DATA SHEET

MANAGED SECURITY SERVICES

Endpoint Security Services

The workforce is becoming increasingly mobile and security risks around 'Bring Your Own Device' remain a key concern for many organizations.

Connecting laptops, tablets, smartphones, and other wireless devices to corporate networks creates a potential entry for security threats. It's critical that endpoints are secure, but the challenge remains that traditional solutions are falling short of what is required to identify risks, remove false positives and stop the spread of infection at any time of the day or night.

With Endpoint Security Services (ESS), NTT offers support for a growing list of endpoint security vendors and products and, at its core, introduces a unique solution designed to increase the speed and accuracy of human-driven response time using Endpoint Detection and Response (EDR) technologies.

Look beyond traditional endpoint security solutions

Anti-virus solutions traditionally provide scanning capabilities to detect and protect users against known malware. Their reliance on automation and up-to-date signatures is often all that stands in the way of a determined attacker, and the identification of security holes in a network may fall under the radar leading to widespread infection.

Encryption of network traffic can provide a layer of protection from attempts to siphon data while in transit, however, a determined attacker could shift focus away from secure network traffic to the decrypted endpoints it hosts, increasing the number of potential targets and opening the door to an entire network.

Response times are also a problem in an industry that requires experts available round the clock. It takes a single click from a trusted source to unintentionally spread malware from one machine to another so it's critical to both identify a breach and stop the spread of infection as quickly as possible.

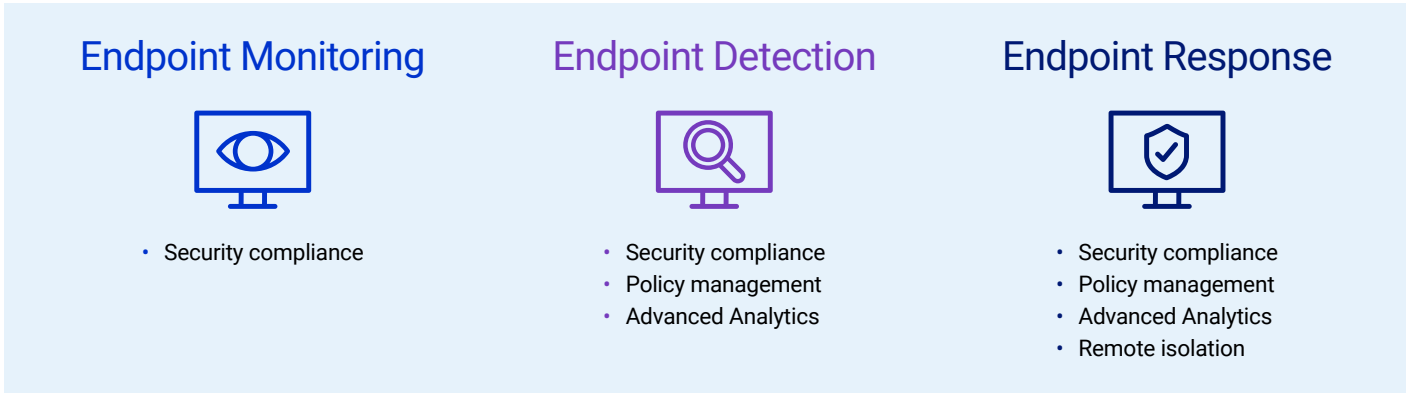
Some endpoint security solutions provide detection and protection capabilities along with automated isolation of endpoints that show symptoms of compromise. While automation does provide a fast response time, the potential for unconfirmed false positives could result in automated quarantine of endpoints that are not truly at risk. Alternately, lost opportunities for identifying new compromises based on human-driven security intelligence could occur.

Benefits of Endpoint Security Services:

- Increased speed and accuracy of response from both automated tools and human review
- Reduced time spent manually reviewing endpoint logs
- Reduced downtime resulting from false positives
- Improved security posture from recommendations for remediation and security best practice

Remediation often begins with a root cause analysis, and to determine the source of malicious activity huge amounts of log data generated from all connected endpoints within a group or network are reviewed. Without the added support of a log analysis engine and experienced security analysts, key evidence, and indicators of compromise may be overlooked and the breach uncontrolled.

Figure 1: Endpoint Security Services offer support for a growing list of endpoint security products and are available at three levels to suit the requirements of your business.



Choose the right level of endpoint security for your business

Endpoint Security Services from NTT is available through the NTT Global Managed Security Service Platform. It combines the capabilities of market leading EDR solutions with NTT Threat Intelligence and Advanced Analytics. With a 24/7 SOC staffed with security experts trained to deliver a variety of MSS support features for your chosen endpoint security technology you will reduce time spent manually reviewing host endpoint logs, benefit from the speed of automation alongside human validation, reduce downtime from false positives, and receive recommendations for security best practices.

Endpoint Security Services are delivered at three service levels

Endpoint Monitoring (EPM): This service level includes monitoring for compliance, security best practices, and business policy compliance reporting. By establishing baselines through log collection and data trending, EPM delivers customized alerting, compliance driven reporting, and best security practice guidance for endpoint detection and protection devices.

Endpoint Detection (EPD): Combines threat detection capabilities of leading EDR solutions with NTT Threat Intelligence and Advanced Analytics. This service level adds a sophisticated layer of machine learning, behaviour analysis and kill-chain modelling overseen by security analysts skilled in reviewing evidence data. Indicators of compromise provided by the vendor are monitored in real time and when paired with network and cloud security services, enable event correlation and enrichment with NTT Threat Intelligence. Research and recommendations are broken down into easy to understand incident reports that provide a summary of events and recommended remediation actions.

Endpoint Response (EPR): Leverages the remote isolation features of an EDR technology to provide fast and efficient 24/7 quarantine support for confirmed instances of compromised endpoints. Alerts generated by indicators of compromise, further validated by NTT watch lists and human-driven advanced analysis, reduces the potential for erroneous user or group lockouts caused by false-positive alerting and provides incident level analysis and remediation feedback when threats are confirmed.

About us

NTT is a leading, global technology services company. We believe that together we do great things. We've combined the capabilities of 28 remarkable companies to create one, leading technology services provider. Partnering with you, we empower your people, strategy, operations, and technology through our full range of unparalleled capabilities and services. Together we enable the connected future.

Want to know more about our range of managed security services?

Visit **hello.global.ntt** for details.