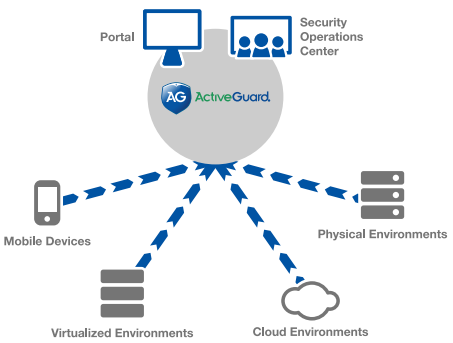
NTT Security

Data Sheet

Log Monitoring and Management Services for Security and Compliance

NTT Security Log Monitoring and Management services provide clients with 24/7 monitoring and log management to protect against threats and comply with regulations that require log monitoring and retention.

Organizations are under constant pressure to protect data and critical systems. Monitoring logs is a critical component of a security strategy and a requirement for regulations such as PCI DSS, HIPAA, SOX and others. Too often, the burden placed on internal teams to monitor systems 24/7 causes organizations to have gaps in their detection or to not monitor logs at all. On-premise Security Information and Event Management (SIEM) systems can monitor systems, but can be a challenge to implement and manage.



Cloud-based Monitoring by Security Experts

The patented, cloud-based ActiveGuard® service platform collects, monitors, and manages logs from virtually any device capable of producing a log file, including applications, databases, endpoints, firewalls, IDS/IPS, UTMs, WAFs, FIMs and network devices. ActiveGuard enriches gathered security data with a variety of contextual information such as vulnerabilities, assets, GeoIP, malicious hosts, privileged and non-privileged users to detect threats and increase accuracy.

Detect and Respond to Emerging Threats

ActiveGuard uses multiple detection methods, including signatures, anomaly detection, statistical analysis, heuristics and global threat intelligence from the Security Engineering Research Team (SERT) to detect threats. Security experts in the Security Operations Center (SOC) provide additional analysis, validation and response for security threats. The advanced analytics in ActiveGuard in combination with threat intelligence from SERT helps to recognize Advanced Persistent Threats (APTs) and zero-day attacks. With a large, diverse client base, NTT Security is able to leverage intelligence across thousands of clients to detect and respond to advanced and emerging threats faster than clients' internal teams are otherwise capable.

Log Management

Retaining logs and keeping them secure from manipulation requires true separation of duties, robust controls, and dedicated IT staff. Compliance mandates such as the PCI DSS, SOX, GLBA, HIPAA and others require organizations to monitor and retain logs.

NTT Security Log Monitoring clients also receive full Log Management services. We retain 100% of gathered logs for one year. Retained logs are stored in a forensically-sound repository in the cloud, requiring no on-site storage or additional investment.

Features Include:

- 24/7 Log Collection and Active Monitoring
- Security Event Escalation and Context-aware Alerting
- Advanced Analytics to Detect Threats
- Multiple Security Operations Centers (SOCs)
- Analysis and Validation by Certified Security Experts
- Patented ActiveGuard Service Platform
- Configurable Analytic Rules and Thresholds - Threats, Privileged Users and Policy Enforcement
- Cross-Device Correlation
- 100% Retention of Collected Logs
- Flexible Service Tiers
- Dedicated Service Delivery Manager

Add On Features:

- Extensible Monitoring to Meet Custom Needs
- Security Engineering Research Team Services
  - Critical Incident Response
  - Forensic Investigations and Expert Witness Support

NTT Security Log Monitoring and Management

A Partner You Can Trust

We don't believe that one size fits all. That's why we deliver a cybersecurity, risk management and compliance program that is as unique as your business. Our goal is to ensure that every organization develops the cyber resilience required to make the most of every business opportunity. We can provide the solution you need in the manner best suited to your specific situation and help you to avoid technical blind alleys, missed exits and roads that lead to nowhere.

The Full Security Life Cycle

NTT Security has created a Full Security Life Cycle model based on many years of providing efficient and effective security, risk and compliance services to organizations around the world. We deliver these services using local resources that leverage our global capabilities.

Plan & Optimize

We'll build a plan that considers your level of risk, potential regulatory and financial impact, ICT environment and staff capabilities; and work with you to optimize your existing security and compliance processes and controls. With a focus on enabling meaningful success criteria, budget and specific solutions to be implemented, our recommendations may range from a straightforward review and suggestions for improvement, to a study of alternative or supplementary solutions.

Architect & Deploy

Getting the most value from security solutions requires experience and expertise in both market-leading technology and delivering change, to reduce risk and make new implementations work seamlessly with your organization's business processes. Our security experts have the training and experience to ensure the right solutions are architected, configured and deployed to solve your security challenges.

Manage & Operate

High-performing security and compliance programs are built on processes and controls that are executed efficiently and consistently while producing the data necessary to monitor and manage their effectiveness within your organization. Effectively managing and operating the controls in your security and compliance program will increase your organization's understanding of your security posture, security and compliance exceptions, effectiveness of controls, and demonstrate cost-effectiveness to executive management.

Respond & Educate

Cyber resilience is based on the premise that incident avoidance is not always possible – you need to be ready and able to effectively respond to a security incident. Should the worst occur, our incident response team can be quickly engaged either remotely or on site. They will identify, document, contain and remediate a security incident to minimize the impact to your organization. We can also develop a comprehensive program for the security education of your organization.

The NTT Security Difference

We provide the necessary services across the entire information and communications technology (ICT) stack and throughout the Full Security Life Cycle. Our services portfolio covers every aspect of information security and risk management, from initial assessment through to strategic program planning, hands-on deployment and around-the-clock management and support. Service options include:

- Security Program Optimization and Enterprise Advisory
- Security Planning and Risk Assessment
- Risk and Compliance Management
- Security Solution Design and Integration
- Managed Security Services
- Cloud and Data Centre Services
- Threat Mitigation and Remediation Strategy
- Incident Response and Forensics

Get Started Today

See how NTT Security can help optimize security, improve efficiency and ease compliance. Contact NTT Security (US) today at us-info@nttsecurity.com or visit our website www.nttsecurity.com.

About NTT Security

NTT Security seamlessly delivers cyber resilience by enabling organizations to build high-performing and effective security and risk management programs, with controls that enable the increasingly connected world and digital economy to overcome constantly changing security challenges. Through the Full Security Life Cycle, we ensure that scarce resources are used effectively by providing the right mix of integrated consulting, managed, cloud, and hybrid services – delivered by local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest information and communications technology (ICT) companies in the world. For more information, visit **www.nttsecurity.com.**

1130DS 11/2016