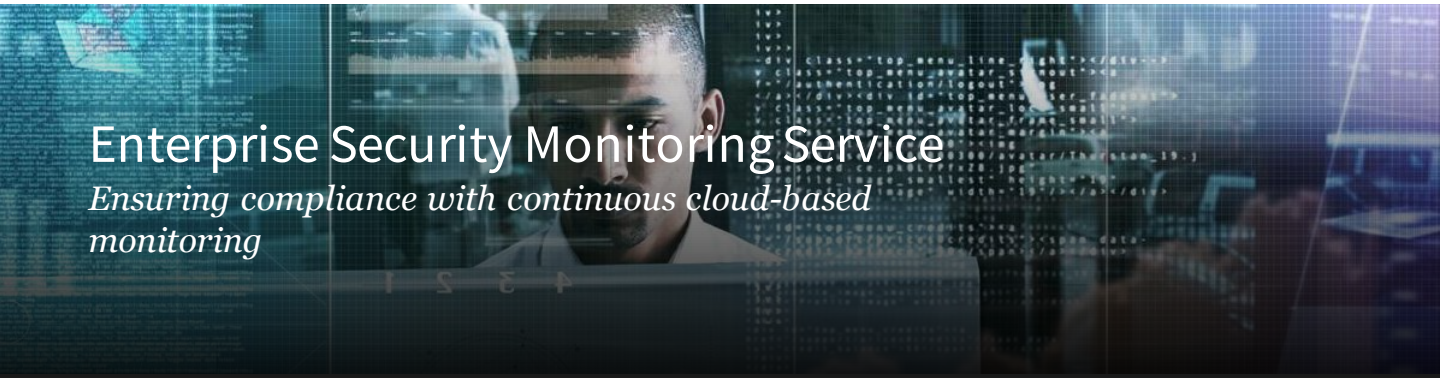
Data sheet



Enterprise Security Monitoring Service

Ensuring compliance with continuous cloud-based monitoring

Flexible cloud-based enterprise security monitoring services for legal and regulatory compliance

Business outcomes

- Enhance legal and regulatory compliance with active monitoring and detailed compliance reporting for regulatory and industry frameworks
- Protect your organisation's data and system 24/7, with cloud-based security and compliance monitoring
- Flexible service levels that allow the service to grow with you
- Customisable use cases and alerting rules that meet your business requirements
- Optimised security monitoring using enterprise security program services

Challenges

Today's organisations 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 organisations have a long way to go to achieve continuous monitoring of networks and any device capable of producing logs. 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.

Solution

Our Enterprise Monitoring Services provides you with 24/7 log monitoring and analysis so you can comply with robust log monitoring requirements. 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, and privileged and non-privileged users. This enables us to provide effective security monitoring for business policy, security best practice and regulatory compliance.

Service Packages

We provide two service Packages for Enterprise Security Monitoring: Standard and Enhanced.

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

The standard service includes access to a customised portal that efficiently communicates security incident and event information, a dashboard view of services, and executive and technical compliance reporting.

Enterprise Security Monitoring Enhanced is designed for organisations with custom security compliance requirements across a wide set of security technologies. We support complex use cases, such as creating correlation and notifications rules to support specific business requirements. We currently support over 200 different vendor technologies.

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

The Enhanced service package includes access to a customisable portal that efficiently communicates event and security incident information, a dashboard view of services, and executive and technical compliance reporting.

'Ransomware volumes increased by 350% in 2017, rising from less than 1% of global malware in 2016, to nearly 7%.'

Executive Guide to the NTT Security 2018 Global Threat Intelligence Report

Security monitoring for best practice and compliance

Both Standard and Enhanced service levels offer 24/7 monitoring by our dedicated Security Operations Centres and benefit from

Delivered on our Managed Security Services platform

We use our proprietary platform to provide effective compliance monitoring ensuring consistent services and experience. The platform-delivered services also ensures your business remains compliant at all times.

Service Element	Service Package	
Enterprise Security Monitoring Service	**Standard**	**Enhanced**
24X7 Security Operations Centre coverage	✓	✓
Standardized event detection and compliance profile	✓	
Customized event detection and compliance profile for large range of devices		✓
Automated analysis with Security Analyst verification	✓	✓
Analyst created security incident reports[1]	✓	✓
Customizable web portal	✓	✓
Customizable monitoring and compliance reporting	✓	✓
Client access to 90 days of Event and Incident data	✓	✓
Client enriched and aggregated log search 'option'		✓
NTT Security Appliance	✓	✓
Service Management		
Service Delivery Manager Client Services Manager	✓	✓
Service Transition		
Sales Engagement Phase	✓	✓
Inception Phase	✓	✓
Definition Phase	✓	✓
Build Phase	✓	✓
Deploy Phase	✓	✓
Close Phase	✓	✓

1. The Enterprise Security Monitoring Standard service is automated for high confidence events, with Security Analyst verification of selected events.

End-to-end services to meet your unique needs

Dimension Data can support you with a holistic approach with Cybersecurity Advisory to help you develop a roadmap to strengthen your security posture and architect a secure hybrid IT environment and a full suite of integrated Managed Security Services offerings.

With our services you can combine our Security Device Management, Enterprise Security Monitoring, and Vulnerability Management with Threat Detection to meet your unique security and compliance requirements.

Dimension Data's Cybersecurity Advisory can support you with a holistic approach to help you develop a roadmap to strengthen your security posture, and architect a secure hybrid IT environment and a full suite of integrated Managed Security Services offerings.

Our advantages

With our extensive portfolio of on-premise and cloud services, ranging from monitoring and operations to threat hunting, we can protect your intellectual property and secure your IT infrastructure.

Advisory Services

Our Cybersecurity Advisory covers the entire lifecycle of security from developing a strategy and plan aligned to your business needs, optimising existing environments, to designing your next-generation enterprise security architecture.

Support Services

Our Uptime support service plans improve infrastructure availability across networking, security, collaboration, and communication assets. We make it easier for you to balance the cost of supporting your infrastructure against the risk of downtime.

Technical Services

We offer Assessment, Design, Compliance and Implementation Services worldwide to support your existing and future applications and infrastructure.

'Identify threats and risks across multifaceted, distributed architectures, including on-premise, cloud, and hybrid environments. Ensure that your detection and incident response capabilities are robust.'

Executive Guide to the NTT Security 2018 Global Threat Intelligence Report

https://www.dimensiondata.com/en/insights/gtir2018

Every link in the kill chain connected

We connect threat monitoring fuelled by rich threat intelligence, our own IP and best in class tools and processes with advanced analytics and threat hunting to accelerate threat detection and response.

End to end security capabilities at scale

We combine Managed Security Services with our Advisory, Support and Technical Services to deliver better business outcomes at scale globally.

Holistic and integrated Managed Security Services

We combine and integrate our Security Operations Centre and threat intelligence capabilities with our third party device management to deliver a better, more sustainable security posture.

Experience and expertise across technology domains

We have the skills and expertise to secure and manage a hybrid IT environment. We have management and operations expertise across security, networking, endpoints and applications.