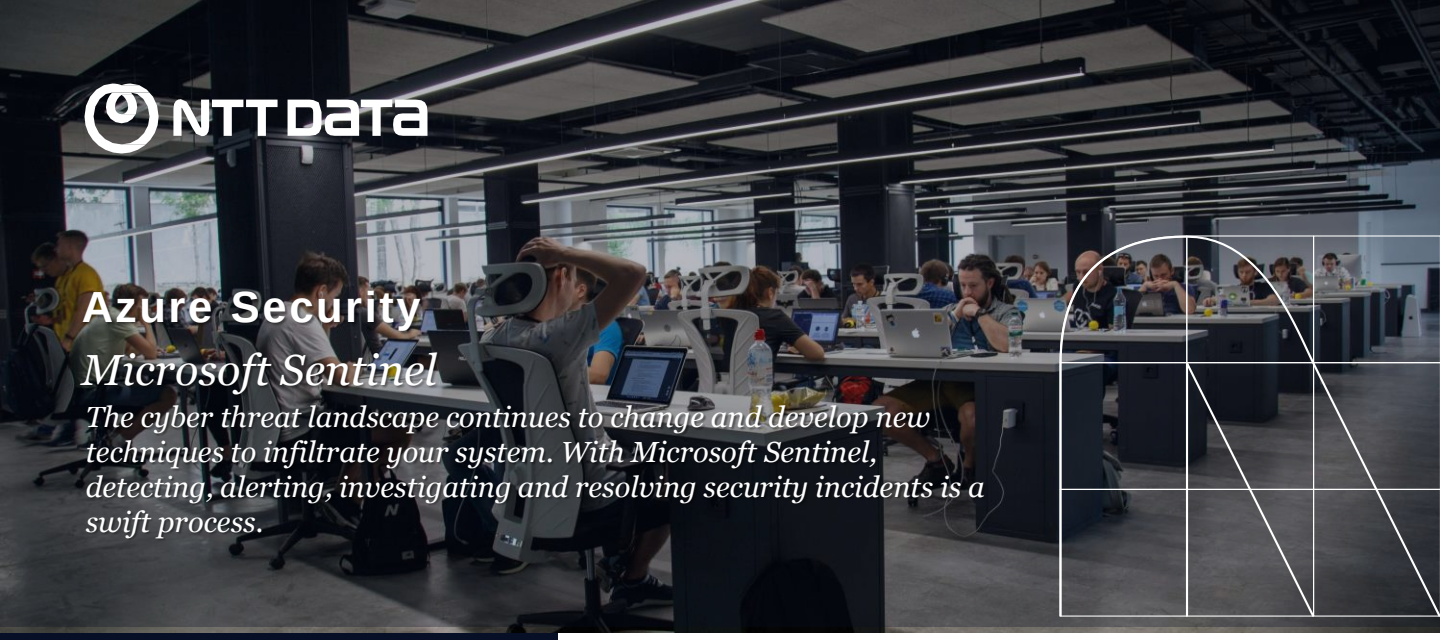

Azure Security

Microsoft Sentinel

The cyber threat landscape continues to change and develop new techniques to infiltrate your system. With Microsoft Sentinel, detecting, alerting, investigating and resolving security incidents is a swift process.

Benefits of Microsoft Sentinel

- Cloud-native security information and event management (SIEM) AND security orchestration automated response (SOAR) solution all in one
- Integrated toolset needed to help fight against attacks that take advantage of today's diverse, distributed, and complex environments.

Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

As the threat landscape continues to evolve, the need to effectively monitor your organization's infrastructure has increased. In the absence of a central place which investigates the alerts or incidents generated from existing security products, Microsoft Sentinel provides your organization with an all-encompassing view of your on-premise, cloud and application infrastructure. Sentinel is secure, scalable and always available because it is a native part of Azure.

1 **External Data Source**
Microsoft Sentinel allows you to add third-party (on-premises) products.
For example, with this solution, an organization can secure its environment by correlating data from the cloud with its firewall logs.

2 **Incident Handling**
Allows you to assign incidents, change the status, assignment to groups, and support for markdown comments
Microsoft Sentinel goes further than Microsoft 365 Defender which simply allows you to assign incidents and change the status

3 **Automation**
Microsoft Sentinel has various API capabilities, but also allows you use Azure Logic Apps to automate incident handling
This feature allows users to centrally manage the automation of incident handling. Microsoft Sentinel and will enable you to simplify complex workflows for your incident orchestration processes.

4 **Support for Managed Security Service Providers**
Capabilities which provide an easier way of management across multiple tenants
Microsoft Sentinel includes some capabilities specifically targeted to Managed Security Service Providers. One example is the ability to view the incidents from all customers in a single view.

How Microsoft Sentinel works to achieve business benefits

NTT DATA Solution

- Receive insights into the raw data and potential malicious events and incidents through overviews, dashboards and custom queries
- Microsoft Sentinel is a native part of Azure. This means that it is scalable, always available and that it is secure.
- Integrate with security systems and provide automation capabilities for those systems

Joint Solution

- Streamlined and cost-effective security data collection
- Connect to and collect data from all your sources
- Behavior analytics to stay ahead of evolving threats

Tangible Benefits / Desired Outcomes

- Intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting, and threat response.
- In-depth perspective across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames.
- Intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting, and threat response.
- Enriched investigation and detection with AI and enables you to bring your own threat intelligence.

Why NTT DATA

NTT DATA has a proven track record as a Microsoft partner with a large skilled and experienced team of Microsoft-certified specialists. From consulting to managed services, we keep your enterprise applications responsive and reliable, enabling collaboration and a platform for innovation. We assess current IT landscape, deliver recommendations and a roadmap for optimisation and assist your organization to better monitor your cloud infrastructure. Along the way, offering guidance through complexities and intricacies. We offer bespoke business solutions using a SAFe Agile methodology and globally integrated ITIL processes. With our highly skilled application, Azure migration and advanced networking teams, we guarantee excellence in delivery. NTT DATA is able to provide a full end-to-end solution to an organisation in every industry vertical. Our capability across the full IT stack enables us to provide supporting services giving you an advantage. With NTT DATA you are also able to gain access and leverage on our Global Threat Intelligence core capability that pulls data from a broad array of sources.

Learn more about NTT DATA
NTT DATA