SECURONIX™

SOLUTION BRIEF

Securonix Cloud Security Monitoring

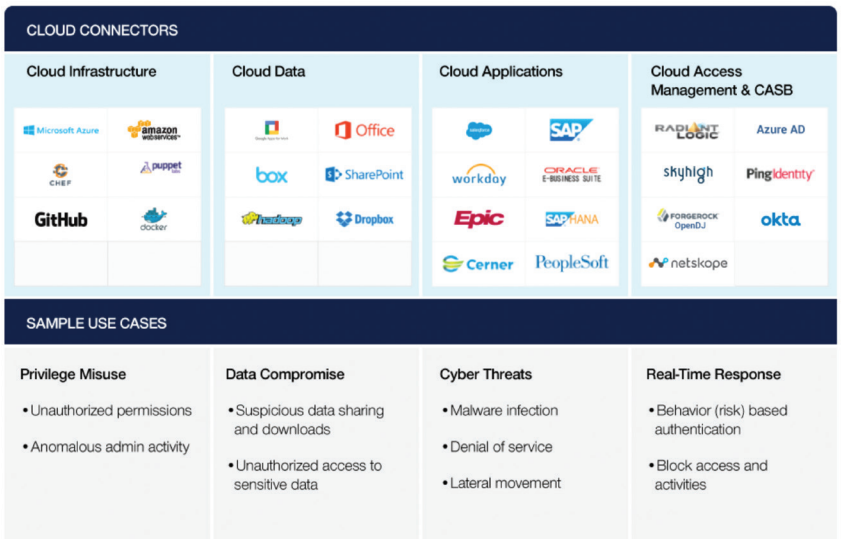
Enterprises are rapidly adopting cloud technologies, resulting in a huge number of enterprise applications and use cases moving to cloud-based systems. However, legacy on-premises security controls are insufficient to secure cloud environments, as their single source of truth ideology is incompatible with modern single sign-on identity systems and applications that span multiple clouds.

Context-Aware Analytics and Detection

Key cloud security monitoring concerns include how to identify sensitive data movement in the cloud, unauthorized activities, privilege misuse or compromise, unauthorized sharing, and data exfiltration as well as access control. Your cloud security monitoring approach needs to incorporate all aspects of the cloud, including cloud infrastructure, cloud data sharing applications, cloud enterprise applications, and cloud access management tools.

Securonix cloud security monitoring extends security to your cloud infrastructure and applications. With built-in integration for APIs for all major cloud infrastructure and application technologies, the solution analyzes user entitlements and events to look for malicious activity. It then correlates cloud-based data with data from on-premises devices and other sources of truth to add entity context information and analyze the end-to-end activities of the entity in order to detect actionable threat patterns.

In addition to detecting threat patterns, Securonix is the only solution that also provides data classification and privileged access governance capabilities. With data classification, you can scan your cloud environment for sensitive data. The privileged access governance capability enables you to do dynamic access management using techniques such as peer group analysis. The solution also provides the ability to perform periodic access reviews to sensitive data in the cloud and to manage access proactively to avoid data breaches.



Solution Benefits

- API integrations with all major cloud service providers.
- Out of the box content for monitoring advanced cloud threats.
- Bi-directional integrations with cloud security tools to take automated remediation action.
- Enrichment of data with additional context for threat modeling.
- MITRE ATT&CK compliance with threat chain methodology that is in line with MITRE's own staged threat framework.

For the Cloud, in the Cloud

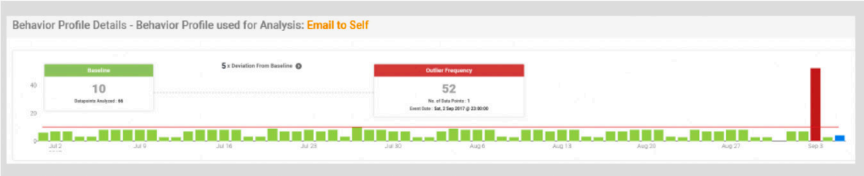
Securonix is a cloud native SIEM solution that deploys as a service and provides organizations with cloud-to-cloud monitoring through built-in API integration and out of the box content.

- API integrations with all major cloud service providers.
- Out of the box content for monitoring advanced cloud threats.
- Bi-directional integrations with cloud security tools to take automated remediation action.

Cloud Security Monitoring Solution Features

User Risk and Threat Monitoring

Securonix cloud security monitoring continuously builds a comprehensive risk profile of a user based on identity, employment, security violations, IT activity and access, physical access, and even phone records. All identity, activity, and access characteristics are compared to their individual baseline, their peers' baseline, and known threat indicators in order to identify true areas of risk. Key use cases include monitoring for suspicious login attempts, unauthorized access to sensitive data, and misuse of privileged accounts.



Cyber Threat Monitoring

Cyberattacks in the cloud are growing exponentially and are a big concern for organizations as their data sits outside the traditional security perimeter. Securonix cloud security monitoring provides out of the box content to monitor for malware attacks, denial of service attempts, and password attacks, among other advanced threats.

Cloud Application and Data Risk Monitoring

Insiders target sensitive data, transactions, or the systems that host them. Securonix addresses this threat by monitoring critical applications and systems at the transaction, data set, and sensitive user record level. Securonix builds and continuously updates a risk profile for enterprise cloud applications such as Salesforce, Workday, Office 365, Google Apps, Box, and Dropbox, among others.

Cloud Technology Ecosystem

Securonix has built a strong cloud security ecosystem with bi-directional API-based integrations. This enables Securonix to integrate with all major cloud technologies and support automated incident response to take action against threats in near real time. Major technology partners include Okta, AWS, Microsoft, Crowdstrike, and Netskope, among others.

Key Use Cases

- Privilege misuse and escalation
- Access hijacking
- Data compromise
- Malware infections
- Lateral movement
- Rapid, real-time response and remediation
- API-driven integrations for alert monitoring and correlation across clouds, identity providers, and SaaS applications

About Securonix

The Securonix platform delivers positive security outcomes with zero infrastructure to manage. It provides analytics-driven next-generation SIEM, UEBA, and security data lake capabilities as a pure cloud solution, without needing to compromise. For more information visit www.securonix.com.

SECURONIX™

LEARN MORE
www.securonix.com

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