securonix

DATASHEET

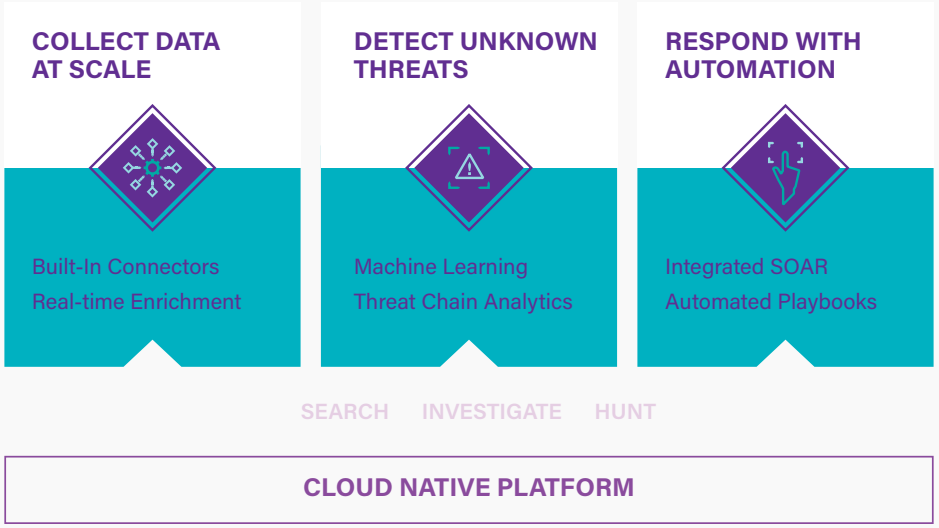
Next-Generation Security Information and Event Management

Combat Advanced Threats at Cloud Scale

Take an Analytics-Driven Approach to Threat Detection

Many organizations today adopt hybrid and cloud environments, making them more vulnerable to complex and sophisticated cyberattacks. Present day threats can span multiple data sources within your cloud, where traditional SIEMs have poor visibility into the cloud. With huge amounts of cloud data, legacy SIEMs often struggle with an inability to scale and use weak rule-based detection techniques to identify complex threats.

Securonix Next-Gen SIEM collects massive volumes of data in real-time, uses patented machine learning algorithms to detect advanced threats, and provides artificial intelligence-based security incident response capabilities for fast remediation. Securonix Next-Gen SIEM gives your security team profound visibility, detection, and response at cloud scale and integrates seamlessly with all the data sources, threat intelligence tools, and other technologies in your SOC that enable your analysts to stay on top of the threats.



Accelerate Threat Detection and Response

Securonix's analytics-driven approach to SIEM helps you automate security operations, analyze data at scale, and simplify investigations in a cloud-native solution.

Gain Unparalleled Visibility

Securonix Next-Gen SIEM provides a flexible, open architecture that allows you to ingest and view all of your data, whether it is cloud-based, on-premises, or hybrid, in a single dashboard.

Respond to Threats Faster

Respond faster with the ability to quickly hunt for threats on historical data without impacting performance. A tight integration with SOAR automates incident response workflows for faster mitigation.

Improve SOC Efficiency

Achieve fast time-to-value with threat content and premium applications for industry-specific use cases through automated threat sweeps.

Industry Leading Next-Gen SIEM

Securonix Next-Gen SIEM is powered by industry-leading analytics. That's why Securonix is trusted by 5 of the Fortune 10 companies.

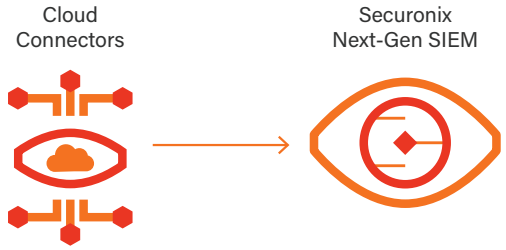
Collect Data at Scale

Built on a cloud-native architecture, Securonix gives you the ability to scale as your data requirements evolve. Ingest data from cloud-based or on-premises sources for unrivaled visibility across your hybrid infrastructure.

Cloud-Native Architecture: Offers on-demand scaling and zero infrastructure to manage.

Data Collection: More than 350 cloud connectors, allows Securonix to seamlessly integrate and easily ingests data from a wide variety of sources across hybrid infrastructures.

Cloud Integrations: Uncover blind spots with Securonix's built-in API-based integrations with cloud applications, infrastructure, and services.



Securonix Next-Gen SIEM seamlessly integrates with more than 350 Cloud Connectors

Detect With Advanced Analytics

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

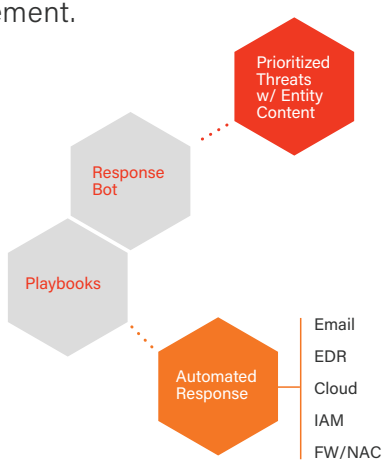
Out-of-the-Box Analytics: Achieve a fast time-to-value with pre-built analytics modules for common threat scenarios.

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

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

Respond With Automated Workflows

Integrated SOAR capabilities help your team to accelerate incident response with automated playbook actions, workflow standardization, and collaborative incident management.



Built-In SOAR: A tight integration between Securonix Next-Gen SIEM and SOAR puts all of your data in one place, allowing you to respond faster.

Long-Term Search: Reduce the time it takes to respond to low and slow attacks already present in your environment with the ability to quickly search on historical data.

For more information about the Securonix Nex-Gen SIEM, schedule a demo at: www.securonix.com/request-a-demo.

securonix