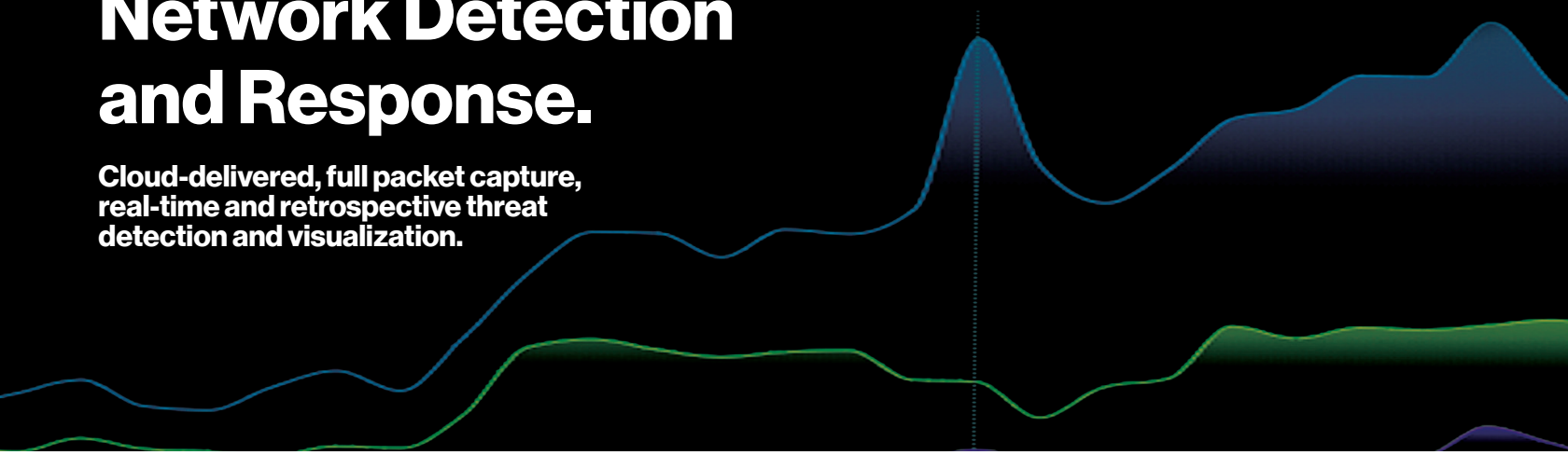
Data sheet

Network Detection and Response.

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



Executive summary.

A cloud-delivered Network Detection and Response (NDR) platform is the evolution of effective IT security. It reliably detects threats and sophisticated attacks, retains full-packet forensics for as long as necessary and enables integrated response. Cloud-delivered Network Detection and Response (NDR) consolidates multiple security point products into a single platform that deploys rapidly. It provides continuous threat visibility as organizations move workloads from on premises to the cloud or expand into other environments such as industrial networks. Network Detection and Response (NDR) also increases the efficiency of security teams to allow them to rapidly mitigate any impact of attacks.

Why Network Detection and Response is needed.

The network provides an incorruptible source of truth about how attackers breach defenses and what has been impacted. Previously, only organizations with large budgets could purchase the software and hardware needed to record and retain network traffic. However, those legacy products captured traffic from on–premises environments only and complex deployments limited the rollout to a few network segments.

Cloud-delivered Network Detection and Response levels the playing field by making what was once a luxury-enterprise-wide packet capture retained for long time periods— available to all organizations. It does not need any specialized hardware and can be rapidly deployed in any segment of the modern network-enterprise, cloud or industrial. The ability to capture traffic from any network is of tremendous importance, given that more and more business workloads are running on infrastructure that is not owned by the organization. By being able to record traffic from any network, this approach provides security teams with what they need most: visibility. Visibility is the key for detection, forensics, containment and verification of threats.

Network Detection and Response delivers visibility, threat detections and forensic analysis of suspicious activities, accelerating the ability for organizations to respond to and prevent security events.

Shifting to proactive detection and response.

It's a known fact that it's not a matter of *if* but *when* cybersecurity defenses will be breached. Prevention-based network security approaches alone, which rely on the ability to control enterprise–owned resources, are no longer sufficient. Organizations are looking for proactive detection and response. Network Detection and Response complements prevention–only security technologies such as Intrusion Detection Systems (IDS) and Intrusion Detection and Prevention Systems (IDPS). It uses advanced methods (e.g., machine learning, anomaly detection, correlation) to augment detections by other products. Its full–fidelity forensics allow security teams to actively threat hunt. When information about a new attack is announced, long–term forensics also allow security teams to search back in time to see if that attack has ever impacted the organization.

verizon

1 **Immediate time to value.**

A key design tenet of Network Detection and Response is rapid deployment, enabled by lightweight software sensors that can ingest network traffic from any environment. Free of any hardware, sensors can be installed in even the most resource constrained network segments, such as industrial environments. For cloud environments where there is no network tap, the platform provides software forwarding agents that directly copy network traffic from the cloud instance and deliver it to the appropriate sensor.

Rapid deployment makes it easy to get pervasive visibility. In addition to visibility into threats on the enterprise network, Network Detection and Response also provides information about threats introduced by unmanaged personal devices accessing corporate resources, and vulnerabilities in workloads running in the public cloud infrastructure.

2 **Advanced forensics.**

The limitless storage of the cloud enables a rapidly searchable network memory at a significantly lower cost than legacy products. Affordable forensics at your fingertips with results in seconds enable game-changing incident response and threat hunting.

The platform provides controls for the fidelity and amount of data stored. An optimized index of stored data enables rapid search which is a valuable feature for threat hunters trying to quickly validate complex hypotheses. An API enables secure access to data for use in other analytic systems.

3 **Detections in depth.**

The platform performs detections at a scale not previously possible because of the elastic compute of the cloud. Machine learning, behavioral analysis, statistical modeling, and heuristics are some of the techniques used. These are augmented by threat intelligence curated by Network Detection and Response, from third party and open source feeds, and in some cases from customers to capture the uniqueness of their environments.

4 **Integrated response.**

Network Detection and Response enables rapid detection-triage-response workflows. Correlation of the suspicious actions with the corresponding incident, unique visualizations that allow analysts to intuitively make sense of massive amounts of security data, and policy-based enforcement and workflows facilitate rapid incident response and remediation. Integrations with hundreds of existing security products–firewalls, endpoint, SIEM, vulnerability systems, and automation and orchestration products–and a robust API that enables additional integrations delivers comprehensive response.

5 **Frictionless scale.**

Its cloud architecture enables Network Detection and Response to frictionlessly scale to secure even the largest enterprises. On a daily basis, the platform analyzes more than 500 terabytes of network data, amassed from hundreds of deployments. Network Detection and Response analyzes over 9 billion network connections per day to surface over 1 million potential threats. Those threats are distilled into 22,000 security events, with completely correlated context from network to endpoint–filtering data points to prioritize threats and reduce the noise for more effective, efficient response.

6 **Organizations want proactive network security.**

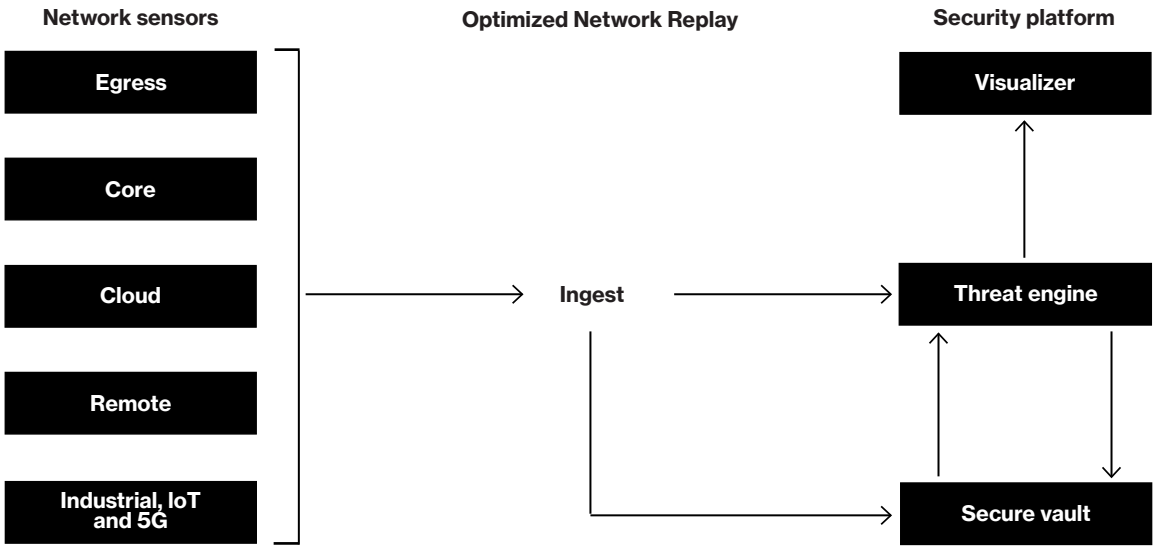
Organizations are looking for proactive detection and response at the network level. Prevention-based security approaches alone, which rely on the ability to control enterprise-owned resources, are no longer sufficient. A similar shift has already occurred at the endpoint, with organizations moving from antivirus (AV) and next- gen AV (NGAV) to Endpoint Detection and Response (EDR).

verizon

Verizon Network Detection and Response.

Network Detection and Response from Verizon is a cloud-delivered platform that unifies network detection, full-packet forensics and integrated response in an on-demand platform for any environment – enterprise, cloud, industrial, IoT, or 5G. Network Detection and Response is uniquely positioned to help organizations shift from network prevention-based security to detection and response.

Network Detection and Response: How it works.



Why Verizon Enterprise Security?

Learn more about Network Detection and Response at enterprise.verizon.com/network-detection-and-response.