



# Managed security services Security Device Management Services

Protect your assets and maintain compliance requirements with flexible, scalable and always-on services

Our Security Device Management Services combined with our **Support Services drive operational excellence and maximizes existing technology investments.**

## Business outcomes

- Reduce overall security risk
- Reduce unnecessary security technology investment
- Enhance protection with correctly configured and optimized devices
- Release valuable in-house security staff to focus on other initiatives

## Challenges

Secure configuration, management and maintenance of security devices is essential to protect assets and meet numerous compliance regulations. Managing security devices, however, requires a specific and specialized skill set that needs constant attention, training and maintenance. Keeping solutions updated and patched while monitoring them 24/7 is a challenge for all organizations, large and small.

Security devices, applications and endpoint security solutions must be properly provisioned, configured, updated and patched to protect against internal and external threats. It's also a compliance requirement for regulations including PCI DSS, GLBA, HIPAA, and SOX. Both security devices and secure access service edge (SASE) require updates on policies, signatures and updates of rules. Security best practice and many regulations also require continuous monitoring to detect and respond to threats.

Attracting and retaining experienced vendor-certified staff can be difficult and expensive. Proving to organizational stakeholders that your devices adhere to vendor and industry best practice is essential; as is demonstrating that change management processes are followed and documented, and that regulatory compliance has been achieved.

Our Security Device Management Services reduces that burden. Our services follow industry best practice and ensure that security devices are available and that organizations maintain compliance with the applicable regulatory requirements.

## Solution

Our Security Device Management Services provide organizations with full maintenance, updates, change management, asset tracking and 24/7 device monitoring by security experts. We operate and manage your security devices including firewalls, intrusion detection and prevention systems, and web application firewalls, by undertaking active and consistent management control on your behalf.

## Service Elements

- On-demand device configuration and tuning
- Timely updates and release management (patch and security hotfix)
- Continuous device health and availability monitoring
- 24/7 coverage via ISO-27001-certified Security Operations Centers (SOCs)
- Highly experienced industry and vendor certified engineers
- Proven operational processes aligned with ITIL best practice and guidelines
- Policy management for security devices and secure access service edge (SASE)
- Device event, incident, problem, capacity management and escalation through to resolution
- Predefined service levels and objectives targeted to meet your organization's security requirements
- Standard and Enhanced service packages to support your organization's specific security needs

## Our Device Management Service includes

- Traditional and next generation firewalls (NGFWs)
- Intrusion detection/prevention systems (IDS/IPS)
- Web proxy and email gateway content filtering systems
- Unified threat management (UTM) systems
- Web application firewalls (WAFs)
- Router, switch and virtual private network (VPN) devices<sup>1</sup>
- Secure access service edge (SASE)

## Our standard and enhanced security device management packages

We offer standard and enhanced packages for security device management to meet your organization's business requirements.

- **Standard** provides health and availability monitoring with capacity, event, incident and problem management to minimize disruption to business
- **Enhanced** provides extended service level agreements and objectives, including device configuration and optimization, with predefined move, add, change and delete (MACD) bundles

Services element	Service package	
Service transition	Standard	Enhanced
Sales engagement, inception, definition, build, deploy and close phases	✓	✓
<b>Health and availability monitoring</b>		
Health and availability monitoring, improvement and recommendation	✓	✓
Health and availability change implementation		✓
<b>Incident management</b>		
Incident generation, diagnosis and reporting	✓	✓
Incident resolution		✓
<b>Capacity management</b>		
Capacity planning, monitoring, improvement recommendation and reporting	✓	✓
Capacity change implementation		✓
<b>Asset tracking and reporting</b>		
Configuration item recording, status reporting	✓	✓
Configuration item control, updates, backup and restore, out of band access		✓
<b>Service request fulfilment</b>		
Service request management, information fulfilment and reporting	✓	✓
Move, Add, Change, Delete (MACD) request fulfilment		✓
Change management, impact analysis, implementation and reporting		✓
<b>Problem Management</b>		
Problem identification, recording and reporting	✓	✓
Solution identification and recording	✓	✓
Solution implementation		✓
<b>Service Options</b>		
Co-Management		✓

## End-to-end Managed Services to meet your unique needs

We offer a holistic approach with our Cybersecurity Advisory, to help you develop a roadmap to strengthen your security posture and architect a secure hybrid IT environment.

With our full suite of integrated Managed Security 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.

Our complementary, platform-enabled Managed Network Services and Managed Collaboration Services enable you to optimize your end-to-end IT environment using leading management tools and operational automation combined with ITIL-aligned service features.

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, optimizing 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.



## The NTT advantage



### Cyberthreat detection

We connect threat monitoring – fueled by rich threat intelligence, our own IP and leading tools and processes with advanced analytics and threat hunting – to accelerate threat detection and response.



### Holistic and integrated Managed Security Services

We combine and integrate our security operations center and threat intelligence capabilities with our device management to deliver a better, more sustainable security posture.



### 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.



### Experience and expertise across technology domains

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



## Get in touch

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