



INSIDER THREAT MANAGEMENT:

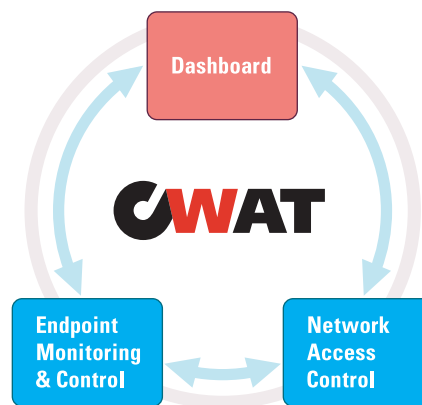
ENFORCE REGULATORY COMPLIANCE AND SAFEGUARD NON-PUBLIC INFORMATION.

Dozens of major enterprises and government agencies have lost confidential information and customer private data through accidents and theft. As The Wall Street Journal warned its readers: *"The biggest threats to information security often don't come from hackers. They come from a company's own employees."* ["The Dangers Within", February 13, 2006, page R1]. Examples of corporate leakage of sensitive information range from stolen laptops to inadvertent email attachments and theft on portable USB drives.

Managing the Insider Threat involves more than company policies. It requires an integrated security software suite able to prevent the unauthorized disclosure of confidential company information and private personal data by employees, contractors, and others with access to the company's IT network. Over 400 leading enterprises and government agencies trust CWAT to protect their organizations from the Insider Threat. CWAT provides a much welcomed addition to compliance monitoring and enforcement for Sarbanes-Oxley, HIPAA, FISMA and Gramm-Leach-Bliley. CWAT (Cyber-crime Warning Alert Termination) detects & stops in real time the unauthorized transfer of digital assets, to protect intellectual property and non-public private information.

CWAT comprises three integrated elements:

- Endpoint (Workstation) Monitoring and Control
- Server-based Network Access Control
- Central Management Console/Dashboard to create, monitor and audit policies



KEY FEATURES

The CWAT software is unobtrusive, requires limited network bandwidth, and does not affect the daily work habits of business staff. It has robust policy-management capabilities which are time efficient for security administrators to manage in a central dashboard.

Endpoint Monitoring and Control

The CWAT host agent safeguards data on individual PCs, both desktops and laptops. The host agent, termed the Operation Defense Controller (OPDC), provides multi-layered security at the file, application and OS levels.

The OPDC provides the following functions:

- Encrypts sensitive files, enforces passwords with expiration dates, and prevents use of Safe Mode to bypass security, to deliver comprehensive laptop anti-theft protection.
- Provides encryption and rights management services (eDRM) for enterprise document security.
- Protects application operations (install, uninstall, start, stop, etc. by application name and by group of applications)
- Protects file operations activities if not authorized, such as creating a PDF, renaming or deleting a file, uploading to a website, etc.
- Prevents sensitive files from being copied to USB cards and other external devices including floppy drives, CD-ROMs and MP3 devices. (Note: users can continue to use removable media; CWAT blocks the transfer of only the sensitive information)

- Scans emails, web mails, file uploads for keywords and FTP for data transfers, to provide robust content monitoring and filtering (CMF).
- Identifies anomalies in user behavior: tracks user activity and baselines against typical behavior.
- Monitors printing and disables print screen of nonpublic information.
- Continues to monitor and enforce policies even when computers are disconnected from the network.
- Collects audit logs with a screen shot as evidence of illegal activity.
- Monitors PC On/Off and Logon/Logoff.

Protective Features

The CWAT Encryption function enables encryption of the entire hard drive, content folders or specific files. CWAT provides three kinds of keys depending on who shares the keys: Group key, public key and private key.

The CWAT ICMP Active Detection function monitors unregistered terminals by sending ICMP packets, to verify correct operations of endpoints.

The CWAT eMail Control function prevents malicious and accidental email of sensitive information. Included in the eMail Control function is protection from web mail, web-based FTP, and other file-sharing services. It prevents, in real-time, non-public data or confidential proprietary information from being disclosed by e-mail or on the Web.

With the CWAT Printout Control function, a digital watermark identifies printing time, date and the source network address.

The CWAT Anti-Theft function for laptop computers enforces password control in normal and safe modes. This function ensures that use of laptop PC disconnected from the network requires a password generated on the OM. The password will be generated by the OM by combining the user name, domain name of the laptop PC, and the organization code. By specifying the validity date and time, it is possible to specify a period for the password to be valid and prevent unauthorized repetitive use.

Network Access Control

CWAT provides Network Access Control security through a Segment Defense Controller (SDC) or an Unknown terminal Defense Controller (UDC). The SDC or UDC locks down the endpoints of the network to prevent unregistered PCs from gaining network access, with

protection against wired Ethernet and WiFi wireless access. Furthermore, the SDC/UDC prevents unauthorized access from handheld data devices such as Smartphones or PDAs.

The SDC/UDC fulfills the following functions:

- Prevents unregistered PCs and handheld data devices from connecting to the network.
- Secures network endpoints.
- Detects missing terminals from the network.
- Enforces network access control policies based on:
 - IP & MAC address
 - TCP & UDP protocol
 - Packet information
- In addition to IP and MAC address controls, SDC/UDC detects and denies access to unregistered PC's by packet sniffing and ICMP polling.

Dashboard

The dashboard provides powerful policy-setting and reporting capabilities. The OM Standard Edition provides policy setting for up to 100 agents. The OM Enterprise Edition scales from a single Host to 10,000 or more.

The software administrator can define groups of users - such as executive management, accounting, legal, operations, etc. - and apply standardized policies appropriate to each group. In the event of a policy breach, the security administrator receives not only an alert/audit log but also a screen shot of the user activity, to provide a quick and authoritative understanding of the activity that generated the CWAT alert.

The OM Dashboard enables the following:

- Centralized monitoring
- Policy setting by nodes and users
- Problem analysis
- Audit logs
- Regulatory Compliance reporting

CWAT enables administrators to grant one-time temporary exceptions. For example, a user that has a business trip and needs to access critical files on a Sunday prior to a flight the following morning can be granted one-time access without disabling the standard policy.

SEA™

SOFTWARE ENGINEERING OF AMERICA®

Phone: 516.328.7000 • Fax: 516.354.4015 • www.seasoft.com

All trademarks & copyrights are the property of their respective owners.