Network Threat Advanced Analytics

Data Sheet

Detect potentially malicious anomalies before they seriously impact your network.

verizon

Actionable intelligence on the real threats to your business

Network Threat Advanced Analytics helps you spot potentially malicious activities in your network. It gives you actionable intelligence that enables you to stop threats in their tracks. It does that by utilizing advanced signature and multidimensional anomaly–based threat detection mechanisms.

Network Threat Advanced Analytics also gives you an independent view of threats outside your network. You benefit from our network and threat intelligence, paired with our proprietary detection capabilities, helping you spot potential attacks early. You benefit from our global security analysis, giving you a full picture of the real threats to your business. That helps you to harden your perimeter and improve your security strategy.

Network Threat Advanced Analytics can ingest NetFlow from the Verizon IP backbone as well as from customer premise devices.

If you don't have Verizon internet services or backbone ingestion, we can pull the NetFlow data from your premise devices (internet-facing customer edge routers).

The following premise-based ingestion variants are available:

- Connection Kit (CK) only*
- VPN only without CK but using a customer VPN concentrator
- MPLS only, used for most implementations where you are using Verizon's Private IP network
- Onsite virtual local event collector (vLEC)

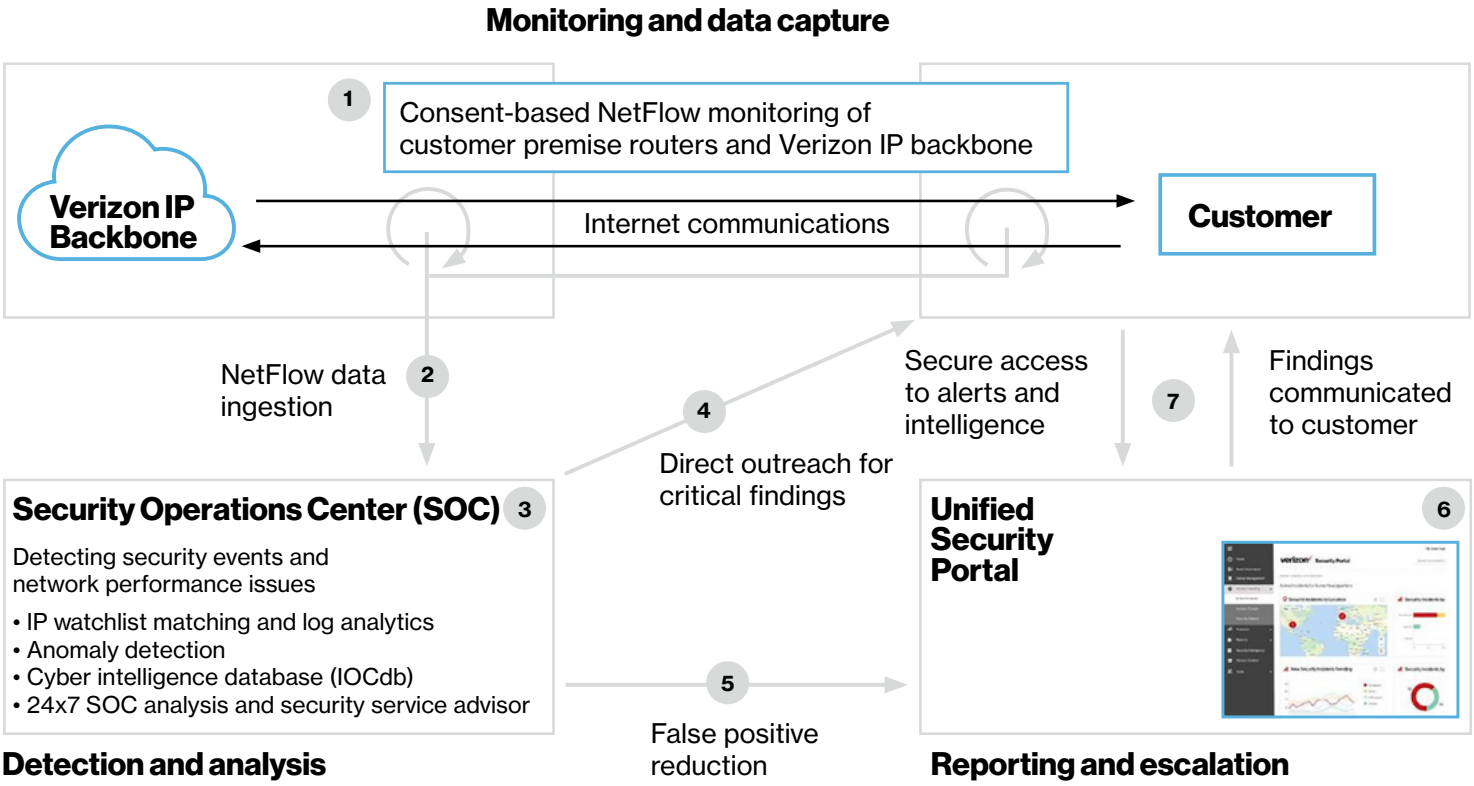
Why choose Verizon's Network Threat Advanced Analytics service?

Our Network Threat Advanced Analytics service offers the following benefits:

- Anomaly-based threat detection from multidimensional detection engines, looking at six different attributes found in NetFlow data (including volume, size, IP and ports)
- Security Operations Center (SOC) analysis – we provide human intelligence on top of threat detection results
- Support from a dedicated advanced security service advisor – we'll work to foster a close relationship with you
- Near-real-time, fully automated watch-list matching based on detailed Verizon threat intelligence from our managed security services monitoring platform
- Results and reports presented in an easy-to-use format, including anomalies in network traffic in near-real-time

*The Connection Kit (CK) is a router located on customer premises helping to collect all relevant logs locally and establishing an IPsec connection with the Verizon Security Management Center (SMC). Your Verizon sales engineer will provide you the specifications for your CK device.

Network Threat Advanced Analytics layered model



How Network Threat Advanced Analytics has helped organizations act on threats early.

Reconnaissance probing

Daily scanning activities are an automated way of checking if ports are left open. But existing security tools don't always pick up on subtle and specific signs that would enable them to take countermeasures and protect the services behind these ports.

In one case, Network Threat Advanced Analytics identified suspicious activity by focusing on three specific ports. Looking at the attack chain, this was likely the pre-cursor for a potential attack.

Policy violation

In another case, we caught an unusual amount of data going to a cloud storage solution that wasn't approved by the company's security policy. This alerted the customer to a policy violation and also a potential data leak.

Potential data exfiltration

Network Threat Advanced Analytics was also able to detected an unusual amount of encrypted tunnel traffic from a previously unseen home IP address. Simultaneously, the service saw unprecedented volumes of encrypted tunnel traffic to a small ISP located in a major US city. The organization was conducting a company-wide sales conference in the city and had stood up a temporary VPN server in the hotel to service all of its remote staff members.

Network Threat Advanced Analytics makes customers aware of new major services and applications appearing on their network.

verizon