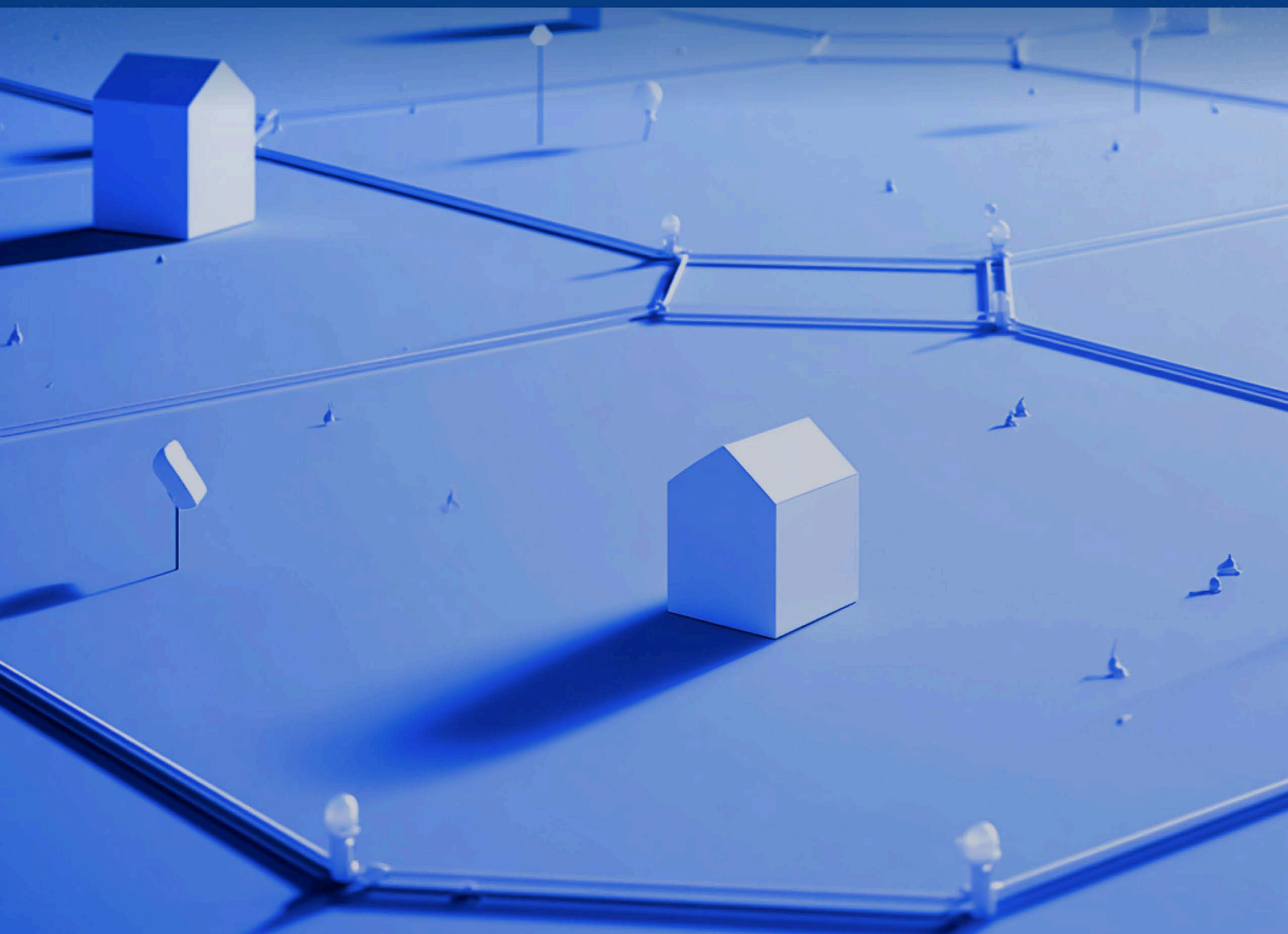
eSHARE

The Threat Hiding in Plain Sight:

Sanctioned External Sharing as Attack Surface



Introduction

For the past decade, most CISOs and their teams have organized data protection strategies around four threat scenarios: intentional insider theft, internal mishandling, third-party mishandling, and external theft. These categories shaped security investments, including DLP for insiders, access controls for errors, vendor risk programs for third parties, and perimeter defenses against attackers.

But there's a fifth scenario that's been hiding in plain sight the entire time. It's not new; email attachments have been flowing to external recipients for decades. It's not invisible; every CISO knows users share files with partners, suppliers, and contractors daily. And it's not unaddressed; DLP tools flag high-risk behaviors, and policies prohibit unauthorized disclosure.

Yet despite all this awareness, sensitive data has been leaving organizations in a slow, steady bleed for years. And while security teams were drawn to higher-visibility initiatives, including cloud-native application protection (CNAPP), data security posture management (DSPM), and SaaS security posture management (SSPM), this bleed continues to metastasize. What was once a single channel (email) fragmented into Teams guest access, SharePoint external links, OneDrive shares, and shadow IT tools. The volume didn't decrease. The visibility didn't improve. The controls didn't scale.

This is Sanctioned External Sharing as Attack Surface: the authorized, everyday collaboration that creates continuous exposure because governance ends the moment data leaves the enterprise environment.

Why the "Slow Bleed" Has Been Deprioritized

This isn't a failure of security competence or oversight. Security leaders have known about external sharing risks for years. But three self-reinforcing forces kept it in the "important but not urgent" category.

Inbound Threats Scream, Outbound Risks Whisper

Ransomware encrypts databases. Phishing triggers credential compromise alerts. These create immediate crises with C-level visibility, emergency response protocols, and clear metrics (i.e., systems down, operations halted).

In contrast, a finance team sharing a pricing model with a partner doesn't trigger alarms. An engineer emailing CAD files to a supplier doesn't generate SOC tickets. External sharing is silent; it requires DLP analytics, manual investigation, and cross-platform correlation to detect. By the time organizations notice, the damage occurred weeks or months earlier.

Industry research consistently shows that external actors remain the predominant source of data breaches, naturally focusing CISO attention on perimeter defenses and endpoint detection. Outbound data governance gets classified as "chronic risk" rather than "active threat."

The "Shinier Object" Budget Trap

Over the past five years, security budgets gravitated toward posture management platforms, such as CNAPP for cloud security, DSPM for data security, SSPM for SaaS security. These tools promised unified visibility, automated compliance, and board-ready dashboards.

And they delivered real value: misconfigured S3 buckets, shadow SaaS apps, overprivileged identities. But here's what they don’t address: what happens to data after users intentionally share it through approved channels.

DSPM discovers "confidential file shared with 47 external users." Excellent. Now what? The file has been downloaded to external laptops, forwarded to colleagues, uploaded to their OneDrive, possibly fed into ChatGPT for analysis. DSPM found the problem. But it can't revoke access to downloaded files, expire shares retroactively, or audit what external recipients did with the data.

Security teams invested in discovering risks they couldn't fully remediate, while the slow bleed of authorized external sharing continued unabated.

The User Experience Paradox

CISOs have been conditioned to avoid controls that require user behavior change. When security creates friction, such as complex password policies, restrictive application whitelisting, the result is predictable: helpdesk floods, executive complaints, shadow IT adoption.

Research on insider threat programs consistently identifies productivity concerns as the primary barrier to implementing stronger data exfiltration controls. The fear is users will route around security obstacles, creating even less visibility than before.

So external sharing remained "managed through policy" - security awareness training, NDAs, acceptable use policies. These create the appearance of control without the friction of enforcement. Meanwhile, users keep doing what they've always done: attaching files to emails, creating "anyone with the link" SharePoint shares, adding guest accounts to Teams channels.

The slow bleed continues because stopping it requires choosing between security and business velocity.

Why "Now" Is Different

Three fundamental shifts have transformed external sharing from a "slow bleed" into a strategic imperative that demands immediate action.

Platform Proliferation Turned One Channel Into Ten

When external sharing meant email attachments, security teams at least had a single channel to monitor. DLP could scan outbound mail. Policies could require encryption. Audits could review email logs.

Today, that channel fragments across Teams guest access granting external users access to entire channel histories, SharePoint "anyone with the link" shares with no expiration, OneDrive personal sharing bypassing enterprise controls, shadow IT tools adopted when enterprise platforms prove too restrictive, and AI agents autonomously exchanging data during procurement workflows.

The diagnostic question most organizations can't answer: "How many external shares occurred across all channels last month?"

The slow bleed doesn’t stop; it metastasizes across a dozen unmonitored pathways while total volume increased.

AI Agent Autonomy Will Multiply Velocity 10-100x

At the 2025 Gartner IT Symposium, analysts predicted that 90% of B2B buying, representing over $15 trillion in transactions, will be AI agent-intermediated by 2028. Consider procurement: today, a human specialist requests quotes and negotiates terms with security review opportunities at each step. By 2028, an AI procurement agent does this autonomously, sharing budget parameters, technical requirements, and internal constraints with vendor AI sales agents; all this at machine speed, potentially thousands of times per day, with minimal human oversight.

Recent research on AI-related security incidents reveals that the vast majority of organizations experiencing these incidents lack adequate AI access controls and governance policies. This could represent a 10-100x multiplication of external data sharing velocity operating on today's governance foundations, or more accurately, the lack thereof.

Regulatory Evolution Ended the "NDA and Trust" Era

Regulatory frameworks have evolved from "implement reasonable security measures" to "demonstrate continuous control over external data flows." GDPR fines reach €20 million or 4% of global revenue for failing to protect personal data transfers. CMMC 2.0 requires defense contractors to technically control CUI shared with vendors; NDAs aren't enough. EU GMP Annex 11 demands data integrity controls throughout the data lifecycle, not just within enterprise boundaries.

This requires a shift from retroactive breach notification to preemptive data governance.

What This Looks Like in Practice

This isn't hypothetical. The slow bleed manifests daily in ways that bypass almost every control CISOs have implemented.

A clinical research organization receives patient data via SharePoint for a trial. Protocol requires deletion post-analysis. But the files were downloaded to local drives, backed up to personal cloud storage, and retained on ex-employee laptops. No technical control enforced the deletion requirement, only an NDA that can't be technically verified.

An aerospace supplier receives technical drawings via Teams guest access. CMMC 2.0 requires the prime contractor to demonstrate continuous control over CUI. But once downloaded, the supplier can forward to sub-tier vendors, upload to ChatGPT for analysis, or retain indefinitely. The prime contractor has authentication logs but no post-share governance.

A partner firm receives M&A due diligence materials via OneDrive link. Deal terms change and access should be revoked. But the link was set to "anyone with the link" with no expiration. Even if the link is disabled, previously downloaded files remain on partner systems with no audit trail of what happened to them.

In each case, note what didn't fail: DLP didn't fail (the sharing was authorized). CASB didn't fail (approved platforms were used). Access management didn't fail (guest accounts were properly provisioned). Email gateway didn't fail (attachments were scanned).

What failed was the assumption that governance ends when the share occurs. Every control stopped at the environment boundary. What happened after download? No visibility. No control. No audit trail.

The Path Forward

The posture management platforms security teams invested in over the past five years weren't designed to solve this problem. CNAPP and CSPM secures cloud infrastructure configurations, not data flows post-share. DSPM discovers sensitive data exposure but can't revoke access to already-downloaded files. SSPM governs SaaS application settings, not what external recipients do with shared data.

These are valuable tools. But they share a critical limitation: they end where the environment ends. Once data crosses the boundary through an authorized share, visibility and control disappear.

Addressing Sanctioned External Sharing as Attack Surface requires a new control category: post-share data governance. This isn't about replacing existing tools, it's about extending their reach to the moment after authorized sharing occurs.

Key capabilities needed include persistent controls that restrict downloads, unified visibility across all external sharing channels, recipient activity monitoring, automated policy enforcement based on data classification, and comprehensive audit trails for regulatory compliance.

Security teams should be able to answer these questions:

- How many external shares occurred last month across email, Teams, SharePoint, OneDrive, and shadow IT?
- Which shares contain data classified as confidential or regulated?
- Can the organization restrict downloads by external recipients?
- Are there audit trails proving what external recipients did with shared data?
- If a partner uploads organizational data to ChatGPT tomorrow, will the security team know?

When the answer is "no," organizations are still experiencing the slow bleed; and it's accelerating. The question isn't whether to address Sanctioned External Sharing as Attack Surface. It's whether organizations will do so proactively, or wait for a breach, audit finding, or regulatory action to force visibility.

Mike Towers

Chief Strategy & Trust Officer

The Threat Hiding in Plain Sight: Sanctioned External Sharing as Attack Surface

eSHARE

About eSHARE

Get in touch to weave your Trusted Collaboration Fabric. eSHARE secures every share while teams move faster with intelligent, Zero-Trust guardrails.

LinkedIn

Contact Us

www.eshare.com