securonix

SOLUTION BRIEF

Securonix for Healthcare

Identify Threats Before They Harm Your Organization

Healthcare firms are custodians of much more than a patient's health. They are bound by HIPAA and several other data security and privacy requirements to protect patient data from compromise. With malicious actors using every trick in the book, healthcare security leaders are looking to implement strong controls to monitor this data.

Most SIEMs do not have pre-built content for healthcare applications. However, the Securonix Next-Gen SIEM solution provides healthcare specific content that includes connectors to leading electronic medical record (EMR) applications, as well as healthcare specific threat use cases that leverage Securonix's security analytics capabilities.

Our Approach

Securonix goes beyond the signature-based detection of legacy SIEM solutions to find unknown threats quickly. To do this, Securonix leverages the latest advances in machine learning and artificial intelligence to baseline normal behavior patterns, detect suspicious data access patterns, and identify real threats to patient data, quickly and accurately.

> **"Our hospital has always been a leader in data driven approaches to clinical problems. Securonix has helped us apply behavior analytics to our security challenges as well. With their help, we are able to detect patient record snooping, HIPAA breaches, insider threats, and targeted attacks that would otherwise go unnoticed."**
>
> — SECURITY LEADER AT A MAJOR HEALTH INSTITUTION

Solution Benefits

Protect patient records and comply with regulatory requirements using advanced security monitoring and industry-leading behavior analytics.

Detect threats to patient privacy

Enable detection in your organization's IT infrastructure and respond to threats such as patient data theft, malware, phishing, and more.

Leverage healthcare-specific threat content

Take advantage of out-of-the-box content for monitoring healthcare specific threats and patient data misuse.

Get 360 degree visibility

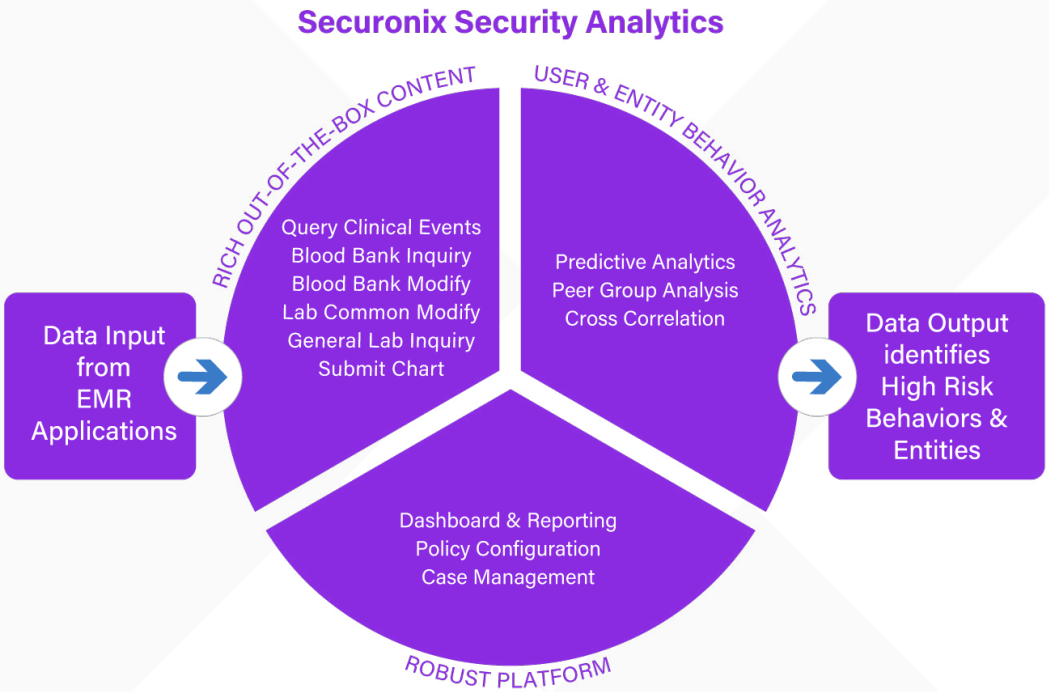
Enrich data with additional context from on-premises data sources and other applications for threat modeling.

How it Works

Securonix ingests a nearly unlimited amount of data from a wide breadth of sources. The solution connects seamlessly to industry standard healthcare applications. The Securonix machine learning engine establishes baselines of normal behaviors within those applications such as logins, chart submissions, lab queries, and clinical event queries, to name a few. It then flags suspicious behaviors that could indicate non-compliant behaviors, record snooping, or data theft.

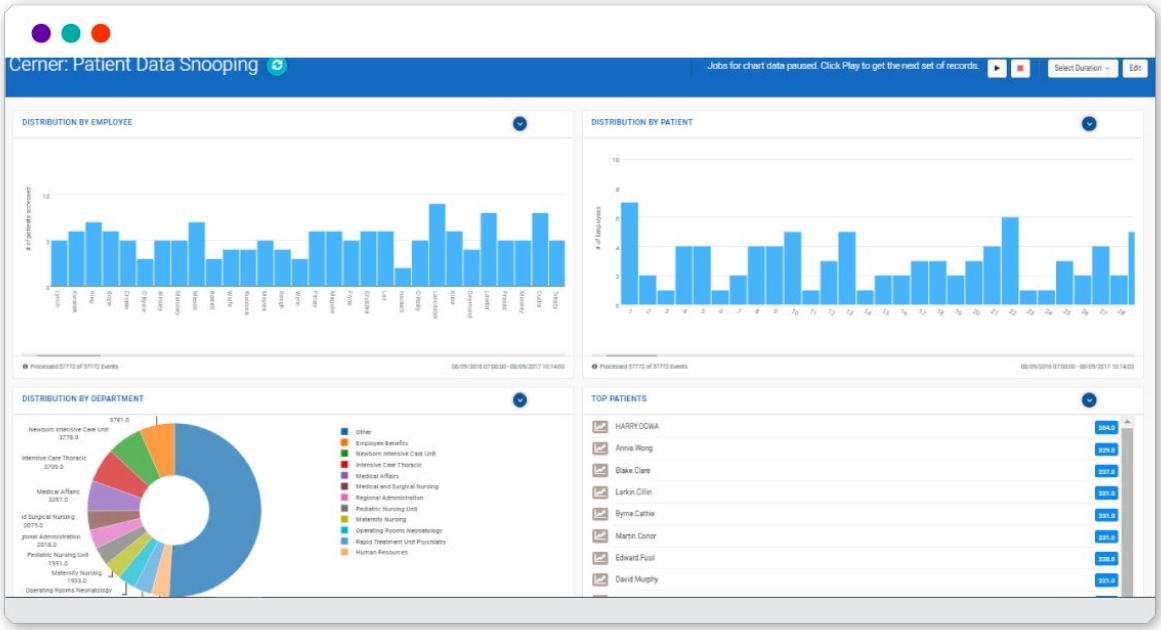
Focus on Visibility and Access Threat Models

To detect compromise effectively, security teams need to integrate network and application information. This can help paint a more holistic picture of the threat. Securonix is able to ingest and correlate your whole IT environment and visualize it so you can understand where and how a malicious actor gained access. You can also see the actions they took afterward, and what the IOCs were present across a variety of different data sources.



Robust Reporting and Dashboards

Securonix provides healthcare-specific visualization, dashboards, and out-of-the-box reporting capabilities. Our Next-Gen SIEM supports role-based access to limit the information that a user can view based on their role. Reports are standardized for various compliance needs and can easily be customized based on organizational needs.



Enable Compliance

To ensure compliance with HIPAA, HITRUST, GDPR, and other regulations, Securonix provides the capability to mask and hide privileged information from end users during the event collection and analysis process.

Cover Top Healthcare Use Cases

Identify sensitive data movement and suspicious login activity on the cloud including:

- **Account Misuse:** Detect unusual access to patient records.
- **Compliance Reporting:** Leverage out-of-the-box reports for compliance mandates such as HIPAA, HITRUST, and GDPR.
- **Snooping:** Determine real incidents of data snooping without false positives.
- **Insider Threats:** Leverage threat chain analytics to detect and prioritize insider threats.
- **Ransomware:** Identify imminent, sophisticated attacks that can lead to ransomware infections.

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