Westcon | Microsoft

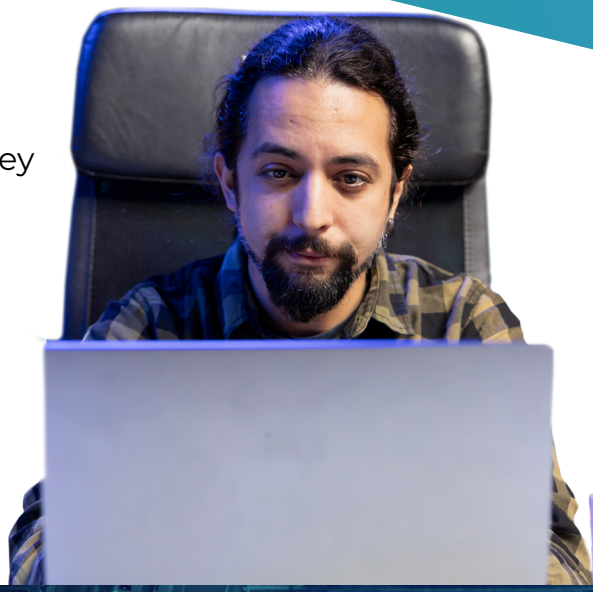
Turn “What’s Defender?” into “Where do I sign?”

An easier way to sell Microsoft Defender — in language your clients get

Introduction

Selling prevention is hard.

You bring up security — your client shrugs. Not because they don't care, but because they don't see the risk the way you do. They hear "Defender" and think antivirus. They think Microsoft 365 already covers it. They see security as a cost, not a safeguard.



Meanwhile, you're sitting on a stack of world-class tools that could protect their business. But if the message doesn't land, none of it moves.

That's what this guide is for.

It gives you the language to make security feel relevant — not optional. It walks you through how to position Microsoft Defender in ways that speak to your clients' real priorities.

> **Clients don't buy what they don't understand.**

Making the Case for Microsoft Defender

Microsoft Defender is a layered security portfolio that covers the real risks your SME clients face every day: email threats, compromised credentials, exposed cloud apps, and more.

But clients don't understand the difference between Defender for Endpoint and Defender for Cloud Apps — or why they need more than what's bundled into Microsoft 365.

This section gives you a clear, business-first breakdown of each Defender product — what it does, what problem it solves, and how to explain the value in client terms.

Microsoft Defender for Endpoint

Enterprise-grade protection for every endpoint in your client's environment — across laptops, desktops, servers, and mobile devices, whether on-site or remote.

Use it to address:

- Ransomware, zero-day attacks, and fileless malware
- Threats targeting remote or hybrid teams
- Slow detection and manual response that drive up recovery costs

The business message:

Defender for Endpoint helps reduce the risk of ransomware or malware shutting down operations. It detects threats early, isolates compromised devices automatically, and helps contain incidents before they escalate — even when users are off-network.

Westcon | Microsoft

Microsoft Defender for Office 365

Purpose-built protection for the communication channels attackers target most — email, Teams, SharePoint, and OneDrive.

Use it to address:

- Phishing, impersonation, and business email compromise
- Malware hidden in attachments or links
- Risks introduced through shared files and cloud collaboration

The business message:

Defender for Office 365 helps prevent account compromise, financial fraud, and data leaks by detecting and blocking malicious content before it reaches the user. It protects email and collaboration tools at the point of entry — where most attacks begin.

Westcon | Microsoft

Microsoft Defender for Business

Built specifically for SMEs, this solution bundles endpoint protection, detection, and response into one streamlined, easy-to-manage package — without requiring enterprise licensing or full security teams. It focuses on endpoint threats and does not include protections like Defender for Cloud or Defender for Cloud Apps.

Use it to address:

- Malware, ransomware, and other endpoint-based threats
- Security gaps in smaller or less-resourced environments
- The need for simplified setup and licensing at SME scale

The business message:

Defender for Business helps SMEs get serious protection without the overhead. It includes key features like threat detection, attack surface reduction, and automated response — all managed from a single interface.

Westcon | Microsoft

Microsoft Defender for Identity

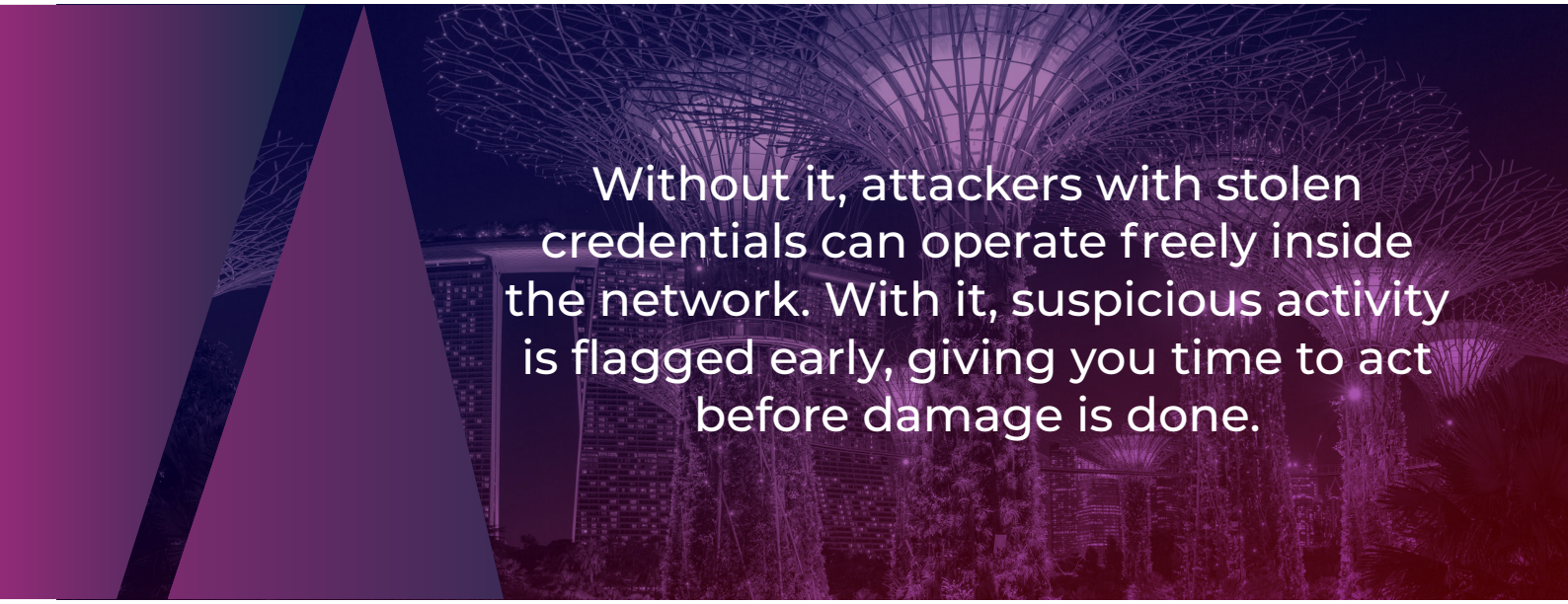
Monitors on-premises Active Directory environments to detect compromised credentials, lateral movement, and insider threats — before they result in a full-scale breach.

Use it to address:

- Credential theft and privilege escalation
- Suspicious behaviour inside the firewall
- Attacks that use valid logins to move across the network undetected

The business message:

Defender for Identity uses behavioural analytics to spot abnormal activity, like unusual logins or attempts to access sensitive systems. It helps identify threats from within — whether malicious or accidental — and adds a layer of defence most SMEs overlook.



Westcon | Microsoft

Microsoft Defender for Cloud Apps

Gives you visibility and control over the unsanctioned cloud apps and services employees use every day — often without knowing the risk.

Use it to address:

- Shadow IT and risky SaaS usage
- Sensitive data leaving the business via unmanaged tools
- Gaps in compliance and policy enforcement

The business message:

Defender for Cloud Apps helps identify and manage cloud platforms being used across the organisation — even those not approved by IT. It flags risky behaviour like file uploads to personal drives and gives you tools to enforce policy and block high-risk apps.

Without it, data can quietly flow through unsecured platforms like personal Dropbox or Google Drive. With it, you get visibility and control — before those blind spots turn into breach points.

Westcon | Microsoft

Microsoft Defender for Cloud

A cloud-native security solution that monitors Azure, AWS, and GCP environments — identifying misconfigurations, exposed services, and insecure workloads.

Use it to address:

- Misconfigured cloud infrastructure
- Unsecured virtual machines, databases, or containers
- Gaps in compliance or audit readiness

The business message:

Defender for Cloud continuously assesses cloud environments, flags high-risk issues, and helps clients stay secure and compliant. It's designed for businesses running in hybrid or multi-cloud environments — giving them a central way to manage cloud risk.

Westcon | Microsoft

Microsoft Defender XDR

Microsoft's unified security platform that connects signals across Defender tools — from endpoint to email to identity — for faster detection and coordinated response.

Use it to address:

- Siloed detection across disconnected tools
- Slow, manual response to threats
- Limited visibility into complex attacks

The business message:

Defender XDR brings together all Microsoft Defender signals to create a single, coordinated threat response. It helps reduce alert noise, highlights what matters most, and automates response actions across your client's environment.

Without it, your clients are relying on disconnected alerts and fragmented tools. With it, detection is faster, response is coordinated, and security becomes easier to manage — even without a full SOC team.

Conclusion

You don't need to oversell Defender. You just need to make it make sense.

The value is already there — layered protection, built-in automation, serious risk coverage. What most clients are missing is the language that connects that value to what they care about: staying online, staying trusted, staying in business.


Westcon
Microsoft