Insight | Microsoft

Strategic guide to cloud confidence

Insight + Microsoft Security

Introduction: the cloud security inflection point

The complexity of securing modern cloud environments has reached a critical inflection point. As the pace of digital transformation speeds up, organisations must embrace hybrid and multicloud infrastructures to drive innovation and agility. To stay ahead of evolving threats, the way we approach security must evolve too.

While hybrid cloud environments offer greater flexibility and scalability, they also create a broader, more fragmented attack surface. The rapid growth of AI-driven workflows adds another layer of complexity, introducing new data pipelines, models and integrations that legacy tools and siloed security approaches may struggle to protect.

Cyber threats are more sophisticated, regulatory demands more stringent, and the cost of failure more severe, ranging from operational downtime and reputational harm to financial losses and regulatory penalties. As a result, security is no longer just an IT concern, but a core business priority that directly impacts operational resilience, customer trust and revenue.

These challenges present a strategic opportunity. By adopting modern, cloud-native security frameworks, organisations can strengthen protection while gaining the visibility, control and agility they need to support innovation at scale.

Insight supports organisations to redesign their security posture for the cloud era.

By combining Microsoft's industry-leading cloud security technologies with Insight's strategic and technical expertise, we can help you take control of governance, risk and compliance; integrate advanced security across hybrid cloud environments and AI initiatives, simplify identity and access management, and elevate security from an IT function to a strategic business enabler.

Security is no longer a siloed IT function. It's a business-critical capability that underpins **operational resilience, stakeholder trust and long-term value.**

Navigating change with confidence

Your opportunity to enhance security

Although the primary drivers for adapting a new security approach come from the challenges organisations face, these challenges also open up valuable opportunities. For example, many enterprises are underutilising the full potential of the Microsoft security suite.

Microsoft continuously expands the capabilities of Microsoft 365 E5 to address today's evolving threat landscape, offering features such as AI-powered threat detection, Zero Trust identity and access controls, and tools that simplify compliance and unify security operations for a faster, more coordinated response.

Microsoft 365 E5 provides organisations the opportunity to replace legacy, siloed tools with an integrated, cloud-native platform that strengthens protection, streamlines operations, and reduces complexity. For businesses concerned about cost, a phased approach, such as leveraging the E5 Security add-on, can deliver immediate value while managing budget impact.

Insight helps you assess the right path forward and demonstrate a clear return on your security investment. Through readiness assessments, licensing optimisation, value mapping, and technical deployment guidance, we ensure you get the most from your Microsoft investment.

Microsoft 365 E5 offers a suite of advanced security solutions designed to enhance automation, enable advanced analytics, and improve threat detection across your environment, including AI initiatives.
The suite includes:

- **Microsoft Entra ID P2** for identity and access management
- **Microsoft Defender Cloud Apps, Defender for Endpoint, Defender for Identity**, and **Defender for Office 365** for threat protection and detection
- **Microsoft Purview Insider Risk Management** for information protection and governance

Compliance imperative

The EU NIS2 Directive represents a critical and immediate compliance imperative for organisations operating in or with the EU. It significantly broadens the scope of security obligations, extending the remit of NIS to a wider range of organisations, including manufacturing, digital services, government, and logistics.

Organisations affected by NIS2 are expected to be compliant, with those classified as 'essential' facing significant penalties – up to 2% of global annual turnover – for failing to meet the directive's requirements.

Key obligations include implementing documented risk management policies, establishing robust incident response and notification procedures, and demonstrating proven business continuity and recovery capabilities.

Insight and Microsoft provide a comprehensive suite of tools and services to support organisations in navigating these requirements. From policy creation and enforcement to continuous security monitoring, compliance reporting and incident management, we deliver end-to-end support to help you meet NIS2 obligations. Rather than responding reactively to the next compliance deadline or breach, security leaders can take this moment to make proactive, strategic improvements.

Insight's support enables you to transform compliance into a catalyst for protection, and business resilience.

Organisations classified as 'essential' face fines of up to **2% of global annual turnover** for failing to meet NIS2 requirements.

Risk has shifted. Has your strategy?

Devices, data and workflows are now distributed across multiple platforms, vendors and geographies, making the attack surface larger and more complex than ever before. The rapid adoption of AI adds to this complexity, introducing dynamic data flows, new access points and emerging risk factors.

Meanwhile, compliance challenges are increasing in number and complexity, requiring organisations to collaborate closely with cloud providers while navigating diverse regulatory requirements across borders.

The threat landscape is evolving rapidly: sophisticated attacks, from ransomware and supply chain compromises to phishing and insider threats, are becoming more frequent and harder to detect.

Against this backdrop, legacy security approaches built around siloed tools and reactive responses struggle to keep pace. Fragmented solutions and limited visibility make it difficult for security teams to effectively identify and manage risks before they escalate.

To safeguard hybrid, multicloud environments and AI initiatives against unauthorised access, breaches and vulnerabilities, businesses need a more holistic, integrated security strategy. This includes comprehensive visibility across users, devices and workloads; proactive risk management through continuous monitoring and threat intelligence; and adaptive controls aligned with Zero Trust principles.

Evolving your security strategy to prioritise these capabilities ensures you can defend today's complex threats, without hindering agility and innovation in a fast-changing digital landscape.

Align security with business requirements

Cybersecurity is often seen as a necessary cost or even a barrier to innovation. But in today's cloud-first, fast-moving digital landscape, security should be reframed not as a constraint, but as a strategic enabler.

Strong security models don't hinder innovation, they support transformation, build resilience, and drive measurable business value. Robust cloud security enables safe collaboration, supports flexible working models, and safeguards business continuity. It also strengthens trust and relationships with customers, partners, and employees.

Many organisations already have a solid security foundation within their Microsoft ecosystem but aren't fully leveraging its potential. Insight's cloud optimisation services uncover hidden savings through rightsizing, license optimisation and FinOps best practices.

We identify underused Microsoft licensing benefits that can enhance security capabilities, allowing you to reinvest those savings into accelerating your security roadmap without increasing overall costs.

By blending technical capabilities with commercial expertise, Insight helps security leaders build a strategy that resonates in the boardroom – with clear metrics and alignment to strategic business objectives.

Insight supports security leaders in building the business case for cloud security investments by positioning it as:

- A driver of business resilience, protecting continuity and strengthening customer trust
- An enabler of innovation, empowering teams to confidently adopt new digital capabilities
- A cost-optimisation opportunity, unlocking budget for critical security priorities through Microsoft licensing optimisation

Governance, Risk and Compliance in the Microsoft cloud

In today's environment of rising regulatory demands, evolving cyber threats, and increasing data complexity, robust Governance, Risk, and Compliance (GRC) practices are essential.

Insight supports organisations in leveraging Microsoft tools as a powerful platform to embed compliance and risk management into everyday operations. The approach is pragmatic and operational, ensuring that security policies aren't just documents but embedded capabilities that scale with your business.

The key to success is turning policy into practice. Whether aligning with NIS2, ISO 27001, GDPR, the EU AI Act, or sector-specific standards, **we support organisations to build a unified security posture that meets multiple compliance requirements**. Using Microsoft tools like Compliance Manager, organisations can map controls to regulations, continuously monitor compliance status and respond to risks in real time.

Adoption of a Zero Trust model is central to this approach, treating identity, device and data access as dynamic, risk-aware components. Microsoft solutions, such as Microsoft Entra for identity governance, Microsoft Defender for Cloud for workload protection, and Insider Risk Management for behavioural insights, help organisations establish Zero Trust across Microsoft 365 and Azure environments.

Unified policy management, continuous assessments and automated remediation enable security, compliance and IT teams to work from a single source of truth, simplifying governance across complex hybrid and multicloud environments.

Insight's pragmatic, operational approach ensures that security policies become scalable, embedded capabilities, transforming GRC from a reactive obligation into a strategic advantage that enables compliance, manages risk, and fosters innovation.

Insight can help you establish a strong governance model, aligned with both industry regulations and internal risk tolerance. We support you in:

- Defining clear roles and responsibilities to ensure appropriate access and oversight
- Extending consistent policies across Azure and Microsoft 365, covering data, endpoints and collaboration tools like SharePoint, Teams and OneDrive
- Integrating security monitoring with tools like Defender for Cloud and Azure Sentinel
- Applying Zero Trust principles broadly, using Microsoft Entra to protect sensitive data from unauthorised access

Design and deploy end-to-end security

Hybrid cloud environments unlock agility and scalability, but they also expand the attack surface. Microsoft provides a powerful security framework, but it's up to you to configure, integrate, and optimise it to suit your unique business context.

Insight helps clients design and deploy comprehensive security architectures across Azure, on-premises, and SaaS environments. As a leading solutions integrator and Microsoft Security partner, we take a holistic, risk-based approach that aligns security with your operations and business goals.

Large-scale security programmes often involve multiple vendors and technologies, adding complexity.

Insight simplifies this by managing the entire project lifecycle, coordinating with third-party providers, and providing a single point of accountability to ensure seamless integration and successful delivery.

Whether you're rolling out Microsoft Defender globally, simplifying identity and access management with Entra ID, integrating with third-party Security Information and Event Management (SIEM) systems, or migrating sensitive workloads to Azure, Insight provides the expertise and proven methodology to support secure growth and innovation.

Insight's cloud and security experts bring years of experience in building and securing complex multicloud environments. Working with Microsoft's integrated security solutions, we help you:

- Gain full visibility across your hybrid and multicloud environments
- Deploy Zero Trust principles across identities, devices and data
- Integrate threat protection with Defender for Cloud, detecting malware, anomalies and insider threats
- Optimise Microsoft 365 licensing to reduce tool duplication and unlock budget for strategic investments

Managed services: ongoing protection without overload

Cybersecurity doesn't stop at deploying the right solutions, it requires continuous optimisation and adaptation. As threats evolve and environments become more complex, many organisations struggle to maintain the expertise, resources, and time needed to manage security effectively. That's where Insight Managed Security Services come in.

Insight offers **24/7 threat detection** and response through our Global Security Operations Centres (SOCs), delivering round-the-clock incident response and protection.

Our services go beyond monitoring. We proactively hunt for threats, tune configurations, and conduct monthly reviews to ensure your Microsoft security environment is aligned with the latest risks and regulatory requirements. Insight helps you move beyond reactive, point solutions. As a leading solutions integrator and trusted Microsoft Azure partner, we bring together governance, compliance and technical execution into a cohesive, long-term security strategy that delivers measurable ROI.

Insight acts as a trusted extension of your team, enabling you to maintain protection without the internal overhead. From implementation to ongoing improvement, we focus on security so you can focus on your business.

Insight's managed services include:

- Continuous optimisation of Microsoft Defender and Azure configurations
- Co-managed options that elevate your internal teams while giving you full control
- Strategic advisory to ensure your security posture evolves with business goals
- Scalable expertise to meet changing operational demands

Accelerate capability with enablement and funding

A strong security strategy doesn't rely on tools alone: it's powered by people.

Building a resilient security posture means equipping your teams with the knowledge, skills and confidence to manage evolving threats and technologies effectively. At Insight, we embed enablement into every stage of delivery, so security becomes a sustained organisational effort, not just a one-off initiative.

Our close partnership with Microsoft helps you unlock the full value of Microsoft-funded training, workshops and enablement programmes. From IT teams to end users, we provide strategic guidance and tailored support to help embed security best practices across your organisation through our education and enablement services.

Integrating enablement into your cloud security journey means your teams are not only supported during implementation but empowered for the long term. Whether it's upskilling your security operations centre or educating end users on secure behaviours, Insight helps you turn security into a shared responsibility and strategic asset.

With the right training, support, and access to funding, you can accelerate adoption, reduce risk, and maximise the return on your Microsoft security investment.

Insight's security enablement services include:

- Microsoft FastTrack and funded technical workshops for Defender, Entra and Purview
- Hands-on Proof-of-Concepts (POCs) to validate new tools before full deployment
- User awareness and secure collaboration training for Microsoft 365 apps like Teams, SharePoint and OneDrive
- Microsoft-funded security assessments to identify gaps, prioritise actions, and unlock additional value

Why Insight + Microsoft: a strategic security partnership

Insight and Microsoft bring expertise, global scale and a business-first approach to help you secure your digital environment with confidence.

As a Microsoft Solutions Partner across Security, Azure, and Modern Work – and a 2023 Microsoft Solutions Assessment Partner – we have direct access to Microsoft's latest innovations, training, and funding programmes.

Our strength lies in bridging the gap between technology potential and your operational reality. From strategy and assessment to implementation, optimisation, and managed services, we provide end-to-end capabilities that build integrated, resilient security postures.

Whether you're modernising security in Microsoft 365, securing hybrid cloud infrastructure in Azure, or navigating evolving compliance requirements, Insight and Microsoft are here to help you achieve your security goals.

Why organisations choose to work with Insight:

20-plus

years of **security transformation** knowledge and experience

Proven expertise

in **governance, compliance** and **IT integrations**

Business-first

mindset that **aligns every security investment** with your strategic goals and measurable outcomes

Global scale

and local presence **ensure consistent, high-quality service** across regions

Turning strategy into action

In today's complex and fast-moving threat landscape, securing your organisation requires more than fragmented point solutions – it demands a holistic strategy, continuous enablement and ongoing improvement. With Microsoft's powerful cloud security tools and Insight's proven expertise across integration, governance and managed services, you can move from reactive defence to proactive resilience.

Whether you're aiming to comply with new regulations, modernise legacy tools, or build a Zero Trust architecture, Insight can help you design a security strategy that delivers real business value while maximising your existing Microsoft investments.

To align security with your business and cloud strategy, contact us to **speak with an Insight Security Consultant.**

Secure your business with Insight + Microsoft

Get in touch

Insight