Solution brief

Verizon Network Detection and Response.

Cloud-delivered, full packet capture, real-time and retrospective threat detection and visualization.

Verizon challenges the way organizations secure their networks with Network Detection and Response, a cloud-delivered security platform that is more intuitive, comprehensive and immersive than legacy products that came before it. Lightweight software sensors record complete traffic from any network segment from the DMZ to the core, on cloud networks, and even industrial environments, to establish a high-fidelity memory of the network in the cloud. These sensors capture complete network data and send it to Network Detection and Response for storage and analysis. The platform acts as a network defense tool, allowing analysts to explore historical data retrospectively with the most up-to-date threat intelligence. Visualizations in Network Detection and Response can be used for real-time situational awareness or as a forensic workbench for incident response teams and threat hunters. It provides actionable intelligence, including a correlated view of threats, and packet-level forensic capabilities to speed incident response and threat hunting.

Benefits

- Delivers pervasive visibility across the network
- Provides unlimited, full-fidelity forensic window
- Reduces detection noise and alert fatigue
- Replay network traffic against the latest threat intelligence to uncover previously unknown latent threats
- Simplifies security and frees up incident responders to hunt for threats
- Complements existing infrastructure through secure APIs
- SaaS model deploys rapidly

Cloud-based network memory

Record traffic from multiple networks into a single haystack for centralized analysis with unlimited, full fidelity retention windows.

- Enables long-term retention and analysis of network traffic
  - Unlimited network packet capture, replay and storage into a single haystack
- Choose to capture what matters to your risk profile.
  - Adaptive capture options for flows, metadata, or full packet capture (PCAP)
- Purpose-built for distributed networks
  - Can be deployed on any network segment for unlimited coverage models

verizon

Intelligence from sensor-driven data

Network data delivered in context.

- Deep packet inspection of data from thousands of protocols and applications
- Network data compared with proprietary and third-party intelligence for community–scaled detection
- Advanced traffic threat analysis performs correlation, heuristics and machine learning

Retrospection

- Analysis engine powered by centralized repository of full–fidelity network data allows for continuous detection and prioritization of threats
- New indicators of compromise from network intelligence make it possible to analyze past network behavior for newly discovered, latent threats

Intuitive data visualization

- Compresses dwell time and incident response with deep forensic exploration using cutting edge visualization tools.

Give security teams an easy-to-navigate system to more quickly act on threat intelligence.

- Advanced forensics visualization allows analysts to interact with data through kill-chain analysis, network connection graphics and event timelines

Powerful security console with customizable flexibility.

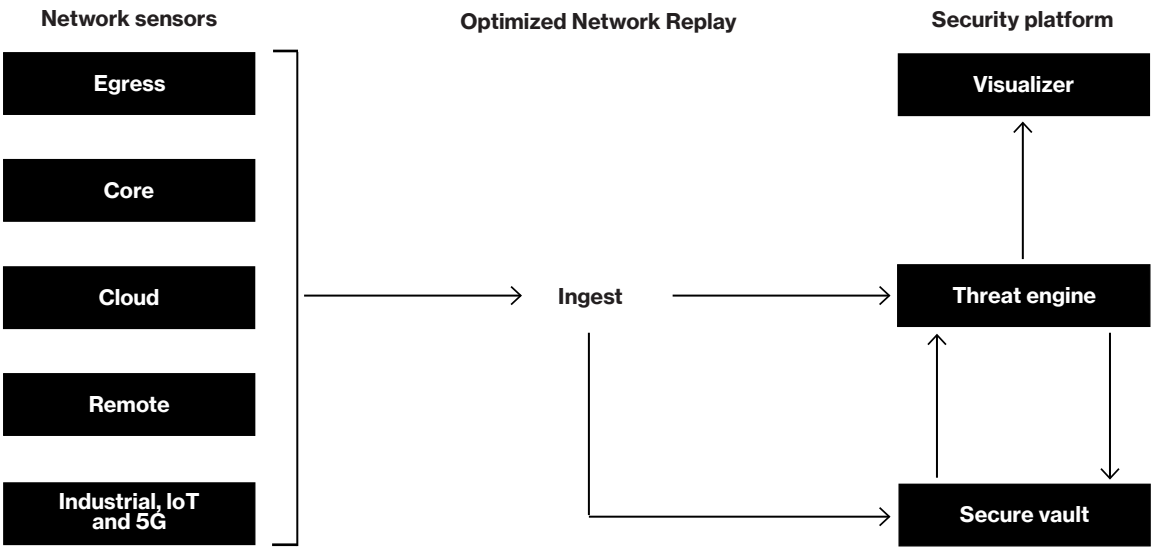
- Integration capabilities to feed threat data into custom SOC and forensics dashboards
- Quick management of policies for sensor deployment, packet capture, user management and alert notification

Technical requirements

- Recommended requirements for sensor (physical or virtual):
- CPU: Intel Xeon with 4+ Cores
- Memory: 8GB or more free
- Disk space: 8GB disk space (required for buffering)
- Internet connectivity for the Relay and Management Interface
- 2 network interfaces
- Monitoring NIC: 10/100/1000 Ethernet connected to a SPAN/Tap/Mirror port Relay and Management NIC: 10/100/1000 Ethernet for relaying optimised and encrypted data and sensor management

verizon

Network Detection and Response: How it works.



Learn more

Find out more about Network Detection and Response at enterprise.verizon.com/networkdetectionandresponse.