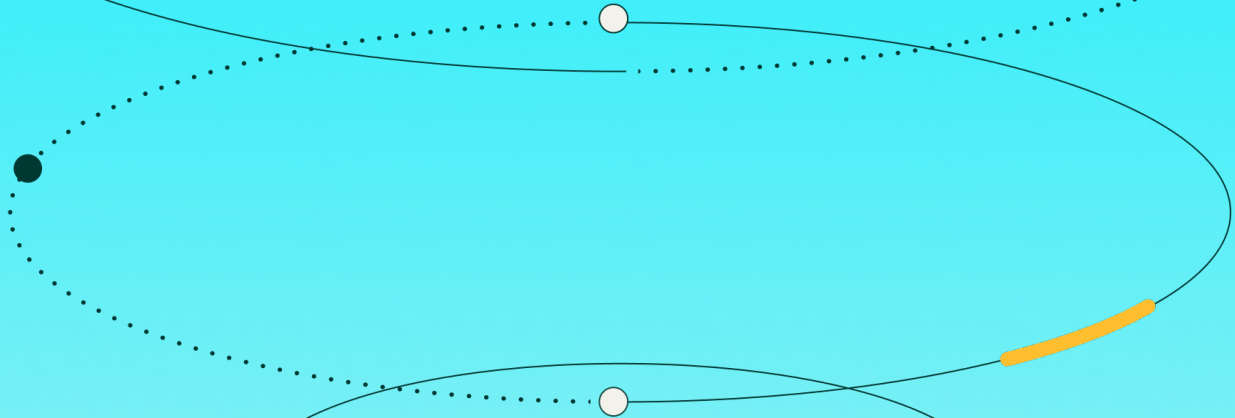
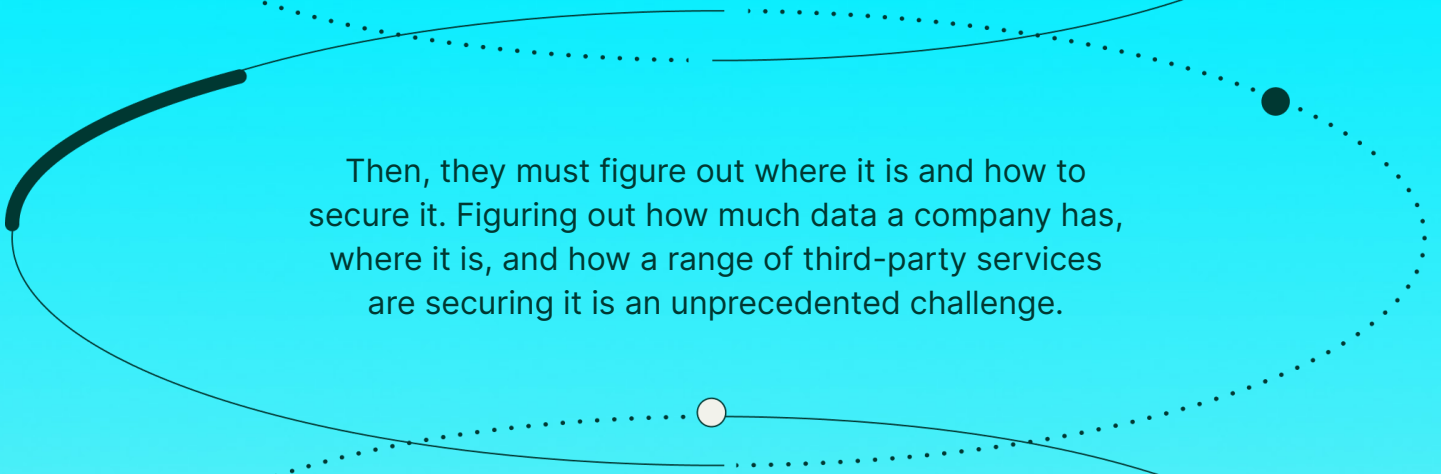
With every new cloud and SaaS use case, businesses lose a tiny bit of control over their data.



IT and security leaders must send their data to more locations, to a point where many corporate data repositories effectively span the world.



Then, they must figure out where it is and how to secure it. Figuring out how much data a company has, where it is, and how a range of third-party services are securing it is an unprecedented challenge.



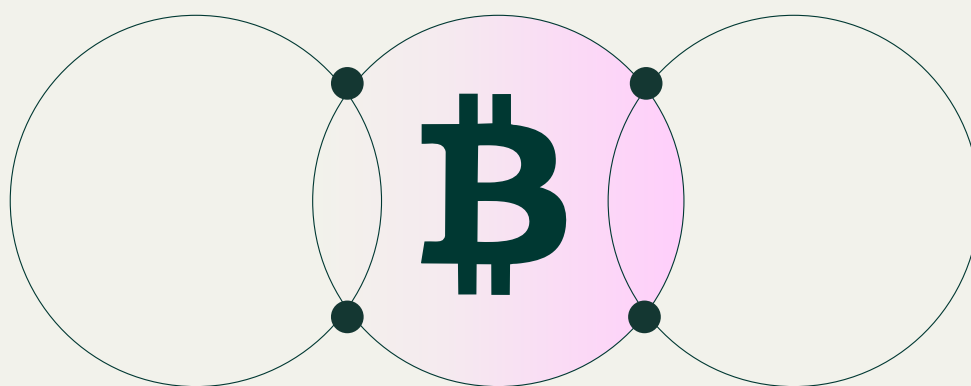
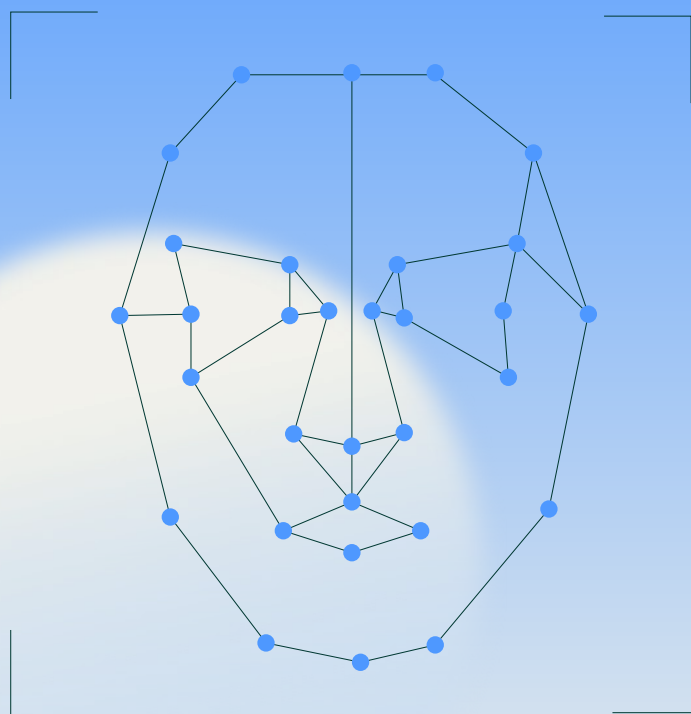
IT LEADERS SEE THE CHALLENGE PRIMARILY ACROSS THREE CATEGORIES:

(Wakefield)



THREAT ACTORS HAVE CHANGED WITH THE TIMES

Today's adversaries operate with purpose, discipline, and business-like precision, constantly adapting their tradecraft to exploit modern enterprise environments.



The broader corporate shift toward cloud infrastructure, identity-driven access, and distributed workforces has forced threat actors to explore new ways to conduct and scale their operations.

As threat actors evolve, they increasingly rely on techniques like valid credential abuse, hands-on-keyboard intrusions, and social engineering—often bypassing traditional malware entirely. Their methods reflect an enterprising mindset that prioritizes innovation, operational efficiency, and technical skill.

According to the CrowdStrike 2025 Global Threat Report, "In 2024, new and unattributed

CLOUD INTRUSIONS INCREASED 26%

compared to 2023, indicating more threat actors seek to exploit cloud services. CrowdStrike observed more intrusions in which attackers gained initial access via valid accounts, leveraged cloud environment management tools for lateral movement, and abused cloud provider command line tools."¹

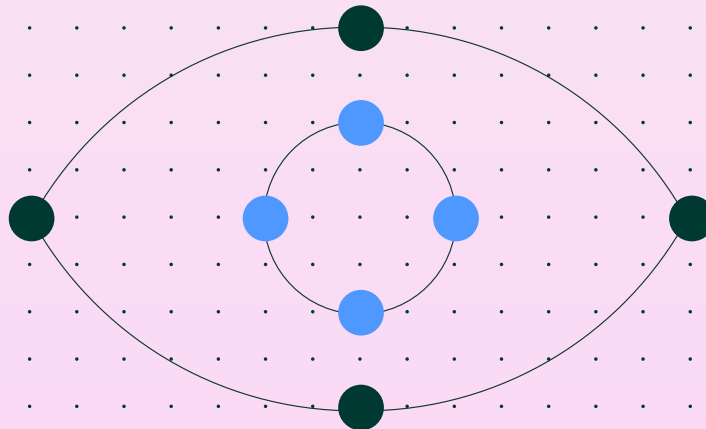
(CrowdStrike)

"Access broker activity surged in 2024, with advertised accesses increasing by nearly 50% over 2023. Meanwhile, valid account abuse was responsible for 35% of cloud-related incidents, reflecting attackers' growing focus on identity compromise as a gateway to broader enterprise environments."¹

(CrowdStrike)

Microsoft noted the eye-watering number of identity-based attacks in their Microsoft Digital Defense Report, where the company said that it blocks over 600 million identity-based attacks daily.²

(Microsoft)



"In 2024, malware-free activity accounted for 79% of detections, a significant rise from 40% in 2019."¹

(CrowdStrike)

And finally, they also observed a dramatic decrease in the amount of time it takes for a threat actor to move from the area they initially compromised to other systems (aka breakout time).

“In 2024, the average breakout time for interactive eCrime intrusions fell to 48 minutes, down from 62 minutes in 2023.

Alarming, the fastest
breakout was recorded at just

00:51

— meaning defenders may have
less than a minute to detect and
respond before attackers establish
deeper control.”¹

(CrowdStrike)

These stats are alarming for any organization with data in cloud or SaaS environments.

EVERYONE'S DATA IS A POTENTIAL TARGET.

And with the growth in identity-based attacks, opponents are logging in, not breaking in, something that is a lot harder to detect and stop in any environment. That initial foothold also makes it much easier to move quickly across IT systems.

HERE'S WHAT IT AND SECURITY LEADERS SAID ABOUT HOW THESE CIRCUMSTANCES ARE AFFECTING THEM ON THE FRONT LINES:

90%



of IT and security leaders said their organization experienced a cyberattack within the last year.

(Wakefield)

18%



of those leaders said they experienced a cyberattack more than 25 times in the past year. That's an average of at least one attack every other week.

(Wakefield)

86%



Of the IT and security leaders that experienced a successful ransomware attack in 2024, 86% said that they paid a ransom to recover their data or stop the attack. That's down 7% from the previous year.

(Wakefield)

74%



Of the IT and security leaders that experienced a ransomware attack, 74% said the threat actors were able to at least partially harm backup and recovery options.

(Wakefield)

35%



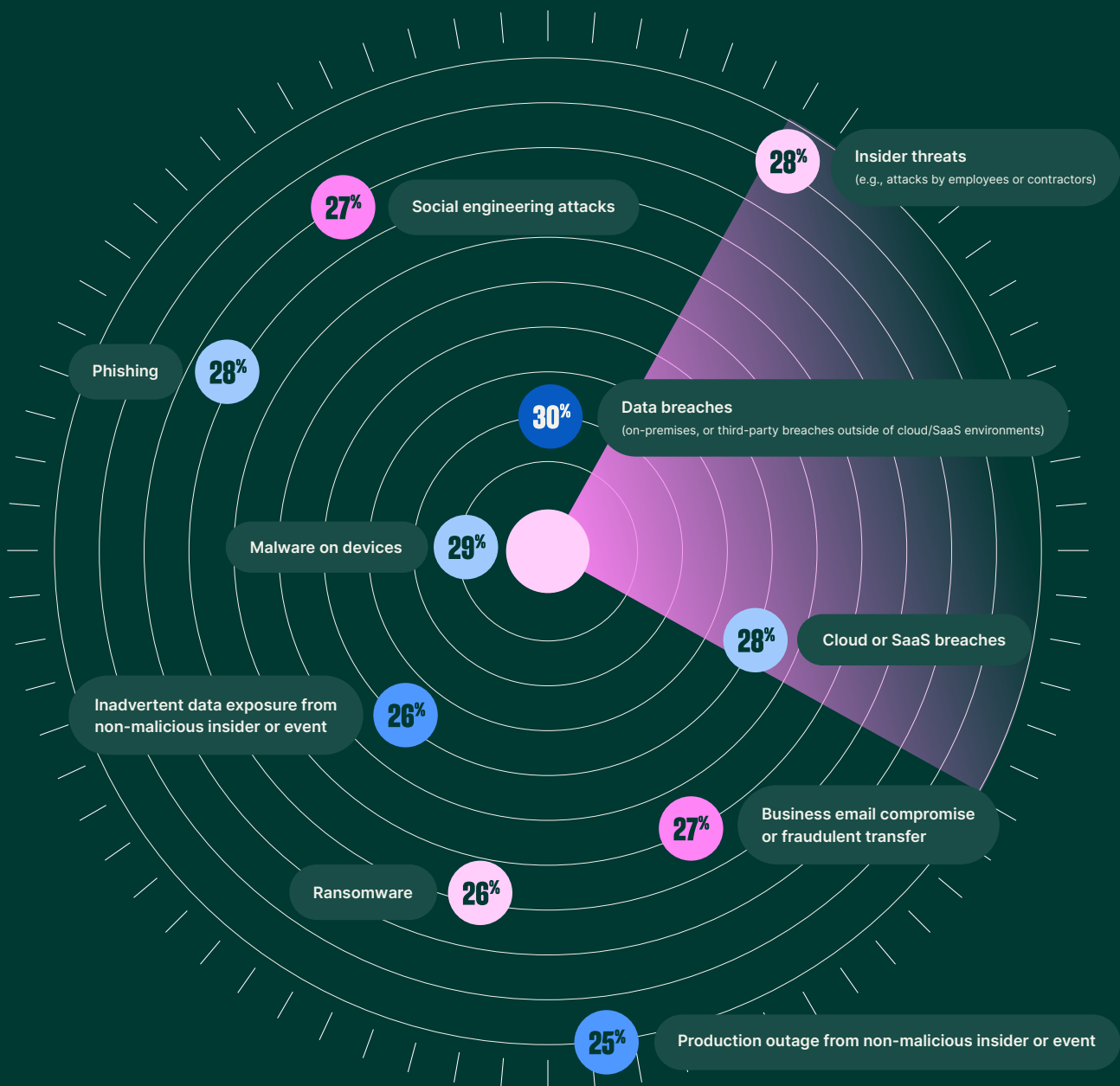
said the threat actors were completely successful in harming backup and recovery options.

(Wakefield)

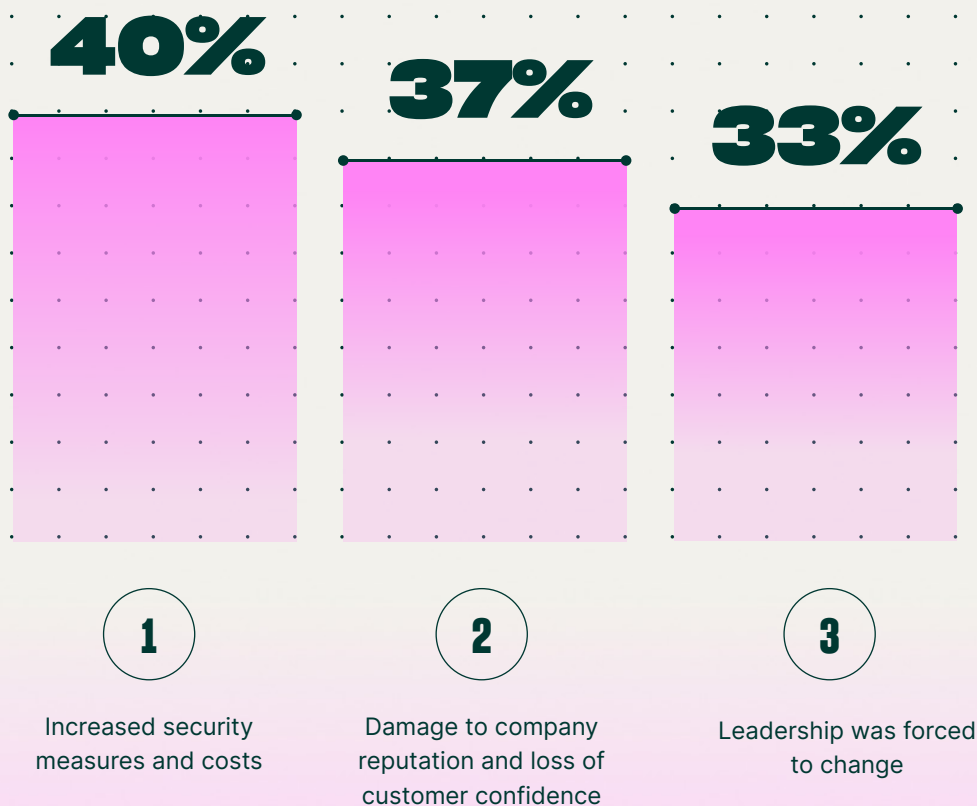
IT and security leaders said that the types of cyberattacks they were experiencing are

COMING FROM ALL DIRECTIONS.

(Wakefield)



HERE'S WHAT IT AND SECURITY LEADERS SAID ABOUT HOW THESE CIRCUMSTANCES ARE AFFECTING THEM ON THE FRONT LINES:



However, it's worth noting that as a whole, their experience ran the gamut from increased security measures and costs to unrecoverable data loss.

¹ CrowdStrike - 2025 Global Threat Report

² Microsoft - Microsoft Digital Defense Report

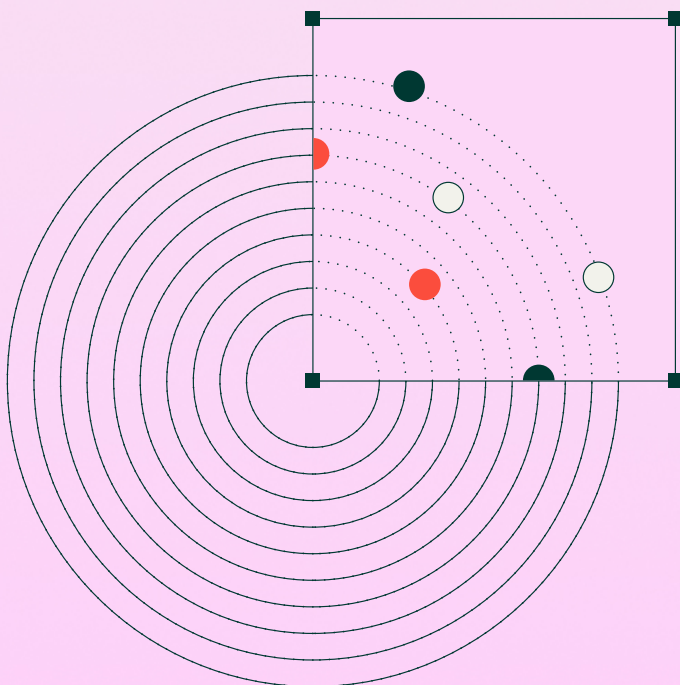
MOVING FROM CHAOS TO CONFIDENCE: A PLAN OF ACTION

Given all this new complexity, and the new threats that have arisen in response to it, how can IT and security leaders feel confident in their data security solutions?



While cloud adoption has become a cornerstone of modern business practices, some organizations remain hesitant to fully embrace the shift. Challenges, such as understanding application dependencies, comparing on-premises and cloud costs, and assessing technical feasibility, often serve as significant barriers.

A ZERO TRUST SECURITY MODEL



In contrast, other organizations are turning to a Zero Trust security model, which assumes no user or device can be inherently trusted, regardless of location.

While this approach can bolster security, it is labor-intensive and requires meticulous planning, including the assessment of every device, application, and user within the organization. The rigorous nature of Zero Trust demands a significant cultural and operational shift, which can drive up costs, increase complexity, and disrupt workflows. This makes it difficult to implement without slowing business velocity, presenting a trade-off between security and operational efficiency.

There's another way. Managing hybrid, globally dispersed data begins with an awareness of where things are. Sensitive data should be located and classified, so companies can identify and protect potentially sensitive targets as early as possible.

For example, through our Rubrik telemetry of production data, we can tell that our customers' sensitive structured data sits in these environments

[Rubrik telemetry - Production data]

DYNAMODB 35.51%

Amazon DynamoDB (**Key-Value Document Store**)

- Social Media User Profiles
- IoT/Device Sensor Data or Telemetry
- Product Catalogs (E-Commerce)

RELATIONAL DATABASE SERVICE 6.81%

Amazon RDS (**Relational Database Service**)

- HR Employee Database
- Order Management (E-Commerce)
- Healthcare Patient Records

SNOWFLAKE 19.9%

Snowflake is a Cloud Data Warehouse

- Customer Data (Retail/E-Commerce)
- Financial Transactions (Banking)
- Sales Transactions
- Analytical Aggregates (Total Revenue, Customer Lifetime Value)
- Security Logs (SIEM integration)

VIRTUAL MACHINES 35.51%

Amazon DynamoDB (**EC2, AzureVM**)

- Hosting databases
- Hosting applications
- Legacy workloads
- Configuration data
- Log data used for analysis

And that its biggest caches of sensitive unstructured data are estimated to sit in these environments:

(Rubrik telemetry - Production data)

56.67%



of OneDrive files are sensitive files

25.56%



of SharePoint files are sensitive files

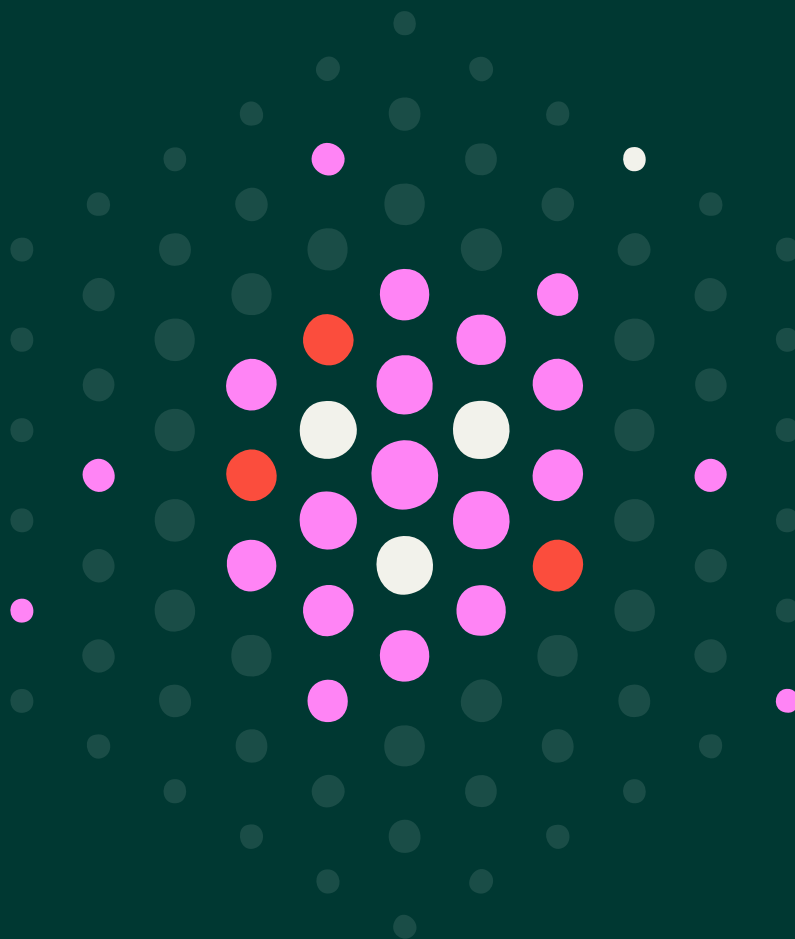
14.27%



of S3 files are sensitive files

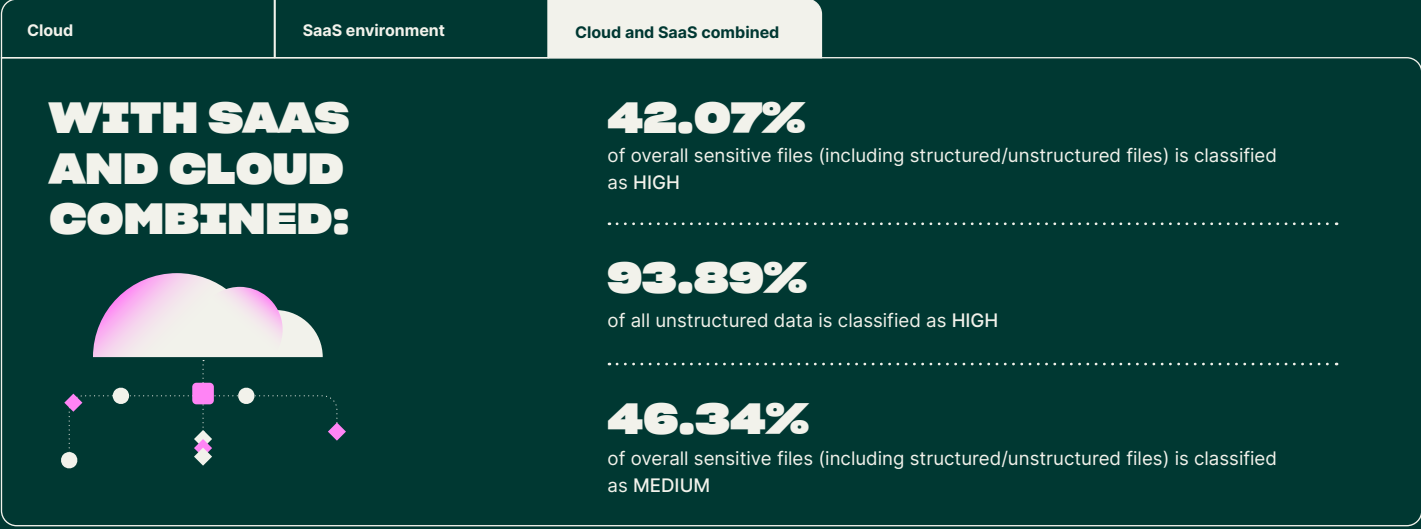
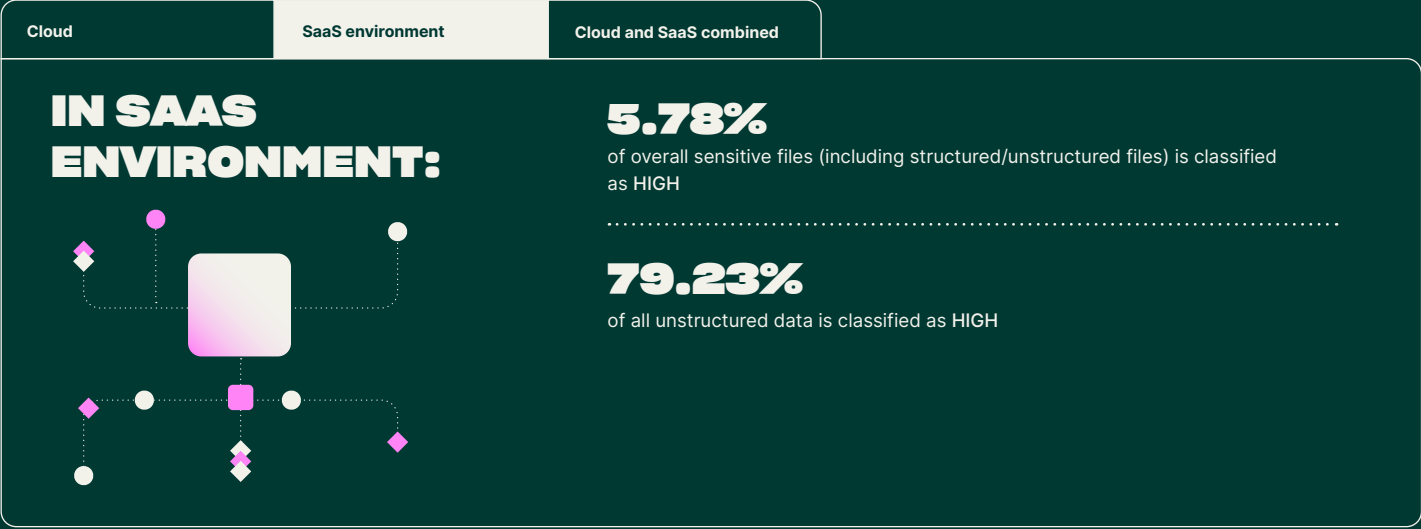
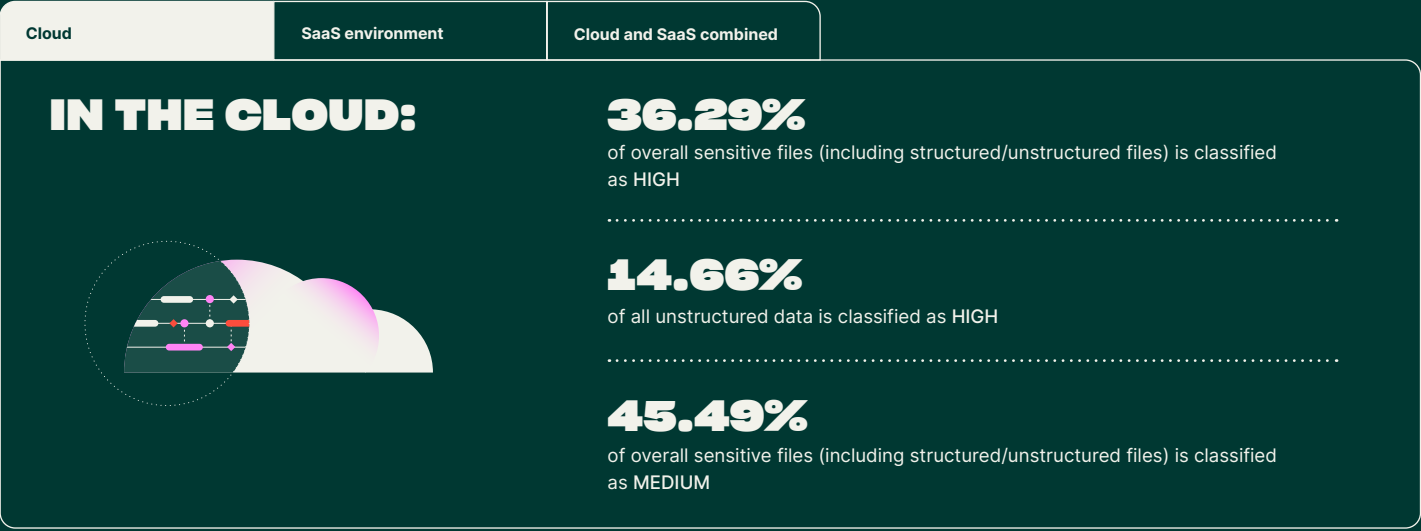
SECURING YOUR SENSITIVE DATA

As an IT and security leader, even with this amount of information, you can start to make some decisions. Ultimately, you care about all your data, but the stuff you really care about is your sensitive data.

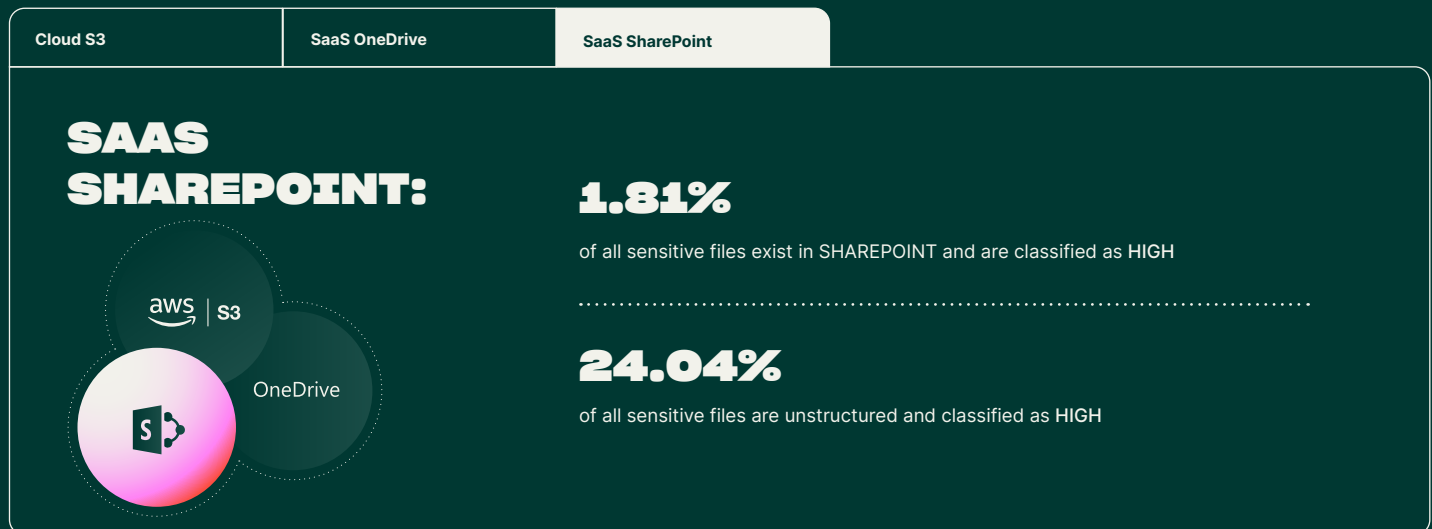
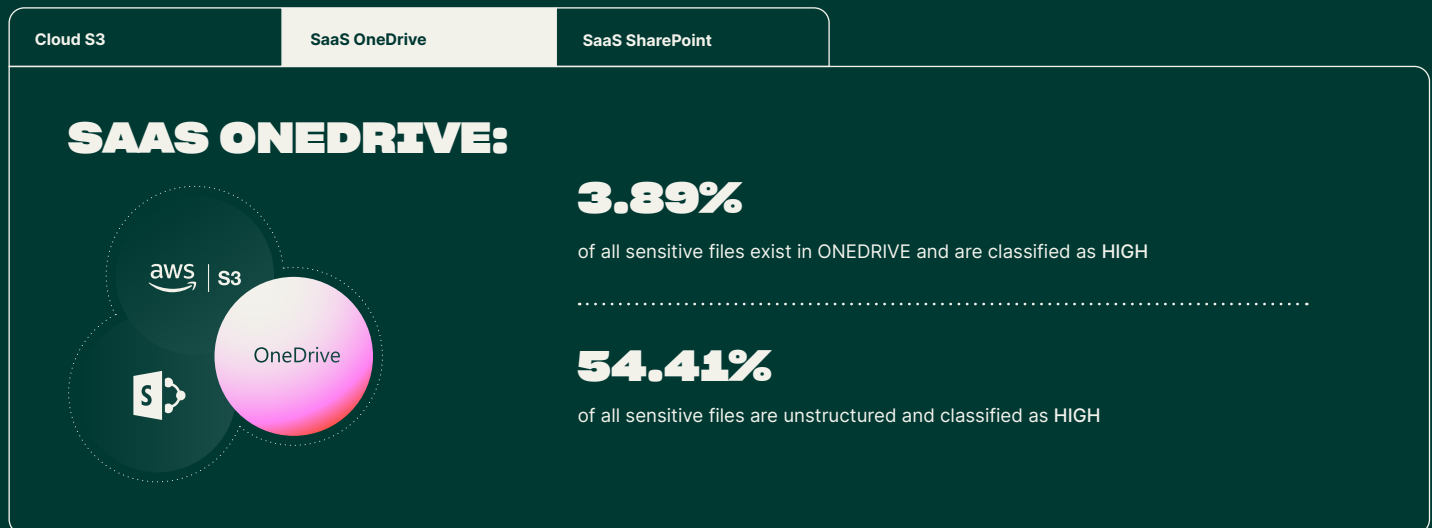
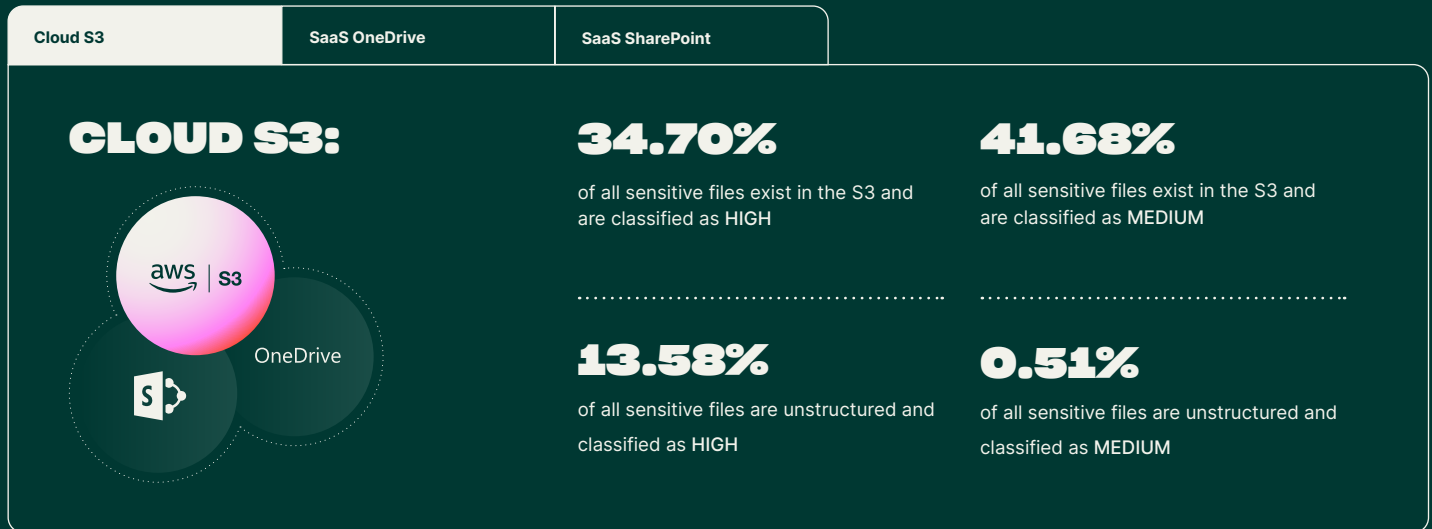


Knowing how much of it you have and where it lives is your first step to better securing it.

From there, you can start to break down just how sensitive your cloud and SaaS data is. Here are some examples to get you started.



And you can start to pinpoint just where that highly sensitive data is.



Then, you can start to draw a clearer picture of what sensitive data might include.



PERSONAL

PII (Personally Identifiable Information), including: Social Security numbers, birthdates, addresses, phone numbers, etc.

64.51%

of all sensitive data is PII

93.84%

of all sensitive unstructured data is PII



DIGITAL

API keys, usernames, account numbers, IP addresses, mobile device IDs, etc.

26.96%

of all sensitive data is DIGITAL

1.89%

1.89% of all sensitive unstructured data is DIGITAL



BUSINESS

Intellectual property, including: product designs, source code, R&D insights, strategic plans, supply chain logistics, inventory information, etc.

24.25%

of all sensitive data is BUSINESS

3.79%

of all sensitive unstructured data is BUSINESS



FINANCIAL

PCI data (Payment Card Industry data), including: transactions records, banking information, credit card/debit card information, tax filings, internal audit reports, etc.

13.97%

of all sensitive data is FINANCIAL

7.82%

of all sensitive unstructured data is FINANCIAL

This exercise is the first step in reasserting knowledge and control. It's also a great way to get board-level support for your security strategy.

The high-level message changes from

**“WE HAVE SENSITIVE DATA
SPREAD ACROSS SEVERAL
UNKNOWN POINTS, WITH
VARYING SECURITY,” TO
“HERE IS A LIST OF HOW
OUR SENSITIVE DATA IS
BEING USED AND HOW WE
ARE PROTECTING IT.”**

ESTABLISH CLEAR AND COMPREHENSIVE POLICIES

After increasing awareness of data location and data type across the hybrid system, it's important to establish clear and comprehensive policies. Unfortunately, at present many companies have a haphazard approach.

Comparing the data that we monitor in production environments to the data that we back up, we have seen the huge disparity between how organizations protect on-premises data and how they protect their cloud and SaaS data.

How organizations handle data backups is particularly stark. On-premises data is routinely backed up with strict retention policies, air-gapped copies, and disaster recovery plans that have been refined over years.

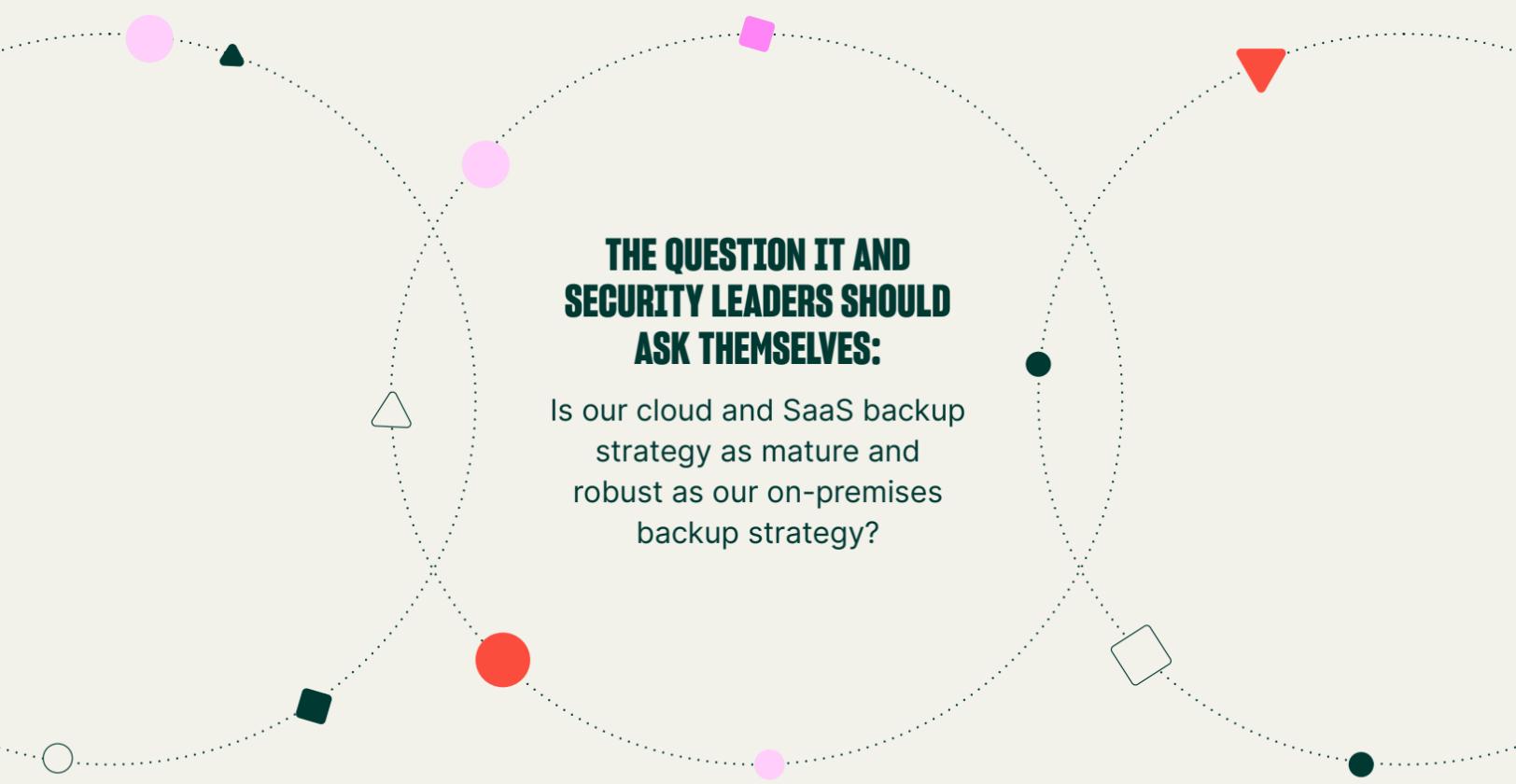
Cloud and SaaS data, in the meantime, is often backed up haphazardly, if at all. The implications for a cloud-centered ransomware attack are sobering.

This information leads us to believe that organizations are relying on their cloud providers' native backup tools to secure their data. Unfortunately, native backup tools are often limited, infrequent, or tied to the provider's infrastructure in ways that may not align with an organization's recovery needs. Even assuming state of the art performance at every cloud and SaaS provider, surrendering your awareness and control is a problematic security approach.

No sensible risk management approach assumes everything is state of the art. The fact is, critical business data stored in cloud applications and SaaS platforms is more vulnerable to accidental deletion, ransomware attacks, and policy misconfigurations than its on-premises counterpart.

Controlling your backup capability, off prem as well as on, is a crucial part of controlling corporate security.

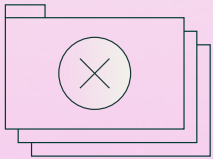
This is beyond a technical problem. It's a strategic blind spot.



**THE QUESTION IT AND
SECURITY LEADERS SHOULD
ASK THEMSELVES:**

Is our cloud and SaaS backup
strategy as mature and
robust as our on-premises
backup strategy?

LET'S REFER TO A REAL WORLD EXAMPLE WITH THE GITLAB DATABASE INCIDENT OF JANUARY 31, 2017.



1.

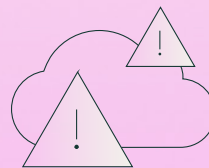
An engineer accidentally deleted the production database, resulting in the loss of six hours worth of critical data. This included issues, merge requests, and comments.



3.

This incident exposed the risks of assuming cloud-native environments inherently provide robust backup protections. GitLab's postmortem revealed that their backup strategy was insufficient compared to traditional on-premises practices.¹

<https://about.gitlab.com/blog/gitlab-dot-com-database-incident/>



2.

The recovery process failed due to multiple backup failures—primary backups were corrupt, LVM snapshots were outdated, and replication was unreliable.

Addressing the problem requires action: a unified approach to data protection that extends backup and recovery policies beyond on-premises systems into the cloud-native world.

RECOMMENDATIONS

Here's how IT and security leaders can increase their capabilities and confidence in their ability to protect their data across cloud, SaaS, and on-premise environments.



#1

First, know where your data, particularly your sensitive data, is, at motion and at rest.

Prioritization matters, since everyone has scarce resources. Don't secure a folder of five-year-old marketing videos with the same intensity required for an organization's most precious intellectual property.

Keep in mind this might be a bigger undertaking than it sounds. Like all data, sensitive data can change over time. For instance, an idea could go from a single employee's random musing to one of the main building blocks of an organization's strategy in a matter of weeks. Still, you need to know where it all is and protect it accordingly.



#2

Inform your policies, processes, and procedures with data awareness and data prioritization.

POLICIES

Set appropriate policies. For instance, control the conditions under which sensitive files are downloaded.

For example, maybe it's a policy to restrict editing access to your organization's source code on a public WiFi network if you aren't using a VPN. These may seem like obvious ideas, but you'd be surprised how often people forget to employ them in a systemic way.

PROCESSES AND PROCEDURES

Define methods for enforcing policies. For instance, if users aren't allowed to download specific files under specific circumstances, then:

- How are you going to enforce that policy?
- How are you going to track when it's violated?
- How are you going to deal with the fallout of that violation?
- Who is responsible for making sure that happens?

Companies must answer all these questions to ensure data safety and to give boards and leadership confidence that you know where all your sensitive data is and you have a plan for protecting it.

#3

Use automation to help your security and IT teams level the playing field.

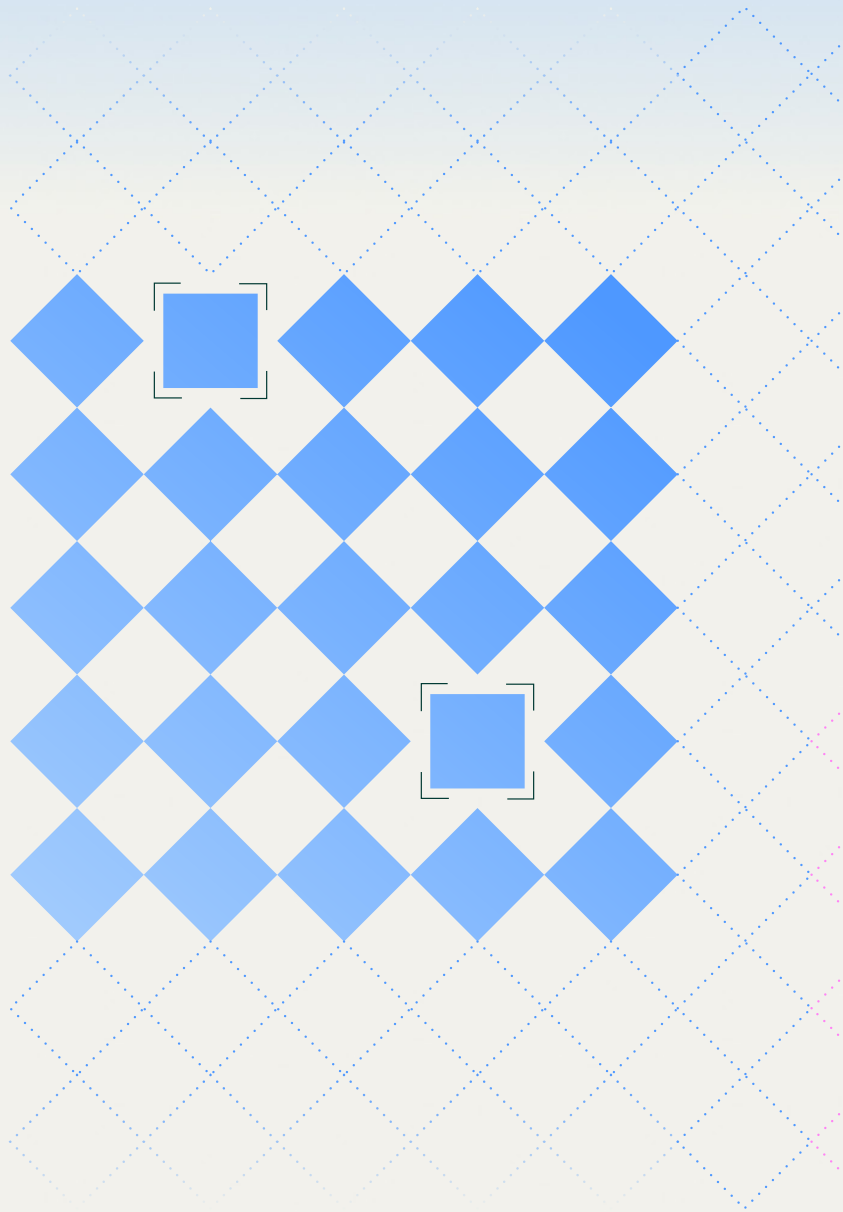
There's no way anyone can expect security and IT teams to keep up with what's happening with the vast amount of data an organization generates without some significant help.

Even with monitoring and aggregation tools, the amount of alerts coming at often short-staffed teams is enough to make even the most talented and hardened IT and security professionals want to bury their heads in the sand.

The only way to effectively ensure that policies are enforced and processes and procedures are followed is through automation.

For example, when a security incident occurs, a root-cause analysis is necessary. Without automation, security analysts must manually sift through large volumes of data—a tedious and time-consuming process. As we know, repetitive tasks increase the likelihood of human error. A common example is an analyst in the SOC mistakenly marking a true positive as a false positive, potentially leaving a threat unaddressed.

By automating routine and repetitive tasks, organizations not only reduce errors but also free up skilled professionals to focus on more strategic and high-value security efforts.



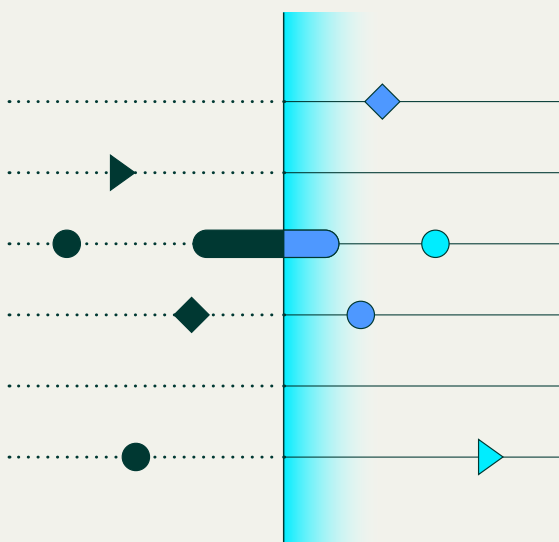
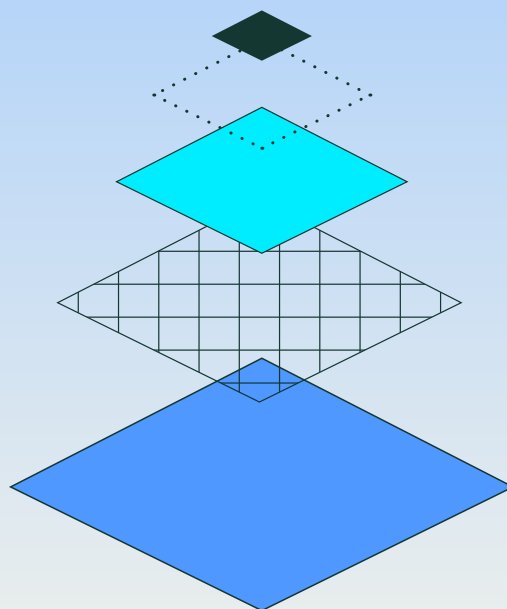
DATA BACKUP & RECOVERY

⊗ WITHOUT AUTOMATION:

IT teams manually manage backups, requiring them to monitor schedules, validate data integrity, and coordinate recovery processes during an incident. The approach is not only time-consuming but also prone to errors, such as missed backups or failed recoveries, leaving the organization vulnerable during critical moments.

✓ WITH AUTOMATION:

Automated backup and recovery solutions ensure that data is consistently and securely backed up without manual intervention. In the event of a ransomware attack or system failure, these solutions ensure backups are fully immutable and available, enable instant data recovery, drastically reducing downtime and minimizing data loss. By automating these processes, IT teams can focus on proactive security measures rather than managing complex recovery workflows, ensuring business continuity and a stronger defense against cyber threats.



THREAT DETECTION AND ALERT TRIAGE

⊗ WITHOUT AUTOMATION:

Security analysts manually sift through thousands of security alerts, leading to alert fatigue and potential missed threats.

✓ WITH AUTOMATION:

Automated threat detection and response tools can categorize, prioritize, and even remediate certain alerts, allowing analysts to focus on investigating novel or advanced threats.

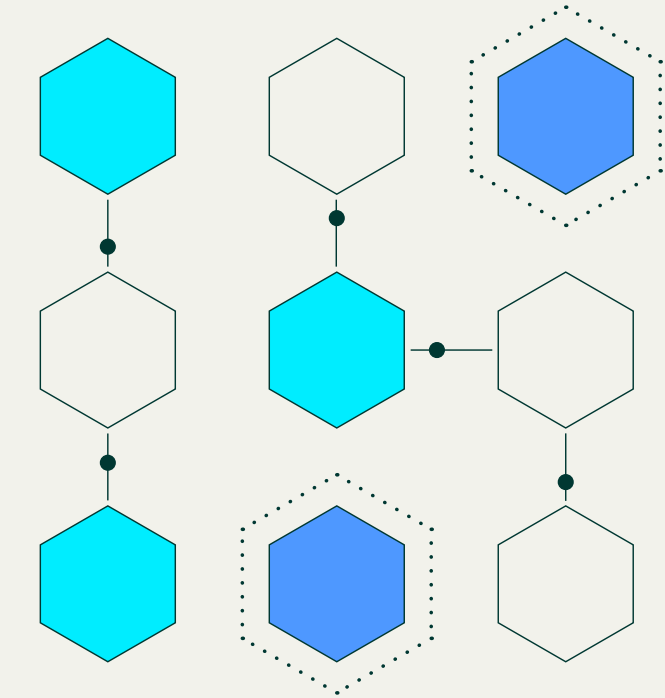
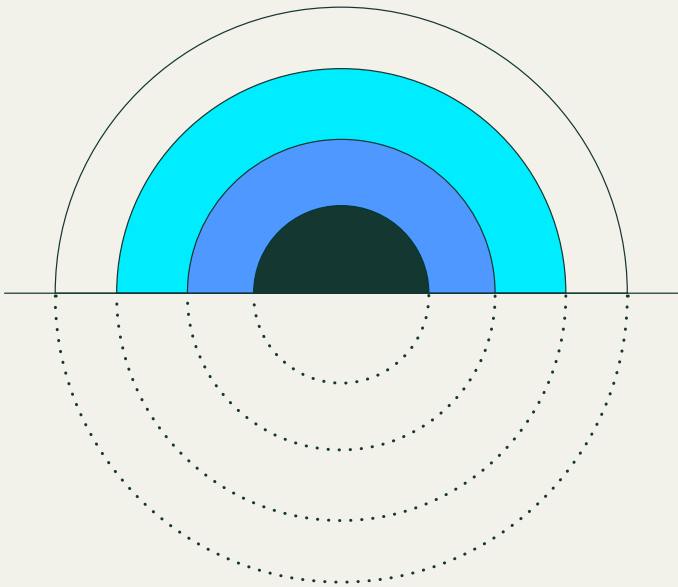
INCIDENT RESPONSE & ROOT-CAUSE ANALYSIS

⊗ WITHOUT AUTOMATION:

Security teams must manually correlate logs from various sources (firewalls, SIEMs, endpoint protection systems) to determine the root cause of an incident.

✓ WITH AUTOMATION:

SOAR (Security Orchestration, Automation, and Response) platforms automatically collect and analyze log data, significantly reducing investigation time.



VULNERABILITY MANAGEMENT & PATCHING

⊗ WITHOUT AUTOMATION:

IT teams manually track vulnerabilities, assess risks, and deploy patches—a time-consuming and error-prone process.

✓ WITH AUTOMATION:

Automated vulnerability scanning and patch management solutions proactively identify and remediate risks without requiring constant manual intervention.

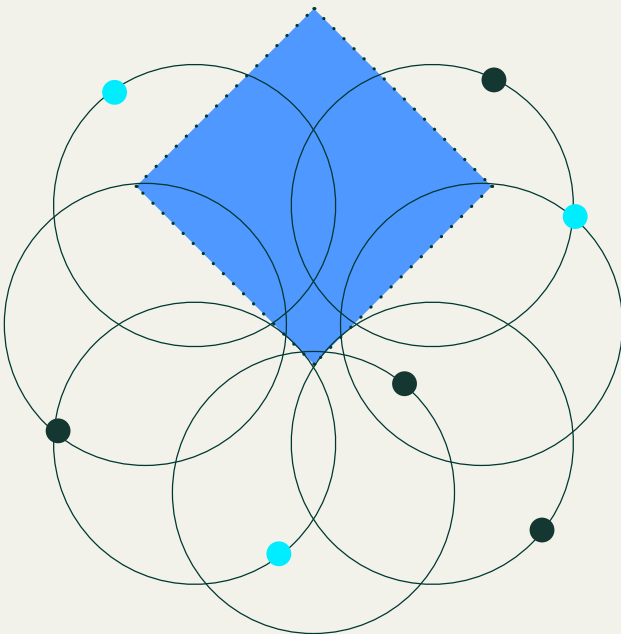
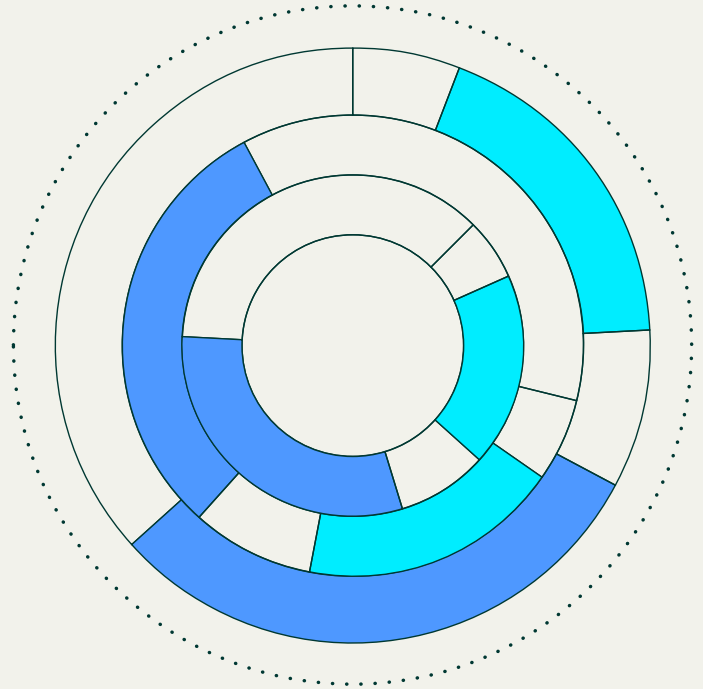
ACCESS CONTROL & IDENTITY MANAGEMENT

⊗ WITHOUT AUTOMATION:

IT admins manually provision and revoke user access, increasing the risk of lingering privileged accounts.

✓ WITH AUTOMATION:

Identity and Access Management (IAM) solutions dynamically adjust permissions based on role changes, reducing insider threat risks.



BEHAVIORAL ANOMALY DETECTION

⊗ WITHOUT AUTOMATION:

Security teams rely on static rules to flag suspicious activities, which can lead to excessive false positives.

✓ WITH AUTOMATION:

AI-driven security tools continuously learn from user behaviors and adapt to detect new attack patterns more effectively.

CONCLUSION

The transition to multi-cloud hybrid environments marks one of the most significant milestones in the history of business computing.

It has become essential for corporate workflows and inter-corporate collaboration.

Yet, as this analysis has shown, these benefits come at a high cost in terms of security risks. Hybrid environments introduce unprecedented hazards: IT leaders report challenges with system-wide data security, lack of visibility, and the inability to establish centralized control. Threat actors are exploiting these weaknesses relentlessly and employing evolving techniques like identity-based strategies, which now account for the majority of attacks.

THE RESULTS ARE ALARMING

~90%

of organizations surveyed have been attacked, with many facing repeated assaults

86%

of companies facing extortion demands report paying the ransom

3/4

confirm attackers were able to breach and harm their data

ACKNOWLEDGEMENTS

Rubrik would like to extend our appreciation to all outside organizations providing their hard-earned data knowledge to this study.

As with all things Rubrik Zero Labs, it takes a village to pull off these studies. Wakefield Research provided external data to make this research as objective as possible. ShapedBy found a way to take the data and bring it to life. Finally, many Rubrikans worked hard to provide capability, context, and guidance. We'd like to extend a specific appreciation to Amanda O'Callaghan, Linda Nguyen, Lynda Hall, Ben Long, Peter Chang, Ajay Kumar Gaddam, Dan Eldad, Gunakar Goswami, Prasath Mani, Ethan Hagan, Kevin Nguyen, Caleb Tolin, Sindhu Nagendra, Trinetra Reddy, Heather Webb, Meghan Fintland, and Fareed Fityan.