Data sheet

Managed Detection and Response for Cisco Secure Endpoint

Maximize business resiliency by disrupting threats on the network and at the endpoint early

NTT partners with Cisco because together, we enable 24/7 human and machine expertise, leading technologies and global threat intelligence to detect and disrupt hard-to-find attacks and make you more secure.

The world as we know it has changed. We work where we choose. Collecting, investigating, sharing data and collaborating all day, every day. The endpoints on which we operate are worldwide. At the same time, threats are more sophisticated and traditional approaches to secure the endpoint are not enough. We envision a hyper-connected world, with less risk and more innovation in any industry.

To make this a reality, we continuously capture events from network and endpoints. By applying advanced analytics, threat intelligence and behavioral analytics to detect, respond to and prevent attacks. With threats identified in real-time, we can respond quickly and effectively by isolating endpoints, blacklisting malicious behaviors, or terminating processes immediately. And, with the number of endpoints growing, security can grow in tandem with cloud-based security applications that are being built into the fabric of your infrastructure.

By bringing together NTT's Managed Detection and Response (MDR) service and Cisco's endpoint detection and response (EDR), you can protect endpoints and both private and public cloud workloads. Under a new cloud of protection, the endpoint is the new perimeter.

How NTT and Cisco innovation works together

NTT's MDR is fully integrated, via APIs and automation, with Cisco EDR. MDR augments endpoint visibility with the NTT Cyber Threat Sensor (CTS), a purpose-built, fully managed network traffic analysis (NTA) technology with full packet capture (PCAP) recording. The combination of event and evidence data from endpoint and network technology stacks gives deep visibility to detect sophisticated cyber-attacks.

The NTT advanced analytics engine leverages big data threat intelligence and an extensive machine learning (ML) framework. The algorithms continuously harvest vast amounts of data from exclusive sources that are applied to multiple supervised and unsupervised ML stages. NTT is uniquely positioned to build robust detection algorithms that quickly and accurately identify suspicious and malicious activity. This is why more security incidents are initially detected by NTT methods rather than by the native detection capabilities of any single technology.

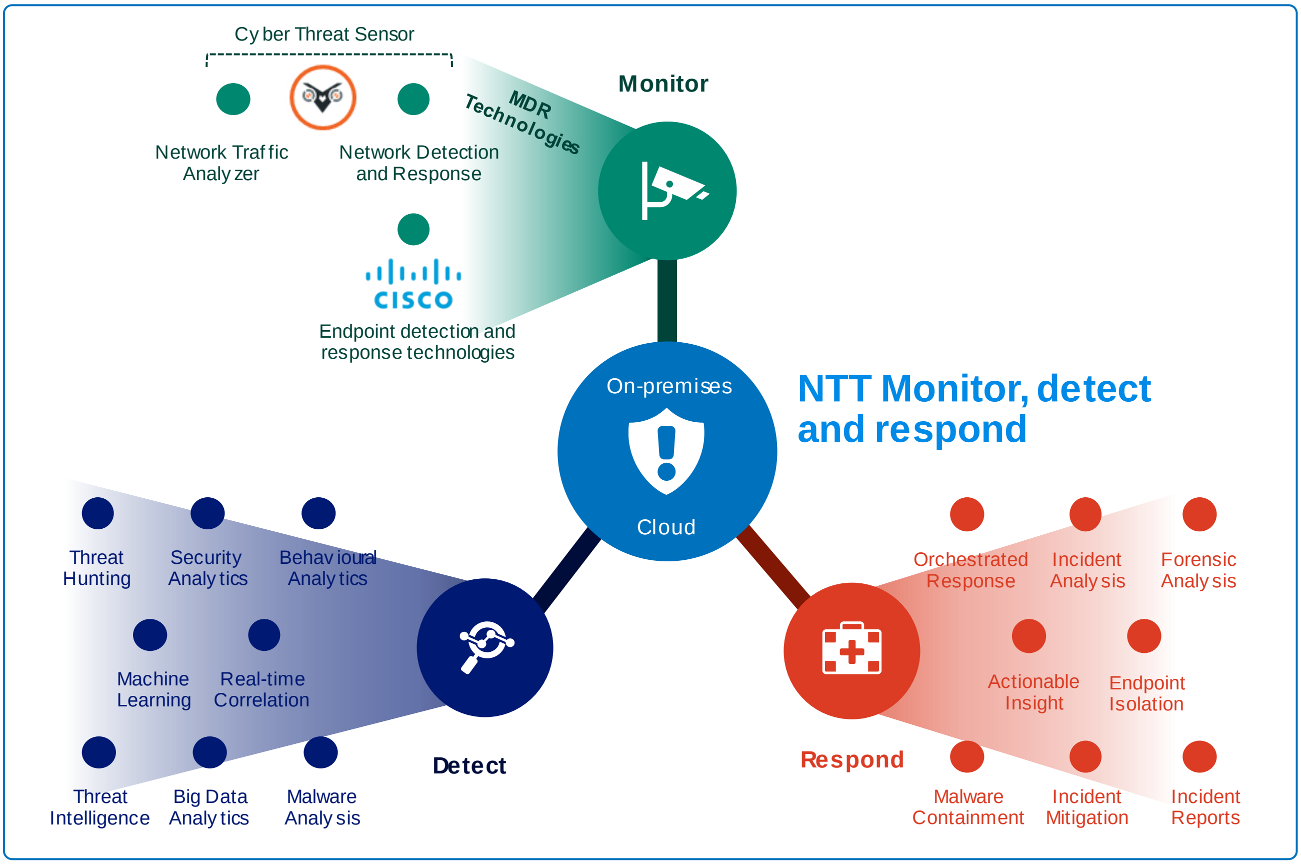
Solution benefits

- Increase speed and accuracy of response from both automated tools and human review.
- Improve security posture from recommendations for remediation and security best practice.
- Accelerate mean-time-to-respond with remote isolation.
- Prioritize threats through advanced analysis with NTT Security Intel.
- Implement a secure by design strategy for holistic attack coverage across the entire infrastructure.

> **'PCAP data helps us detect four times more incidents than without.'**
> - Security analyst

Evidence data is like having all the clues from a crime scene, enabling the detective to develop plausible theories. Security analysts use digital evidence from EDR and PCAP data from the Cyber Threat Sensor. The analysts hunt for threats as they pivot from one piece of evidence to another until they find an attack path that leads to a security incident. After detecting signs of initial compromise, it is imperative to respond as fast as possible to reduce potential impact. MDR includes response capabilities in the form of automated remote isolation of compromised hosts. Security analysts can remotely quarantine specific devices after ensuring that the target devices were the source of a security incident. NTT's solution success team then offer dedicated guidance and risk based oversight, helping you to make the right decisions every step of the way.

MDR Features: Monitor, detect and respond



Cisco Secure Endpoint

Stopping threats at the earliest point in time ensures minimal damage to endpoints and less downtime after a breach. Though malware prevention techniques are necessary for a complete next-generation endpoint security solution, combatting advanced threats requires additional measures. Secure Endpoint continuously monitors endpoints to help detect new and unknown threats.

As the largest enterprise cybersecurity company in the world, Cisco leads the way with solutions that are driving the industry in SASE, XDR, and zero trust. Integrating it all is Cisco SecureX, the security platform that provides simplicity, visibility and efficiency across your security infrastructure. SecureX is an open and integrated platform that includes extended detection and response (XDR) capabilities and beyond with every Cisco Secure product.

Cisco Secure Malware Analytics (formerly Threat Grid) is included as an integrated component of many secure products. When integrated with Secure Endpoint, Secure Malware Analytics provides rich contextual information to the integrated product to not only determine if a file is malicious, but enhance the ability to detect a wider range of known and unknown malware. IT combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware. With a robust, context-rich malware knowledge base, you will understand what malware is doing, or attempting to do, how large a threat it poses, and how to defend against it.

Our joint solution provides:

- Immediate network and endpoint visibility with Cisco EDR and NTT Cyber Threat Sensor.
- NTT advanced analytics with machine learning and threat intelligence applied across network and endpoint data.
- 24/7 Analyst-driven investigation and disruption of attacks using NTT'S threat hunting platform.
- Comprehensive incident reports.
- Orchestrated remote isolation of compromised hosts.
- Portal for centralized information and reports.
- Collaborative workflow with Technical Account Manager to increase cyber-resilience.

About NTT

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 services?

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

About Cisco

Cisco Systems Inc. is the worldwide leader in networking for the internet. Cisco's networking solutions connect people, computing devices and computer networks, allowing people to access or transfer information without regard to differences in time, place or type of computer system. So, as you explore the possibilities for your business, start at the beginning. Cisco Systems built the internet, so we know exactly what it takes to get your business online. Take advantage of our experience and knowledge to get the internet working effectively for your business.

Visit **cisco.com** for details