Apex Endpoint detection and response (EDR)

Advanced, real-time threat detection and response capabilities that go beyond traditional antivirus solutions

What is Apex EDR

Apex EDR provides advanced, real-time threat detection and response capabilities that go beyond traditional antivirus solutions. It continuously monitors endpoints, identifies malicious activity, and responds autonomously to prevent breaches. With features like behavioural analysis and threat hunting, Apex EDR ensures that even the most sophisticated attacks are detected early and neutralised. It offers cloud-based centralised management, making it easier for businesses to protect their devices both on and off the network.

How Does Apex EDR Work

Traditional antivirus software often struggles to keep pace with modern, sophisticated threats like ransomware, zero day exploits, and advanced malware. Businesses are at risk of breaches due to insufficient real-time threat detection and response capabilities. Moreover, with the increasing adoption of remote work and mobile devices, consistent endpoint security becomes a challenge. Many organisations also lack visibility into their network's overall security posture, making it difficult to detect, isolate, and remediate threats across multiple endpoints.

The Importance of Apex EDR

As cyber threats become more complex and targeted, relying solely on traditional antivirus software leaves businesses vulnerable to attack. Apex EDR provides next-generation protection that's designed to combat modern threats in real-time, preventing costly downtime, data breaches, and reputational damage. By offering a managed solution, Apex takes the burden of constant threat monitoring and response off the shoulders of business owners, allowing them to focus on their operations while their network remains secure.

The Outcome

Customers using Apex EDR will benefit from significantly enhanced endpoint protection, including proactive threat detection and automatic response to malware, ransomware, and zero-day exploits. With continuous monitoring and the ability to quickly isolate and rollback infected devices, businesses experience reduced downtime, fewer breaches, and overall improved security posture. The managed service provided by Apex ensures that updates, monitoring, and responses are handled seamlessly, giving business owners peace of mind.

What This Product Does:

Proactive Threat Detection and Response: Automatically detects, isolates, and responds to suspicious activity across all endpoints.

Managed Security Service: Apex monitors and manages your EDR solution, ensuring continuous protection and immediate responses to threats.

Cloud-Based Management: Centralised management allows for consistent security across all devices, whether on-premise or remote. Rollback Capabilities: In the event of an attack, Apex EDR can roll back systems to a pre-infection state, mitigating the damage caused by malware or ransomware.

Real-Time Threat Hunting: Deep visibility into endpoint activity allows for proactive threat hunting and analysis, keeping businesses ahead of cybercriminals.

What This Product Doesn't Do:

Not a Full Security Solution: Apex EDR provides endpoint security but does not cover all aspects of cybersecurity. For complete protection, it's recommended to use the Apex Cyber Security Sphere and Apex Firewalls for comprehensive network security.

Doesn't Replace Endpoint Awareness: While it detects and responds to threats, EDR solutions work best alongside employee training to prevent accidental downloads or malicious clicks. Businesses with poor IT infrastructure may not fully benefit from EDR's capabilities.

Doesn't Address Internal Threats: EDR focuses on external threats but does not completely cover insider threats or physical security breaches. Internal security policies must also be in place.

Security

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk