OpSusSentry

Get the next layer of defense against data leakage, theft, employee snooping, and exposure of health records.

Healthcare Privacy & Data Security

THE SOLUTION

OpSus Sentry, powered by Bottomline Technologies, offers a first-of-its-kind cross-platform surveillance system for unparalleled visibility of end-user activity in sensitive health information systems and back office applications across heterogeneous environments. The solution provides a critical infrastructure to help health systems and hospitals combat HIPAA violations and data theft by replacing human adherence to policy and procedure with technology that ensures that inappropriate or suspicious behavior can be stopped before it is too late.

- **Unparalleled Visibility in End-User Activity** – Complete visibility into end-user activity is provided with visual replay of the data accessed in key applications. All actions are visible, including update and read-only actions. All types of end-users are tracked, including privileged end-users such as System Administrators and Database Administrators that may pose a higher risk as they have higher authorization levels.

- **Complete Audit Trail** – Records full user activity 24x7, not just events detected as suspicious in real time. This is crucial for making end-users accountable for their actions. Regardless of whether appropriate rules are in place at the time of an event, post-event replay enables forensic investigation at a later time.

- **Cross Application and Platform Search including Legacy** – A unique solution for tracking user activity across major applications. It allows you to search for any specific value across multiple applications and environments from one simple query screen. The rules track cross-application business processes. For example, a process tracked by the solution may start on a mainframe, continue in a client-server application and end on the web.

- **User Behavior Profiling at the Application Level** – The only solution on the market that analyzes the user activity at the application screen level (not at the network or database level). Rules track all user actions and the flow of screens accessed by the user, detecting the relevant user process. This information is correlated in real-time with the activity of other end-users, with previous activity and other types of information generating alerts on suspicious behavior near real-time.

Create accountability. Reduce the risk of privacy breaches.

Healthcare organizations around the world are facing a growing threat to their assets and brand from within – their own management and employees. Suspicious behavior committed by knowledgeable and capable employees who utilize their knowledge of IT systems and controls to manipulate internal systems can cause much greater damage than third parties. In addition, HIPAA and other privacy regulations require a full audit trail of access to patient's data. Mechanisms that track changes to corporate databases re not sufficient, as they typically track update transactions but do not capture critical "read-only" access to data.

Powered by

Bottomline Technologies

CloudWave

100 Crowley Drive, Marlborough, MA 01752 877-991-1991 gocloudwave.com

REALIZE BENEFITS QUICKLY

The OpSus Sentry Healthcare Privacy and Data Security solution provides exceptional business value out-of- the-box. Immediately following installation (which typically takes just a few hours), The solution begins capturing all user activity, allowing internal auditors to perform thorough investigations with complete visual replay. Security officers can immediately search for all data in which specific values appeared during a specific timeframe in any application across any platform in the enterprise. Hospitals and health systems begin benefiting from the solution without delay, with no need for time-consuming integration with any of the organization's systems or application-related configurations.

UNIQUE BUSINESS VALUE

OpSus Sentry provides a unique business value to leading healthcare organizations around the world:

·Reduce internal fraud losses by detecting fraud and other malicious activity in real-time

·Comply with HIPAA and other regulations by generating a detailed cross-platform audit trail of any access to protected health information, including queries, without changing a single line of code

·Improve internal audit effectiveness by alerting on suspicious user behavior and providing full visibility for the internal auditors of all the actions of each specific suspicious end-user, as if looking over his or her shoulder

KEY SCENARIO PROTECTION

Identity Theft
A hospital employee browses through the records of patients, documents the PII of these individuals, then sells this information on the black market. How do you detect it in real time?

External Account Takeover
An employee falls victim to a phishing attack and now a hacker is using their valid user credentials to search for valuable data. How do you recognize the change in user behavior?

Co-worker Snooping
A rumor has spread through your organization about an employee's medical condition after their fellow employee looked up their patient record. How do you modify this behavior in your organization?

HITRUST CSF Certified

Powered by

Bottomline Technologies

Certified HIT 2014 EDITION

This EHR Module is 2014 Edition compliant and has been certified by an ONC-ACB in accordance with the applicable certification criterion adopted by the Secretary of Health and Human Services. This certification does not represent an endorsement by the U.S. Department of Health and Human Services.

Bottomline Technologies' Investigation Center, version 5.1.2, certification number IG-3584-15-0057 and IG-3584-15-0058 is compliant with the ONC 2014 Edition criteria on October 8, 2015 by Infogard, an ONC-ACB, in accordance with applicable Hospital certification criteria adopted by the Secretary of Health and Human Services.

Bottomline Technologies' Investigation Center, version 5.1.2, certification number IG-3584-15-0057 and IG-3584-15-0058 is compliant with the ONC 2014 Edition criteria on October 8, 2015 by Infogard, an ONC-ACB, in accordance with applicable Hospital certification criteria adopted by the Secretary of Health and Human Services. Details of the EHR test report can be found at http://infogard.com/health-care_it/ onc_certification/ehr_certificates and the official listing can be found on the ONC website at http://oncchpl.force.com/ehrcert/productdetails?productNumber=85272 and http://oncchpl.force.com/ehrcert/ productdetails?productNumber=85273

There may be additional costs required to implement this EHR based on implementation decisions that are unique to each user of the EHR Module. These additional costs relate to the selection of database server, directory server, and operating systems for the environment in which the EHR module is to be installed. There may also be costs related to the integration of any homegrown or otherwise non-standard applications in order to provide users with the most robust complete data possible for investigations that take place in the EHR module. There are no other known limitations of the software.

CloudWave

Learn More at www.gocloudwave.com.

CloudWave offers a complete suite of services to provide customers with options for end-to-end EMR/EHR, Imaging, and enterprise systems support and management.

OpSus CloudCare

100 Crowley Drive, Marlborough, MA 01752 877-991-1991 gocloudwave.com