FirstWave

What Microsoft Missed

Essential Add-Ons for Organisations Relying on Microsoft 365 Email

Microsoft 365 is the backbone of email and collaboration for organisations across Australia, from private enterprises to federal agencies. While Microsoft provides native email security through Exchange Online Protection (EOP) and optional Defender for Office 365, these tools alone are no longer enough for organisations to protect themselves.

Not only are today's targeted cyberattacks designed to bypass default protections, many IT teams also fail to enable or correctly configure advanced policies, even when Microsoft Defender is fully licensed. The result: critical threats slip through, often unnoticed until the damage is done.

The cost of over-relying on a single vendor for email security is no longer justifiable.

This report reveals common blind spots in Microsoft 365 email security, showing where Microsoft's defences break down and the risks of relying on a single-layer email security model.

Based on real-world testing, industry analysis, and input from ICT leaders across sectors, it explains why layered security—already standard for endpoint, identity, and network protection—must also apply to email.

Whether you're a CISO, ICT manager, or compliance officer, this asset will help you assess your risk exposure, compare current configurations against compliance expectations, and identify gaps that a second layer of defence can close.

For high-value, high-compliance sectors like finance, healthcare, critical infrastructure, defence, education, and government, this is an essential conversation – not a critique of Microsoft, but a call to protect your data over this essential service.

THE THREATS MICROSOFT COMMONLY MISSES

Despite Microsoft 365's broad adoption and built-in email protection, relying solely on native defences comes with many limitations. Even with Defender for Office 365 Plan 1 or 2, empirical data gathered across multiple environments tells the same story: sophisticated threats frequently evade detection.

In deployments where a second layer of email security was added on top of Microsoft 365, FirstWave observed alarming numbers of threats that would have gone undetected by single-layer security, including:

Business Email Compromise (BEC):

These socially engineered attacks often lack payloads, making them difficult for Microsoft to detect through conventional scanning. In live environments, a second layer consistently flags impersonation attempts, CEO fraud emails, and supplier spoofing missed by Defender.

Zero-Day Malware & File-Based Threats:

Advanced malware sent via attachments often bypasses initial Microsoft scans, especially when sandboxing isn't fully enabled or properly configured. In one customer instance, over 400 unique malicious attachments were intercepted by the second layer in a 30-day period; none had been blocked by Microsoft 365.

Phishing Links in Clean Emails:

Microsoft's Safe Links protection is reactive and reputation-based. In multiple deployments, time-delayed phishing attacks (where benign links later redirect to malicious sites) were only caught by real-time URL inspection from the second layer.

Credential Harvesting:

Many credential-stealing emails were delivered to user inboxes due to minimal visual deception. These were flagged as clean by Defender but caught by the second layer's advanced heuristics and threat intelligence.

Microsoft 365, even at its best, is not designed to operate as a standalone perimeter. Without layered detection techniques, organisations are exposed to low-signal, high-impact threats that evolve faster than Microsoft's default protections.

WHY LAYERED EMAIL DEFENCE IS THE NEW STANDARD

Email remains the most targeted attack surface for organisations, and relying solely on Microsoft 365 Defender, even at its highest tier, is no longer enough. Modern threat actors use advanced tactics that bypass default protections, exploiting social engineering, behavioural blind spots, and zero-day techniques.

That's why layered email defence has become the new global standard, not just according to vendors, but in line with frameworks like the **ASD Essential Eight**, **ISO 27001**, and **NIST SP 800-53**. It's no longer a luxury; it's expected.

In live environments where a second layer was added downstream of Microsoft 365, real-world data shows a significant improvement in protection. FirstWave's Cisco-powered email security platform **CyberCision**, acting as a second-layer of defence, intercepted threats that Microsoft had delivered as benign.

Over a recent evaluation period, it:

blocked 6,704 high-risk messages missed by Microsoft, including:

- 50 malicious attachments;
- 478 malicious URLs;
- 6,803 outbreak and QR threats, which were neutralised

flagged messages Microsoft had categorised as "safe" or "low-confidence"

reduced phishing risk by identifying behaviours requiring sandboxing, link rewriting, or deep header inspection

This isn't just marginal value. It's mission-critical protection. Without a second layer, organisations are exposed to the very threats they assumed were covered. A layered model introduces multiple inspection points—signature and behavioural analysis, global threat intel, contextual policies, and advanced heuristics all without disrupting end-user experience.

For compliance-heavy sectors like government, finance, and healthcare, this architecture is not optional – it's a baseline for responsible risk management. Microsoft 365 alone leaves gaps. A second layer closes them.

MEETING MANDATES FOR GOVERNMENT AND REGULATED ENTITIES

Government departments, defence contractors, healthcare organisations, and public sector agencies face a unique set of cybersecurity challenges. They are high-value targets for sophisticated attacks like nation-state actors, and operate under strict regulatory mandates like the ASD Essential Eight, ISM, and the Protective Security Policy Framework.

In these environments, email is a primary threat vector, and the consequences of a breach are significant. Yet many agencies continue to rely on Microsoft 365's baseline email protection, which—as real-world telemetry shows—allows a substantial volume of phishing, impersonation, and credential-harvesting threats to slip through.

To meet these risks and compliance obligations, a second layer of email defence is essential.

Our Cisco-powered solution is already in use across IRAP-assessed environments and supports agencies in aligning with the Essential Eight, ISM controls, ISO 27001, and other regulatory frameworks.

Key capabilities include:

- **policy enforcement**
- **SPF/DKIM/DMARC alignment**
- **real-time URL analysis**
- **sandboxing, and threat intelligence from Cisco Talos**

Government-aligned procurement is made easy through **AWS Marketplace Private Offers** which streamlines purchasing, integrates with existing contracts, and offers faster time to value by removing delays often associated with vendor onboarding or security reviews.

Deployment is backed by **Ingram Micro**-certified partners with NV1-cleared personnel, delivering configuration audits, policy tuning, and compliance-ready reporting. These services ensure the solution is not only deployed, but hardened to your unique operational and risk context.

Whether securing agency email or uplifting defences in highly targeted organisations like defence suppliers, regulated utilities, or hospitals, this approach delivers a practical path to cyber resilience that's fast, frictionless, and fully aligned with government mandates.

If your agency uses Microsoft 365, this is the uplift you need to meet your cyber mandate without overhauling your environment.

CYBERCISION: THE ENTERPRISE-GRADE SECOND LAYER

For security-conscious organisations, CyberCision delivers what Microsoft 365 can't: enterprise-grade, multi-layered email protection powered by Cisco Talos, the world's most trusted commercial threat intelligence team.

While Microsoft 365 provides a solid baseline, its default protections often fall short against targeted attacks like BEC, spear phishing, credential harvesting, and zero-day malware. That's where CyberCision comes in, adding a proven, high-efficacy second layer of defence that integrates seamlessly with Microsoft 365.

ADVANCED SECURITY TOOLS

Built on Cisco's global threat intelligence and real-time detection capabilities, CyberCision uses advanced tools like sandboxing, real-time URL rewriting, anti-spoofing (SPF, DKIM, DMARC), and deep policy control to catch the threats that Microsoft misses. These capabilities are especially critical in sectors with high compliance requirements and low risk tolerance.

QUICK DEPLOYMENT

CyberCision is frictionless to deploy via the AWS Marketplace, with no lengthy vendor onboarding or procurement delays – ideal for IT teams looking to move quickly while maintaining control.

ONBOARDING SUPPORT

Every deployment includes expert onboarding from an Ingram Micro-certified partner, covering configuration, policy tuning, compliance mapping, and Tier 1 support. This ensures CyberCision isn't just deployed,but optimised from day one.

AUDIT ASSURANCE

CyberCision supports alignment with global frameworks such as ISO 27001, GDPR, SOC 2, HIPAA, and the ASD Essential Eight. Whether you're protecting intellectual property, regulated data, or national infrastructure, CyberCision strengthens your security posture without complexity.

In a landscape where compliance is non-negotiable and threats are constant, CyberCision offers a fast, effective way to uplift your email security, without replacing your Microsoft environment. It's not just a safety net – it's a strategic upgrade.