Network Detection and Response (NDR)

PRODUCT BRIEF

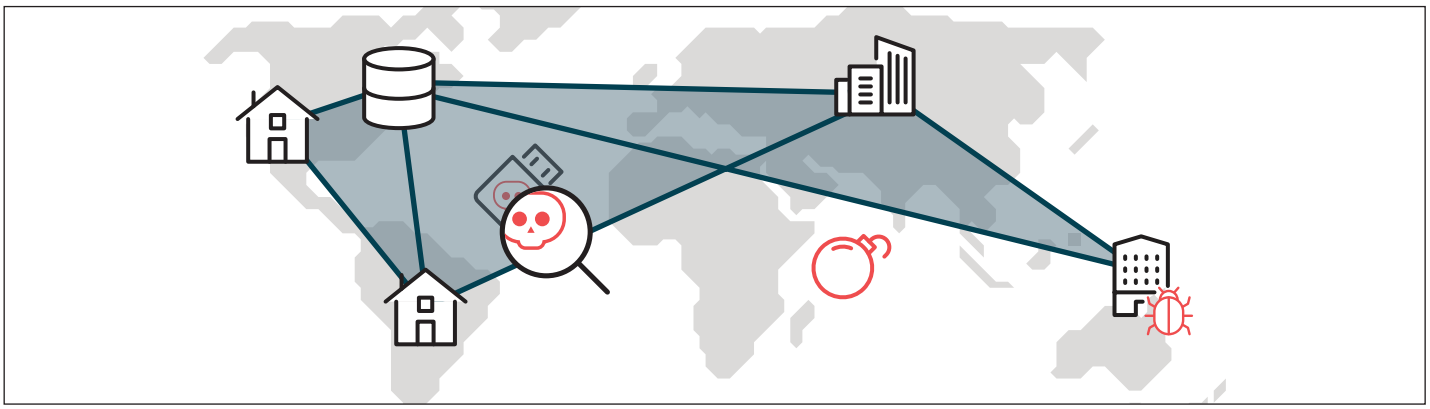
Get holistic situational awareness of your network to act on cyberattacks immediately.

Protect your network by eliminating blind spots

Networks can have both internal and external blind spots
As network attacks get more sophisticated, perimeter security is no longer sufficient to protect the WAN from external threats. Internal threats, such as infected machines and USB sticks, also contribute to the threat landscape.

Protect your network by acting on signs of a possible cyberattack
The NDR solution acts on multiple stages of the kill chain. Early on, NDR checks for malware during delivery. Further in, to protect against existing intrusions, NDR assigns threat scores to internal assets. This surfaces suspicious activity, making it possible for you to act when malicious software attempts to communicate outside the WAN or spread laterally. SASE integrated monitoring, with a combination of human and machine intelligence, provides the detection and actionable alerts needed to prevent sophisticated attacks.

Eliminate both internal and external blind spots



Get holistic situational awareness of your network with threat scores of internal assets.

Why choose Network Detection and Response by Open Systems?

Fully SASE integrated

Unlike traditional intrusion detection systems (IDS), the NDR solution is fully integrated in the Secure SD-WAN. This means all traffic passing the Firewall or Secure Web Gateway is scanned. Additionally, dedicated sensors can be placed at strategic locations within the WAN.

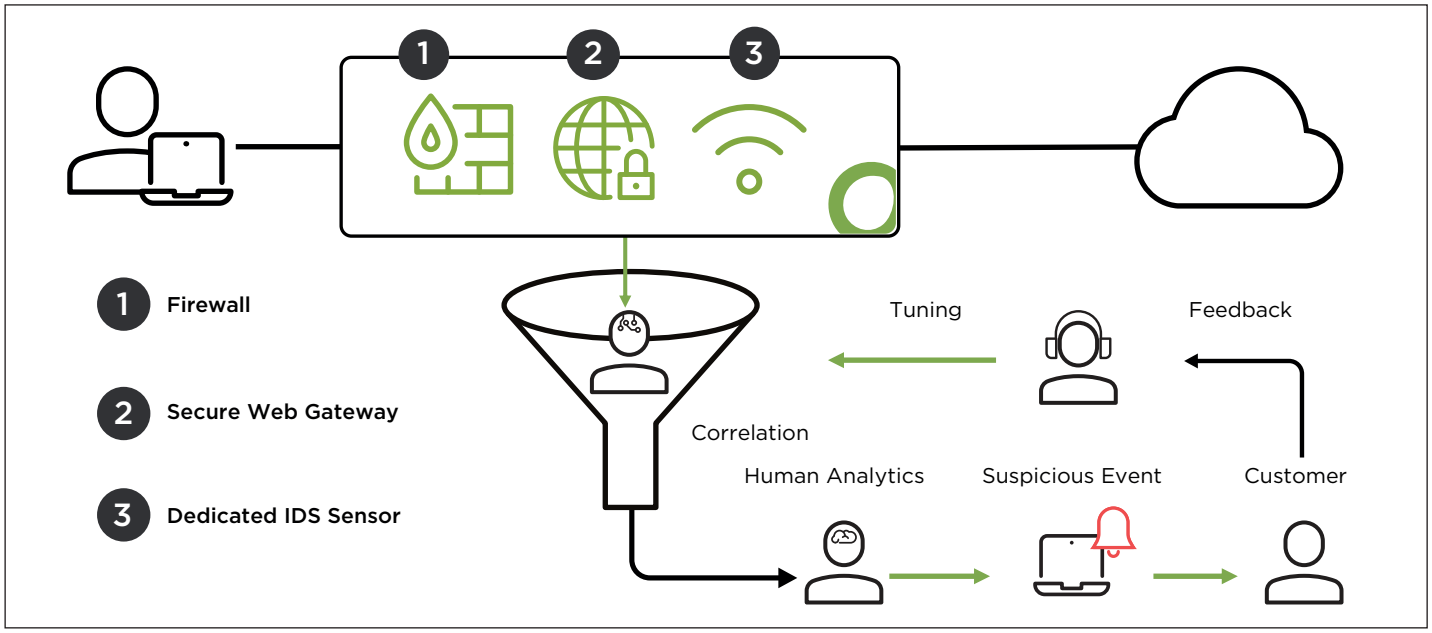
Customizable algorithms

Standard IDS algorithms are signature based and well defined, leaving no room for customization. With NDR you have the option to implement customized signatures which will always be rated with a high threat score. This ensures that signals can be separated from noise, with continual fine-tuning specific to your network.

Enhanced by humans

Rather than depend only on machine intelligence, NDR augments AI-driven data analysis with human intelligence. Expert-level engineers focus on filtering out false positives from assets with high threat scores. So, rather than promoting resource-intensive operations, the NDR service model focuses on dealing with the most relevant alerts.

How does NDR analyze, correlate, and tune monitoring to alert you when needed?



Centralized correlator

- Network data coming from the Firewall, the Secure Web Gateway or from dedicated sensors are logged and fed into the correlator
- The correlator analyzes the matched signatures and assigns threat scores accordingly

Alerting

- Any assets with a high threat score generate an alert
- The alert creates a ticket that is analyzed by an Open Systems engineer
- Customers are only alerted if human expertise deems the event as sufficiently suspicious

Tuning

- The correlator is continuously tuned by Open Systems engineers based on customer feedback
- This ensures the correlator learns from false positives, to continually improve its performance

Global Threat Isolation

If malware penetrates your network, it typically pursues two objectives: to spread undetected laterally and to communicate with an external command and control server. Our Global Threat Isolation feature provides an effective response to both these actions by immediately blocking any outbound connection from a host at network level — whether it's to an external server or to other hosts within the network — thus isolating the affected host. With just a single click, you have an immediate, remote response to malicious activity.

opensystems

Open Systems is a secure access service edge (SASE) pioneer that enables organizations to connect to themselves, to the cloud, and to the rest of the world. With cloud-native architecture, secure intelligent edge, hybrid cloud support, 24x7 operations by level-3 engineers, and predictive analytics, the Open Systems SASE delivers a complete solution to network and security.

Learn more at **open-systems.com** | Copyright 2021 Open Systems. All rights reserved. Approved for public use. (CC, VV, March 2021, v1.1)