Microsoft security, in business outcomes.

Engineering on Entra ID · Intune · Defender · Purview — plus attack surface monitoring and penetration testing.

1 DIAGNOSIS · *start by knowing where you stand*

Security X-Ray

Know exactly where you stand. We review your Microsoft environment and hand you a clear report of what is already solid and what is worth improving — so you decide with a plan, not a hunch.

Remediation Plan

Walk into the board room with a plan that defends itself. A phased roadmap with the risk, cost and priority of each stage, plus the licensing business case (E5 or add-ons?) already worked out.

2 IDENTITY · *Microsoft Entra ID*

Identity Hardening

Make a stolen password stop being a crisis. Multi-factor authentication and context-based access rules company-wide; and when someone leaves, they lose all access the same day.

Privileges Under Control

Remove the risk of the all-powerful admin. Sensitive permissions are activated only when needed, for a limited time and with everything logged.

Single Sign-On (SSO)

One login for all your applications. Fewer passwords to steal and automatic onboarding and offboarding — zero orphaned access when someone leaves the company.

VPN-less Remote Access

Your internal apps, secure from anywhere, without opening the network. We publish each application behind identity verification, without exposing everything else.

3 DEVICES · *Microsoft Intune*

Modern Endpoint (Windows)

New laptops ready out of the box; stolen ones, just lost hardware. Automatic setup, encryption and remote wipe — support hours per device become minutes.

App Catalog

The apps your people need, up to date across the fleet — no tickets. Automatic installation and updates, with a self-service portal for users.

Protected Mobile (iOS/Android)

Company information protected on any phone, even personal ones. If the person leaves, corporate data is wiped; their photos and personal data stay intact.

4 THREATS · *Microsoft Defender*

Endpoint Detection & Response (EDR)

Stop ransomware in minutes, not after days of downtime. Detection and response across the whole fleet, validated with a real attack simulation.

Hardened Email

Make sure no one on your team wires money to a fake account. Phishing and domain impersonation stopped before they reach the inbox.

Defender XDR Consolidation

All your security alerts in one place, with automated response. Less noise and fewer silos — ready to be run by your team or your SOC.

Cloud App Protection (Cloud Apps)

Take back control of shadow IT. We discover which cloud services your people actually use, block the risky ones and keep your information from leaving to unmanaged devices.

Azure Workload Protection (Defender for Cloud)

Your Azure servers under security governance, not adrift. Prioritized posture and workload protection — with the cost sized before anything is switched on.

5 DATA · *Microsoft Purview*

Sensitive Data Map

Know where your critical information lives and who touches it. We discover and label customer, payroll and contract data — because you cannot protect what you cannot see.

Data Loss Prevention (DLP)

Keep what your business is worth from walking out with whoever resigns. Data leaks blocked across email, Teams and USB — in phases, without slowing operations.

Compliance & Retention

When an auditor or a lawsuit asks for evidence, it shows up in hours, not weeks. Retention of what the law requires and eDiscovery ready to respond.

6 CONTINUITY · *so the investment does not erode*

Monthly Security Advisory

An expert watching your security every month, without adding headcount. A monthly hour bank for configuration reviews, tuning, advice and questions — you decide how it is used, with a report of the work done.

7 ATTACK SURFACE · *in-house service · continuous monitoring*

External Attack Surface Monitoring

See your company the way an attacker sees it — before they strike. Continuous monitoring of domains, ports, leaks and brand impersonation, prioritized by what actually gets exploited. Basic · Business · Enterprise plans.

8 PENETRATION TESTING · *in-house service · pentesting*

Penetration Testing

Prove your security holds — with evidence for audits and cyber insurance. A controlled, authorized attack that exposes what is exploitable in practice, with a remediation plan and a verification re-test included.

Modular · fixed price by scope. Hire only the services you need. Everything is built on the tools in your Microsoft 365 subscription — we don't sell licenses, we make what you already pay for perform. If you need additional licenses, our partners provide them hassle-free.