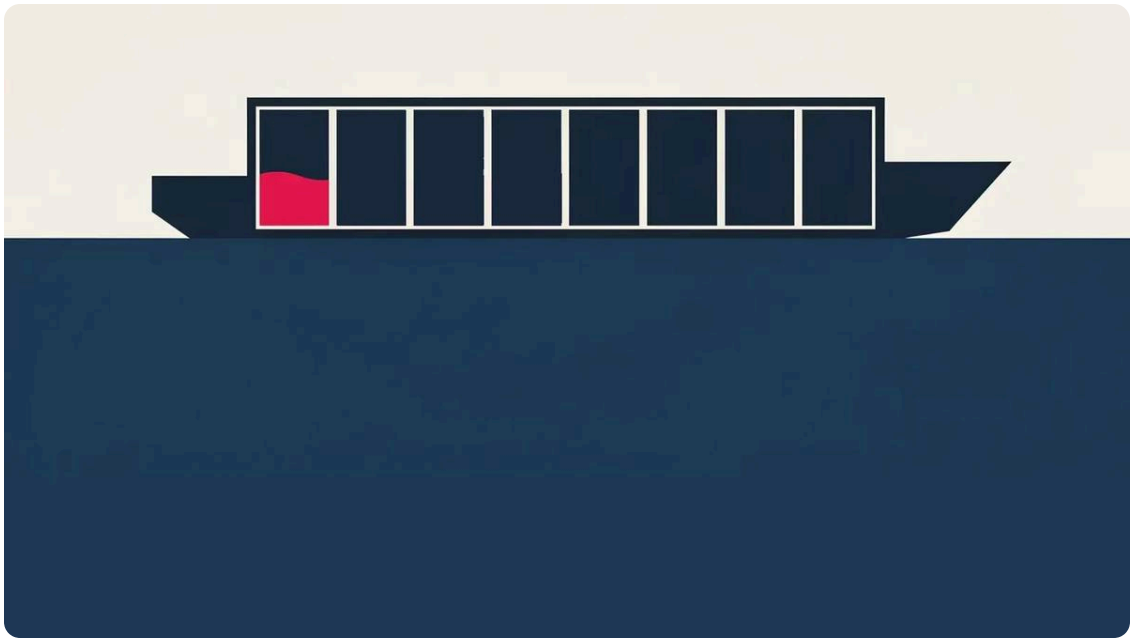
FUSION COMPUTING FIELD GUIDE

Data Security Posture Management: Limit the Blast Radius, Then Prove It

Mike Pearlstein, CISSP

November 11, 2026



WHAT'S INSIDE

1. Why does data security posture matter when exploits arrive before the patch?
2. What is data security posture management (DSPM)?
3. Why is blast radius the number that matters?
4. What can a small business do in Microsoft 365 today?
5. How do you limit the blast radius in Microsoft 365?
6. How do you prove your data security posture to an insurer, auditor or board?
7. Who helps Canadian SMBs with data security posture on Microsoft 365?
8. Posture is the part you control
9. Frequently Asked Questions

© 2026 Fusion Computing

Ask a small business how secure it is and you usually get a list of finished jobs. Updates install on a schedule. Multi-factor sign-in is on. The cyber-insurance renewal went through in the spring.

That list rests on an assumption: that the business gets to fix a flaw before anyone uses it. In 2026 that assumption is gone. Attackers now reach many vulnerabilities on or before the day a fix ships, and some reach them days earlier.

I lead Fusion Computing, a CISSP-led managed IT and cybersecurity firm founded in 2012, and my view is simple. When the race to patch is lost before it starts, measure something else: what an attacker can reach once they are in. Shrink it, and keep the proof. That discipline has a name: data security posture management.

Key Takeaways

- Mandiant estimates the mean time to exploit at minus seven days in its M-Trends 2026 report, down from 63 days in 2018 and 2019 (Mandiant, 2026).
- Data security posture management (DSPM) finds where sensitive data lives, who can reach it and how it is shared, then keeps a dated record.
- Blast radius, the data one compromised account can open, is the exposure a business controls before an attack starts.
- Microsoft 365 Business Premium includes sensitivity labels and Purview Data Loss Prevention; Microsoft lists E5 or the Purview Suite for DSPM (classic).
- Proof means dated evidence, such as sharing reports, label coverage, admin lists and a breach record kept for 24 months from the day you determine a breach occurred, under PIPEDA.

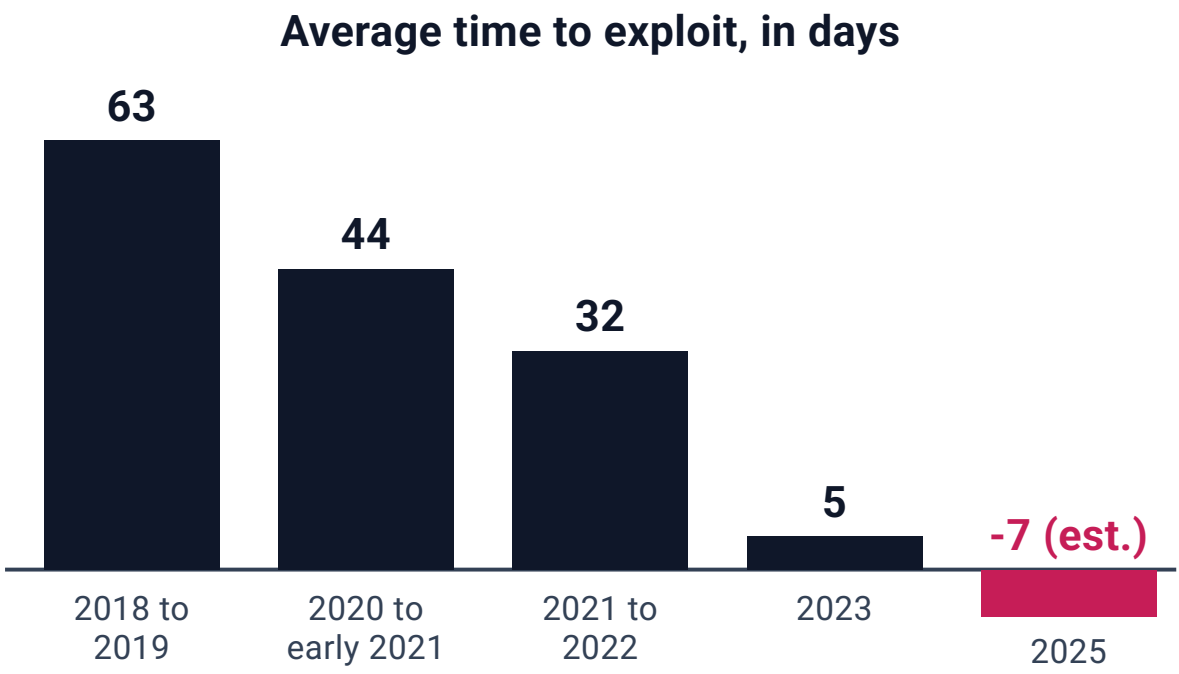
Why does data security posture matter when exploits arrive before the patch?

> Data security posture matters because exploitation now routinely starts before a patch exists. Mandiant's M-Trends 2026 report estimates the mean time to exploit at minus seven days, down from 63 days in 2018 and 2019. Once that window is gone, the damage depends on how much data one compromised account can open.

Book a Consultation

Mandiant measured an average time to exploit of 63 days in 2018 and 2019, 44 days from 2020 into early 2021, 32 days across 2021 and 2022, and 5 days in 2023 (Mandiant, 2024).

Its M-Trends 2026 report puts the 2025 figure at an estimated minus seven days. The report describes that as exploitation "routinely occurring before a patch is even released."



Sources: Mandiant, Analysis of 2023 Time-to-Exploit Trends (2024); Mandiant, M-Trends 2026 (mean, estimated).

Mandiant's average time to exploit, from its 2024 analysis and M-Trends 2026. A negative figure means exploitation began before the fix was published.

The same report says the hand-off from the group that breaks in to the group that runs the ransomware fell from more than 8 hours in 2022 to a median of 22 seconds in 2025. Exploits were the most common way in for the sixth year running, at 32% of the intrusions investigated.

Volume is climbing too. Google's Threat Intelligence Group counted 5,045 vulnerability disclosures in January 2026 and 10,477 in July. Exploited vulnerabilities rose from an average of 10.5 a month in 2025 to 18 a month in 2026 (GTIG, 2026).

Exactly half of the flaws GTIG attributes to AI discovery allow remote code execution. Across all published flaws, the share is 26%.

Where the counterweight fits

Keep the hype in proportion. GTIG calls the AI finding an early indicator, and only 0.23% of 2026 disclosures were seen exploited. VulnCheck found that 14 of 1,061 AI-assisted discoveries, or 1.3%, had been exploited (VulnCheck, 2026).

The flaws that do get used still arrive fast. In the first half of 2026, VulnCheck found 23.43% of exploited flaws were attacked on or before the day they were published.

Book a call to map what one phished account reaches in your tenant →

I read those numbers as one instruction for a firm on Microsoft 365. Keep Windows, browsers and firewall firmware on automatic updates, and plan for at least one flaw to be used against you before its fix ships. What that flaw reaches depends on your posture.

What is data security posture management (DSPM)?

> Data security posture management (DSPM) is the ongoing practice of finding where sensitive data lives, who and what can reach it, and how it is labelled, shared and used, including by AI tools. A DSPM programme closes the gaps it finds and keeps a dated record, so the business can show its posture on any day.

Most security tools watch doors and devices. DSPM starts from your data and works outward, and I like it as a frame for that reason: it begins with the thing an attacker wants. It answers four questions most small businesses never write down:

1. Where are the sensitive files, mailboxes and records: client files, payroll, Social Insurance Numbers, health numbers, card numbers?
2. Which people, guests, apps and AI assistants can open each of them?

3. How are they labelled, shared and copied, inside and outside the company?
4. Has any of that changed since the last review, and who signed off on the change?

The first question has a geographic half. A data-residency map records which country holds each copy, including backups and any AI service that reads your data.

Under PIPEDA's accountability principle, you remain responsible for personal information you transfer to a third party for processing, according to the Office of the Privacy Commissioner. A cloud or AI vendor counts, so the map belongs in the inventory.

How does DSPM differ from CSPM and DLP?

The three acronyms overlap in vendor marketing. In practice each one asks its own question:

Discipline	The question it answers	Typical finding
DSPM (data security posture management)	Where is sensitive data, and who can reach it?	A payroll folder open to every staff member
CSPM (cloud security posture management)	Are cloud services configured safely?	A storage account reachable from the internet
DLP (data loss prevention)	Is sensitive data leaving right now?	An email carrying ten Social Insurance Numbers to a personal address

DLP acts in the moment. DSPM shows where DLP should point, and how big the problem is before anything moves. For a 30-person firm on Microsoft 365, both live in the same portal: Microsoft Purview. For the wider obligations, see our guide to data security and compliance.

Why is blast radius the number that matters?

> Blast radius is the amount of data and the number of systems that one compromised account or device can reach. It is the exposure a business controls before an attack begins. Patch timing depends on software vendors. Who can open which files is a setting you own today and can change this week.

Every intrusion starts with one foothold. In Mandiant's 2025 investigations the most common were exploited flaws, at 32%, and voice phishing, at 11%. From there the attacker inherits whatever that identity can open. An account that can read everything puts all of that data within reach.

> **Illustration.** Assume a firm runs 12 SharePoint sites, and nine of them grant access to every staff member through the built-in "Everyone except external users" group. One phished account opens 9 of 12 sites, or 75%. Scope each site to its team, and the same account opens the 2 sites its owner works in, or 17%.

The illustration uses round numbers. On your own tenant, count the sites one account can open as a first exposure measure, then check its file shares, mailbox access and apps. Repeat it for an admin account and the number is usually far worse.

Admin accounts sit at the top of the checklist below. If I could change one tenant setting first, it would be the default sharing link. The same idea sits under zero trust security: assume a breach, then make the breach small.

AI assistants raise the stakes. Microsoft 365 Copilot answers from whatever the signed-in user can open, so an over-shared tenant becomes an over-shared assistant. Our post on Microsoft 365 Copilot oversharing covers the Copilot-specific steps.

What can a small business do in Microsoft 365 today?

> A small business on Microsoft 365 Business Premium already owns sensitivity labels and Microsoft Purview Data Loss Prevention, enough for most of the first year of posture work. For Purview DSPM (classic), Microsoft lists Microsoft 365 E5 or the Microsoft Purview Suite; confirm the current version separately. Most firms start with the controls they pay for and add DSPM later.

Microsoft lists sensitivity labels, Purview Data Loss Prevention and Purview Message Encryption among the information protection capabilities in Business Premium. With them your staff can label sensitive files and emails, and you can warn or block on Canadian identifiers and encrypt messages.

The DSPM dashboard is a licence step up. Microsoft's getting-started page for DSPM (classic) names Microsoft 365 E5 or the Microsoft Purview Suite, formerly Microsoft 365 E5 Compliance (Microsoft Learn).

The current version of DSPM points to the Purview service description for licensing. Confirm your plan there before you budget for it.

I would buy the dashboard last. A dashboard shows you the over-shared folders, and the sharing settings and site permissions that fix them are already in Business Premium. Add the continuous measurement once the basics hold.

How do you limit the blast radius in Microsoft 365?

> Limiting the blast radius in Microsoft 365 means shrinking what each identity can reach, in order of risk. Admin accounts come first, then open sites and default sharing links, then labels and data loss prevention on the sensitive locations. Most steps are settings a Business Premium tenant already has, and each can be checked and dated.

Fusion Computing recommends working through the list in this order, because each step makes the next one smaller:

1. **Write the inventory.** List on one page which sites, mailboxes and shares hold client files, payroll, Social Insurance Numbers, health numbers and card numbers, and which country each sits in.
2. **Separate the admin accounts.** Give administrators a second account used only for admin work, with the smallest role that does the job. The Canadian Centre for Cyber Security baseline asks for exactly this under its access control and authorization measures.
3. **Change the default sharing link.** In the SharePoint admin centre, under Policies and then Sharing, set the default link type to “Specific people” so a quick share opens the file to the named recipients only.
4. **Close the open sites.** Remove “Everyone except external users” from sites meant for one team, and grant access through that team’s membership.
5. **Label sensitive files and emails.** Publish a short label set and have staff apply it, starting with client and payroll records from the step 1 inventory.
6. **Turn on data loss prevention.** Start from Microsoft’s Canada PIPEDA template, which covers Social Insurance Numbers, health service numbers, bank accounts and passports. Run it in test mode for two weeks before it blocks anything.
7. **Review guests every quarter.** Remove guest accounts and external shares nobody can explain.
8. **Decide where AI may read.** Finish steps 3 and 4 before any assistant indexes the tenant.

Each step needs an owner and a date, and the software is already in the tenant. For a wider list of controls to check, see our cybersecurity assessment checklist.

Get a second opinion on your Microsoft 365 sharing and admin settings →

Data security advice from Fusion Computing

CISSP-led, securing IT for Canadian SMBs across Toronto, Hamilton, and Metro Vancouver since 2012.

How do you prove your data security posture to an insurer, auditor or board?

Proving data security posture means keeping dated evidence a reviewer can check, such as sharing reports, label coverage, admin role lists and a breach register. Insurers, auditors and boards weigh records over statements. Under PIPEDA, you must keep a record of every breach of security safeguards for 24 months from the day you determine it occurred, reportable or not.

The breach rule comes from the Office of the Privacy Commissioner of Canada, which can ask to see your records. Each one should show the date, what happened, what information was involved and whether it was reported.

Small businesses are covered where PIPEDA applies; Quebec, Alberta and British Columbia have their own private-sector privacy laws. The 24-month rule is in section 6 of the Breach of Security Safeguards Regulations.

I count a breach register as posture evidence too, because it shows you noticed.

For the controls themselves, I would map your evidence to a standard someone outside the company recognizes. CIS Control 3, Data Protection, asks for processes to identify, classify, handle, retain and dispose of data. CIS Control 6 covers access control management.

The Canadian Centre for Cyber Security's baseline controls for small and medium organizations cover the same ground in control 3.12, access control and authorization.

What you claim	Evidence to keep	How often
Only the right people open client files	Site permission export and sharing report, dated	Quarterly
Sensitive files are labelled	Label coverage on files and emails in the inventory locations	Quarterly
Admin access is minimal	Admin role list with each holder's sign-off	Quarterly and at every staff change
Guests are reviewed	Guest list with removal dates	Quarterly
Every breach is recorded	Breach register: date, description, information involved, reported or not, and the reasoning	Each breach, kept 24 months from determination
Controls follow a standard	Mapping to CIS Controls 3 and 6 or the Canadian baseline 3.12	Annually

Microsoft notes that Purview DSPM pauses the processing that refreshes Microsoft 365 data when no admin has opened it for more than 60 days (Microsoft Learn). A posture nobody looks at stops being measured.

Want to know whether Business Premium covers your data posture work →

Insurers ask about these controls at renewal. Our page on cyber insurance requirements in Canada covers the questionnaire.

Who helps Canadian SMBs with data security posture on Microsoft 365?

> Canadian small businesses usually get data security posture work on Microsoft 365 from an internal administrator, a Microsoft partner on a fixed project, or a managed security provider that runs the controls as an ongoing service. Fusion Computing is a CISSP-led managed security provider for Canadian businesses with 10 to 150 employees, aligned to CIS Controls v8.1.

Whoever you pick, I would ask four questions, and I would ask them of us too. Will they tell you when Business Premium is enough? Will they leave you with dated evidence you own? Do they map the work to CIS Controls or the Canadian baseline? Who reviews your posture after the project ends?

Fusion Computing prices managed cybersecurity from CA$185 to CA$230+ per user per month, by scope, with its CIS-Aligned service at about CA$230. The seats include the Microsoft and Huntress security stack, with managed detection and response, identity threat detection, SIEM and posture management for identities and endpoints.

Fusion Computing scopes and quotes Microsoft Purview data protection work as a separate project, covering labels, data loss prevention and DSPM where your licence allows. The control packages are laid out in our CIS controls managed cybersecurity guide.

Posture is the part you control

Exploits will keep arriving before patches. How much one stolen account reaches, and the dated proof of it, are decisions you can make today. I would start with the admin accounts this week. To see where your controls stand now, try the cybersecurity assessment.

Talk to Fusion

Frequently Asked Questions

Q. What does DSPM stand for in Microsoft Purview?

DSPM stands for data security posture management. In Microsoft Purview it is the dashboard that finds unprotected sensitive data and risky user activity across Microsoft 365 and other connected sources, then recommends data loss prevention and insider risk policies. Microsoft runs a current version and a classic version, and says most new features will be added to the current version.

Q. What is the difference between DSPM and CSPM?

CSPM, cloud security posture management, checks whether cloud services are configured safely, such as a storage account left open to the internet. DSPM starts from the data and asks where sensitive information lives and who can reach it. A small business on Microsoft 365 usually needs the data view first, because its exposure sits in SharePoint, OneDrive, Teams and mailboxes.

Q. Is DSPM the same as data loss prevention?

The two work together. Data loss prevention watches for sensitive data leaving in the moment, such as an email carrying Social Insurance Numbers. DSPM maps where that data sits and who can open it, so you know where to point data loss prevention policies and how large the exposure is before anything moves. In Microsoft 365, both are managed in Microsoft Purview.

Q. Which Microsoft 365 licence includes Purview DSPM?

Microsoft documentation for DSPM (classic) names Microsoft 365 E5 or the Microsoft Purview Suite, formerly Microsoft 365 E5 Compliance. The current version of DSPM refers to the Microsoft Purview service description for licensing, so confirm your exact plan there. Microsoft 365 Business Premium includes sensitivity labels and Purview Data Loss Prevention, which cover much of the hands-on posture work.

Q. Can a small business improve its data security posture on Business Premium?

Yes. Business Premium includes sensitivity labels, Purview Data Loss Prevention and message encryption, and every tenant has the SharePoint sharing settings and site permissions that set blast radius. Separating admin accounts, changing the default sharing link to specific people, closing sites open to all staff and manually labelling sensitive files and emails all work on Business Premium. The DSPM dashboard can come later.

Q. What does blast radius mean in cybersecurity?

Blast radius is the amount of data and the number of systems one compromised account or device can reach. If a phished account can open every SharePoint site, every site is exposed. Limiting blast radius means giving each identity only the access its work needs, with admin accounts separated and kept to the smallest role that does the job.

Q. How often should a business review its data security posture?

A quarterly review suits most small businesses: sharing reports, label coverage, admin role lists and guest accounts, each saved with a date. Review admin access again whenever staff change. If you use Purview DSPM, open it at least monthly: Microsoft pauses its Microsoft 365 data updates after more than 60 days without an admin visit.

Put this guide to work

Fusion Computing is CISSP-led, securing Canadian businesses since 2012.

- Managed IT support; for work-stopping (P1) issues, we aim to respond within 15 minutes, 24/7
- Cybersecurity, managed detection and response, and compliance reviews
- Microsoft 365 management and licensing

Book a 30-minute scoping call

fusioncomputing.ca/contact-us · 416-566-2845
Toronto · Hamilton · Metro Vancouver