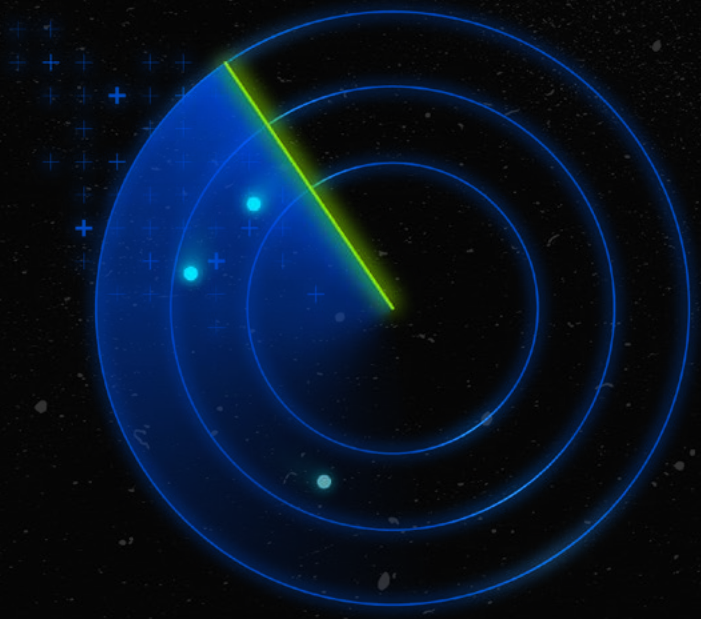
VARONIS

DSPM Snapshot

Four Key Findings From Hundreds of Data Security Posture Assessments



The evolution of DSPM

Data security posture management (DSPM) provides visibility into your data — where sensitive data is located, who has access to it, how it's being used, and where it could be exposed. Although not a new concept, DSPM has risen in popularity due to many organizations moving to the cloud and the complexities of securing data that come with it.

While the cloud helps organizations collaborate, it also presents unique data security challenges. A morass of confusing permission settings, overshared sensitive data, vulnerable stale accounts, and misconfigured settings widen the blast radius to a potential attack — which is already growing faster than security teams can keep up with.

The truth is that most organizations still need to secure data both in the cloud and on-prem. Your DSPM solution needs to go beyond visibility to fix the problems it surfaces and continuously monitor for threats — wherever your sensitive data lives.

To assess the true state of data security within hybrid cloud environments, Varonis analyzed 15 billion files and more than one billion folders by reviewing 180,000 accounts from over 300 organizations.

Take a look as we explore the current state of DSPM and shed light on how data is at risk.

What we found:

- **Almost 50% of files shared with all users contain sensitive information.** Threat actors could access sensitive information almost half of the time by compromising one account.
- **35% of stale accounts still have active permissions.** These ghost users haunt networks, giving attackers a path inside.
- **Nearly one-third of permissions for sensitive data are stale.** Employees have way more access than they need to do their jobs.
- **60% of admin accounts, on average, do not have multifactor authentication (MFA) enabled.** Admin accounts without MFA are prized targets for attackers.

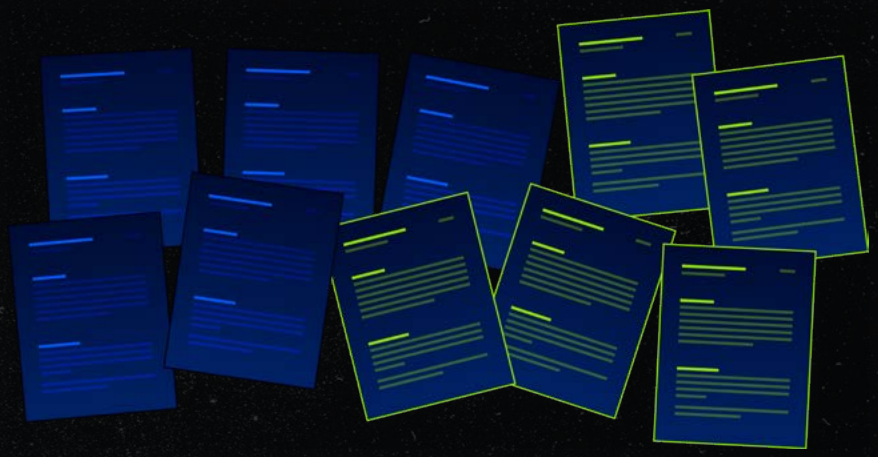
The expanding blast radius

The “click to share” option is one of the most helpful new tech features for businesses, whether used in social media, sales, or for other workplace efficiencies. Yet this one-click convenience creates a problem with oversharing information, leaving a massive, growing blast radius in its wake that weakens your data security posture.

All it takes is one valid set of stolen credentials, and a hacker can access everything a user can.

IN THE AVERAGE ORGANIZATION:

Almost 50% of files shared with all users contain sensitive information.



WHY THIS IS A CRISIS WAITING TO HAPPEN

When users have access to files — especially sensitive files — that they don’t need, it opens up pathways to data that hackers can exploit. At the average organization, all it would take is compromising one user for the hacker to have a high chance of finding sensitive data in files shared with the compromised user.

Despite the dangers of password reuse, **52% of people use the same password** across multiple sites. Meanwhile, half of the files shared with all users contain sensitive data. That means a compromised password could have a one in four chance of providing access to sensitive data.

HERE’S WHAT YOU CAN DO:

The best way to reduce risks from oversharing links is to limit access to only those who truly need it. Having an activity audit trail also helps identify stale data or access that could unintentionally expand the blast radius further.

Ghost users: A hidden risk haunting your data

Ghost users are accounts that belong to employees or vendors who are no longer with the organization. When old accounts retain access to corporate assets, it creates an unnecessary risk and increases the likelihood of threat actors accessing your environment.

IN THE AVERAGE ORGANIZATION:

35% of ghost users are still enabled.

WHY THIS IS A CRISIS WAITING TO HAPPEN

Old accounts are easier to compromise because they're usually unmonitored, providing attackers more opportunities to crack credentials.

Ghost users with access to applications and data allow attackers to quietly attempt a brute-force attack without tripping alarms.

HERE'S WHAT YOU CAN DO:

Routine cyber hygiene, such as disabling user accounts immediately after employees and contractors leave the organization, drastically reduces a company's cyber risk.

Set up and enforce processes for off-boarding users at your organization. The growing adoption of SaaS apps and services increases the odds of ghost users. Revoke permissions across your cloud services whenever employees or contractors leave the company.

The problems of stale data and outdated access

Individuals and teams alike are constantly creating new information and sharing it broadly.

Unfortunately, failing to delete and archive data and remove access after a project is complete increases the likelihood of a breach. Even moving stale data to a long-term storage solution rather than deleting it can significantly reduce risk and associated costs.

IN THE AVERAGE ORGANIZATION:

Nearly one-third of permissions for sensitive data are stale.

WHY THIS IS A CRISIS WAITING TO HAPPEN

Stale and outdated access weighs down a company's cybersecurity posture while providing low-effort fodder for threat actors. Numerous high-profile data breaches in recent years have involved attackers abusing a company's stale permissions.

HERE'S WHAT YOU CAN DO:

Automated least privilege can reduce and remove stale privileges, preventing compromised accounts from giving threat actors easy access to sensitive data.

Susceptible: Unprotected administrative accounts

Accounts missing basic security controls like MFA — including rogue admin accounts — are easier to infiltrate. Attackers can breach SaaS apps and steal internally exposed data. MFA adds an extra layer of security to user accounts, making it far more difficult for attackers to gain access, even if they have your password.

IN THE AVERAGE ORGANIZATION:

60% of accounts with admin-level permissions do not have MFA enabled.

WHY THIS IS A CRISIS WAITING TO HAPPEN

Without MFA enabled, attackers have a straightforward path to compromise an organization.

Cybercriminal groups like EvilProxy, LAPSUS$, and others often use stolen credentials to access victims' networks. **According to Zippia,** MFA can help prevent 99% of automated cyberattacks and up to 76% of targeted cyberattacks.

HERE'S WHAT YOU CAN DO:

Enable MFA across your company's cloud apps and services, especially your service/admin accounts.

Make MFA mandatory and don't give users the option to opt out. This simple step is critical, yet frequently overlooked; too many organizations allow single-factor authentication on internet-facing services.

Improving your data security posture

Organizations are leaving a strong data security posture on the table by not automating or incorporating business processes and cybersecurity best practices.

The threats listed in this report are not complicated vulnerabilities; they are all within an organization's control. Varonis is the No. 1 rated DSPM in **Gartner Peer Insights** because it is the only solution that automatically remediates risk, enforces policies, and detects threats in real time.

Don't settle for partial visibility and a lack of results. Embrace proper security operations and empower your team with automated outcomes to protect sensitive data and reduce cyber risks.

ABOUT VARONIS

Varonis is a leader in data security, fighting a different battle than conventional cybersecurity companies. Our cloud-native Data Security Platform continuously discovers and classifies critical data, removes exposures, and detects advanced threats with AI-powered automation.

Thousands of organizations worldwide trust Varonis to defend their data wherever it lives — across SaaS, IaaS, and hybrid cloud environments. Customers use Varonis to automate a wide range of security outcomes, including data security posture management (DSPM), data classification, data access governance (DAG), data detection and response (DDR), data loss prevention (DLP), and insider risk management.

Varonis protects data first, not last. Learn more at **www.varonis.com.**