SureView® Insider Threat

UNRIVALED VISIBILITY INTO USER BEHAVIOR TO PROTECT IP AND DETECT THREATS FROM WITHIN

FORCEPOINT
POWERED BY Raytheon

SureView® Insider Threat

UNRIVALED VISIBILITY INTO EARLY ACTIVITY ON USERS' COMPUTERS PREVENTS DATA THEFT AND LOSS BY HIJACKED SYSTEMS, ROGUE INSIDERS OR NEGLIGENT END USERS.

INTRODUCTION

SureView Insider Threat (SVIT) has been identifying and stopping threats from within for government and Fortune 100 customers for more than 15 years. With more than 1 million endpoints deployed, SVIT's proven solution protects some of the most sensitive organizations on the planet. One Fortune 100 retail client realized 60% ROI in the first year of deployment.

15

STOPPING INSIDER THREATS FOR MORE THAN 15 YEARS

1,000,000

OVER 1 MILLION ENDPOINTS PROTECTED

ROI: 60%

Payback: <16 months

SVIT gives you unrivaled visibility into computer users' early activity, helping you to stop data theft and loss by:

DETECTING

Detecting suspicious activity, whether accidental or intentional.

PREVENTING

Preventing a hijacked system, a rogue insider or just a user making a mistake, ensuring that your intellectual property is not compromised.

ESTABLISHING

Establishing a normal behavior' baseline, giving you early indications of a potential risk when a user begins to stray for their normal activity.

PROVIDING CONTEXT

Providing context into a user's behavior, aiding your investigation.

IDENTIFY

Automatically identify your riskiest users. An over-the-shoulder view enables you to put context around risky behavior. This lets you determine if the system was hijacked, the employee action was malicious, or if it was an accidental act.

Forcepoint SVIT Empowers Your Business

SVIT saves you time and effort by automatically scoring and prioritizing your riskiest users, reducing the need to dig through thousands of alerts. This frees your team to focus on high priority tasks and improves efficiencies. SVIT also provides the context and forensic evidence needed for undeniable attribution and chain of custody – simplifying investigations, prosecution, and compliance.

SVIT BENEFITS:

No other vendor combines all of these advantages to defend your data against the threats from within in a single product.

- Only Forcepoint SVIT offers DVR capture and playback on both Windows and Mac OS endpoints.
- Our Command Center provides a highly intuitive way to identify the riskiest users and quickly see patterns that can uncover broader risk.
- Forcepoint SVIT provides granular control over when to collect data and what to specifically gather to protect users' privacy.
- Only SVIT integrates with TRITON® AP-DATA to help you quickly drive to smarter remediation decisions after risky behavior is detected.

KEY FEATURES:

Forcepoint is the only vendor to provide these key insider threat defense features in a single product.

- Metadata collection and aggregation to baseline user and workgroup behaviors, enabling you to later automatically detect when a user strays into abnormal behavior.
- Integration with TRITON AP-DATA, providing the forensics capabilities you need to quickly drive to smarter remediation decisions after risky user behavior is detected.
- Alert aggregation quickly identifies the riskiest users.
- Video collection and playback helps expedite investigation, allowing for attribution as well as showing employee intent and is admissible in a court of law.

Unrivaled visibility into user behavior

SureView Insider Threat Capabilities

Built as an insider threat solution, SVIT is not an existing solution retrofitted to the problem – it's a unique and unrivaled security tool designed specifically to protect your data from malicious or accidental threats. SVIT's development was headed by a team of domain security experts who have spent their careers in information protection.

SVIT delivers these unmatched data protection capabilities:

- **Protects** against unintentional insider threats as well as malicious insider behavior.
- **Video replay** provides full behavioral context to rapidly discern malicious from benign actions, easily reviewed and understood by non-technical personnel – all while respecting employee privacy guidelines through customizable, business-driven policies.
- **Analytics** prioritizes users who have anomalous behavior and provides deep visibility into their actions, including past behaviors.
- **Integrated**, enterprise-wide system – no need to buy or maintain a number of independent software applications.
- **Distributed** architecture prevents performance impact.
- **Proven**, stable, lightweight agent.
- **Data collection** from multiple sources, including TRITON AP-DATA.
- **Detects** risky behavior even when users are off the corporate network.

SureView Insider Threat Components

ANALTYICAL USER BEHAVIOR RISK SCORING ENGINE

• Forcepoint gives you the visibility needed to have early warning signs that users have been hijacked, gone rogue, or are just making mistakes – before sensitive data gets breached or stolen.

• SVIT saves you time and effort by automatically scoring and prioritizing your riskiest users, reducing the need to dig through thousands of alerts.

• The SVIT Command Center provides a highly intuitive way to identify the riskiest users and quickly see patterns that can reveal broader risks.

• SVIT video capture and replay capability gives you unparalleled visibility into suspicious behaviors before they become problems (e.g., creating back doors, stockpiling data).

HOW SVIT GIVES YOU INSIDER THREAT PROTECTION

• Baselines both individual and organizational behavior across channels to understand what behavior is normal and expected.

• Searches for anomalies in an individual's behavior to detect potential insider threats (both intentional and unintentional).

• Provides a consolidated user risk score for each user on each day, as well as quickly highlighting 30 day risk trends.

• Simplifies the investigation process by prioritizing risky users.

Simplifies the investigation process by prioritizing risky users

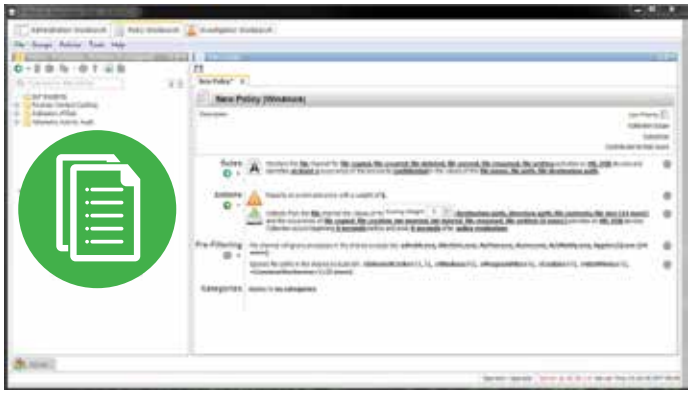
POLICY-DRIVEN IDENTIFICATION OF RISKY BEHAVIOR

• Customers can define specific behaviors that are known to be risky, based on a set or sequence of activities.

• These policies allow for detection of a wide range of activity monitoring from PII and HIPAA compliance requirements to IP protection and limited malware detection.

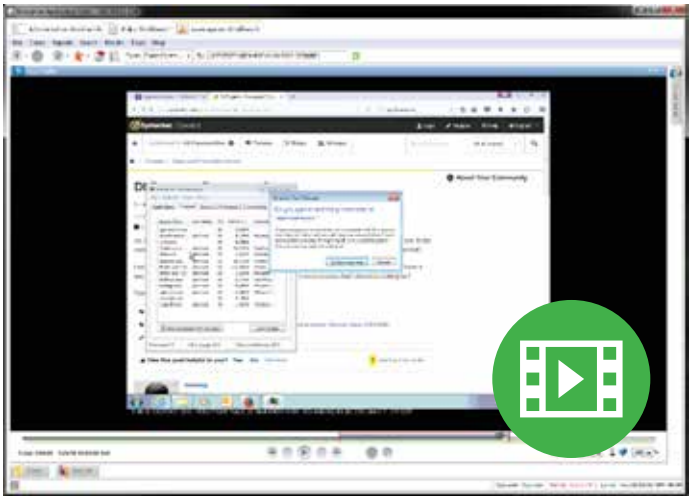
• These customer-specific policies weigh into the overall risk score.

• Customers can manually tune the weighting of these policies to adjust the level of their contribution to the overall risk score.



VISUALIZATION SHOWING RISK SCORE CONTRIBUTORS

• For each user on each day, an intuitive chart is generated allowing an investigator to quickly understand what types of activities caused them to receive a high risk score.



DVR-LIKE DESKTOP VIDEO REPLAY

• Screen shot captures and play back provide an over-the-shoulder view, giving you unparalleled visibility into suspicious behaviors before they become problems.

• Policies provide you with the context and the evidence needed to attribute an incident to a user and to determine if they have been hijacked, gone rogue, or are just making mistakes.

• Investigators can easily call the desktop video replay for high-risk users and view any suspicious activity, with user-attribution that is admissible in a court of law.

TIMELINE ACTIVITY REVIEW AND ADDITIONAL FORENSIC DETAILS

• The SVIT Command Center saves you time and effort by automatically scoring and prioritizing your riskiest users, reducing the need to dig through thousands of alerts.

• An easy drill down into the risky user and an expandable timeline, showing you the actual acts that the user is doing to that is making them a risky user.

• Record and playback gives you visibility into the user's intent and simplifies the investigation process.

• Provides you with the context and content around users' actions, helps with attribution and aides in the prosecution of malicious behavior.

To schedule a demo or for more information, visit www.forcepoint.com/contact.

Detect suspicious activity, whether accidental or intentional.

CONTACT
www.forcepoint.com/contact

[BROCHURE_SUREVIEW_INSIDER_THREAT_EN] 400011.062316

FORCEPOINT
POWERED BY Raytheon