securonix

SOLUTIONS BRIEF

# Securonix for Healthcare

## The Challenge

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 and protect this data.

Most SIEMs do not have pre-built content for healthcare applications. However, the Securonix platform 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 analytics 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.

## Key Use Cases

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

- Streamlined Integration: Collect relevant events from all major EMR applications.
- Context Enrichment: Prioritize the highest-risk threats in your environment.
- Behavioral Analytics: Detect threats to patient data privacy using out-of-the-box healthcare use case content.
- Data Privacy: Strict data privacy controls protect patient data privacy while you collect and analyze EMR events.
- Compliance Reporting: Leverage out-of-the-box reports for compliance mandates such as HIPAA, HITRUST, and GDPR.
- Robust Data Insights: Visualize activity and threat patterns in your environment.

## Solution Benefits

- Secure your organization's IT infrastructure from patient data theft, advanced threats, malware, phishing, and other attacks.
- Take advantage of out-of-the-box content for monitoring healthcare specific threats and patient data theft.
- Enrich data with additional context from on-premises data sources and other applications for threat modeling.
- Utilize threat models specific to healthcare and patient data theft.

**"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 MAJORHEALTH INSTITUTION



securonix

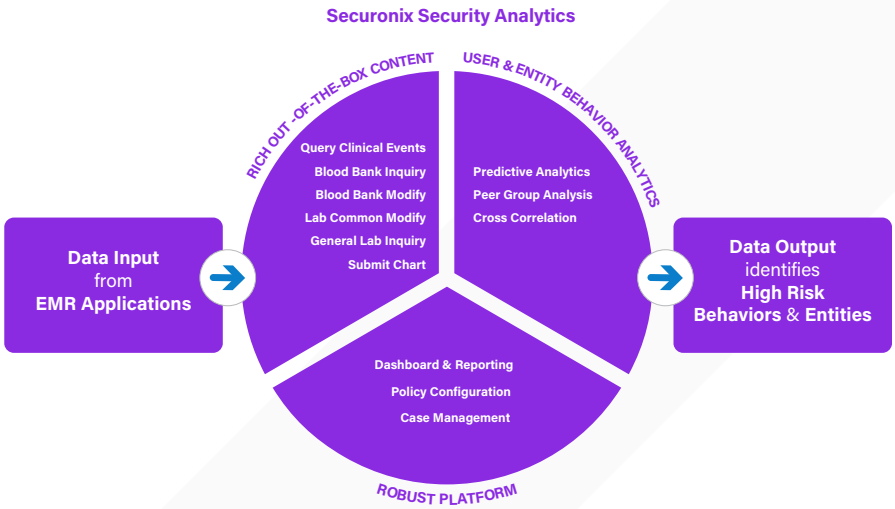
## Integrated Security for Healthcare

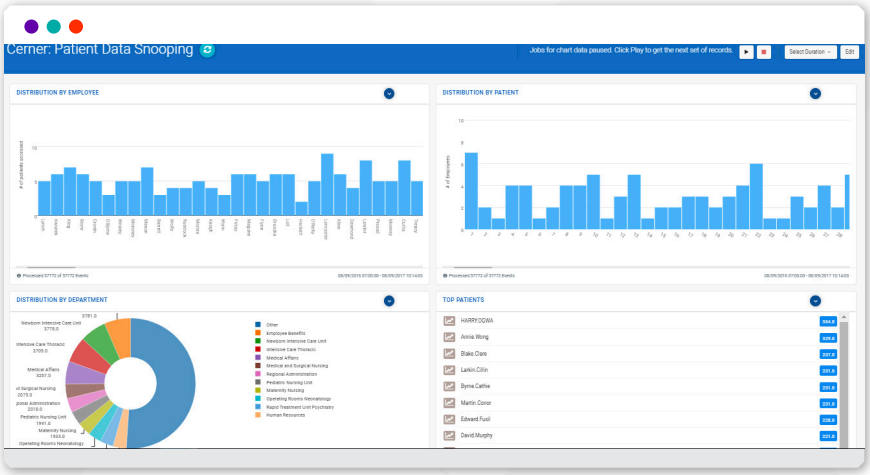
Securonix ingests nearly unlimited volumes of data from a wide breadth of sources. The platform connects seamlessly to industry standard healthcare applications. The Securonix machine learning engine establishes baselines of normal behaviors within those applications such as logins, chart submissions,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

## Focus on Visibility and Information Access

Other behavior-based threat detection tools only analyze activity logs from EMR systems. To protect effectively, however, 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 all of this data and visualize it so you can understand where and how a malicious actor gained access, the actions they took afterward, and what the indicators of compromise were across a variety of different data sources.




## Reporting and Dashboards

Securonix provides healthcare-specific visualization, dashboards, and out-of-thebox reporting capabilities. The dashboards support 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.

## Compliance Focus

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.

### About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, XDR, SOAR, Security Data Lake, NDR and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise and prioritizes high fidelity alerts with behavioral analytics technology that pioneered the UEBA category.
For more information visit securonix.com