



# Security-as-a-Service for MSPs

How to Package, Sell and Deliver Modern Security  
Using Microsoft 365



Cybersecurity has shifted from “optional add-on” to a core business expectation. Customers assume their MSP is protecting them, even when they haven’t paid for security services. This gap creates risk, liability, and missed revenue.

This short guide shows how to use Microsoft 365 as the backbone of a profitable, standardised Security-as-a-Service offering that any MSP can deploy and scale.

# Why Microsoft 365 Is the Security Platform MSPs Can Build On

Microsoft 365 already contains the core tools SMBs need to close the biggest security gaps:



Identity protection through Entra ID security feature



Device hardening with Microsoft Intune



Threat detection & response with Defender for Business



Compliance and data protection with Purview



Zero Trust-aligned controls already built in

Most MSPs are already selling or managing M365 licenses. Turning these capabilities into a structured, packaged service is the fastest path to recurring security revenue.



# The Core Problem for MSPs: Customers Think They're Secure

Even when customers are only licensed with Business Basic or Business Standard, they assume:

- Their devices are managed
- Patches are happening
- MFA is enforced
- Email threats are blocked
- Data is protected

Your Security-as-a-Service offer solves this by making security explicit, measurable, and bundled.

# The Security-as-a-Service Package: What MSPs Should Include

A modern MSP security bundle built on M365 should cover four pillars.

## 1. Identity Security

Protect access to everything.

- MFA + Conditional Access
- Passwordless setup
- Entra Identity Protection alerts
- Privileged identity controls for admins

## 2. Device Security

Standardised, automated, enforceable.

- Device onboarding via Intune
- Baseline security configuration
- OS and app patching
- Defender AV and EDR enabled on every device

## 3. Threat Protection

Detect and stop attacks early.

- Defender for Business EDR
- Email filtering and Safe Links/Safe Attachments
- Automated investigation and response
- Alert triage and monthly reporting

## 4. Data Protection & Compliance

Reduce accidental and malicious data loss.

- Purview DLP policies for email, device and cloud
- Sensitivity labels for confidential information
- Conditional Access blocking risky downloads
- Secure sharing defaults

This structure keeps your offer consistent, supportable, and profitable.





# How to Package and Price It (Straightforward)

Your bundling should be simple enough to explain in 20 seconds.

## Example tiers

### Essential Security

*For customers on Business Premium.*

MFA + Conditional Access

Intune device onboarding

Defender AV + EDR

Basic email security

Monthly reporting

### Advanced Security

*For customers with higher risk or compliance needs.*

Full device compliance policies

DLP

Sensitivity labels

Threat investigation

Security operations reporting

### Premium Security

*For customers wanting full coverage.*

Advanced threat hunting

Privileged identity controls

Insider risk policies

Quarterly security reviews

Keep it modular. The foundation is always the M365 licensing they already own.

# How to Sell It: A Practical, Repeatable Conversation Flow

MSPs win more security deals when they stop talking about “features” and start talking about “gaps.”

Here’s the simplest structure that consistently works.

## **Step 1. Show the gaps**

Run a lightweight security posture review using:

- Secure Score
- Compliance Score
- Device compliance status
- MFA adoption
- Email threat reports

Customers instantly see what is and isn’t in place.

## **Step 2. Map gaps to risk**

Translate gaps into real consequences.

Example:

“No MFA” = anyone can log into your email with a leaked password.

“No device management” = no way to wipe a stolen laptop.

“No DLP” = staff can email customer data without restriction.

## **Step 3. Present the Security-as-a-Service package**

Explain your bundle as the standard baseline for modern security.

Keep it simple:

“We secure identity, devices, data and threat protection. Your team gets visibility, automation and reduced risk.”

## **Step 4. Tie licensing to outcomes**

Help the customer understand why they need Business Premium or E5 Security add-ons.

Lead with outcomes, not SKU names.

## **Step 5. Close with ongoing service**

Position the package as a continuous program, not a project.

Security needs monitoring and enforcement every month. That’s your value.

# Delivery: How MSPs Run This in the Real World

This is the practical checklist for operational delivery.

## Onboarding

- Confirm licensing (Business Premium recommended baseline)
- Enrol devices in Intune
- Deploy baselines
- Enable Defender for Business EDR
- Enforce MFA + Conditional Access
- Configure email security
- Review compliance score


## Monthly

- Review alerts and incidents
- Patch compliance
- Email threat reports
- Device compliance status
- Update security baselines if needed

## Quarterly

- Security review with customer
- Secure Score improvement plan
- New threats or policy enhancements
- Renewal planning

Make this repeatable and template-driven.

Abstract blue geometric shapes, including overlapping circles and sharp, angular forms, creating a modern, layered design on the right side of the slide.

# Why M365 Makes This Profitable for MSPs



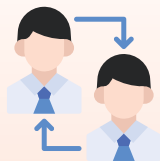
## High margin

You already manage the customer's environment. Adding structured security enables recurring revenue without adding heavy labour.



## Standardisation

When every customer uses the same stack, support becomes predictable and scalable.



## Vendor consolidation

Customers appreciate reducing point solutions. They would rather have email, identity, endpoint and data security under one ecosystem.



## Strong renewal foundation

Security strengthens your position, reduces churn, and grows lifetime value.



# The MSP Security Playbook (Simple Script You Can Use Today)

You can use this exact wording in calls or meetings.

## Situation

*"We ran a quick security posture check on your tenancy. There are a few gaps we should address to reduce your risk."*

## Gap explanation

*"We ran a quick security posture check on your tenancy. There are a few gaps we should address to reduce your risk."*

## Recommendation

*"We ran a quick security posture check on your tenancy. There are a few gaps we should address to reduce your risk."*

## Outcome

*"We ran a quick security posture check on your tenancy. There are a few gaps we should address to reduce your risk."*

## Close

*"We ran a quick security posture check on your tenancy. There are a few gaps we should address to reduce your risk."*

# Final Word

Security is no longer optional for SMBs, and MSPs are uniquely positioned to deliver it. By building your offer around Microsoft 365, you get:

- Predictability in service delivery
- Strong margins on recurring revenue
- Clear differentiation from break-fix providers
- Higher customer trust and stickiness

This playbook gives you a realistic, implementable pathway to scale Security-as-a-Service with confidence.

