FORCEPOINT
POWERED BY Raytheon

Datasheet

SureView® Insider Threat

USER BEHAVIOR ANALYTICS: STOP INSIDER THREATS BEFORE THEY BECOME A DISASTER WITH FULLY AUTOMATED VISIBILITY

FEATURES AND BENEFITS

- **Trusted mission partner** of government organizations and Fortune 100 companies since 2001
- **Behavioral analytics** discovers top riskiest users, and provides deep visibility into those behaviors, including past behaviors
- **Video replay** for full context to rapidly discern malicious from benign actions
- **Protects Personal Privacy** through customizable, business-driven policies
- **Data collection from multiple sources**, including TRITON® AP-DATA
- **Protects against unintentional insider threats** as well as malicious threats
- **Integrated, enterprise-wide system** rather than purchasing and maintaining a number of independent software applications
- **Unique** fingerprinting solution
- **Proven,** stable, lightweight Agent
- **Built as an Insider Threat solution** from the ground up

Historically, the term "insider threat" conjures up images of malicious employees creeping into dark offices, stealing company secrets in order to profit or create irreparable damage to the company. The truth is that this type of evil insider is rare, with instances of these types of threats occurring once in a decade or less. The real insider threat is the negligent employee A.K.A. the accidental threat. Negligent employees invite risk through uninformed, highly questionable behaviors. Via social media and email scams, adversaries target them, to con them into doing something that appears legitimate, but actually allows the adversary to slip "inside the gate" of the network. One-half of organizations view these staffers as their biggest threat.

UNINTENTIONAL INSIDERS: THE REAL INSIDER THREAT

A lack of awareness accounts for much of the negligent employee's behaviors, as 45 percent of workers receive no cybersecurity training on the job, according to CompTIA[1]. Nearly two-thirds depend upon business-intended devices for personal activities like shopping, banking and social media surfing. Virtually all of them connect their devices to public Wi-Fi networks, with seven out of ten calling up company-related data while doing so. And when USB storage drives are involved, the results can be frightening (See Figure 1).

1 https://www.comptia.org/resources/cyber-secure-a-look-at-employee-cybersecurity-habits-in-the-workplace

The Unintentional Insider Threat

- Three-of-five employees rely upon potentially insecure USB storage drives to transfer files among devices.
- Thirty-five percent have borrowed someone else's USB stick to transfer files.
- More than one-fifth would pick up a stick they found in public.
- An astonishing 84 percent of those who'd pick up a stick they found would plug it into one of their work devices.

Figure 1. Source: "Cyber Secure: The State of Employee Cybersecurity 2015," CompTIA

Clearly, traditional security tools – while still playing a key role in safeguarding systems – no longer suffice as a sole remedy. Organizations need to match technology with human oversight, paving the way for 24/7/365 visibility into how users behave, no matter when or where they're connecting to the network. Then, they have to prioritize each risk and launch remediation/mitigation measures.

SUREVIEW INSIDER THREAT: SEE THREATS BEFORE THEY BECOME DISASTERS

SureView Insider Threat identifies risky behaviors by baselining "normal" for each user, the organization then captures deviations from "normal" such as: a change in data access, working hours, email activity etc. These deviations are risk indicators that serve as warning signs leading up to a breach. The riskiest users are pinpointed with deep visibility provided into their behaviors.

SureView Insider Threat's integration and correlation with TRITON AP-DATA and multiple enterprise data sources provides enterprise-wide visibility into how users handle data, to detect both unintentional insider threats and malicious activity, that would otherwise go unnoticed. Combining enterprise-wide data sources with behavior analytics does the investigating for you — providing insight into activity that, on its own, may seem benign, but in context could result in a costly breach.

SureView Insider Threat was designed as an insider threat solution starting in 2001. It is not, like some technologies, a solution retrofitted to the problem. The SureView Insider Threat team are domain experts who have spent their careers in information protection. Whether the incident is accidental or deliberate, or somewhere in-between, SureView Insider Threat gives you complete visibility and quickly identifies the riskiest users in your organization, all while preserving employee privacy guidelines.

PRODUCT CAPABILITIES

The Command Center:
The command center provides analysts their organization's risk level at a glance: it displays the organization's overall 30-day risk trend and a summary of the day's riskiest users (Figure 2).

Video Replay:
Video replay provides complete, near-real-time context with an "over-the-shoulder" view of the end-user's workstation. A security analyst can create a case and easily share data and replay with non-technical management or security personnel.

Identifying the Threat:
SureView Insider Threat comes with pre-configured policies identified by Forcepoint™ experts who have been implementing Insider Threat Programs for Fortune 100 and Government agencies since 2001. These policies are ready to protect your organization against the insider threat the day it is deployed.

Protecting Civil Liberties:
SureView Insider Threat policies are easily customized and created using The Policy Workbench or "policy wizard" and allows users to specify what information to collect and what information not to collect to preserve civil liberties and personal privacy.

Unique Fingerprinting Capabilities: SureView Insider Threat features an extensive ability to fingerprint an organization's critical intellectual property or sensitive document library. Most 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 Insider Threat 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/

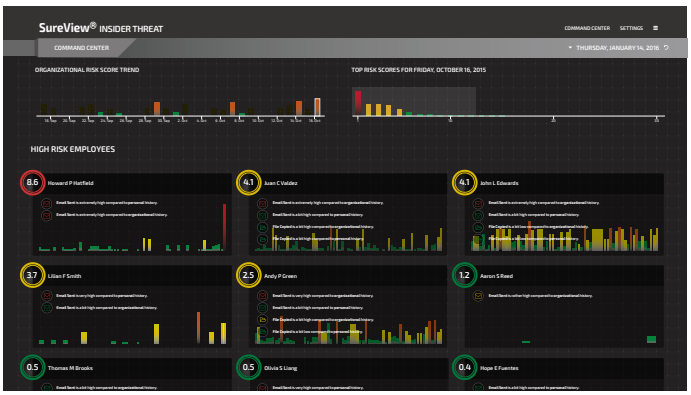

Figure 2. The Command Center - Organizations 30-Day Risk Trend

laptop level. This enables detection of abusive behaviors and capture of sensitive documents before encryption or deletion.

Light Footprint: A distributed architecture reduces the processing load required to monitor an entire organization.

Forcepoint SureView Insider Threat provides ongoing, automated visibility into accidental or malicious activity that otherwise goes unnoticed. It effectively consolidates and prioritizes security alerts sent from other systems and data sources, providing rich historical context and video replay. SureView Insider Threat acts as an "early warning system" to collect user data from all endpoints to pinpoint risky behavior. It records the activity for your review, giving you critical context and proof to stop threats before they become disasters.

KEY PROBLEMS SUREVIEW INSIDER THREAT SOLVES

Problem	Capabilities	Methods
Too many false positives	**Provides insight into:** "Who does what how often?" "What does normal behavior look like?" "Which activities appear to be unusual?"	**Metadata collection & aggregation**
Enterprise-wide visibility	**Enterprise-wide visibility** Provides comprehensive view of the enterprise	**Alert aggregation**
Lack of resources	**Investigates for You** Quickly identify which users have performed the riskiest activities	**Behavioral analytics**
Lack of context	**Context** Provides the ability to discern malicious from non-malicious acts	**Video collection**

Figure 3. Key Problems SureView Insider Threat Solves

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[DATASHEET_SUREVIEW_INSIDER_THREAT_EN] 100039.011416