Raytheon

SureView® Insider Threat

Insider Threat Monitoring and Enterprise Audit Management

Enterprise visibility and user activity monitoring to detect, deter, and mitigate insider threats

Benefits

- Endpoint user and system monitoring, including data-at-rest
- Providing military grade protection for more than a decade
- Simplified policy management
- Privacy protection
- Universal SIEM Integration
- Log analysis
- DVR-like replay reduces dependency on technical expertise
- Full activity capture
- Scalable solution with proven, stable agent
- Role-based access controls
- Enables safe and effective use of mission-critical technologies
- Measures the impact of new and existing threats and compliance in real-time
- Pioneered information protection since 2001

The Advanced Persistent Threat (APT) is continuously evolving and targets an agency's most vital information assets. Although technology introduces avenues for threats to enter an organization, genuine cyberthreats do not originate from technology.

Cyberthreats originate from the actions of humans who misuse or abuse technology as they access information assets. Billions are spent each year on cyber threat technologies that attempt to keep the bad guy out via pattern matching algorithms, that cannot effectively discern incident context or end-user intent. These content-blind technologies inhibit real-time, review and response to incidents and attacks. SureView Insider Threat focuses not only on the patterns of network attacks, but also captures human behaviors such as policy violations, compliance incidents or malicious acts at the endpoint that serve as warning signs leading up to a breach.

This plugs the gap left by traditional Data Loss Prevention (DLP) tools that focus on data. Data is important but organizations struggle to identify all their data, classify its importance, tag it, store it in certain containers, and wrap DLP around it. Just reading that list is a daunting task and few organizations can actually do anything about it. But insider threat is a user behavior issue. The solution is to pay closer attention to user behavior.

Overview

SureView® Insider Threat is headed by a team of domain experts who have spent their careers in information protection. They have pioneered an active strategy to protect critical data by monitoring technical observables, including not only data's location and movement, but also the actions (including precursor actions) of users who access, alter and transport that data.

The SureView Insider Threat team has been a trusted mission partner of government organizations and Fortune 100 companies since 2001. Raytheon SureView Insider Threat is a proactive, information protection solution. It identifies and supports investigations of users throughout an enterprise. SureView Insider Threat provides full context for rapidly discerning malicious from benign actions that are easily reviewed and understood by non-technical personnel—all while respecting employee privacy guidelines: through customizable, business-driven policies.

SureView Insider Threat can effectively detect both unauthorized access to information and unauthorized transfer of information. SureView Insider Threat can be deployed for audits and investigations across multiple network architectures using a wide variety of security concepts of operations that range from standalone, single-server systems in a two-person investigation shop to large-scale clusters on a distributed enterprise with multiple stakeholders doing auditing and investigations.

Product Capabilities

SureView Insider Threat helps protect organizations' information and manage insider threats using an integrated, enterprise-wide system rather than purchasing and maintaining a number of independent software applications to monitor user activity.

SureView Insider Threat integrates a suite of features to capture threats in complex desktop applications. Collected data can be viewed in video-like, near real-time replay that displays the user's activity, including keys typed, mouse movements, documents opened or websites visited. This unique capability provides irrefutable and unambiguous attribution of end user activity.

SureView Insider Threat has APT detection capabilities, including malware detection and social-networking auditing, including web posting policies that detect when a user posts information to social networking sites.

Protecting Information

SureView Insider Threat provides a number of pre-defined policies that are based on Raytheon's broad experience in federal and commercial markets. Many scenarios have been predefined, such as protecting sensitive documents and personally identifiable information. Customized policies can also be created to meet organizations' requirements. Nearly all SureView Insider Threat engineers hold government clearances.

SureView Insider Threat also features an extensive ability to fingerprint an organization's critical intellectual property or sensitive document library. Most current technologies simply hash these documents and compare the stored hash with files as they leave your network. This process is easily thwarted. A simple word change or even an extra period will significantly alter the hash value of the newly changed document.

Therefore, typical detection methods require the entire document to be copied for detection while SureView can detect fractional movement from any part of a finger-printed document. SureView Insider Threat is a point-of-use discovery tool capable of capturing intentional and unintentional insider threats to an organization at the desktop/laptop level. This enables detection of abusive behaviors and capture of sensitive documents before encryption or deletion. A distributed architecture also reduces the processing load required to monitor an entire organization.

SureView Insider Threat incorporates the Investigator Workbench, an intuitive organization and collaboration tool, which allows users to group and organize data, including video replay and notes, into a virtual briefcase for easy sharing and export. The Investigator Workbench maximizes the capability to monitor while minimizing the effort required to manage and react to captured alerts. SureView also includes a powerful search engine that facilitates the ability to enhance data searches across the enterprise collection, enabling a more comprehensive understanding of the event threat and potential new threats. SureView Insider Threat's "policy wizard" offers simplified policy creation that allows users to specify what information to collect and what information not to collect to protect civil liberties and personal privacy. It also enables integration of collected data in a central place, such as a Security Information and Event Management (SIEM) system. The data can then be analyzed with other types of collected data to further improve security policies and procedures.

SureView Insider Threat makes it possible for employers to trust their employees and devices through verification. It compliments other security solutions and is necessary for bridging the gap that exists from a user's interaction at the end point to what is happening on the network. SureView Insider Threat also ensures other security tools are properly configured and functioning as advertised. The U.S. Government's increased focus on insider threats has prompted many companies to claim they have an insider threat solution. However, Raytheon is the only organization that has been developing insider threat and counterintelligence solutions from the ground up for over a decade.

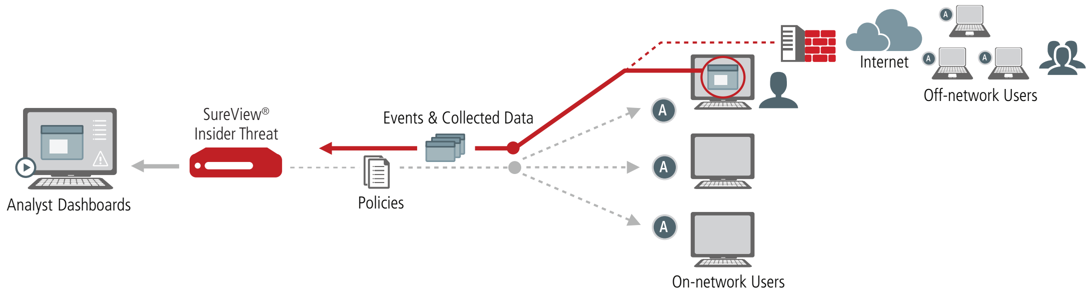
Accreditation

SureView Insider Threat has met the most rigorous and demanding security certification and accreditation criteria required by the Department of Defense.

Cover All Major Communication Channels

Cover the major user communication channels – for fixed and mobile users, including file systems, communication protocols and removable devices.

- Web
- IM
- Email
- File
- Removable media
- Printer
- Keyboard
- Clipboard
- Office
- Processes
- File discovery
- User events
- Registry
- Linux
- Terminal services
- Mobile workforce
- Pre-encryption/ post decryption
- Event logs
- Network collector
- Terminal services
- Hard drive anomalies
- Post script print job text collection



For further information contact:

Intelligence, Information and Services
Cyber Products
12950 Worldgate Drive, Suite 600
Herndon, Virginia
20170 USA
866.230.1307

www.raytheoncyber.com

Cleared for International Release. Internal Reference #IIS2013-091

Raytheon
Customer Success Is Our Mission