

Over the last decade, organizations have focused on keeping external threats at bay, spending billions on intrusion detection systems, firewalls, anti-virus solutions, and other network security tools. But the threat from inside the organization is often far greater than from outside.

Network Security – from the Inside Out.

Your organization could be vulnerable to theft of proprietary information, inappropriate sharing of private customer data, vendor collusion, regulatory and compliance violations, breaches of confidentiality, and insider trading. A complete Insider Threat Management system will protect your organization from insider misuse of your intellectual property.

Point-of-use monitoring and easy-to-use discovery tools capture intentional and unintentional insider threats to your organization and allow you to easily monitor and manage user activity without being overwhelmed with information. Oakley Networks' SureView is a secure system that provides enterprise-wide deployment of client-based software to one of the most valuable parts of your network: employee workstations and laptops.

SureView provides comprehensive monitoring combined with intelligent filtering and analysis of a user's activity, even if encrypted, because collecting at the point of use means activity is captured pre-encryption or post-decryption. Monitored insider communications include the Web, email and webmail, instant messaging, files, removable media, the Clipboard, and printers. Data gathered by SureView can be viewed in "TiVo-like" real-time Replay in Context that displays everything the user did, including keys typed, mouse movements, documents opened and modified, and websites visited.

- **Protect your organization's IP** in and out of the office. SureView can monitor your off-site employees who use laptops.
- **Enable your employees to use secure channels** and encryption because collection at the point of use allows the Agent to collect data pre-encryption or post-decryption.
- **Protect your employees** against unintentional policy and regulatory violations.
- **Quickly deploy client-based software** using your existing software asset management program.
- **Monitor thousands of employees at once** and immediately find your worst offender with easy-to-use analytic discovery tools.

Enterprise-Wide Communications Monitoring



Web Browsers



Email & Webmail



Instant Messaging & Chat



File Migration & Modification



Clipboard Activity



Keyboard Activity



Printer Activity



System & User Information

► The SureView System

The SureView product components described below are responsible for the generation, collection, transfer, and replay of all data that flows through the system.

Server

The Server is a hardened 1U appliance that is responsible for recording user activity collected and transported by the Agent. The Server also hosts the web-based Operator Interface. Operators can monitor and remotely manage Agents and Policies by accessing any Internet Explorer browser on the same network. Servers can be clustered together to support the monitoring of thousands of employees.

Users

Users are managed through the Operator Interface by placing them within the group structure. Users can be assigned to one or more groups of Policies. The Agent software can be configured to take the user-specific Policies into account when it decides what the Effective Policy Configuration is for that User-Agent pair.

Agents on Monitored Workstations

The tamper-resistant Agent software runs as a process on monitored workstations. The process name and installation location of the Agent are configurable at the time the Agent is created. Operators can create reusable Agents that can be installed using existing asset management software, such as SMS or Altiris. The Agent actively responds to user activity only when an operator-specified Policy is violated.

Policies

A Policy tells the Agent when and how to respond to user activity. Possible responses to policy violations include the following:

- Collect data and send it to the Server for operator Replay and analysis
- Collect data but cache it for later retrieval
- Block the mount of removable media
- Temporarily lock the user out of their workstation
- Temporarily lock the user out of network resources
- Shut down the user's workstation
- Generate an alert

Alerts & Replay in Context™

When an Agent collects data and sends it to the Server (through an encrypted channel), an Alert will be generated, letting operators know which policy was violated. User activity is viewed using our patent-pending Replay in Context.

