



CYBERSECURITY ADVISORY

MFA Isn't Enough

Protect Your Business
Before the Next Breach

What your organization needs to know now

MFA Isn't the Finish Line

Multi-factor authentication is still a critical cybersecurity control, but it can't carry cyber resilience on its own.

This guide covers 3 steps business leaders can take to protect your business beyond MFA.

GET THE FULL STORY

Read the complete blog for deeper insights on strengthening cyber resilience.



Endpoint Protection

FOCUS AREA 1

Deploy EPP and EDR Everywhere

No gaps. Every endpoint (laptop, desktop, server) must be covered. Partial deployment leaves open doors for attackers.

Enable Fully Automated Mode

Allow your EDR to identify, hunt, and remediate threats in real time without waiting for human intervention. Speed is everything

Microsoft Defender for Endpoint

Enable Tamper Protection + EDR Block Mode + Fully Automated Investigation & Response for maximum coverage.

MFA Hardening

FOCUS AREA 2

1

Switch to Phishing-Resistant MFA

Move Admins, IT Staff, & Senior Leadership off push-notification MFA. Require FIDO2 security keys instead.

2

Enable Number Matching

Turn on Number Matching in Microsoft Authenticator to prevent MFA fatigue and approval fraud.

3

Close the SSPR Enrollment Window

Pre-register MFA for all privileged users. If attackers can register their own device during SSPR, they own the account.

4

Remove Weak Reset Methods

Audit and eliminate easily spoofable or weak authentication factors from your reset options.

5

Implement Risk-Based Conditional Access

Trigger additional verification automatically when unusual sign-in behavior is detected.

Cloud & Access Security

FOCUS AREA 3

Microsoft Defenders

- Defender for Endpoint
- Defender for Cloud
- Defender for Resource Mgr
 - Key Vault & App Service
- Defender XDR
 - Threat hunting across cloud

Azure Hardening

- Harden Key Vaults
- Least-privilege cloud roles
- Lock Graph PowerShell & Explorer for non-admins
- Lock down VM utilities
- Review all session tokens

Principle of Least Privilege:

Audit & minimize all broad custom cloud roles.

Ready to Strengthen Your Cyber Resilience?

OneDigital turns risk into business strategy using the RiskIP framework. For organizations ready to stop reacting and start leading, there's a measurable difference.

Connect with a OneDigital Cyber Risk Advisor



Review your current controls, identify gaps beyond MFA, and build a strategy that helps protect your business before an incident occurs.