

The Great SaaS Data Exposure The Great SaaS Data Exposure The Great SaaS Data Exposure The Great SaaS Data Exposure The Great SaaS Data Exposure

The average organization has more than \$28M in SaaS data-breach risk.

Table of contents

- 4 About this report
- 5 Key findings
- 7 Snapshot: a terabyte in the cloud
- 8 Data exposed organization-wide in Microsoft 365
- 9 Out-of-control permissions
- 10 Weakest links: internal sharing-links overexpose data
- 11 Data free-for-all: data exposed to everyone on the internet
- 12 Missing MFA
- 13 Stale user accounts
- 14 State of cloud security
- 15 Cloud data security checklist
- 16 Recommendations
- 17 Case study
- 18 About Varonis

Key terms

Administrator (admin) accounts

User accounts with extra permissions to allow IT to perform tasks like installing software.

Organization-wide access

Indicates records, files, and folders open to all employees.

Public access

Indicates records, files, and folders open to everyone via the internet.

Stale data

Information no longer needed for daily operations.

Sensitive objects

Indicates data, such as file metadata, that are stored and accessible in the cloud.

Privileged accounts

Provides elevated permissions for accessing systems and sensitive data.

Stale user accounts (aka “ghost users”)

Enabled accounts that appear inactive, and often belong to users who are no longer employed by the organization.

Sharing-links

Allows users to quickly and easily share data with others.

Sensitive records or files

Instances of PII or otherwise sensitive data. A single spreadsheet file can contain multiple records. Sensitive records and files can contain payment card information, health records, or personally identifiable information (PII) subject to regulations such as PCI, HIPAA, GDPR, and others.

About the report

Our research team analyzed:

10 billion objects

15 petabytes of data

717 organizations

This metadata came from a number of SaaS and IaaS applications and services such as Microsoft 365, Box, and Okta.

Firmographics

This report includes data analysis across numerous industries:

Financial services

Pharma and biotech

Energy and utilities

Technology

State and local gov

Healthcare

Manufacturing

Retail

Education

Data was collected from companies worldwide, including the U.S., Canada, the U.K., France, Germany, Spain, Brazil, and Australia.

Key findings

The average company has an alarming amount of sensitive data exposed not only to all employees, but in many cases, to the entire internet. It's a data-breach crisis waiting to happen.

81% of organizations had sensitive SaaS data exposed.

The average company has:

10% of cloud data exposed to every single employee

representing massive internal risk.

4,468 user accounts without MFA

(multi-factor authentication) enabled, making it easier for attackers to compromise internally exposed data.

40+ million unique permissions

across SaaS applications — creating a nightmare for IT and security teams responsible for managing and reducing cloud data risk.

12,000+ Microsoft 365 sharing-links

which expose data organization-wide to every employee.

157K sensitive records exposed to everyone on the internet

via SaaS sharing features — representing \$28 million in data-breach risk.

33 super admin accounts

more than half of which do not have MFA enabled. Compromising super admin accounts can allow attackers to steal more data, create backdoors, and sow chaos.

6% of cloud data exposed to the entire internet.

Why this is a crisis waiting to happen:



One out of every 10 records in the cloud is exposed to all employees.

The average company has an impossibly large internal blast radius, giving any employee broad access to steal 10% of a company's cloud data.

Missing MFA makes attackers' jobs easier.

Accounts missing basic security controls like MFA — including rogue admin accounts — make breaching SaaS apps and stealing internally exposed data easier for attackers.

Untangling data exposure within SaaS is a monumental task.

SaaS apps are built to auto-create more exposure but many do not include any features to find and reduce exposure. There are exponentially more SaaS permissions to manage than on-prem permissions.

IBM Security, [Cost of a Data Breach Report](#), Page 5. The report found customer PII was the costliest record type, at \$180 per lost or stolen record. We found the average company has 157,000 exposed records — and that adds up to \$28 million in risk in the average company.

A terabyte in the cloud

611,478

files

6,116

sensitive files

3,998

folders shared externally

4,324

stale sensitive files

1,924

private Microsoft Teams channels (per org)

295

Microsoft Teams (per org)


On average, each terabyte in the cloud contains more than 6,000 sensitive files, nearly 4,000 folders shared with external contacts, and more than 2.1 million permissions (access control entries).

With this much hiding in a single terabyte, it's easy to see how data can get out of hand.

2,152,543

permissions

Organization-wide exposure in Microsoft 365



7%

of companies had more than 10K exposed files

10

companies had more than 100K exposed files

1

organization had more than 1.5M exposed files

Organization-wide access allows every employee to create, read, update, and delete critical and sensitive data on the network. When everyone can access data, organizations create a broad attack surface that's highly vulnerable to cyberattacks like ransomware and insider threats.

In the average organization using Microsoft 365:

One in 10 sensitive files is exposed to every user.

One in 10 folders is exposed organization-wide.

1,000 (9%) sensitive files are exposed organization-wide.

97,638 (8%) folders are exposed organization-wide.

On average, it takes about **six hours** per folder to locate and manually remove global access groups, create and apply new groups, and then subsequently populate those groups with the right users who need access to the data. For 1,000 folders, that's 6,000 hours of manual work!

Case study

Collaboration involving sharing data is part of every organization — but it's rarely done securely. A U.S. county found sensitive information on criminal cases open and exposed to all employees in its Microsoft 365 environment. With thousands of employees and sprawling permissions, the IT team wasn't making the progress they needed to lock down their data with confidence. Visibility, automation, and alerting were key to protecting their data in the Microsoft cloud.

Out-of-control permissions

The average company has 40+ million unique permissions across SaaS applications, creating a nightmare for IT and security teams attempting to manage and reduce cloud data risk.

When it comes to analyzing accessibility, most CISOs don't realize how many folders, files, and records they need to examine. A single terabyte of data routinely holds tens of thousands of objects with specific, unique permissions that determine which users and groups have access. Organizations now have thousands of terabytes of data. All the relationships between users and groups need to be analyzed, too. To make matters worse, each SaaS application implements permissions mechanisms differently.

Case study

At one global real estate company, a dozen contractors were given access to the company's Salesforce instance. Months later, after their project ended, the ex-contractors could still log in and access all of the company's records. Two former contractors were super admins — and one had recent login activity. Additionally, 182 standard users could export every single record, and one sales rep was caught exporting opportunities and accounts after he had given notice of his resignation.

Case study

At a national bank, the security team lacked visibility into the company's Salesforce instance. Local Salesforce admins had cloned ten "shadow" instances without the security team knowing. Within those instances, 23 regular users had obscure permission sets that allowed them to perform password resets for other users, create new users, and view, delete, and export all data. Additionally, the security team was unaware of ongoing brute-force attempts by attackers trying to gain access to one of these instances.

Internal sharing-links overexpose data



>27K

sharing-links to information in Microsoft 365

12,803

sharing-links open to all employees

Sharing-links are helpful for collaboration, but they are also a significant security risk.

Easy sharing makes protecting sensitive data challenging. When insiders or external attackers gain access to data they shouldn't, information is immediately at risk from ransomware and theft.

Overshared links to sensitive data can expose that data to everyone in the organization. Even one minor misconfiguration can leave a big security gap and lead to a data breach.

The average organization had thousands of sharing-links to data in Microsoft 365, with nearly half of these open to all employees.

Case study

A **private university** needed to mitigate the risk posed by threats such as ransomware. The university's hybrid on-prem and cloud environment had grown complicated, making managing external sharing and data exposure difficult. Visualizing existing permission structures for its Microsoft 365 files made it possible for the university's small IT team to manage external sharing for users with substantial access.

Data exposed to everyone on the internet

Public sharing makes data accessible to anyone on the internet and it's as scary as it sounds.

Using SaaS and IaaS apps and services can increase risk exponentially — rather than just exposing sensitive data to every employee, data could be exposed to everyone, anywhere, via the internet.

Many organizations struggle with locking down access. The typical organization has more than 150,000 records and files shared publicly. We found, on average, nearly 50,000 sensitive records in Microsoft 365 and more than 113,000 sensitive records in SaaS applications open to everyone on the internet. These sensitive records included information protected under HIPAA, CCPA, GLBA, and GDPR, including social security numbers, PCI, and even plain-text passwords.

In the average organization, there are:

157,181

files shared publicly

6%

of sharing-links open to anyone on the internet

18,763

folders shared publicly

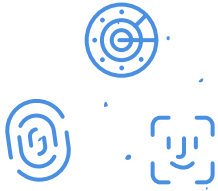
48,896

sensitive records shared publicly in Microsoft 365

113,632

sensitive records shared publicly in SaaS applications

Missing MFA



Enabling MFA makes you

99%

less likely to get hacked.

4,468

user accounts without MFA enabled.

Multi-factor authentication (MFA) is a critical security measure that can protect users even if their passwords are leaked — but MFA only helps when it's enabled and enforced.

According to CISA director Jen Easterly, enabling MFA makes you 99% less likely to get hacked.

On average, companies had 4,468 user accounts without MFA enabled — that's more than 4,000 accounts requiring only a user's login credentials. Organizations, on average, had 33 administrative accounts, which provide elevated privileges for managing and modifying user accounts, systems, and settings. Of these, 18 (55%) did not have MFA.

Without MFA, attackers have a more straightforward path to compromise an organization. Criminal groups, such as BlackMatter, are known to grab usernames and passwords from data breach dumps on the dark web. They try out every credential to brute-force internet-facing systems and gain access.

33

admin accounts total

41

privileged accounts total

55%

admin accounts have no MFA

44%

privileged accounts have no MFA

Security doesn't stop at MFA; multi-factor authentication can be cracked by attackers again and again. Varonis Threat Labs researchers discovered techniques to bypass Box's **TOTP-based MFA**, and another to bypass Box's **SMS-based MFA**. Until Box fixed these issues, attackers could use stolen credentials from the dark web to silently infiltrate Box accounts — even with MFA enabled.

Stale user accounts

Stale user accounts (sometimes called “ghost users”) are enabled accounts that appear inactive and often belong to users who are no longer with the organization.

Stale user accounts often remain enabled but inactive — and can be easily overlooked. These accounts provide access to applications and data and may allow attackers to quietly “test the waters” or attempt a brute-force attack without creating noise and tripping alarms that an attack is underway.

1,197

inactive users

1,322

number of guest users

56%

number of stale guest users
enabled at 90 days

33%

number of stale guest users
enabled at 180 days

Case study

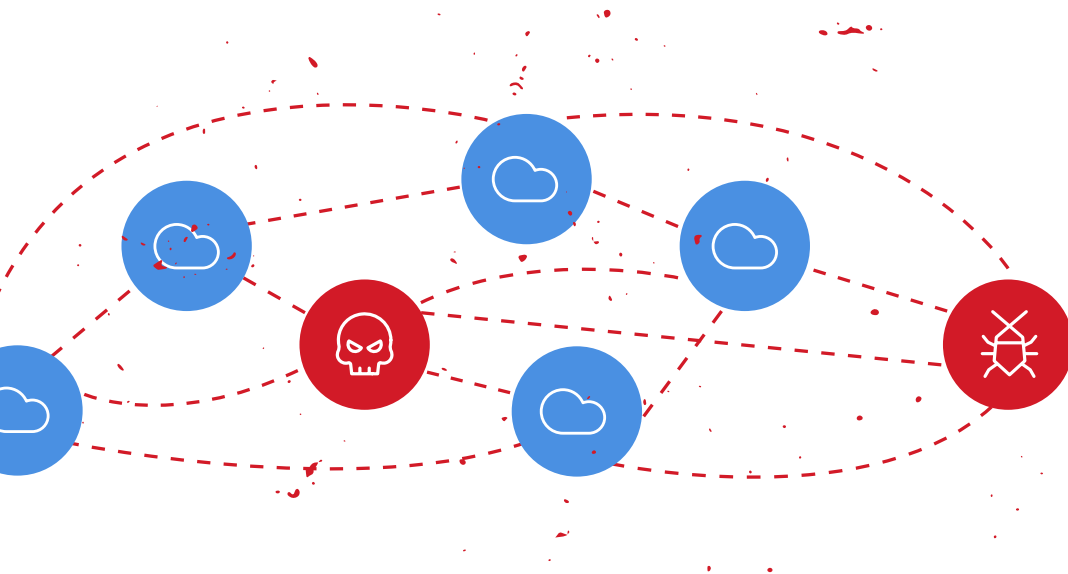
A **leading manufacturer** in the automotive industry had been hit by back-to-back ransomware attacks, which drove home the need for modern cybersecurity solutions. After gaining the ability to visualize user activity on-prem and in Microsoft 365, the company identified and disabled more than 500 stale users, and reduced Microsoft 365 groups from 280 to 31.

State of cloud security

Cloud applications and services create a broad, interconnected attack surface that can be compromised in new ways by insiders and external actors. Attacks have become highly effective and impactful. State-sponsored actors have become more sophisticated, and their techniques are already spilling into the commercial space, as they have many times before.

The cloud unlocks tremendous value for organizations. But along with convenience and collaboration, the cloud makes it much harder to spot threats. Every endpoint serves as an access point — an on-ramp to digital environments with critical and sensitive data. And SaaS applications are often the biggest blind spots for organizations looking to defend their data.

The availability of exploits and chances of a big payout from victims means that attackers will not quit. Any system, account, or person can be a potential attack vector at any time. With such a vast attack surface, you need to assume attackers will breach at least one vector — if they haven't done so already.



Cloud data security checklist

✓ Understand and reduce your SaaS blast radius.

If an attacker compromised a user, what would the potential damage be? Reducing your cloud blast radius — everything an attacker can access with just one compromised account or system — before an attack makes the cybercriminal's job more difficult.

✓ Watch for unusual activity across your cloud environment.

Attackers are more likely to trigger alerts if they must jump through more hoops to access your sensitive data. Keep an eye on user activity and watch for anomalies and out-of-policy activity.

✓ Adopt a Zero-Trust approach.

Zero Trust is likely your best defense against data-related attacks such as ransomware. No person, application, or system should be able to access or do more than they need. Restrict access to systems, applications, and data — especially sensitive data.

✓ Check your SaaS application settings.

It only takes one misconfiguration to expose sensitive data. If your configurations aren't perfect, you can open your applications — and data — to massive risk. Re-check settings to ensure updates do not leave data exposed, restrict sharing outside your organization, and audit cloud-sharing configuration settings.

✓ Enable MFA for all your employees.

This simple step is critical yet frequently overlooked. Enable MFA across cloud apps and services and for service/admin accounts. Make MFA mandatory and don't allow users to opt-out. Too many organizations allow single-factor authentication on internet-facing services.

✓ Set up and enforce processes for off-boarding users.

As companies adopt more SaaS apps and services, the odds of ghost users — active but unused accounts — increase. Be sure to revoke permissions across your cloud services whenever employees or contractors leave the company.

✓ Find the balance between productivity and security.

SaaS apps are often more valuable when integrated, but interconnectivity via APIs can make it easy for attackers to move laterally. Watch for misconfigurations and ensure you have a proper cloud security posture.

✓ Put your data first.

Instead of starting from the outside with endpoints and vectors, it's far more practical to protect your large, centralized repositories first — and work from the inside out.

Recommendations

Once you “assume breach,” think about where an attacker would most likely navigate to if they wanted to maximize their profits. If your organization is like most, that’s straight toward your biggest critical data stores. Your mission is to make your blast radius as small as possible so that users can only access what they need, and you can detect unusual access that could indicate an attack is underway.

Every extra step you force an attacker or insider to take slows them down and gives you an opportunity to detect and thwart an attack.

Suppose a cyberattack or malicious insider hits your organization. In that case, you’re already dangerously behind if you can’t see instantly what a compromised user could have taken — or did take — across your SaaS applications and services.

Starting with a data-first approach is crucial.

Ask yourself these critical questions:

1. Do you know **where your important data is stored?**
2. Do you know **that only the right people have access to it?**
3. Do you know **that they’re using it correctly?**

These three questions frame the three dimensions of data protection — importance, accessibility, and usage. To make meaningful decisions and improve your risk posture, you must see where critical data is concentrated and exposed (at risk), and who is using it or not (stale).

Put your data first. Instead of starting from the outside with endpoints and vectors, it’s far more practical to protect your large, centralized repositories first — and work from the inside out.

Case study

A real estate company secures Salesforce with Varonis.

A top real estate organization adopted DatAdvantage Cloud to protect sensitive data in their most relied-upon SaaS apps, including Salesforce. Thanks to better visibility and high-fidelity alerts that integrate seamlessly with existing security solutions, the organization decreased containment and response times and gained peace of mind knowing their data was protected.

“We can easily run reports and see who has super-admin rights or admin rights and where they overlap. The cross-cloud visibility is where DatAdvantage Cloud comes in extremely handy because trying to do that manually is nearly impossible. It would be a crazy, massive spider web, and you would definitely miss something.”

Tony Hamil, U.S. Real Estate Company

[Read the case study](#)



amazon
S3

GitHub

okta

box



salesforce

zoom

aws



Want to see if your cloud data is exposed?

Get a free Varonis Cloud Data Risk Assessment. Uncover hidden risks to your most important data fast, and without adding work to your plate.

[Get your risk assessment](#)

About Varonis

Varonis is a pioneer in data security and analytics, specializing in software for data protection, threat detection and response, and compliance. Varonis protects enterprise data by analyzing data activity, perimeter telemetry, and user behavior; prevents disaster by locking down sensitive data; and efficiently sustains a secure state with automation.

