Managed Zero Trust

Why choose Ekco

Ekco's fully managed Zero Trust Service gives organisations powerful, modern protection against cyber-attacks. Powered by ThreatLocker and managed by our expert Security Operations Centre (SOC), this service places strict Zero Trust controls on every endpoint. With application allowlisting, ringfencing, elevation control, and network control, we stop unauthorised software, prevent lateral movement, and block privilege misuse before it becomes a threat.

Our SOC team continuously monitors and investigates all security events, ensuring fast and accurate threat detection. When a real threat is identified, our analysts escalate it as a Security Incident and work directly with the customer to drive rapid remediation.

Arrange a solution demo

Powered by THREATLOCKER

How it works

Application Allowlisting: Default-deny approach that blocks everything not explicitly allowed. Critical for stopping malware and ransomware at the endpoint level.

Ringfencing: Limits the actions of allowed applications, blocking misuse such as script spawning, lateral movement, or data exfiltration, even in legitimate software

Network Control: A dynamic, host-based firewall that opens ports only when needed and automatically closes them, reducing unauthorized network access.

Managed Endpoint Security

This service delivers proactive endpoint protection by locking down devices at the operating system level. It prevents unauthorised applications from running, tightly controls what approved applications can do, blocks malicious network activity, and protects devices against misconfiguration.

Delivered as a fully managed service, it enables a Zero Trust security model without adding operational overhead for your organisation.

info@ek.co