infinigate cloud

Microsoft E5 Security Add-on Go-To-Market Partner Strategy

March 2025

Microsoft 365 E5 Security Add-on is a critical evolution in your customers security posture

01

Positioning the Microsoft 365 E5 Security Add-on

Ensuring you position the solution in a way that resonates with your customers, increasing your chance of conversion and added value.

Positioning the Microsoft 365 E5 Security Add-on

Enabling your customers to understand the value

Elevate Security from Basic to Proactive Defense

Instead of selling it as just an “upgrade”, position it as a critical evolution in their security posture. Emphasize the shift from reactive to proactive threat hunting and prevention.

Frame it as a “security shield” that extends beyond basic protection, providing advanced threat intelligence, automated response, and comprehensive visibility.

Address the Growing Threat Landscape

Highlight the escalating sophistication of cyberattacks targeting SMBs. Use real-word examples of ransomware, phishing, and data breached impacting businesses of a similar size.

Emphasize that Business Premium provides a solid foundation, but E5 Security addresses the advanced threats that can bypass basic defences.

Business Continuity and Peace of Mind

Focus on the business impact of security breached. Emphasize how E5 Security minimizes downtime, protects sensitive data, and safeguards their reputation.

Position it as an investment in business continuity, allowing them to focus on growth without constant fear of cyberattacks.

Identifying the best people to talk to

Ensuring you have the right audience, and know your audience is key to ensuring the best opportunity to convert

Business Owners / CEOs	They are concerned with the overall risk to the business, financial implications, and reputation. Focus on the business impact of security breaches and the ROI of E5 Security.
IT Managers / Directors	They are responsible for the technical implementation and day-to-day security operations. Highlight the ease of management, automation features, and advanced threat detection capabilities.
Finance / Operations Managers	They are concerned with the cost of security solutions and the impact on productivity. Demonstrate the ROI of E5 Security and how it reduces the risk of costly data breaches and downtime.
Compliance Offers	If the SMB is in a regulated industry, compliance is key. Show how E5 security helps meet those compliance requirements.

Key Elements to Focus on for SMBs

SMBs will have unique elements for what's going to add value to their business and increase the overall ROI.

Simplified Security Management

- SMBs often lack dedicated security personnel. Emphasize the centralized management and automation features of E5 Security.
- Highlight how it integrates seamlessly with their existing Microsoft 365 environment, minimizing complexity.

Cost-Effectiveness

- Demonstrate the ROI of E5 Security by comparing the cost of the add-on to the potential cost of a data breach or ransomware attack.
- Highlight how it consolidates multiple security tools into a single platform, reducing overall security expenses.

Proactive Threat Protection

- Focus on the advanced threat intelligence and automated response capabilities of E5 Security.
- Emphasize how it can detect and prevent attacks before they cause damage.

Data Protection and Compliance

- Highlight how E5 Security helps protect sensitive data and meet regulatory compliance requirements.
- Emphasize the importance of data loss prevention and access control.

90%

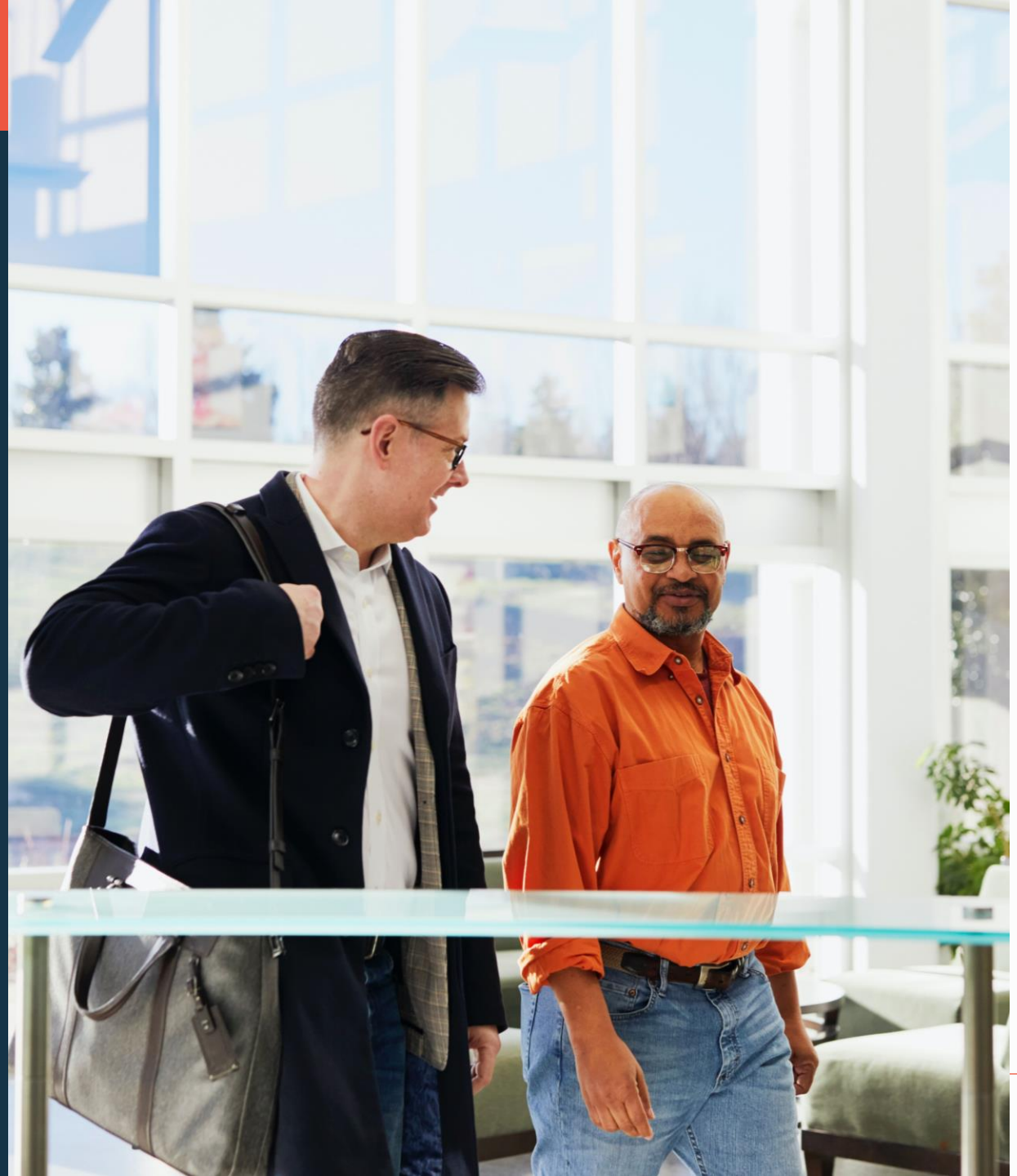
Of UK SMBs required the services of an MSP.

47%

Of businesses in 2024 find it difficult attracting new customers and retaining customers following a cyberattack.

40-60%

Average reduction in incident costs when proactive cybersecurity strategies are in place.



Maximizing ROI

A key element for any business

Reduced risk of data breaches:

- The most significant ROI comes from preventing costly data breaches, which can lead to financial losses, reputational damage, and regulatory fines.

Improved productivity:

- Automated threat detection and response minimize downtime and allow employees to focus on their core tasks.
- Single sign-on (SSO) and streamlined access management improve user experience and productivity.

Reduced security management costs:

- Consolidating multiple security tools into a single platform reduces the need for separate licenses and management efforts.

Enhanced compliance:

- Avoiding regulatory fines and penalties through robust security protocols.

Biggest Risks for SMBs & How E5 Security Solves Them

	Risk	Solution
Ransomware	• Data encryption, business disruption, and financial loss.	• XDR, device security, and email security detect and prevent ransomware attacks, while data recovery features minimize downtime.
Phishing and Business Email Compromise (BEC)	• Stolen credentials, financial fraud, and data breaches.	• Email and collaboration security, identity access controls, and ITDR detect and prevent phishing attacks and BEC scams.
Data Breaches	• Loss of sensitive data, reputational damage, and regulatory fines.	• Data loss prevention (DLP), identity access controls, and SaaS security protect sensitive data across devices, applications, and cloud environments.
Insider Threats	• Data theft, sabotage, and unauthorized access.	• Identity threat detection & response (ITDR), identity access controls, and device security monitor user activity and detect anomalous behavior.
Shadow IT	• Unauthorized access to data, data leaks, and compliance violations.	• SaaS security and Defender for Cloud Apps provide visibility and control over unsanctioned SaaS applications.
Compromised Credentials	• Account takeovers, lateral movement and data breaches.	• ITDR, identity access controls, and multi-factor authentication (MFA) prevent and detect compromised credentials.

50%
Of UK businesses have suffered a cyberattack in the last 12 months.

84%
Of breaches and attacks are phishing.

42%
Of applications within a company are shadow IT.

45%
Of businesses state that Insider Attacks take longer to recover from.

Go-To-Market Strategy

Partner with Infinigate Cloud

Infinigate Cloud can support with every step of your go-to-market strategy, whether it's with our GROW platform for market, delivering webinars to your customers, presales and post sales support and ongoing services.

Targeted Marketing Campaigns

Develop targeted email campaigns, webinars, and content marketing materials focused on the specific security challenges faced by SMBs. You can use Infinigate Clouds GROW platform or Microsoft's DMC for content and campaigns in a box. There are also fantastic resources within the Modern Work and Security Partner Portals. You can find a customer pitch deck downloadable HERE via the Modern Work Partner Portal.

Security Assessments

Offer free or low-cost security assessment to identify vulnerabilities in their existing security posture. Use the assessment results to demonstrate the value of E5 Security. You could use Microsoft Secure Score.

Value-Added Services

Offer managed security services, such as threat monitoring, incident response, and security awareness training. You could also create packaged offerings that contain the E5 Security license, your support, monitoring and remediation services. You can work with Infinigate Cloud to offer these additional services to your customers.

Ongoing Value & Opportunities

Use your success stories with customers and create case studies and testimonials to generate further ongoing business.

Also, scheduling regular security reviews with your customers to discuss the latest threats and ensure their security posture remains strong is a great way to increase stickiness & become their trusted advisor.

Up to **53%** Of UK businesses consider security the main reason to use an MSP.

220% Increase in engagement with targeted marketing Vs non-targeted.

Up to **95%** Increase in profitibality when increasing focus on customer retention with value-added services.

Value proposition

Business Premium + E5 Security

Microsoft 365 Business Premium

- **Standard Conditional Access** based on predefined conditions like device compliance, location, and app sensitivity

  Lacks identity protection tools for detecting compromised accounts and monitoring for suspicious activities
- **AI-powered endpoint security** across Windows, macOS, Linux, Android, and iOS—including attack disruption
- **Email and collaboration security**, including anti-phishing, anti-malware, and safe links/attachments threat protection
- See and manually block risky apps

+

Microsoft 365 E5 Security

- Delivers **comprehensive XDR capabilities** across identities, endpoints, apps, and email to detect sophisticated attacks, provide alerts and offer response recommendations
- **Identity Protection**, which adds AI-driven risk detection and automated response to **compromised accounts, risky sign-ins, and user behavior anomalies**
- Additional **endpoint security for IoT devices** and threat hunting capabilities
- Email and collaboration security including advanced security features such as **automated response capabilities**, **post-breach investigation**, **cyberattack simulation trainings**, and **detailed reports**
- **Automatically block apps** based on risk level, unusual user activity, or data-sharing behaviors

Value comparison

Business Premium + E5 Security

	Security capability	Business Premium	Microsoft 365 E5 Security
Identity and access controls	Basic Identity and access management (single sign on (SSO), multi-factor authentication (MFA), self-service password reset)	✓	✓
	Risk based MFA: require MFA if a user is accessing resources from an unrecognized device or unfamiliar location		✓
	Adjust authentication requirements based on risk assessment, such as asking for MFA only if login behavior is unusual		✓
	Self-service password reset with enhanced policies. Example: Only allow password reset if the user has passed security questions or an additional validation step		✓
	AI-driven risk detection analyzes user behavior to detect compromised accounts or risky sign-ins		✓
Identity security	AI-driven risk detection analyzes user behavior to detects compromised accounts and suspicious activities (e.g., impossible travel or unusual logins) that suggests an account has been compromised		✓
	Provides detailed alerts on identity-based threats		✓
	Protects on-premise Active Directory from attacks		✓
Device security	Endpoint protection with basic features like anti-virus and firewall	✓	✓
	Cloud-delivered protection, which includes near-instant detection and blocking of new and emerging threats	✓	✓
	Detects unusual system activity, flags suspicious processes, and provides attack timelines to help security teams contain the threat before data is stolen or encrypted	✓	✓
	Automated Investigation and Response (AIR) immediately correlates data across identity, email, and endpoint activity; If it detects a compromised account, it automatically revokes access, isolates the device, and generates an incident report		✓
Email and app security	Basic email protection from phishing and malware with simple filtering	✓	✓
	Automatically scans files and links in emails, Microsoft Teams, SharePoint, and OneDrive before they can be opened or shared; If a file or link is unsafe, it's blocked to prevent harm	✓	✓
	AI-driven phishing protection that detects and stops sophisticated phishing attempts, impersonation attacks, and email fraud	✓	✓
	Detailed reports on who is being targeted, which attacks were blocked, and potential weaknesses in the organization		✓
Cloud access security	Shows what apps employees use	✓	✓
	Shows what apps employees use, and evaluates how safe they are		✓
	Automatically blocks or restricts risky apps		✓
	Detects suspicious behavior in cloud apps, such as strange file access patterns or unusual downloads		✓

Thank you!

infinigate cloud