The most complete endpoint security solution for the cloud generation

Aptronics Endpoint Security as a Service, powered by Symantec Endpoint Protection (SEP) to protect endpoints from all attack vectors at industry-leading efficacy within a single agent architecture.

Prevention:

SEP protects endpoints regardless of where attackers strike. This level of prevention is only possible with a combination of core technologies and leading-edge technologies.

Signatureless Technologies:

Detect new and evolving threats before they execute with Advanced Machine Language (AML. Defuse zero-day exploits with Memory Exploit Mitigation and monitor and block suspicious files with Behaviour Monitoring.

Advanced Capabilities:

Leverage the world's largest civilian threat intelligence network informed to determine the safety of files and websites with Reputation Analysis using artificial intelligence.
Thanks to Intelligent Threat Cloud, downloading all signature definitions to the endpoint to maintain a high level of effectiveness is no longer required. New programmable REST APIs make secure web gateway integration possible to orchestrate quick response at the endpoint to halt the spread infection.

Core Capabilities:

Tuneable security called Intensive Protection is now available with a new cloud console that integrates automatically with the on-premises SEP Manager and provides an easy workflow to blacklist suspicious files or whitelist any false positives.

- **Antivirus:** Scans and eradicates malware that arrives on a system.
- **Firewall and Intrusion Prevention:** blocks malware before it spreads and controls traffic.
- **Application and Device Control:** Manages file, registry, and device access and behaviour; with whitelisting and blacklisting.
- **Power Eraser:** Aggressive tool that can be triggered remotely to address advanced persistent threats and remedy tenacious malware.
- **Host Integrity:** Enforces policies, detects unauthorised changes, conducts damage assessments and can isolate endpoints that do not meet requirements.
- **System Lockdown:** Allows whitelisted applications (known to be good) to run, or block blacklisted applications (known to be bad) from running.

Detection and Response (EDR):

Incident investigation and response can be deployed within an hour to expose advanced attacks. EDR capabilities let incident responders quickly search, identify and contain all impacted endpoints while investigating threats with on-premises and cloud-based sandboxing. Continuous recording of system activity supports full endpoint visibility and real-time queries.

Symantec EDR:

Detects and Exposes – Reduce time to breach discovery and quickly expose scope.

- **Investigates and Contains** – Increase incident responder productivity and ensure threat containment.
- **Resolves** – Rapidly fix endpoints and ensure threat does not return.
- **Enhances Security Investments** – Pre-built integrations and public APIs.

Deception:

SEP Deception plants deceptors (i.e. baits) to expose hidden adversaries and reveal attacker intent and tactics. This early visibility enhances security posture. Accurate and insightful detection is possible while delivering fast time to value.

Adaptation:

SEP Hardening is a cloud-delivered advanced application defense that can isolate suspicious apps and shield trusted ones to maintain high employee productivity by fully supporting standard employee workflows.

SEP Hardening:

Comprehensive application security by minimising the attack surface

- Unprecedented visibility by discovering and categorising all endpoint applications.
- Fastest speed to value by leveraging SEP's single agent architecture.