securonix

DATASHEET

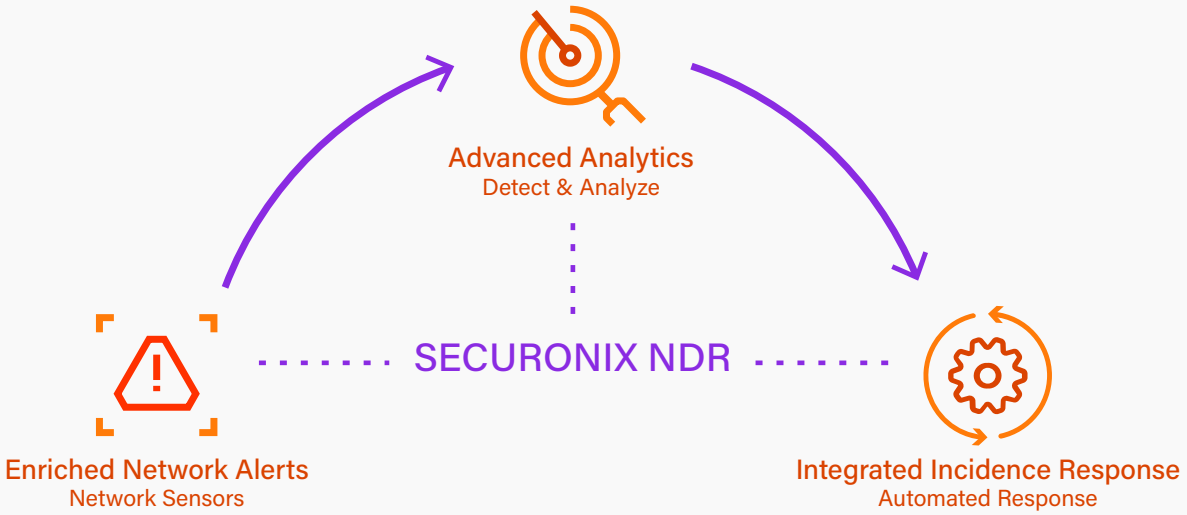
# Network Detection and Response

Robust, Scalable Network Forensics

## Why Securonix?

Network-borne threats are difficult to detect, and legacy network protection tools and firewalls don't always give you the full picture. Securonix Network Detection and Response (NDR) tackles this challenge by correlating security incidents across your entire IT environment with network activity and alerting your team to anomalies when combined with our Next-Gen SIEM.

Securonix NDR helps security operations teams to secure their enterprise from cyberthreats with increased network visibility and context, all in a single console.




## The Benefits of Network Visibility for Detection and Response

### Maximize Your SIEM Investment

Identify advanced threats that standalone NDR or SIEM solutions are not able to detect. When all of your network and security data is in one place your security team can unlock insights that provide the context needed to detect and respond to complex threats.

### Cover Your Blind Spots

NDR covers your blind spots by collecting and aggregating network activities with the rest of your IT environment. In combination with Securonix Next-Gen SIEM, the solution tracks users, accounts, and system behaviors across your network, endpoint, and beyond to detect and respond to threats in real-time.

### Detect Sophisticated Threats

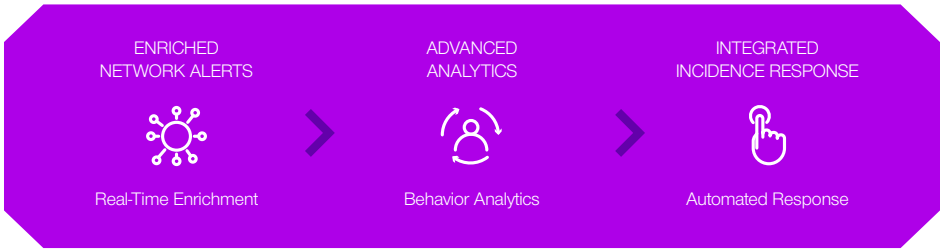
Advanced cyberattacks often involve multiple steps over time, making them difficult to detect. Securonix leverage machine learning and powerful analytics to weave disparate IOCs into a complete story. Our solution simplifies complex threats spanning multiple alerts into actionable insights while reducing noise for your SOC.

## Connected Ecosystem

**Network Sensors:** Bring in network data and enrich it with security insight. Combine data from third-party network sensors with other security data and give your SIEM an extra layer of insight. We support integration with all major network sensor products including strategic partnerships with Corelight, Verizon Protectwise, and Gigamon.

**Network Threat Hunting:** Empower threat hunters with 360-degree visibility of log, endpoint, and network data. By expanding hunting to network-borne threats, you can connect the dots faster and lower your time to detect and respond.

**Securonix NDR - Visibility, Detection, & Advanced Analytics**




## Actionable Analytics

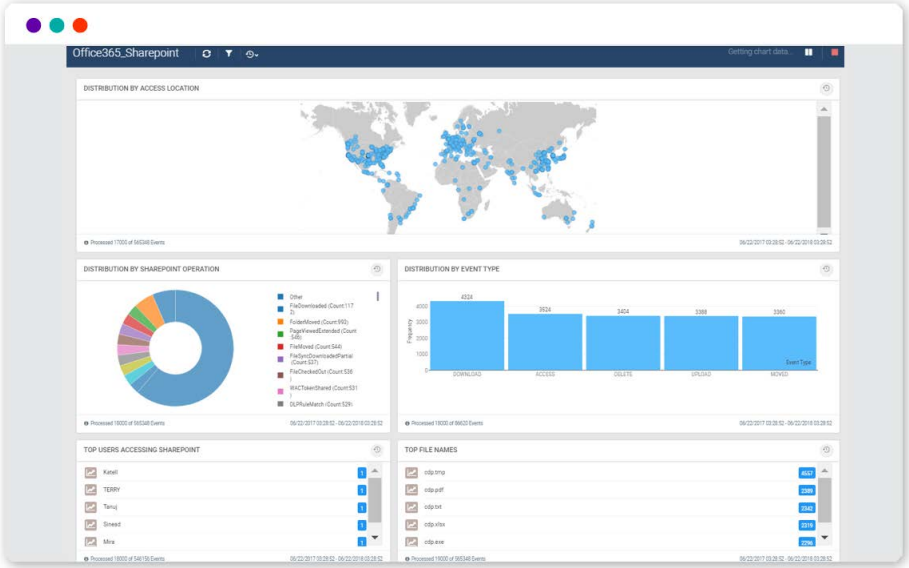
**Threat Chains:** Reduce the volume of alerts using threat models that map to both the MITRE ATT&CK and US-CERT frameworks. Our threat chain analytics uses identity context to help you trace low and slow threats that span across both your network and security events.

**Advanced Analytics:** Leverage advanced analytics, powered by machine learning, to understand when network behaviors are deviating from established baselines. This is critical in today's complex environment where a rule-based approach would result in an abundance of false positives.

## Holistic Data Insights

**Single Platform:** Reduce operational complexity with a single, fully integrated backend architecture. With zero infrastructure to manage your SOC can focus on detecting threats before they escalate.

**Robust Reporting:** Leverage network data insights including reports on network traffic and built-in, shareable dashboards to make data-informed decisions. Our consolidated platform empowers your team to collaborate and optimize threat hunting.




## Integrated Incident Response

Integrated SOAR capabilities help you improve your incident response times. Our solution provides your team with smart automation and suggests playbook actions to guide analysts to remediation.

For more information about Securonix NDR, schedule a demo at: www.securonix.com/request-a-demo.



securonix