Westcon | Microsoft

AI and cybersecurity compliance

How to sell Microsoft Copilot as a cybersecurity solution

As AI adoption accelerates, your clients face a double-edged sword: how to embrace AI-driven productivity without compromising their defensive perimeter. Generative AI tools are rapidly entering the workplace, but many are built without the security guardrails, network controls, or compliance alignment that regulated businesses depend on.

This eBook equips you with the information to guide your clients through these cybersecurity compliance questions.

1.

Why your clients should be concerned about uncontrolled AI usage

Generative AI is transforming business productivity — but it's also raising new compliance and security concerns for your clients. In regulated industries like finance, healthcare, and legal, customers are asking:

Where does my data go when I use AI tools?

Can I prove to auditors that my AI usage aligns with cybersecurity compliance standards?

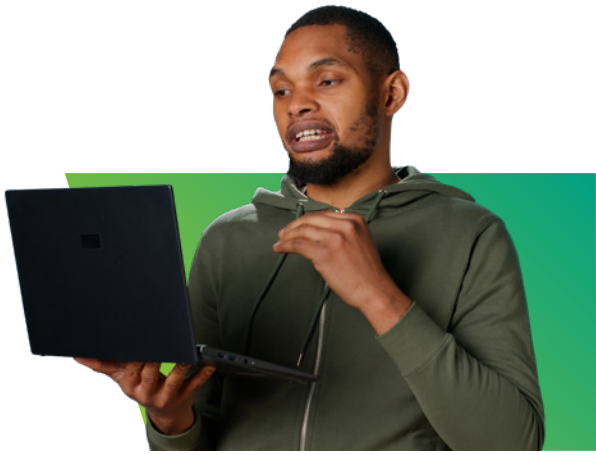
How do I control who accesses AI features?

Public AI platforms (like ChatGPT or Gemini) don't meet these compliance needs. They process data outside your client's security perimeter, lack enterprise-grade access controls, and provide little auditability.

Westcon | Microsoft

2.

The compliance and security gaps in consumer AI



a) Infrastructure exposure

Consumer AI platforms operate across global cloud infrastructures, often without transparency or control over data routing, processing, or retention. From a cybersecurity standpoint, this raises critical concerns:

Enterprise firewalls and network monitoring tools may not see where traffic is going.

Security teams cannot enforce trusted network boundaries or apply geofencing policies.

Data in transit may pass through or terminate in regions with unknown threat postures or state-level surveillance risk.

b) Lack of role-based access controls

Consumer AI tools typically lack integration with enterprise identity platforms like Microsoft Entra ID (Azure AD), meaning they don't enforce existing role-based access controls (RBAC). This creates a critical compliance gap.

Anyone with access to the tool can interact with sensitive or regulated data without restriction, regardless of their role, department, or clearance level. Security teams lose visibility into who is doing what, when, and with which data.

This lack of RBAC not only undermines Zero Trust principles, but also fails to meet the minimum access control standards required by cybersecurity frameworks such as NIST SP 800-53 (AC family of controls), ISO 27001 Annex A, and CIS Controls. For regulated businesses, this makes such tools non-compliant by design.

c) No audit trail or control visibility

Generative AI tools that operate outside enterprise control typically lack robust logging, correlation, and oversight capabilities. From a cybersecurity compliance perspective — particularly aligned with NIST frameworks — this violates core requirements around auditability, accountability, and incident response readiness.

Without audit trails, security teams cannot verify user actions, detect anomalies, or trace potential breaches. This absence directly undermines capabilities required in frameworks like NIST SP 800-53 (AU family of controls) and ISO 27001 Annex A. It's not just a visibility issue — it's a breakdown in verifiable, accountable system behaviour, which is essential to passing audits and detecting advanced threats.

d) Shadow AI adoption

Without your help, employees may adopt generative AI tools independently, without IT oversight or security controls. This "Shadow AI" introduces unmanaged endpoints, unmonitored data flows, and inconsistent usage patterns that directly violate cybersecurity compliance requirements. It undermines visibility, disrupts enforcement of access policies, and increases the risk of configuration drift or tool misuse — all while leaving no audit trail behind.

Westcon | Microsoft

3.

Microsoft Copilot: The secure AI alternative

This is where you step in as the trusted adviser — the knight in shining armour your clients need. Microsoft 365 Copilot gives you a practical, secure way to help your clients embrace AI without compromising their cybersecurity posture. Instead of leaving clients to navigate compliance risks alone, you become their partner in building a controlled, compliant AI strategy that strengthens their security, not weakens it.

Key points for MSPs to highlight:

Data stays in the tenant:

Copilot runs entirely within Microsoft 365 — ensuring data remains under the customer's control, with full visibility into how it's accessed and used.

Built-in security and compliance:

Copilot honours Microsoft Entra ID (Azure AD) permissions and integrates seamlessly with Microsoft Purview, allowing enforcement of DLP, audit logging, and sensitivity labelling at scale.

Aligned with cybersecurity frameworks:

Microsoft 365 Copilot supports enterprise controls aligned to Zero Trust, NIST SP 800-53, and ISO/IEC 27001, helping clients satisfy technical and operational cybersecurity requirements.

Operational simplicity:

No need for third-party monitoring tools — security teams can leverage Defender, Sentinel, and Purview to manage and monitor Copilot through existing security infrastructure.

4.

Microsoft Security Copilot: A value-add for SOC conversations

For MSPs offering SOC services, Microsoft Security Copilot takes secure AI to the next level. While Microsoft 365 Copilot is the safe AI your clients use to boost productivity within their compliance boundaries, Security Copilot is the AI your security team uses to defend those boundaries.

Unlike productivity-focused AI, Security Copilot actively assists your SOC in detecting, analysing, and responding to cyberattacks — including threats powered by AI itself. It leverages Microsoft's global threat intelligence and real-time telemetry to help your clients fight back against adversaries who are increasingly using AI to scale phishing campaigns, automate malware creation, and evade detection.

Helps your SOC respond faster by summarising incidents and recommending actions.

Maintains auditability for compliance teams.

Automates threat hunting across Microsoft Defender and Sentinel.

Position Security Copilot as an advanced add-on that helps your clients not just stay compliant, but also proactive in defending against AI-driven threats.

5.

The MSP opportunity

Your clients want AI, but they need an MSP who can do more than simply deploy tools — they need a strategic security partner. Most businesses don't have the in-house expertise to assess cybersecurity compliance gaps created by generative AI, much less implement a secure framework to close them.

This is your opportunity to lead. As their MSP, you can:

- Translate AI security risks into actionable strategies that align with ISO 27001, SOC 2, and Zero Trust frameworks.
- Help your clients define an AI usage policy that controls where and how AI tools operate.
- Implement Microsoft 365 Copilot as a productivity solution that aligns with cybersecurity compliance frameworks — ensuring visibility, control, and operational safeguards are maintained even as AI capabilities expand.
- Introduce Microsoft Security Copilot as the AI defender that actively monitors, detects, and responds to evolving threats — including AI-generated attacks.
- Deliver continuous monitoring, governance, and incident response as a managed service.

By doing so, you position your MSP practice not as just a technology provider, but as a cybersecurity compliance partner.

Westcon | Microsoft

Conclusion

The rise of generative AI creates both urgency and opportunity for MSPs. Your clients want to move fast — but moving without a cybersecurity-aligned AI strategy puts them at serious risk.

Uncontrolled AI adoption can result in unmanaged agents, unmonitored data activity, and failure to meet core cybersecurity compliance standards.

As an MSP, you're in a unique position to lead your clients through this shift. You can show them how to integrate AI into their environment securely and in full alignment with modern cybersecurity frameworks. From audit-readiness to threat response, you help make AI safe, operational, and compliant.

Westcon | Microsoft


Westcon
Microsoft