


Building a layered defence around Microsoft 365

Even Microsoft needs security partners. Why shouldn't you?





Microsoft 365 is built for productivity. Not complete protection.

Microsoft 365 is the backbone of modern business. It handles your email, files, chat, calendars, and authentication—often through a single set of credentials. That centrality is what makes it essential. It's also what makes it vulnerable.

Microsoft has invested heavily in security. Defender for Office 365, Conditional Access, built-in DLP, and now Copilot for Security offer real protection. But here's the uncomfortable truth: attackers are evolving faster than the platform.

According to Microsoft itself, over 300 million fraudulent sign-in attempts hit its cloud services every day. AI-enhanced phishing kits are being deployed in seconds. QR-code phish and token-hijacking campaigns are bypassing traditional filters. And while Microsoft blocks the known and obvious, it struggles with targeted, low-signal threats.

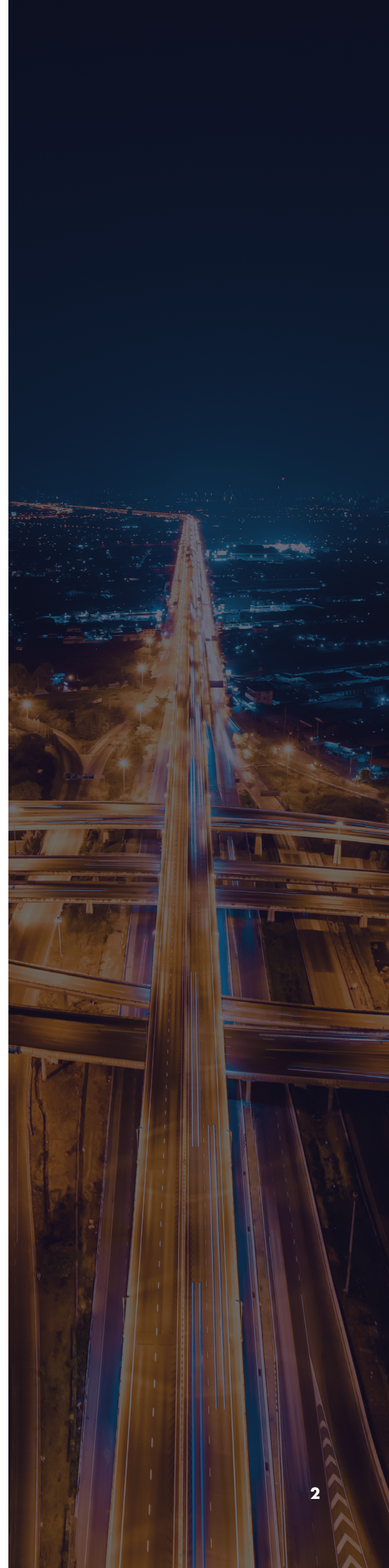
This isn't just theoretical.

- 94% of organisations were targeted by phishing in the past year (Gartner Magic Quadrant for Email Security, 2024)
- 36% of phishing emails now originate from legitimate cloud services like Microsoft, Google, Amazon (Darktrace Threat Report, 2024)
- 82% of breaches involve human interaction, not malware (Verizon DBIR, 2024)
- 1 in 5 phishing emails bypasses Microsoft's filters (Avanan, 2023)

Meanwhile, Microsoft's own roadmap tells the same story. In the past year alone it has:

- Partnered with Darktrace to extend behavioural defence
- Added Copilot for Security to triage response at scale
- Continued to push customers toward third-party archiving, analytics, and compliance add-ons

This isn't a failure of Microsoft. It's recognition that layered security is becoming the norm, even for Microsoft itself.



1. Where Microsoft 365 starts to slip

Secure-by-default is no longer enough.

Microsoft's native controls are improving. But modern attacks don't respect neat product boundaries. They cross between inboxes, cloud drives, browsers and identity layers, and they rely on one thing: users who think the tech already has it covered.

And that's the problem.

Most mid-sized IT teams assume that Defender blocks the bad stuff, Microsoft logs everything important, and data loss prevention is quietly running in the background. But once you look closer, cracks start to show:

- **Outbound threats are under-protected.**
Defender is built for inbound threats. There's limited visibility into what's leaving your environment – whether it's a compromised account, a misdirected email, or an unapproved file share.
- **Compliance is bolted on, not built in.**
Features like audit-ready archiving, legal hold, and granular discovery controls sit behind expensive add-ons or high-tier licences. Even then, they're complex to configure and slow to use under pressure.
- **Behavioural insight is shallow.**
Native Microsoft controls focus on signatures, rules and known tactics. Emerging threats – like QR phishing, token hijacking or mailbox manipulation – often fly under the radar until damage is done.
- **Risk is siloed.**
Microsoft splits its security layers across portals: Defender, Entra, Purview, Compliance Centre. Each has its own language, settings and learning curve. That slows down investigation and limits response when time matters most.



These aren't just theoretical gaps – they're the kind that get exploited in the real world. And they're exactly why Microsoft is pushing its own customers toward third-party behavioural analytics, layered threat detection, and more accessible compliance tooling.

“Microsoft's customers are facing an astounding 600 million attacks daily from both cybercriminals and nation-state actors.”

Microsoft, Digital Defence Report



2. The gaps that matter most

You can't fix everything. So fix what matters most.

Security doesn't break evenly. Some risks are more urgent, more damaging, and more often exploited – especially when you don't have enterprise-scale resources. Larger organisations might absorb the cost of sprawling security stacks, dedicated compliance teams, and niche threat detection tools. But for most mid-sized IT and security teams, that's not reality.

You're working with limited tools, fewer people, and a sharper focus on outcomes. That means your strategy has to be ruthless. Not in how much you cover, but in what you choose to cover first.

These are the areas that deserve focus – and the ones you can actually do something about today.



1. Monitor what's going out

Inbound protection is standard. But threats don't stop at the perimeter. Compromised users often operate undetected from inside your organisation – sending, forwarding or sharing sensitive content. And everyday human errors, like emailing the wrong recipient, remain the leading cause of reported breaches.

Focus your effort on:

- Visibility into outbound and internal traffic
- Detecting signs of account compromise or BEC
- Reducing the risk of misdirected or mishandled sensitive data

2. Catch risky user behaviour

Attackers aren't relying on malware anymore. They're relying on your users. Actions that seem normal – replying to a colleague, sharing a document, clicking a link – often aren't. Especially when those actions are manipulated, automated or subtly redirected.

Focus your effort on:

- Recognising behavioural anomalies (not just flagged threats)
- Detecting impersonation, tone-shift and trust-based exploitation
- Surfacing risks before they escalate into incidents

3. Get audit-ready

Whether it's a DSAR, an FOI request, or an internal investigation, the ability to search, recover and present email data under pressure is essential. Microsoft's built-in archiving and legal hold functions exist – but often behind complex configurations or licensing limitations.

Focus your effort on:

- Retaining all communications – inbound, outbound and internal
- Making historical search and discovery fast and reliable
- Enabling simple audit and legal workflows, without complexity

You can't fix every gap. But you can fix the ones that expose your people, data and reputation the most.

3. Microsoft gives you the foundation. We build on it.

Microsoft 365 delivers essential productivity and baseline protection. But when it comes to email security, behavioural insight and compliance readiness, native tools often fall short. Especially for organisations without enterprise licensing or dedicated security teams.

TrustLayer doesn't replace Microsoft. It strengthens it. Here's how the two compare when it comes to visibility, protection and control with email-centric risks:

Category	Microsoft 365 (Standard)	TrustLayer
Inbound threat protection	Built-in filtering (EOP), with Defender available in E5	Complements Microsoft's filtering with detection for advanced, emerging threats
Outbound email inspection	Scanning and policies available with Defender & Compliance	Extends outbound protection with simplified configuration and unified reporting
Email archiving	Litigation hold and retention (E3/E5)	Immutable, searchable archive with role-based access and support for DSAR, FOI and legal hold
User access to mail data	Recovery via Outlook or IT support. Limited visibility into historical events	Self-service email restore and audit timeline from Outlook add-in
Deployment	Requires tuning, Conditional Access configuration, and advanced setup	Wizard-based deployment for Microsoft 365 with no MX record changes
Cloud app data control	Microsoft Defender for Cloud Apps (E5) with complex setup	App discovery, shadow IT visibility, and inline controls with fast setup

4. What better protection actually looks like

You don't need more dashboards or more rules. You need visibility. Control. The confidence that when something slips through, you'll catch it – or better yet, stop it before it starts.

TrustLayer helps mid-sized IT and security teams cover the Microsoft 365 blind spots that matter most, without throwing headcount, licences or months of setup at the problem. Here's what that looks like in practice:

Catch what Microsoft misses

Attackers know exactly how Microsoft filters work – and how to get around them. With TrustLayer, you add behavioural signals and modern threat detection that stop payload-less phishing, reply-chain impersonation, QR-code scams and other techniques that fly under the radar of EOP and Defender.

“Microsoft does a lot, but it's not built for what the mid-market is seeing now – AI-generated phish, shadow access, insider stuff. TrustLayer gives the additional support with ”
– Security lead, financial services firm (500 seats)

Stop risk from spreading

Threats don't end at the inbox. Compromised accounts, misaddressed emails, and unsanctioned app use all lead to data exfiltration, and they're harder to catch. TrustLayer inspects outbound and internal traffic too, with policies that flag the unusual and prevent the avoidable.

Make compliance less of a firefight

When the DSAR comes in or Legal wants last quarter's mail trail, you need tools built for the job – not duct-taped admin consoles. TrustLayer provides immutable email archiving, role-based access, and multi-mailbox search designed for real-life audits, not just regulators' checklists.

Give users tools, not tickets

Outlook-integrated restore means staff don't need to call IT when they can't find that email from two weeks ago. Timeline views and self-service access reduce helpdesk load and keep users productive – and security happy.



See beyond the inbox

Email is just one way data gets out. TrustLayer's built-in CASB shows you which apps users are logging into, what data's moving out, and where risk is creeping in from the shadows. It's a natural extension of your Microsoft 365 visibility – no extra console needed.

About TrustLayer

TrustLayer is a cybersecurity platform built for the realities of modern business. We help mid-market organisations protect email, apps, and users with smart, layered security that's simple to manage and fast to deploy.

Our platform combines real-time visibility with flexible policy control – helping IT teams stop threats, reduce risk, and keep people productive.

Trusted by companies across finance, retail, healthcare, and the public sector, TrustLayer is reshaping what secure feels like.

Find out more at trustlayer.co.uk