SECURONIX™

DATASHEET

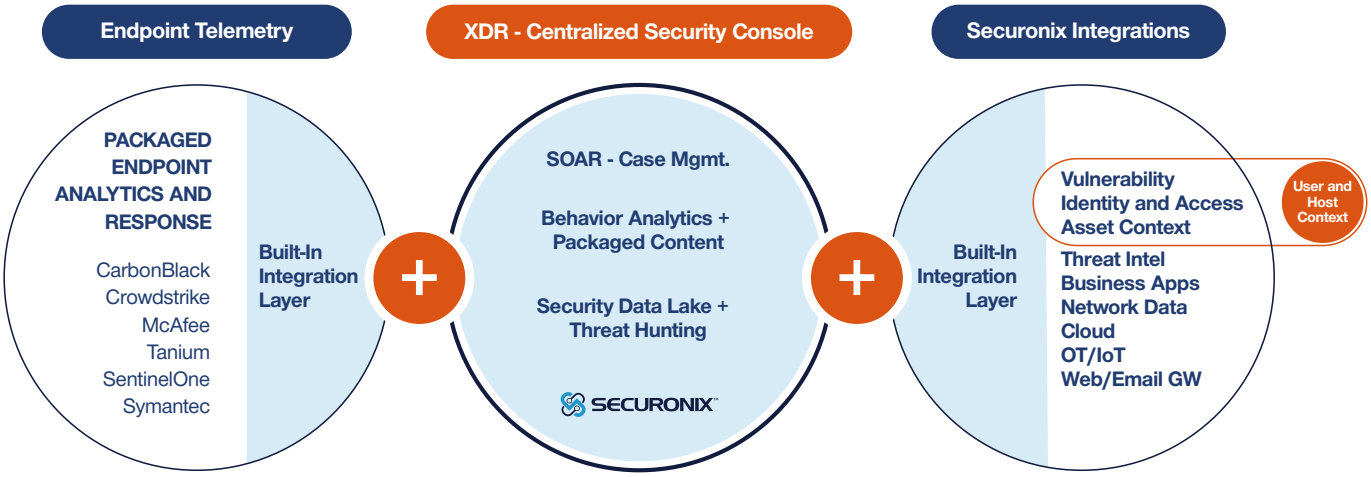
Open XDR

Comprehensive Fabric for Threat Detection and Response

Cyber threat actors are employing more sophisticated attacks to bypass security controls. Meanwhile, security teams struggle to secure environments that have grown beyond the traditional endpoint to include new cloud services, business apps, and IoT devices. However, an expanding security footprint usually leads to alert overload with uncorrelated alerts and events coming from disparate tools. They need to not only improve threat detection, but also accelerate incident response, reducing containment and remediation times.

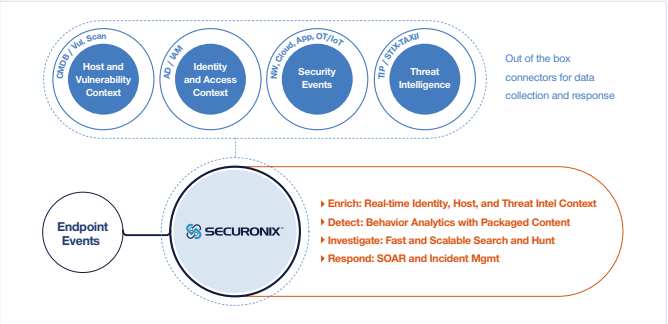
Securonix Open Extended Detection and Response

Securonix Open Extended Detection and Response (XDR) is a comprehensive security fabric that combines the core components required for fast and effective threat detection and response. Connecting multiple sources of telemetry with advanced behavior analytics, powered by an industry pioneering UEBA, Securonix XDR continuously delivers threat detection content aligned to the MITRE ATT&CK framework. Automated response capabilities, powered by pre-built connectors and playbooks, mitigate threats quickly and efficiently.



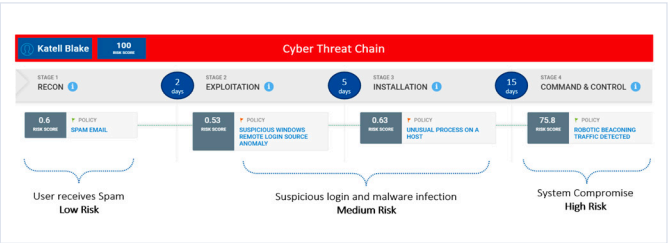
Solution Benefits

- Machine learning-powered behavior analytics provide enhanced detection.
- Enriched events with identity and asset context provide proper risk prioritization.
- Built-in investigation and automation capabilities decrease time to respond.



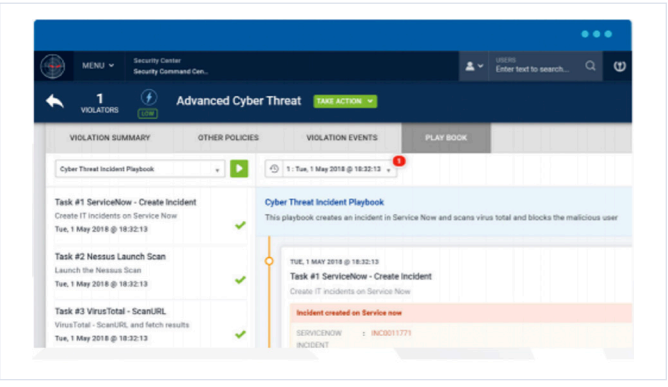
Complete Real-Time Visibility Into Threats

XDR solutions assembled using legacy security systems struggle to integrate and communicate swiftly and effectively. With Securonix Open XDR, there is no need to struggle to integrate disparate SOAR and SIEM platforms. Threat detection is natively integrated with orchestration and response capabilities and response actions and playbooks can be directly integrated with detection policies and threat models.



Accurately Detect Advanced and Insider Threats

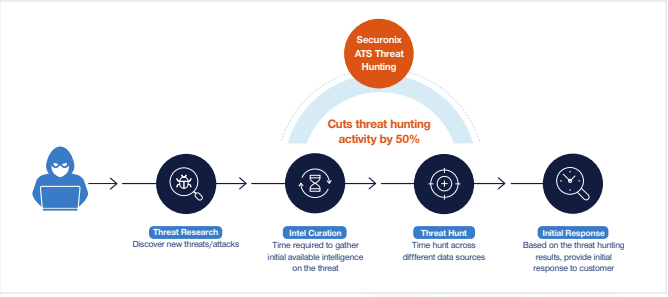
Legacy rule-based correlation is simple, but it often misses larger, more advanced threats. Securonix Open XDR leverages UEBA and patented machine learning (ML) based threat detection to connect together anomalies and other suspicious activities based on identities and other entities.



Intelligent, Automated Incident Response

Security incidents, if not acted upon in a timely manner, can cause a lot of damage in a very short time. Automated response increases the productivity and efficiency of your SOC team, instead of relying on time-consuming manual investigation.

Securonix Open XDR provides automated incident orchestration and response with 275+ connectors and 3000+ playbook actions. Securonix playbooks are provided out of the box and are fully customizable.



Find Hidden Threats With Autonomous Threat Sweep (ATS)

Advanced threats, such as Sunburst, have been discovered and disclosed long after the initial intrusion has occurred – with attacker dwell time measured in years and months.

Acting like your own dedicated Cyber Rapid Response Team, Securonix ATS provides air-cover for your security operations team. It automatically, continuously, and retroactively hunts for new and emerging threats in current and long-term historical data based on the latest, up-to-date threat intelligence.

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

SECURONIX™

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000