Network Detection and Response as a Service

Due to their complexity, highly distributed and hybrid networks are difficult to analyse and monitor. The network traffic is often encrypted and barely visible, making it difficult for security tools to detect malware.

Threat detection on the network using static indicators of compromise for known malware is no longer sufficient. New and modified forms of attack require a behaviour-based response

What is NDR as a Service?

Encrypted network traffic and threat detection using static IOCs opens up too many points of access for cyber attackers. The required protection is no longer guaranteed.

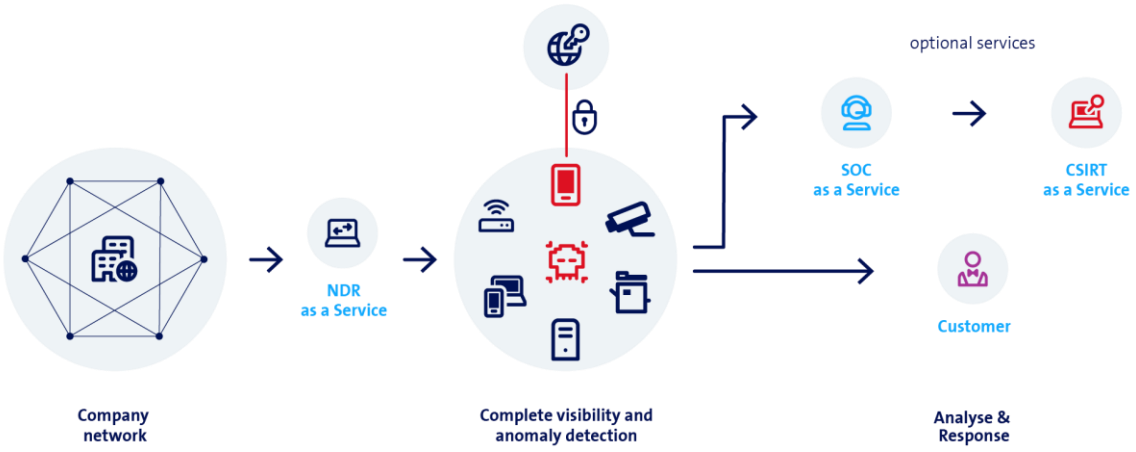
Network Detection and Response (NDR) uses powerful and advanced AI algorithms to reliably secure corporate networks. Cyber attacks can be swiftly identified and resolved.

An important focus for NDR is maximum visibility of all network activities.

The benefits of NDR as a Service

- Visibility within your network
  Identify vulnerabilities in your network before they are exploited by attackers (e.g. vulnerable services, shadow IT).
- Visibility of encrypted network traffic
  Automated detection of attackers on your network before data is exfiltrated or encrypted.
- Pre-configured use cases and ML models
  Automated correlation across all sources and intuitive visualisations.
- Fast deployment
  No additional hardware or agents required.

How Network Detection and Response works



swisscom

Facts & Figures

Basic services	On premise: The NDR appliance is hosted on premise at the customer and monitored by the customer. Security patches are installed in consultation with the customer and manufacturer. If the customer has opted for Security Analytics as a Service (SAaaS) and Security Operation Center as a Service (SOCaaS), a software-based forwarder can be installed on the customer's environment to forward incidents from the appliance to the SOC for analysis. The customer will be informed of any suspicious security incidents.
	Managed by Swisscom: The NDR appliance is hosted and monitored together with a logging platform in a Swisscom data centre. Security patches are installed by Swisscom. If the customer has opted for SAaaS and SOCaaS, Swisscom ensures that incidents are forwarded from the appliance to the SOC for analysis. The customer will be informed of any suspicious security incidents.
Supplementary services	Security Analytics as a Service (SAaaS): We are experts in security and big data, and provide you with our proven security analytics infrastructure. Connect additional log sources from the cloud, on premise or from a managed provider, and see an overview of potential security incidents on the dashboard. You can analyse and respond to security incidents yourself.
	SOC as a Service (SOCaaS): This dashboard provides an overview of potential and confirmed security incidents from your company's defined log data as well as analyses with specific recommendations for action. You react independently to critical security incidents.
	CSIRT as a Service (CSIRTaaS): You call in Swisscom experts for the analysis and management of security incidents. We manage the security incident management process remotely or on your premises and support you in securing evidence and communicating with customers and partners.
	Digital Risk Protection as a Service (DRPaaS): You are proactively informed if sensitive business and personal information from your company is found on public and closed networks (e.g. the dark web). You implement our recommended actions for confirmed security incidents independently.

You can find more information and our expert's contact details at **swisscom.ch/ndr**

Swisscom (Switzerland) Ltd Enterprise Customers, P.O. Box,
CH-3050 Berne, Telephone 0800 800 900, www.swisscom.ch/enterprise

swisscom