

securonix + WIZ

SOLUTION BRIEF

Securonix + Wiz Integration

Detect Threats Across Cloud and
On-Prem Environments



securonix + WIZ

The Problem

Organizations adopting cloud technologies have to navigate the complexity of cloud infrastructure and address potential misconfigurations and vulnerabilities. On top of this, they must also ensure they have comprehensive risk analysis across their ecosystem. Traditional security tools may not fully address these cloud-specific risks and threats. Wiz.io specializes in identifying and mitigating cloud-related security issues, while Securonix provides comprehensive event analysis and real-time monitoring. Together, these solutions help enterprises prevent cloud-based security incidents.

Why Securonix + Wiz?

Wiz continuously prioritizes the critical risks based on a deep cloud analysis across misconfigurations, network exposure, vulnerabilities, malware, and identities to build a single prioritized view of risk. Securonix collects and analyzes security data from various sources across an organization's network, including servers, applications, firewalls, and more. By integrating Wiz's cloud security insights into the SIEM, you can achieve a more comprehensive view of your overall security posture, including cloud and on-premises environments.

Solution Benefits

Detect Threats More Effectively

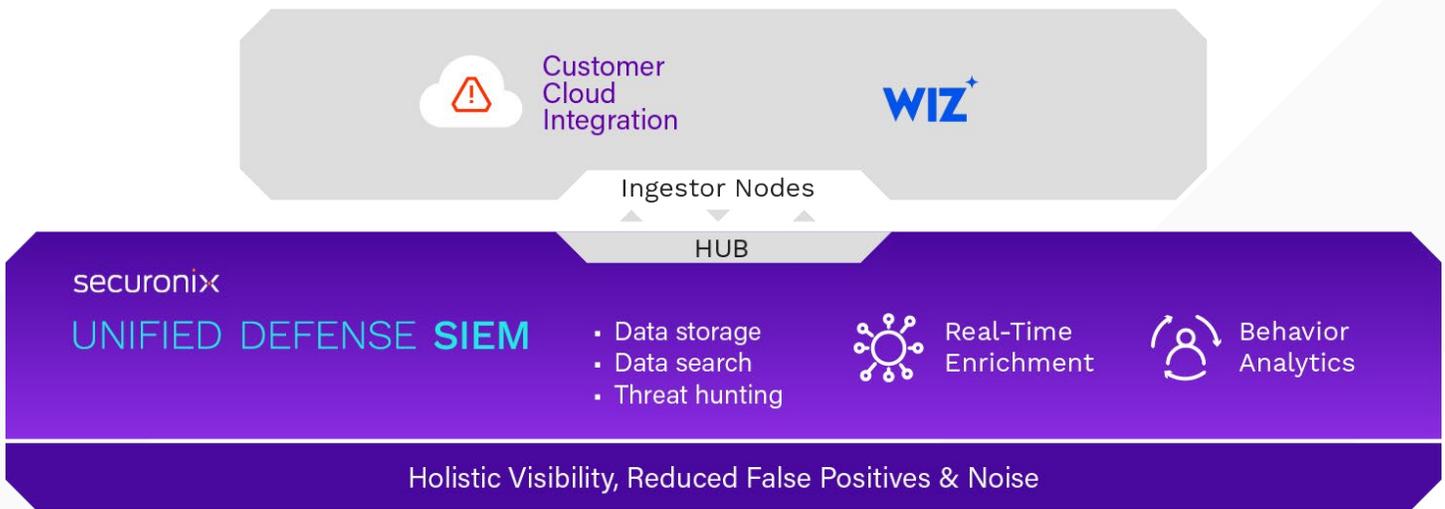
Eliminate gaps in your environment. The integrated solution allows you to monitor security events and incidents across cloud platforms and on-premises infrastructures alike for a holistic view of your environment.

Understand Security Incidents In Your Environment

Securonix Unified Defense SIEM leverages threat chains to correlate and connect seemingly unrelated security events across different layers of an organization's infrastructure. When integrated with Wiz.io's cloud-specific insights, you can understand where the threat or attack is occurring in your cloud environment. This context helps you understand the blast radius of how it can impact your infrastructure.

Stay Ahead of Emerging, Cloud-born Threats

Stay ahead of emerging threats in the cloud with up-to-date threat content, curated by Securonix global experts. Our threat content, combined with Wiz's cloud security research lets you quickly add or update your system for fast coverage of newly discovered threats.



How It Works

By combining Securonix’s advanced security analytics and threat detection capabilities, along with Wiz’s cloud-native application protection platform, organizations can enjoy a unified approach to safeguarding their digital assets. This includes tracking vulnerabilities, misconfigurations, and assets across complex on-prem and cloud environments. This is useful for risk management, alert enrichment, and tracking enterprise SLAs and metrics.

Features of the Securonix and Wiz Integration

Unified Security Investigation Dashboard

Wiz eliminates blind spots by scanning every layer of your cloud environment without agents to provide complete visibility into every technology running in your cloud. Wiz adds enrichment to correlate risks across the environment and prioritize them accordingly. Combining Wiz.io’s cloud security insights with Securonix creates a unified view of security events and incidents. This helps security teams better understand the context and relationships between events happening across different parts of your organization’s infrastructure.

Enrichment & Threat Modeling

When Wiz.io detects a cloud security issue, Securonix can pull this data into the SIEM and stitch together related alerts paired with events. The SIEM can identify low, slow threats that occur over several steps. Alerts may not be significant on their own, but when tied together into a threat chain with Securonix, connected to a single entity (user, IP address, login ID, etc.) it can indicate a severe security event.

Compliance Monitoring & Reporting

Many industries and regions have specific regulations governing data security and privacy. By using both Securonix and Wiz, you can more effectively monitor and enforce compliance in your cloud and on-prem environments, helping avoid potential penalties and reputational damage. Organizations can also use the integrated solution to analyze security trends, track incident response metrics, and generate comprehensive security reports for stakeholders.



Use Cases for Securonix + Wiz

When customers bring in Wiz.io data into Securonix Unified Defense SIEM, they can address a variety of use cases to enhance your organization's overall security posture, particularly in cloud environments. Bolster your cloud security posture for the following key use cases:



Cloud Security Monitoring



Reducing False Positives



Security Analytics and Reporting

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

securonix

About Securonix

Securonix is leading the evolution of SIEM for today's hybrid cloud, data-driven enterprises. Securonix Unified Defense SIEM provides organizations with the first and only content-driven threat detection, investigation and response (TDIR) solution built with a highly scalable data cloud and a unified experience from the analyst to the CISO. The innovative cloud-native solution enables organizations to scale up their security operations and keep up with evolving threats. For more information visit securonix.com

About Wiz

Wiz transforms cloud security for customers – including 35% of the Fortune 100 – by enabling a new operating model. With Wiz, organizations can democratize security across the development lifecycle, empowering them to build fast and securely. Its Cloud Native Application Protection Platform (CNAPP) drives visibility, risk prioritization, and business agility, and is #1 based on customer reviews. For more information, visit www.wiz.io