PROTECTWISE™

Network Detection and Response (NDR)

EXECUTIVE SUMMARY

A Cloud-delivered Network Detection & 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 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. NDR also increases the efficiency of security teams to allow them to rapidly mitigate any impact of attacks.

WHAT IS NDR?

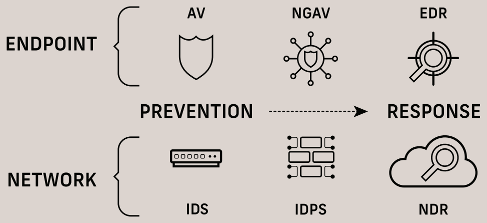
Network Detection & Response (NDR) is a platform security category that delivers network visibility, threat detections and forensic analysis of suspicious activities which dramatically accelerates the ability for organizations to respond to and prevent security events.

WHY IS NDR IMPORTANT?

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

Cloud-delivered NDR levels the playing field by making what was once a luxury—enterprise-wide packet capture retained for long time periods—available to all organizations. Cloud-delivered NDR 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, NDR provides security teams with what they need most: visibility. Visibility is the key for detection, forensics, containment and verification of threats.

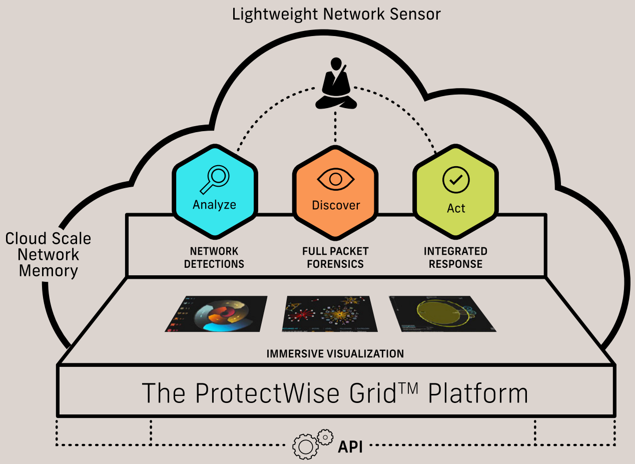
It's a known fact that it's not a matter of if but when cybersecurity defenses will be breached. Prevention-based security approaches alone, which rely on the ability to control enterprise-owned resources, are no longer sufficient. Organizations are looking for proactive detection and response. This shift has already occurred at the endpoint, with organizations moving from antivirus (AV) and next-gen AV (NGAV) to Endpoint Detection & Response (EDR).



NDR enables a similar shift on the network, complementing 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 legacy products. It also provides full-fidelity forensics, which can be captured from any network and retained for as long as valuable. This allows security teams to actively threat hunt. When information about a new attack is announced, long-term forensics also allows security teams to search back in time to see if that attack has ever impacted the organization.

PROTECTWISE: UNIQUELY POSITIONED TO ENABLE THE SHIFT TO NDR

The ProtectWise Grid™ is a Cloud-delivered NDR platform that unifies network detection, full-packet forensics and integrated response in an on-demand platform for any environment—Enterprise, Cloud or Industrial. Protectwise™ is uniquely positioned to help organizations shift from network prevention-based security to detection and response.



IMMEDIATE TIME-TO-VALUE

A key design tenet of the NDR platform 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 concept of a 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, ProtectWise also provides information about threats introduced by unmanaged personal devices accessing corporate resources, and vulnerabilities in workloads running in the public cloud infrastructure.

ADVANCED FORENSICS

The limitless storage of the cloud enables a perfect and rapidly searchable network memory at a significantly lower cost than legacy products. Instead of spending millions for a few weeks of retention with a legacy product, organizations can get a year of retention with ProtectWise at the same price. 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 hence 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.

DETECTIONS IN DEPTH

The platform performs detections-in-depth and 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 ProtectWise, from third party and open source feeds, and in some cases from customers to capture the uniqueness of their environments.

Automatic retrospection is a unique capability. Historical packet data is replayed against new threat intel to determine if that threat has ever impacted the organization. Being able to confidently determine that an attack has not impacted the organization—now or at any time in the past—is a powerful capability for any security team.

INTEGRATED RESPONSE

The ProtectWise Grid 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.

FRICTIONLESS SCALE

Its cloud architecture enables The ProtectWise Grid 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. The ProtectWise Grid 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.

CONCLUSION

ProtectWise provides a new approach to how enterprises acquire, manage and operate security, fomenting the evolution of network security that organizations need. The ProtectWise Grid is effectively a massive state machine in the cloud that observes attacks unfolding over long time periods and sees through the false warnings to generate extremely reliable detections, with forensic evidence to support investigations. The ProtectWise Grid consolidates multiple point products into a single platform, with a cloud architecture enabling features not possible with legacy products. Detections-in-depth enable maximum detection efficacy. Advanced forensics enable rapid discovery for maximum team efficiency. And integrated response, which recognizes the value of existing security investments and integrated delivery, reduces the cost and complexity of network security operations.

About ProtectWise

ProtectWise™ provides Cloud-Powered Network Detection and Response (NDR). Organizations can achieve defense-in-depth via advanced analytics on Enterprise, Cloud, and Industrial traffic with real time and retrospective detections. Full-fidelity packet captures, indexed and retained indefinitely, create a perfect, rapidly searchable network memory. By unifying analytics and forensics in an intuitive and immersive visualizer, The ProtectWise Grid™ delivers unique advantages over current network security products. The platform features the industry's only automated retrospection, the ease and cost-savings of an on-demand deployment model, and rapid, more effective incident response and threat hunting.

PROTECTWISE™

1601 Wewatta St • Suite 700 • Denver, CO 80202 • 1.303.625.6802
www.protectwise.com • info@protectwise.com