SECURONIX™

DATASHEET

Security Operations and Analytics Platform

Positive Security Outcomes with Zero Infrastructure

The Securonix Security Operations and Analytics Platform combines log management; user and entity behavior analytics (UEBA); next-generation security information and event management (SIEM); network traffic analysis (NTA); and security orchestration, automation and response (SOAR) into a complete, end-to-end security operations platform.

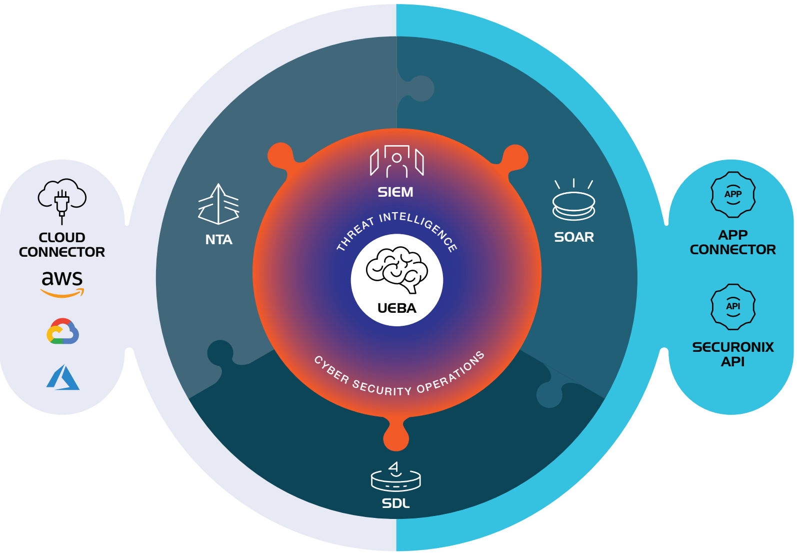
The Securonix platform delivers unlimited scale, powered by advanced analytics, behavior detection, threat modeling, and machine learning. It increases your security through improved visibility, actionability, and security posture, while reducing management and analyst burden.

aws partner network

Advanced
Technology Partner

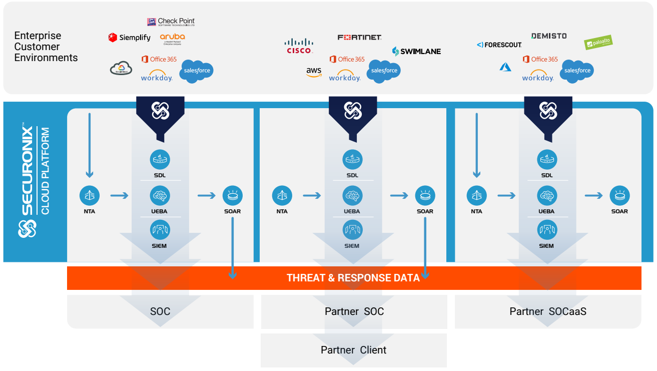
Security Competency

Security for the Cloud, in the Cloud



Product Features

Flexible Multi-Tenant Architecture with AWS Certification



Amazon Web Services (AWS) Security Competency status recognizes that Securonix has demonstrated technical proficiency and proven customer success in delivering SIEM as a service on the AWS platform.

A platform with a multi-tenant architecture lets you use as much resources as needed for your organization now and expand as you grow with the click of a button.

Secure by Design

AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

SOC 2 Type 2, ISO 27001:2013, and HITRUST CSF certified.

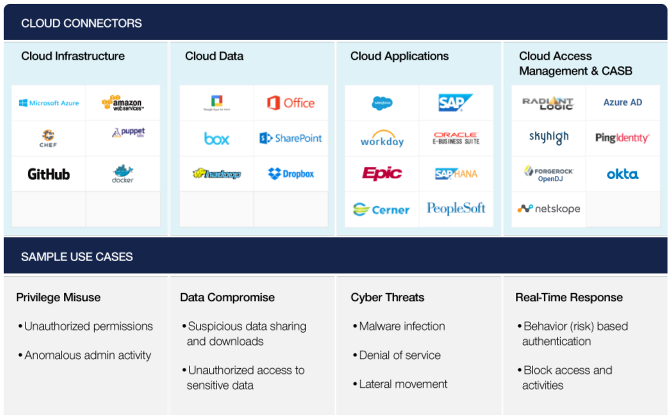
In a multi-tenant architecture, individual tenant IDs and dedicated tenants are used to maintain complete data segregation.

Data is kept encrypted while it is in transit, and data at rest can be encrypted if you choose to.

Limit access to your data using granular, role-based access control.

Detailed logging capabilities ensure a full audit trail of all activities within the solution.

Cloud-to-Cloud Monitoring



CLOUD CONNECTORS

Cloud Infrastructure	Cloud Data	Cloud Applications	Cloud Access Management & CASB
Microsoft Azure amazon web services CHEF puppet GitHub docker	Google Drive Office box SharePoint Box Dropbox	salesforce SAP workday ORACLE E-BUSINESS SUITE Epic SAP HANA Cerner PeopleSoft	RADIANT LOGIC Azure AD skyhigh PingIdentity FORGEROCK OpenDJ okta netskope

SAMPLE USE CASES

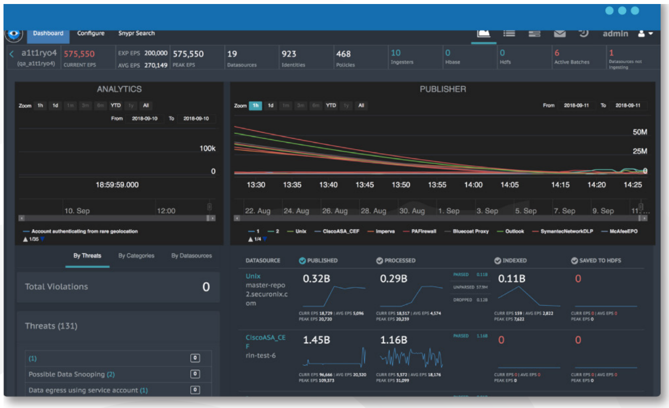
Privilege Misuse	Data Compromise	Cyber Threats	Real-Time Response
• Unauthorized permissions • Anomalous admin activity	• Suspicious data sharing and downloads • Unauthorized access to sensitive data	• Malware infection • Denial of service • Lateral movement	• Behavior (risk) based authentication • Block access and activities

Extend seamless security monitoring across your cloud environment without needing to rely on on-premises solutions that were not designed for the cloud.

Analyze user entitlements and events to look for malicious activity using built-in APIs for all major cloud infrastructure and application technologies.

Eliminate blind spots when you can correlate between on-premises data and cloud data to analyze end-to- end activities and detect actionable threat patterns.

Results, Not Infrastructure



Security visibility, threat hunting, and response without an application to manage. That's the result of using next-generation SIEM as a service.

There is no loss of control – analysts and management can still monitor nodes, clusters, and all application jobs, including imports, analytics, and storage.

Receive alerts and notifications for node issues, cluster issues, and application issues.

For more information about the Securonix cloud security platform visit:
www.securonix.com/platform/securonix-security-operations-and-analytics-platform/

SECURONIX™

LEARN MORE
www.securonix.com

©2020 Securonix

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