Secure SD-WAN in action

open systems

CASE STUDY

Open Systems detects and neutralizes aggressive malware

swiss safety center ISO 27001 certified system

Open Systems services are ISO 27001 certified.

Repelling a dangerous intrusion in real time for a global company

The only thing missing was a suspenseful soundtrack. Open Systems recently detected and resolved a potentially damaging malware intrusion — possibly a ransomware delivery attempt — for a global customer with over 5,000 end users at 130 locations in 30 countries. In the end, no damage was done, and the customer experienced only limited interruptions in network services.

This worldwide organization employed the Open Systems Secure SD-WAN with our SOC-as-a-Service features, including Network Security Monitoring (NSM) and Endpoint Detection and Response (EDR). All products played critical roles in stopping the intrusion, but it was the incident handling that was key to keeping the damage to a minimum.

Rapid detection, alert, and response

To begin, our EDR feature detected suspicious activity on a particular endpoint. An Open Systems engineer received the intrusion alert at our operations center, analyzed the situation, and escalated to the customer. As an initial response, we quickly blocked file execution on all endpoints protected by EDR.

Soon afterward, our NSM sensors detected global lateral movement within the WAN — confirming that the malware had immediately started to spread. Remaining continuously in touch with the customer, the Open Systems engineers proposed strong countermeasures, which were executed leveraging our Next-Gen Firewall to block certain network protocols globally. This action successfully prevented the spread of the malware. Meanwhile, we implemented local exceptions network-wide in order to minimize business impact.

Our engineers provided ongoing identification and reporting of infected hosts and assistance in cleaning those hosts. We continued to monitor the situation and forensically analyze the initial infection to find its root cause. The intruding malware was highly aggressive, and caused substantial damage with other known victims. We don't know what damage it might have done, but the potential was significant.

Throughout the incident, the customer fully relied on the response of the Open Systems team and was pleased with the results. Outside of IT, the network disruption was so minor that the incident as a whole wasn't even perceived as severe!

Chain of events

Initial infection

Detection of suspicious behavior on endpoint by Endpoint Detection and Response (EDR)

Human analysis of events by operations engineer

Escalation to customer

Blocking of file execution on all endpoints protected by EDR (first response)

Detection of global lateral movement in the network by Network Security Monitoring (NSM)

Incident coordination with customer

Complete blocking of certain network protocols, globally on the Firewall

Continuous addition of local exceptions to minimize business impact

Continuous identification and reporting of infected hosts

How the Open Systems Secure SD-WAN succeeded

Open Systems Secure SD-WAN combines best-of-breed technology for both detection and protection, and the expert-level engineers you need to truly maximize the potential of your technology.

Powerful tools

Open Systems Endpoint Detection and Response enabled rapid detection of the intrusion and provided the capability to take immediate, global action to prevent file execution. In addition to EDR, our Network Security Monitoring and Next-Gen Firewall provided the means to monitor the malware actions and quickly and completely quarantine the affected hosts.

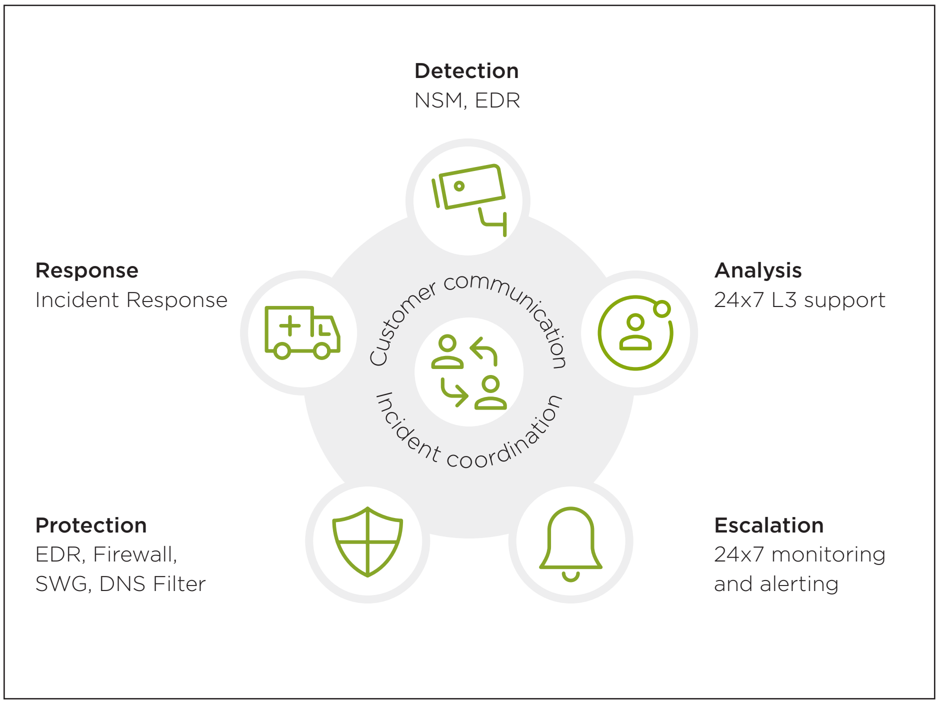
Fast response

As part of our 24x7 monitoring, highly experienced engineers identified the malware as a true positive in the flow of NSM events. Analysis of the intrusion and escalation to the customer were followed by immediate countermeasures.

Expert response

From the initial analysis by the operations engineer, to the coordination and advice of our Computer Emergency Response Team (OS-CERT), to the technical account managers who involved the right people in the customer's organization, Open Systems staff brought expert experience and coordination to every aspect of the incident.

Incident handling



Detection
NSM, EDR

Analysis
24x7 L3 support

Escalation
24x7 monitoring and alerting

Protection
EDR, Firewall, SWG, DNS Filter

Response
Incident Response

For successful handling of a malware infection, powerful technology needs to be combined with expert-level engineers

Open Systems is a leading global provider of a secure SD-WAN that enables enterprises to grow without compromise. With assured security, AI-assisted automation and expert management that free valuable IT resources, Open Systems delivers the visibility, flexibility and control you really want with the performance, simplicity and security you absolutely need in your network.

To learn more, visit **open-systems.com** Follow us Open Systems proprietary 2019