Data sheet

Managed Security Services

Enterprise Security Monitoring Services

Cloud-based security monitoring for **business policy, security best practice and regulatory compliance.**

Today's organizations are under constant pressure to protect their data and critical systems.

Ensuring compliance with tightening regulations is key to an effective security strategy, but most organizations have a long way to go to achieve continuous monitoring of networks. Too often, the burden placed on internal teams to monitor systems 24/7 results in gaps in security monitoring or the complete failure to monitor logs at all.

Regulations such as PCI DSS, HIPAA, and SOX demand that logs are regularly monitored, and failure to do so can result in stiff penalties.

Our Enterprise Security Monitoring Services provides you with 24/7 log monitoring and analysis so you can comply with robust log monitoring requirements.

Cloud-based monitoring by security experts

We monitor logs from virtually any device capable of producing a log file, including applications, databases, endpoints, firewalls, intrusion detection and prevention systems (IDS/IPS), unified threat management systems (UTMs), web application firewalls (WAFs), file integrity monitoring systems (FIMs), and other network devices. We enrich the gathered security data with contextual information such as vulnerabilities, assets, GeoIP, malicious hosts, and privileged and non-privileged users. This enables us to provide effective security monitoring for business policy, security best practice and regulatory compliance.

Security monitoring for best practice and compliance – two service levels share common features

We provide two service levels for enterprise security monitoring: Enterprise Security Monitoring Standard and Enterprise Security Monitoring Enhanced. Both offer 24/7 monitoring by our dedicated Security Operations Centers. Each service benefits from the comprehensive threat intelligence delivered by our Global Threat Intelligence Center.

Enterprise Security Monitoring – Standard

Our Standard service is designed for organizations with standardized security compliance requirements across a core set of security technologies. It includes 24/7 monitoring using a standard set of detection rules across these technologies. This cloud-based service offers first-level Security Operations Center monitoring and response, with escalation to your organization for further investigation or closure.

We use our proprietary platform to provide effective compliance monitoring. This ensures your business remains compliant. The standard service includes access to a customized portal that efficiently communicates event information, a dashboard view of services, and executive and technical compliance reporting.

Enterprise Security Monitoring – Enhanced

Our Enhanced service offering is designed for organizations with custom security compliance requirements across a wide set of security technologies.

We support complex use cases, such as creating correlation and notification rules to support specific business requirements. We currently support over 200 different vendor technologies.

This service includes 24/7 monitoring by our Global Security Operations Centers. Our team identifies events and escalates them to experienced, certified level one and two security analysts for review and validation. Once validated, the events are escalated to you as security incident reports for additional investigation.

Enhanced services are backed by our Global Threat Intelligence and includes access to a customizable portal that efficiently communicates event and security incident information, a dashboard view of services, as well as executive and technical compliance reporting.

Figure 1: Feature comparison between the Enterprise Security Monitoring – Standard and Enterprise Security Monitoring – Enhanced Services.

Capability	Enterprise Security Monitoring - Standard	Enterprise Security Monitoring - Enhanced
24/7 Security operations center coverage	✓	✓
Service enhanced by NTT Global Threat Intelligence Center		✓
Standardized security compliance profile	✓	
Customized security compliance profile for a large range of devices		✓
Analyst reviewed security incident reports[1]	✓	✓
Customizable web portal	✓	✓
Customizable monitoring and compliance reporting	✓	✓
Access to 90 days of event and security incident data	✓	✓
[Option] Raw log search		✓
[Option] Secure long-term log storage and management	✓	✓

[1] The ESM Standard service is automated for high confidence events, with Security Analyst verification for selected events.

Benefits of our Enterprise Security Monitoring Services

- Enhance legal and regulatory compliance with active monitoring and detailed compliance reporting for regulatory and industry frameworks.
- Protect your organization's data and systems 24/7, with cloud-based monitoring and response.
- Multiple Security Operations Centers (SOCs) available to you 24/7.
- Security event escalation and context-aware alerting.
- Customizable use cases and alerting rules that meet your business requirements.
- Optimized Enterprise Security Monitoring through our Enterprise Security Program Services.
- Flexible service tiers that allow the services to grow with you.

About us

NTT is a global technology services company bringing together the expertise of leaders in the field. We partner with organizations around the world to shape and achieve outcomes through intelligent technology solutions. For us, intelligent means data driven, connected, digital, and secure. As a global ICT provider, we employ more than 40,000 people in a diverse and dynamic workplace, delivering services in over 200 countries and regions. Together we enable the connected future.

Get in touch

If you'd like to find out more about our services, speak to your client manager or
visit our website