Smarttech
YOUR 24/7 SECURITY PARTNER

Entra ID Protection

INCIDENT RESPONSE

Turn risk detections into decisive action

Microsoft Entra ID Protection produces incredibly powerful insights – risky users, risky sign-ins, user risk policies, sign-in risk policies. But without a team that knows how to interpret and act on them, they become yet another noisy dashboard.

Our Entra ID Protection Incident Response service is built to turn that signal into swift, confident decisions.

THE CHALLENGES WE SOLVE

- Hundreds of “risky users” with no clear sense of which ones matter now.
- Conditional Access policies that exist on paper but are too loose in practice.
- No joined-up process between Entra ID Protection alerts and SOC incident workflows.
- Difficulty demonstrating to auditors and regulators that identity risk is actively managed.

WHAT YOU GET

- Continuous monitoring of Entra ID Protection signals: risky users, risky sign-ins, leaked credentials, password spray, atypical travel.
- Risk-based triage: differentiating between benign anomalies and genuine account compromise.
- Investigation playbooks tailored to Entra ID: investigating user history, device signals, sign-in origins, and downstream resource access.
- Risk resolution actions: confirming compromise, lowering risk level when proven benign, and triggering containment when required.
- Policy tuning recommendations: we help you refine user and sign-in risk policies, MFA enforcement, and Conditional Access rules.
- Compliance-grade reporting that shows how identity risk is monitored, acted on, and reduced over time.

HOW IT WORKS

1. Baseline: We review your current Entra ID Protection policies, risk thresholds, and Conditional Access design.
2. Integrate: We plug Entra ID Protection into our MDR workflows and define response rules for each risk scenario.
3. Operate: We monitor alerts, investigate suspicious activity, and work with you to resolve user risk.
4. Optimise: Over time, we tune detections and policies to reduce noise and strengthen protection without harming productivity.

WHY ORGANISATIONS CHOOSE US

- Specialised Entra expertise: We work with the Microsoft stack daily, including complex hybrid identity setups.
- Holistic view: We correlate Entra ID Protection data with email, endpoint, and SaaS telemetry for full context.
- Business alignment: We help you translate risk scores into actions that business leaders and auditors understand.

Ready to get started?

Send us a sample suspicious email and we'll walk you through our process

info@smarttech247.com