



NCL

Endpoint Protection

Powered by



Protect your user and server endpoints from attack through AI-based proactive monitoring and behavioural based threat protection.

By analysing files before and after they execute, the service identifies the tell-tale signs of attacks, including zero-day malware, fileless and script-based attacks. Our protection techniques cover the MITRE ATT&CK[™] Framework.

Our software agents provide response options to quickly contain threats while allowing analysts to collect additional endpoint information and further their investigations. Threat containment options include:

- Endpoint isolation – disabling network access except to our management console for investigation and remediation
- Terminate processes to stop any running malware
- Blacklist files to stop further execution
- Quarantine malicious files
- Retrieve files from endpoints for further analysis and investigation
- Directly access endpoints to view, delete, move, or download files
- Enforce configuration through centrally managed policies



MITRE | **ATT&CK**[™]

Protection that covers the entire MITRE ATT&CK[™] Framework

Features & Benefits

Features

- AI-based endpoint analysis
- Detection of common and advanced attacks
- Ransomware and malware protection
- Remote control corrective action
- Cloud based centralised Management
- Integration with cloud-based WildFire® malware prevention

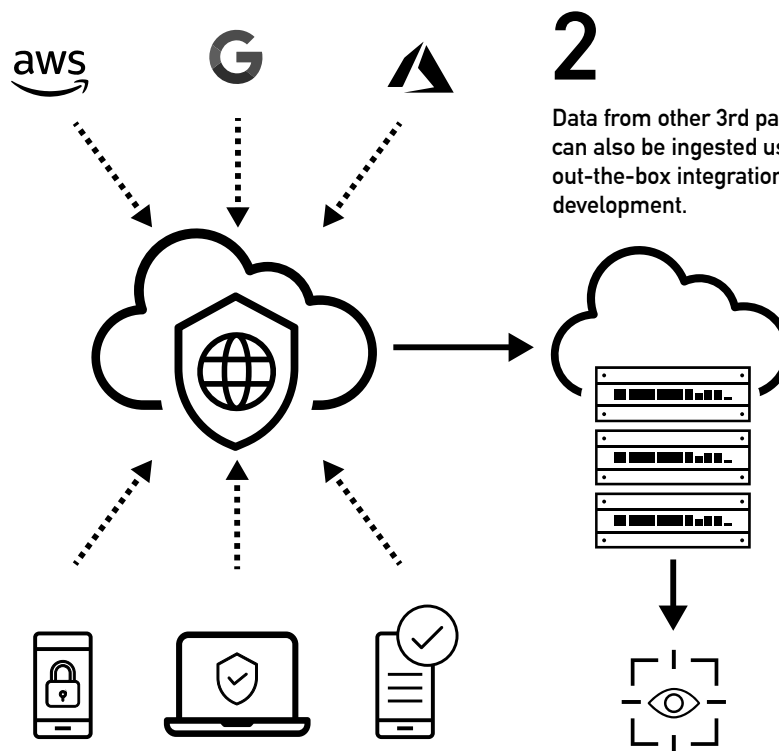
Benefits

- Reduced meantime to detect and to respond
- Minimise cost, time and effort in dealing with attacks
- Centralised management of end point security configuration
- Reduce impact of attack

Solution Overview

1

The Endpoint Protection solution is cloud based with agents installed on endpoints (laptops, desktops, tablets and servers) within your enterprise, and can be deployed in a matter of days.



2

Data from other 3rd party tools can also be ingested using out-the-box integrations or development.

3

We facilitate the software purchasing and licensing to enable you to manage protection from the central cloud platform. We can also help further with developing enhanced security policies to block USB drives or automatically isolate and endpoint in the event of malware detection.