



## SureView™

### Cybersecurity and Information Assurance Technology



**Proactive monitoring and investigation tools to manage insider threats**

#### Key Features and Benefits

- An alternative to debilitating security technologies
- Measure the impact of new and existing threats and compliance in real-time
- Reduce dependency on technical expertise
- Monitor endpoint user and system activity
- DVR-like replay
- Full activity capture
- Privacy protection

Insider risk management is a continuous process of assessment, policy definition, risk mitigation, situation analysis and remediation of problems that occur. This is always a reactive process unless proactive methods are employed to monitor and track whether policies are followed.

Raytheon's SureView is a host-based insider risk management solution that proactively identifies and supports investigations of user violations so that organizations can proactively manage insider incidents.

#### SureView Overview

SureView provides point-of use auditing and monitoring of workstations throughout an enterprise. SureView enables the organization's stakeholders to defend against the insider threat, i.e., a potential compromise of confidentiality, integrity or availability of the organization's

systems or assets by a user who has legitimate access. SureView can effectively detect both unauthorized access to information and unauthorized transfer of information. SureView can be deployed for audits and investigations across a variety of 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 investigative stakeholders doing auditing and investigations.

#### Product Capabilities

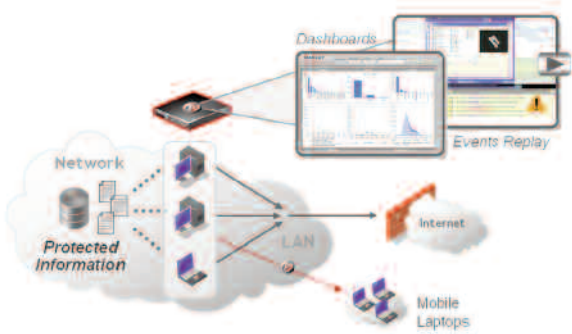
SureView allows the organization to manage insider threats using an integrated, enterprise-wide system rather than purchasing and maintaining a number of independent software applications to monitor user activity. To provide comprehensive coverage of corporate electronic

communications, SureView 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 Web sites visited. With video replay, man-hours can be saved by quickly determining the user's motivation and intent.

SureView can also prompt users to comment in real-time, automatically stopping actions such as copying to USB drives, and producing actionable information to enable conclusive issue resolution.

Start-up is easy with Raytheon's library of more than 200 pre-defined policies, which satisfy requirements for regulatory compliance and numerous other common use case scenarios.



Raytheon's SureView monitors network computers and laptop user activity

**Use sophisticated SureView policy architecture as an alternative to debilitating security technologies**

- Monitor and audit your enterprise
- Avoid poring through endless event logs
- Reduce prescribing tedious security settings

**Measure the impact of new and existing threats and compliance in real-time**

- Easily add SureView policies to measure frequency of threats
- Track trends and determine whether risks are being reduced
- Make informed decisions about security budget allocation based on measured trends

**Reduce dependency on technical expertise**

- Engage non-technical subject matter experts to resolve security issues that previously required very technical personnel
- Quickly determine root cause with full contextual DVR-like replay
- Discover leading indicators across the enterprise to determine further investigation

**Monitor endpoint user and system activity**

- Monitor fixed and mobile users, including activity that does not touch the network
- Cover major user communication channels, including access to file systems, email, chat, clipboard, Internet, printer, processes, services, applications and removable devices

**DVR-like replay**

- DVR-like replay of captured user activities
- Provides over-the-shoulder view of user activity
- Shows suspicious behavior in context with other activities

**Full activity capture**

- Unravel potentially evasive technologies, such as the use of encryption, the clipboard, screen capture and removable media that may nullify other security measures

**Certification standards**

- FIPS 140-2 compliant crypto algorithms
- DISA STIG tested

**Privacy protection**

- Product's role-based policies ensure that monitoring will be seen only by authorized individuals
- Pre-built policies detect the abuse of Personally Identifiable Information (PII)
- Two-factor authorization, dual-user authorization

Raytheon's SureView covers the major user communication channels for both fixed and mobile users. This includes file systems, communication protocols and removable devices.

- Web
- IM
- Email
- File
- Removable media
- Printer
- Keyboard
- Clipboard
- Office
- Process
- User events
- Terminal services
- Mobile workforce
- Pre-encryption/ post-decryption

**Protecting Information**

SureView provides a number of pre-defined policies that are based on Raytheon's broad experience in federal and commercial markets. Many scenarios common to the government customer have been pre-defined, such as protecting sensitive documents and personally identifiable information.

Customized policies can also be created to meet the customer's requirements. All SureView engineers possess TS/SCI clearances.

In addition to the numerous pre-defined policies, SureView also features an extensive ability to fingerprint your 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. Hence, typical detection methods require the entire document to be copied for detection, while

SureView can detect fractional movement from any part of a fingerprinted document.

SureView is a point-of-use discovery tool capable of capturing intentional and unintentional insider threats to your 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, by pushing the detection to the end nodes rather than attempting to intercept on overwhelmed network bandwidth.

Finally, SureView provides a concise user dashboard that prioritizes the reporting of events and data according to the requirements of the organization. This maximizes the monitoring capability while minimizing the human intervention required to manage and react to the alerts provided. SureView's unique replay capability can reconstruct an incident in complete detail, including activities leading up to and after the triggering event.

**Specifications**

- Hardened Linux-based appliance
- Dual Xeon processors
- Multiple gigabit interfaces
- Cluster enabled appliances for broad expansion
- Support for copper and optical networks
- Default storage starts at 1.6 TB
- Redundant power supplies

For further information contact:

**Intelligence and Information Systems**  
 2755 E. Cottonwood Parkway  
 Suite 600  
 Salt Lake City, Utah  
 84121 USA  
 801.733.1100  
 insiderthreat@raytheon.com

www.raytheon.com  
 Keyword: Oakley