securonix

DATASHEET

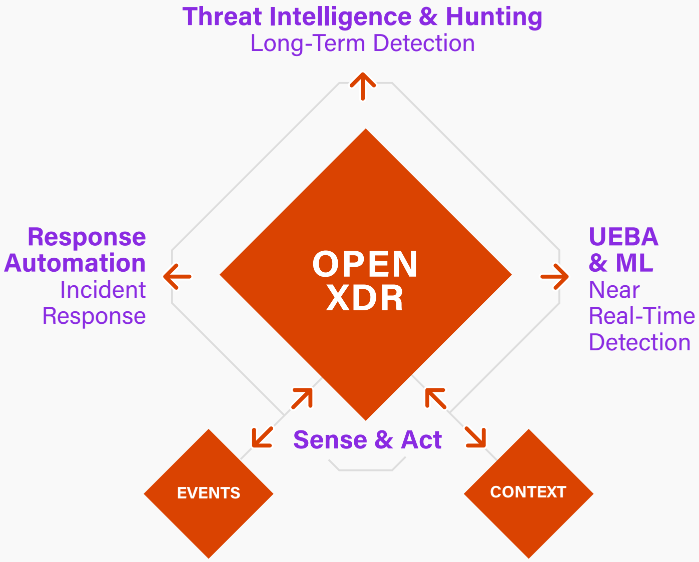
Open XDR

Comprehensive Fabric for Threat Detection and Response

Empower Your SOC for Faster Threat Detection and Response

Many organizations have adopted hybrid and cloud environments that create cybersecurity blind spots, making them more vulnerable to complex and sophisticated cyberattacks. Today, threats can span multiple data sources within your cloud. With Securonix Open XDR (eXtended Detection and Response), threat visibility and context are surfaced to rapidly detect and respond to hidden threats. Security teams can then quickly eliminate any further impact and reduce the severity and scope of the attack.

Securonix Open XDR simplifies the user experience by combining behavioral analytics, threat hunting, and response into a single solution.



Benefits of Open XDR

Gain a Comprehensive Solution to Extend Analytics

Open XDR extends advanced analytics and detection capabilities to endpoint data and beyond. Gain stronger analytics and automation to collect data and detect threats across your entire IT environment. Our Open XDR solution provides an easy path for those looking to quickly mature their threat detection and response capabilities. We even offer a frictionless upgrade path to easily expand to full SIEM in the future.

Detect Advanced and Insider Threats with More Accuracy

The attack surface is ever expanding. It is critical to determine if you have threats undetected in your environment.

Securonix Open XDR combines multiple sources of telemetry with advanced behavioral analytics to find complex threats with minimal noise even those currently lurking in your environment. Our solution leverages out-of-the-box analytics, UEBA, and machine learning (ML) to connect anomalies and other suspicious activities based on identities.

Accelerate Incident Response

Manual investigation and response are time consuming. Securonix Open XDR provides automated incident response with out-of-the-box playbook actions that cover the most common use cases. This reduced complexity helps you increase the productivity and efficiency of your SOC.

Product Features

Extend Visibility and Analytics

Endpoint solutions often lack advanced analytics to correlate and detect sophisticated threats. Securonix Open XDR brings advanced analytics to your cloud, on-premises, and endpoint data for better threat detection and response.

ML-Based Behavioral Analytics: Enable behavioral analytics on logs collected from endpoints, networks, cloud, and other sources. Securonix Open XDR helps you detect anomalous behavior with machine learning (ML) and risk-scoring algorithms. Leverage a library of built-in threat content to detect threats for specific use cases. Our XDR solution evaluates individual events and activity data, cross-correlates the data, and then applies analytics to detect sophisticated, unknown, and insider threats.

Extended Visibility with Connector Library: Gain faster time-to-value with out-of-the-box integrations and connectors that cover technologies including endpoint, network, cloud, business applications, and more. These integrations help support data ingestion, context enrichment, threat hunting, detection, and automated response. Gain more value from your existing security investments in a tightly unified single pane of glass for the SOC.

Advanced Detection of Threats

Designed with advanced analytics at its core, our solution includes contextualized enrichment and user-based risk scoring to help you uncover complex threats with minimal noise.

Built-In User and Entity Behavior Analytics: Identity-centric behavior analytics provides visibility beyond just endpoint activity. MITRE ATT&CK based threat chains combine individual alerts into threat patterns to prioritize high-risk threats.

Risk Scoring: Know when to act with comprehensive identity and risk profiles for every user and entity.

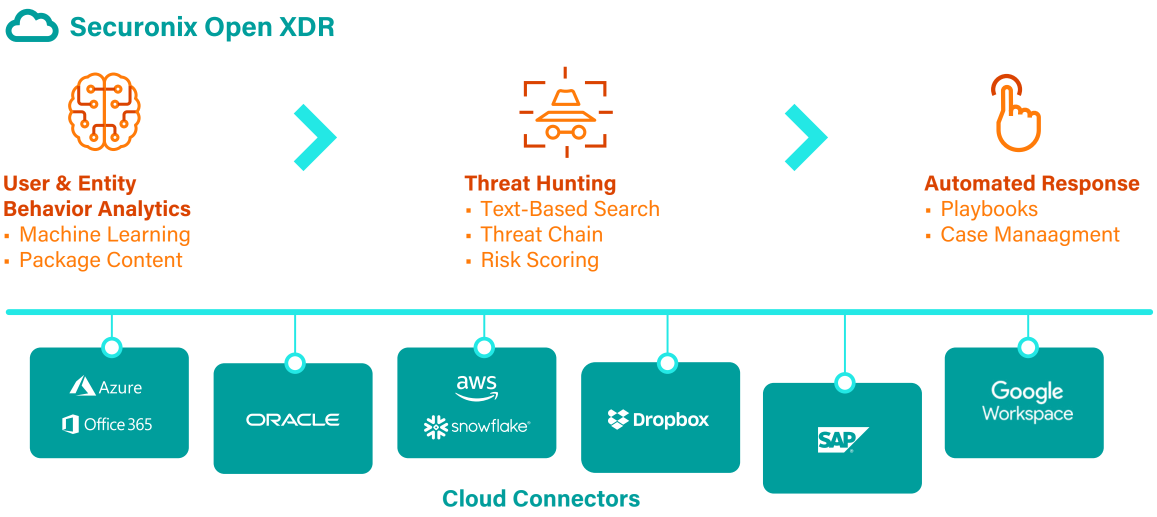
Threat Chain: Reduce the volume of alerts using threat chain models that map to both the MITRE ATT&CK and US-CERT frameworks.

Security Orchestration, Automation, and Response (SOAR)

Security incidents, if not acted on quickly, cause damage to an organization fast. Automated incident response can help mitigate risk with a rapid response. Security orchestration, automation, and response increase the productivity and efficiency of your SOC team.

Built-In Playbook Actions: Securonix Open XDR lessens the workload for analysts with with out-of-the-box, or fully customizable playbook actions. They allow analysts to automate response actions for common use cases.

Incident Management: Built-in incident management capabilities efficiently track and report on the incident response process. This workflow starts the minute an analyst starts investigating a possible event to when an identified threat is mitigated.



Securonix Open XDR

User & Entity Behavior Analytics
- Machine Learning
- Package Content

Threat Hunting
- Text-Based Search
- Threat Chain
- Risk Scoring

Automated Response
- Playbooks
- Case Manaagment

Cloud Connectors

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