SOC

SECURITY OPERATIONS CENTRE

Managed EDR & EPP

Next-Gen Endpoint Security & Response

01 Managed Endpoint Detection, Response & Protection

Nettitude is an award-winning cybersecurity organisation with unparalleled capability in delivering managed security services. Through our managed global Security Operations Centres (SOCs) we can deliver round the clock services that secure our clients and detect and respond to sophisticated cyber-threats, providing assurance that your organisation is protected.

Technology alone cannot completely mitigate the risk from cyber threats. Instead, businesses must respond through a well-managed security service considering all aspects of risk and using processes that extend through technology and into the workforce.

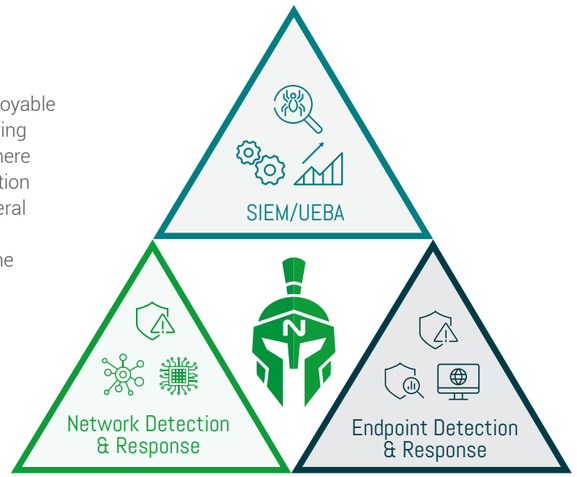
A Managed EDR or EPP service can provide a level of visibility and security that can be difficult to maintain in-house, both in terms of availability and expertise. The Nettitude Managed EDR/EPP service can be utilised for organisations that have limited resources and expertise to assist with the provision, management and monitoring of EDR and EPP technologies to provide a world-class capability in detection and response.

02 What is Managed EDR/EPP?

Endpoint Detection and Response (EDR) tools provide an integrated endpoint security solution that provides real-time continuous monitoring and detection, combined with response and analysis capabilities.

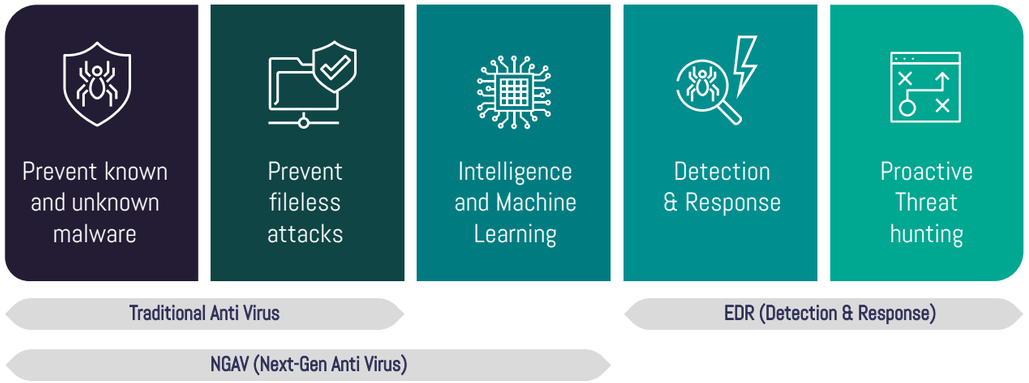
Endpoint Protection Platform (EPP) is an evolution of the next-generation anti-virus capabilities, providing prevention, detection, and monitoring for both file-based and file-less malware using static Indicators of Compromise (IOCs), signatures, and behavioural analytics.

Advanced endpoint protection solutions provide integrated EDR and EPP capabilities in a single deployable agent. Endpoints are a critical area for both monitoring and protection as the majority of attacks will land there and are where an attacker will look to get the execution of their tooling, achieve privilege escalation, and lateral movement. The importance of endpoint security monitoring was recognised by Gartner and forms the cornerstone of their security monitoring triad.



Nettitude's Managed EDR and EPP is a next-generation endpoint security solution providing advanced detection, protection, and response use cases across a wide variety of network environments.

Nettitude delivers the service using the Crowdstrike and Carbon Black suite of tools, enabling our clients to choose the right solution for their environment. The service is delivered 24/7 365, providing constant protection, detection, and monitoring across all your endpoints.



NGAV + EDR = Next-Generation endpoint security

03 About Crowdstrike

The Crowdstrike falcon platform is a Gartner leading technology, providing best of breed endpoint detection and response. It includes integrated threat intelligence and additional bolt-on modules including firewall management, USB device control, vulnerability management, and IT hygiene capabilities.

Crowdstrike uses a lightweight agent that has no impact on user performance and prevents both commodity and sophisticated attacks for file-based and file-less attacks.

The solution provides real-time endpoint visibility and insight into applications and processes across the environment. It protects all workloads, able to operate across Windows, MacOSX, Linux, mobile devices, as well as servers and containers in modern hybrid multi-cloud data centres.

04 About Carbon Black

VMware Carbon Black provides a next-generation AV and EDR solution that protects against the full spectrum of modern cyber-attacks. Using the universal agent and console, the solution applies behavioural analytics to endpoint events to streamline detection, prevention, and response to cyber-attacks.

Protection is provided through multiple layers which include file reputation, heuristics, machine learning, and behavioural models to analyse endpoint activity and block malicious behaviour to stop all types of attack before they reach critical systems. With flexible behavioural prevention policies, protection is easily tailored to your distinct needs.

Carbon Black records all process activity on an endpoint, making it ideal as a threat hunting and incident investigation platform.

05 Why do you need EDR & EPP?

Most attacks will first manifest themselves on an endpoint. Organisations must deploy both protection and detection capabilities across the endpoint estate to prevent attackers from gaining a foothold in the network, limiting their options for lateral movement and further exploitation. Nettitude offers two next-generation detection, response, and prevention solutions, enabling our clients to choose a solution that matches their needs.

Better Protection

Complex threats require active and integrated tooling at the most likely point of malicious activity (the endpoint). It is no longer sufficient to just monitor activity, it must be blocked/prevented to prevent catastrophic attacks such as ransomware. EDR/EPP solutions use a combination of advanced analytics, threat intelligence to block threats and provide a platform for responders to operate from.

Reduced Complexity

The SOC-as-a-Service offering provides a single dashboard interface for managing the deployed agents. No on-premise infrastructure is required.

Increased efficiency

The managed service increases security and provides a workaround to the problem of skills shortage by accelerating security operations, using automation, and reducing the time and effort to respond to incidents.

06 Benefits of Managed EDR & EPP

The Nettitude Managed EDR and EPP service significantly reduces the likelihood of an adversary completing their attack, leading to a data breach or other malicious action. It also reduces the time to detect and respond to an incident. These metrics (known as Mean Time to Detect or MTTD and Mean Time to Respond or MTTR) are key indicators of an effective detect and respond capability.

The specific objectives of the service will be customised to each client collated through the BI workshop and service reviews on an ongoing basis. This is because every client will face different threats and operate a unique set of critical assets. Nettitude understands this and therefore can customise the detection through a unique set of use cases.

Defence Sophistication

Next-Gen Endpoint Security is far superior to traditional Anti-Virus technologies

Designed to prevent and detect sophisticated threats including Ransomware

Leverage Machine learning, Threat analytics & Intelligence

Reduced Complexity

Security Architectures can be incredibly complex, Simple Cloud based SaaS solution

Single lightweight agents deployed within minutes

Easily integrated into other security products and tools to achieve automation & orchestration

Advanced Expertise

Security tools need expertise and training to ensure they are deployed, configured and managed properly

Using Nettitude managed service provides world class expertise that's always on and always available

Efficiency

Built in automated actions covering containment and response managed through a single management console

Log based and traditional AV generate large amounts of false positive alerting

Advanced Next-Gen protection means more threats are blocked at the point they land, meaning less remediation

Rapid Response

Traditional Monitoring only solutions don't 'Block' which means complex attacks like Ransomware are not prevented

Sophisticated detection, response & forensic capability allows defensive teams time to contain and limit harm

Automated blocking & live response features ensure a rapid response in real-time

07 Managed EDR & EPP – Service Features

Nettitude's Managed Endpoint Detection and Response service provide the most highly accredited expertise combined with Gartner Magic Quadrant leading security technology to deliver industry-leading protection for your organisation.

Our approach is proactive, and threat led; informed by our offensive and threat intelligence teams to shape our defensive stance and protect against the latest industry threats providing in-depth unrivalled detection and alerting capability where it is needed most.

24/7/365 Always on

24/7 x 365 Expert Security Analysis: always there, monitoring & alerting and advising for your peace of mind

Global Delivery

Nettitude has been at the forefront of cyber security SOC Operations since 2003. Our Managed EDR & EPP services can be deployed and managed Globally through our Global Security Operations Centres

Global Expertise

Certified expert knowledge within Offensive and Defensive Cyber operations, our SOC team are on hand as an extension of your teams to provide expert advice, guidance and remediation where required

Security Simplicity

Security Achitecture and security tools deployment can be complex. Nettitude's Managed EDR & EPP service is provided using a cloud-based SaaS solution through a single lightweight agent that can be rapidly deployed

Leading Technology

Managed EDR & EPP solutions are Gartner leaders in protection, detection, prevention and response providing your organisation with best in class defensive capability

Dashboard & Reporting

Custom real-time dashboards created in line with your business requirements combined with Nettitude Security & Service reporting to provide you complete visibility and insight to your security stance

Performance & Availability

Nettitude maintains best in class performance across our Managed Security Services covering MTTD, MTTR and MTTE. Ensuring a rapid response to sophisticated cyber threats

Customisation & Engineering

Nettitude has certified experts that can assist in customisation, configuration and engineering to ensure complete coverage of bespoke systems and applications

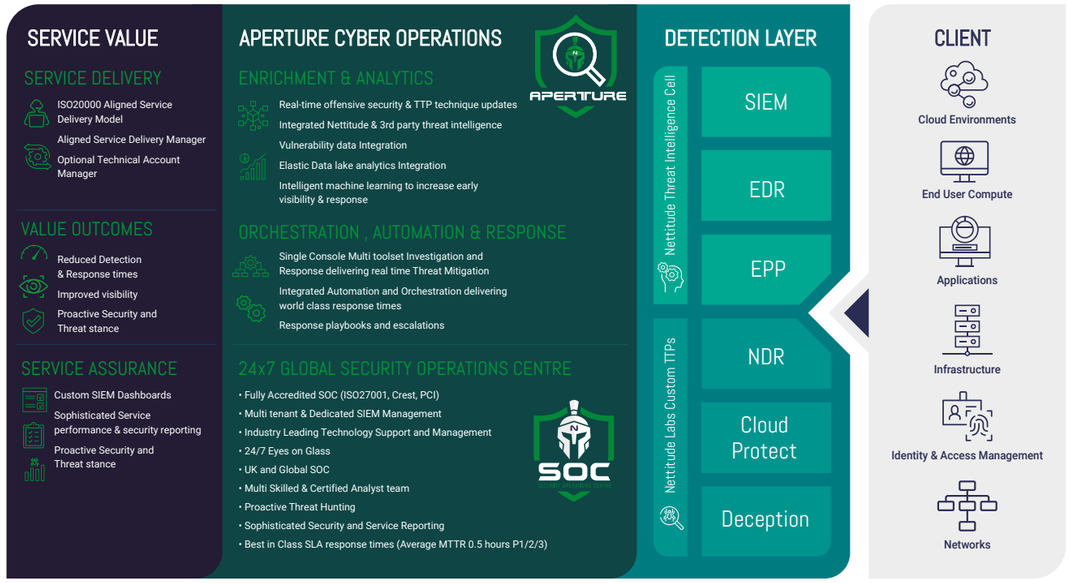
08 Nettitude Value Proposition

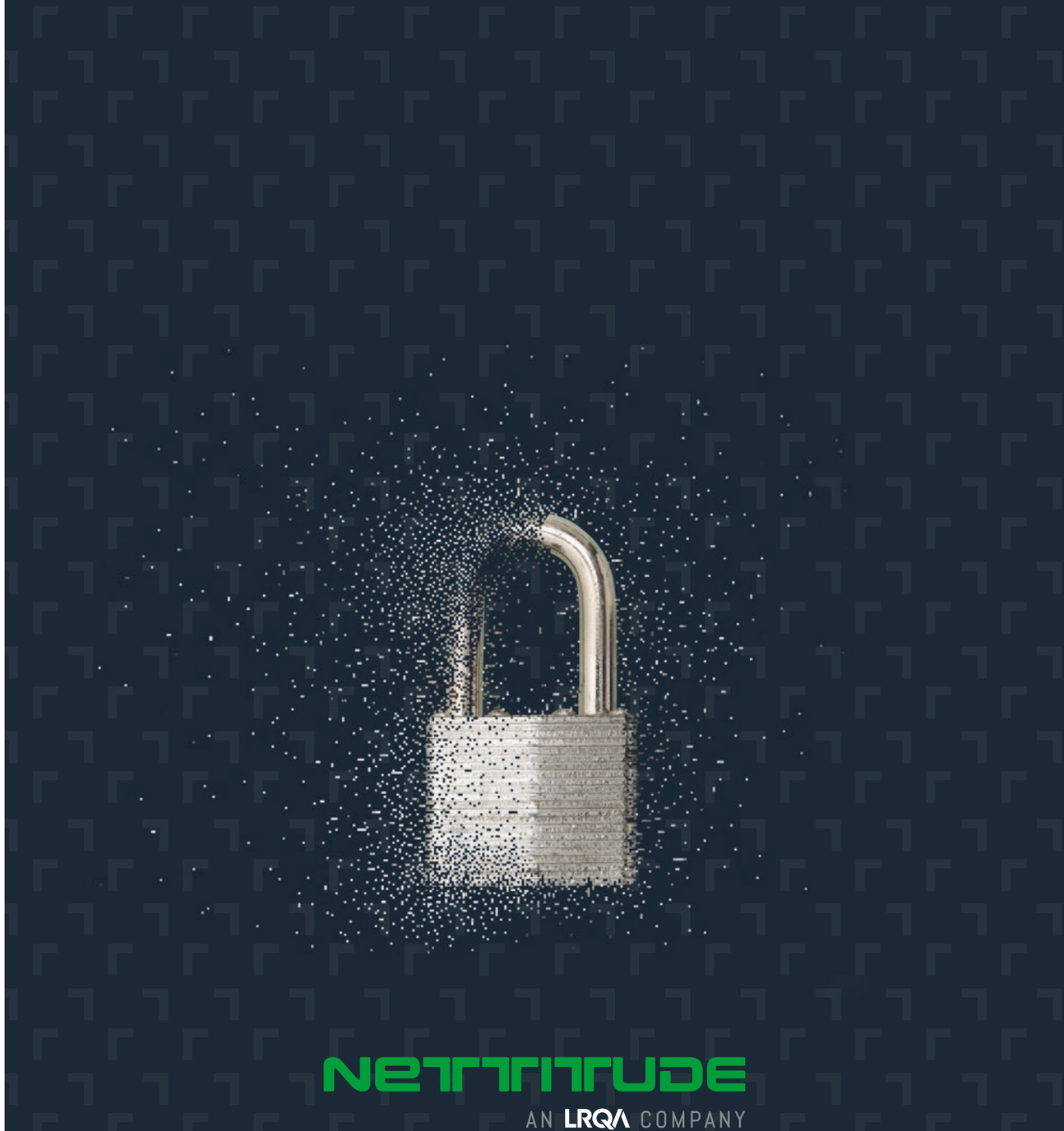
The Nettitude SOC provides advanced 24/7 monitoring and alerting to protect your business.

We use our custom developed Aperture Cyber Operations Management platform integrated with leading Gartner technologies to provide enhanced automation, orchestration & response capabilities to our SOC team.

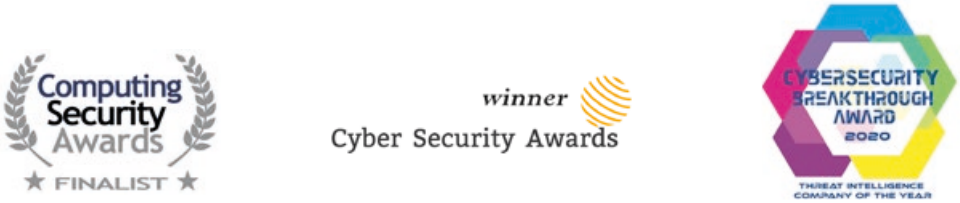
The Aperture Cyber Operations platform provides enhanced enrichment, analytics, and intelligent learning to increase early visibility and response to cyber threats in an evolving world.

By combining these technologies with our highly accredited people and processes we can deliver best in class outcomes and value for your organisation.





NETTITUDE
AN LRQA COMPANY



NETTITUDE
AN LRQA COMPANY

UK Head Office
Jephson Court, Tancred Close, Leamington Spa, CV31 3RZ

Americas
50 Broad Street, Suite 403, New York, NY 10004

Asia Pacific
1 Fusionopolis Place, #09-01, Singapore, 138522

Europe
Leof. Siggrou 348 Kallithea, Athens, 176 74
+30 210 300 4935

Follow Us

solutions@nettitude.com
www.nettitude.com