



# MSS-i Managed Network Security

Network security around the clock.

The central role of IT and network infrastructures for companies requires strategies and measures that effectively prevent third-party attacks and ensure unlimited availability. Of central importance here is ensuring the stability of the networks, the availability of the central applications and the communication between those involved. Only in this way can data and key assets be protected effectively. With MSS-i, Swisscom provides unique Managed Security Services, optimized for Switzerland.

## Swiss SOC, staffed by security experts around the clock.

Swisscom operates its own Security Operation Center (SOC), in which highly qualified specialists ensure the security of your infrastructure around the clock. Because the security experts are on site 24/7, they can react immediately in the event of an incident and ward off threats as quickly as possible. The catastrophe-proof site in Zurich, together with geo-redundancy, a multi-stage concept for physical security and the redundant arrangement of electricity, network and system

components, guarantee the highest availability. Furthermore, the Swisscom SOC meets all the key national and international guidelines and recommendations.

Threat intelligence, optimized for Switzerland  
To recognise threats early and draw the right conclusions, MSS-i relies on multiple factors. The focus is on threat intelligence, optimized for Switzerland. Swisscom continuously analyses numerous manufacturers' own, public, state and own feeds. In addition, a sophisticated system ensures that people and machines work perfectly together for maximum security. The security engine automatically resolves incidents that can be clearly classified. In the case of more challenging tasks, experts need to intervene. According to a tested and proven procedure, they perform a specific analysis in order to quickly and selectively avert the threat. The security engine learns from this procedure and can then solve the incident independently if it occurs again. All Swisscom customers benefit from this increase in intelligence.

## The modular service offer from MSS-i



Managed VPN



Managed Web Security



Managed Firewall/VPN



Managed Mail Security



Managed IDS



Managed Web Application Firewall



Managed Proxy



Managed WAN Encryption

# MSS-i Managed Network Security

## Security Dashboard: all security information at a glance

The organisation and processes of the SOC allow companies access to the expert knowledge of the security specialists at any time. However, you can also find information yourself. A Security Dashboard gives you a quick overview of the security-related matters at your company in real time. The summary shows the current security status and threat situation appropriate to the target group; the history informs you about the events during a particular time period in the past. The information on the Security Dashboard is updated regularly.

## Compliance never stops

As a partner that aligns itself with international standards, Swisscom supports companies in adhering to the various specifications of different stake holders.

With Swisscom, you play it safe because MSS-i fulfils all the key standards: ISO27001, ISAE3402, the FINMA recommendations and Swiss data protection law. And, as a responsible security provider, Swisscom is audited by external auditors every year. This means Swisscom can also provide evidence of its customers' compliance. The customers can thus avoid time-consuming and costly audits.

## Modular SLAs, flexible financing

The Swisscom service level agreements (SLAs) have a modular structure and can be flexibly combined into tailored service packages. Whether you want to combine or uncouple high availability and short response times depends entirely on your requirements and demands. The service offer is also flexible when it comes to financing, with various options to choose from.

## Recurring services

MSS-i works in accordance with ITIL. The distribution of recurring services to the relevant areas follows this standard. The recurring services are an integral service component of all modules. They are all reported via the Security Dashboard and customers can view them in their entirety.

<b>Health Incident Monitoring and Management</b>	In the scope of this module, Swisscom monitors the utilisation of your security devices and, in the event of bottlenecks, develops a solution together with the customer. In the event of a complete failure, Swisscom takes care of the exchange.
<b>Security Incident Monitoring and Management</b>	Log data and events form the basis for the creation of security incidents and their classification. Relevant and critical security incidents are solved via direct customer contact.
<b>Release and Patch Management</b>	Swisscom tests all releases and patches in its own laboratory before installing them on the managed objects.
<b>Availability Incident Management</b>	The SLAs specify the extent to which availability is guaranteed. Adherence to these is continuously monitored.
<b>Problem Management</b>	If incidents occur regularly, Swisscom examines the causes of actual and potential faults. Problem Management ensures that these are resolved permanently.
<b>Change Management</b>	Changes can be recorded via the Security Dashboard around the clock. They are implemented in accordance with the values defined in the SLA. The status of every change can be seen on the dashboard.

## How you benefit

- > You receive certified security for your system environment at a constant cost that can be planned.
- > You receive access to the expertise of security specialists who monitor your IT and network infrastructure around the clock.
- > You meet regulatory and industry-specific compliance requirements and recommendations.
- > A Security Dashboard gives you a real-time overview of the security situation at your company.