



# **CWAT Insider Threat Management**

## **WHITEPAPER/TECHNICAL REVIEW**

SEPTEMBER 2006

***CYBER-CRIME WARNING, ALERT & TERMINATION***

***/COMPREHENSIVE INSIDER THREAT FOCUSED  
SOFTWARE SOLUTION PROVIDING INFORMATION  
LEAKS AVOIDANCE IN REAL-TIME***

***/ UNIQUE ENDPOINT MONITORING AND CONTROL  
SYSTEM, NETWORK ACCESS CONTROL AND  
CENTRAL MANAGEMENT FOR***

***PREVENTING CORPORATE OR GOVERNMENT  
INSIDERS TO EXTRACT CONFIDENTIAL  
INFORMATION AND PROTECT INTELLECTUAL  
PROPERTY AND NON-PUBLIC PRIVATE  
INFORMATION***

***/ SUSPICIOUS BEHAVIOR MONITORING AND  
ANALYSIS***

## Table of Contents

1. Product	3
1.1. Executive Overview	3
1.2. Key Functions	5
1.3. Central Management of Host Based Capabilities	8 9
1.4. Recommended Architecture and Deployment Strategy	10
1.5. Technical Specifications	
2. Feasibility Assessment	12
2.1. Installation	12
2.2. Network Loading	12
3. Compliance with Technical Requirements	14

## 1. Product

### 1.1.Executive Overview

Managing the Insider Threat involves more than company policies, law enforcement or a point-product security software program. It requires an integrated security software solution, suitable to prevent the unauthorized disclosure of confidential Corporate and Government information and private personal data by employees, contractors, and others with access to the organizations IT network (i.e. authorized users who conduct malicious activity within the network or on a system).

The threats are real and losses have already been greater than many imagined. Besides, companies, regardless of industry, are becoming subject to a number of regulations that vary by industry and type of corporate entity. Not complying with these regulations will be just ruinous for the corporate U.S. and multi-national world. To cite the most important ones:

- FISMA – U.S. government must comply with the Federal Information Security Management Act, as well as to other strict regulations like ITAR – International Traffic in Arms Regulations including control and monitoring of the so-called “dual purpose” technologies and goods.
- Sarbanes-Oxley Act of 2002, which specifies that business information and process must be strictly controlled and that chief executives are accountable for missing or leaked critical information.
- HIPAA regulation for the healthcare industry from April 21, 2005 requires protection of patient privacy information through a set of strict security rules.
- SB1386 California Data Breach Notification Law, which requires any business or government agency doing business in the state to notify California residents when personal information is exposed.
- AB1950 which requires businesses that store or manage “private” information of California residents to provide “reasonable” security for that data.
- GLBA - the Gramm-Leach-Bliley Act, which addresses customer privacy in the financial services industry sector.
- DPA – the United Kingdom’s Data Protection Act; PIPEDA – Canada’s Personal Information Protection and Electronic Documents Act; EUPD –

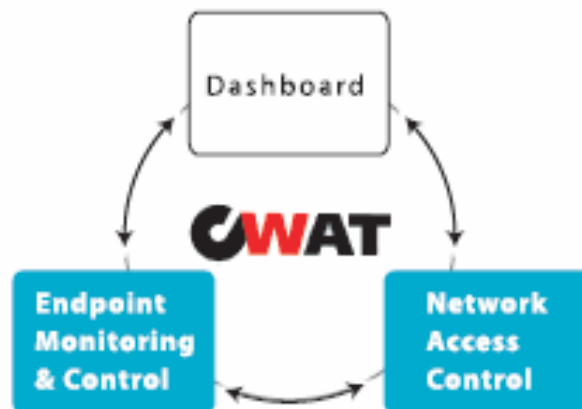
the European Union Privacy Directive are just other multi-national examples of global regulations that companies must consider.

Our approach emphasizes compatibility with other elements of the IT security architecture including Intrusion Prevention and Network Firewalls. For additional application integration, CWAT ships with a Service Oriented Architecture (SOA).

Cyber-crime Warning Alert Termination – CWAT – detects and stops in real time the unauthorized transfer of digital assets, to protect intellectual property and non-public private information. CWAT prevents the damaging threat posed by those who have access to information systems and networks and operate from within, regardless of whether or not this access was acquired through legal channels.

CWAT is a Software Application comprised of three integrated elements: Endpoint Monitoring and Control via a Host Agent, server-based Network Access Control, and a central management console/Dashboard which provides the centralized monitoring and allows setting and auditing of policies, problem analysis and regulatory compliance reporting.

CWAT monitors all terminals including laptop computers and even missing terminals that are disconnected from networks. CWAT saves the time and cost of installing and setting each solution for a single purpose, involves simple management and operation, and provides for reliable digital asset protection.



The primary benefits of CWAT include;

- Monitors file upload/download and email
- May be operated in either a stealth or visible mode
- Creates screen captures that are usable as forensic evidence
- Artificial intelligence engine capable of profiling user behaviors
- Customizable alarm generation for three separate levels of notification
- Creates, maintains, and archives customizable audit logs for all activities
- Monitors removable/writable media such as DVD, CD, USB, MO, IDE, FD
- Scalable up to 12,000 Hosts (PCs) with minimal impact on Network operations
- CWAT operates in a controlled environment with access only through the dashboard
- Hosts (PC) will enforce a policy even if the terminal is disconnected from the network
- Monitors PCI, USB, RS-232C, Printer port, IEEE1394, SCSI, IDE, LAN I/F, Modem, Infrared light/Bluetooth

## **1.2.Key Functions**

**CWAT is a total software solution** that is unobtrusive, requires limited network bandwidth, and does not affect the daily work habits of business staff. It has robust policy-management capabilities that can be managed by existing security administrators from a central dashboard.

### **Endpoint Monitoring and Control (Host Agent)**

The CWAT host agent safeguards data on individual PCs, both desktop 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, webmails, 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 (for example, a Mon-Friday 9-5 employee logging in on a Sunday).
- Monitors printing and disables print screen of nonpublic information.
- Provides watermarking of documents to show which PC and which printer was used.
- 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 individual content folders, or individual content files. CWAT AT provides three kinds of keys depending on who shares the keys: Group key, individual 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 webmails, web-based FTP, and other file-sharing services. It prevents, in real-time, non-public data or confidential proprietary information from being disclosed by eMail 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.

### **Kernel mode monitoring and user mode monitoring -**

CWAT monitors user operations at various points such as “file operation”, “printout”, “external devices”, “application”, ”logon”, ”power on”, ”mail use”, “Web use”, “encryption”, “unregistered terminals”, “network”, etc.

Two types of client operation monitoring are provided;

- Kernel mode monitoring using the device driver
- User mode monitoring at the application level and/or Win32 function level.

### **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 polices 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:

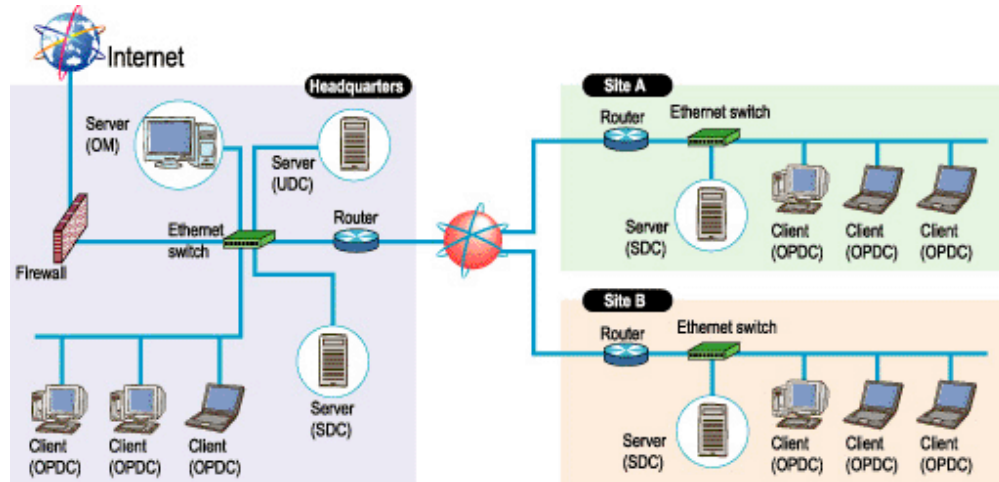
- Centralized monitoring
- Policy setting by nodes and users
- Problem analysis
- Audit logs
- Regulatory Compliance reporting

CWAT enables administrators to grant one-time 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.

### **1.3. Central Management of Host Based Capabilities**

After configuration of the entire CWAT system, including registering all the users/nodes and after defining and tuning up the policies settings at the central manager (OM), the host agents (SDC, UDC, and OPDC) will receive this configurations from the OM (we call this process "delivery of the configurations/policies"), and then the agents will individually enforce these configurations/policies.

## 1.4.Recommended Architecture and Deployment Strategy



In large organizations, a spiral design and installation approach provides the highest degree of assured success with minimum impact on organizational operations. Initially, stake holder meetings are held to define the company's security policy for data, storages, users, terminals, and operations. With this information, a site survey is conducted to investigate the network structure, hardware specifications of the terminals, and applications (current and planned) installed on the terminals. Once a complete assessment has been made, a project plan is developed and agreed to which defines the installation phases, in a manner consistent with the existing security policy and the operating environment.

Upon approval of the installation plan, a pilot phase is implemented to install the CWAT application in a limited environment within the organization. This pilot period provides the opportunity to test interfaces, and ensure business sensitive applications and data are not affected. Based in the results of the pilot, any needed modifications are made to the installation plan and/or security policies and the initial installation is extended to additional terminals/groups as defined by the installation plan.

## **1.5. Technical Specifications**

### **System Requirements**

- Server CPU/RAM: Minimum Intel Pentium IV 2 GHz or greater / 1 GB or greater
- Dashboard/OM Display: 1280 x 1024 resolution or greater
- Windows Client Access License ("Windows CAL"). Windows CAL is required for a each client accessing the Server OS
- SQL Server Client Access License ("SQL Server CAL")

### **Operating Systems**

- Microsoft Windows 2000/2003 Server (SDC, UDC and OM)
- RedHat Enterprise Linux 3 WS (SDC and UDC)
- TurboLinux 8 Server (SDC and UDC)
- Microsoft Internet Explorer High Encryption Pack or IE version 5.5 or higher

### **Agent Platforms**

- Microsoft Windows XP and Windows 2000

### **Database**

- Microsoft SQL Server

### **Scalability**

The central manager, OM can manage and collect information up to 12,000 client PC's. The network monitoring module SDC/UDC has capability to relay the configurations/policies to each terminal (OPDC), thus reducing network traffic to the central management console (OM).

### **Testing and Certification, and IPv6 compatibility**

Testing and certification in accordance with the Common Criteria for Information Technology (IT) Security Evaluation and the Cryptographic Module Validation Program (CMVP), as well as IPv6 compatibility testing are ongoing and are expected to be complete in 2006

### **Software Modules**

- Available either by Module or in a Fully Integrated Package
- Dashboard / Organization Monitor (OM) Enterprise Edition and Standard Edition, installed on a dedicated server
- Operation Defense Controller Pro (OPDC Pro), software agents on mobile and desktop PCs
- Segment Defense Controller (SDC), installed on a dedicated server
- Unknown Terminal Defense Controller (UDC), installed on a dedicated server
- CWAT Encryption Option\*, installed on each PC
- ICMP Active Dedication, installed on each PC
- CWAT eMail Control Option, installed on each PC
- CWAT Printout Control and Watermarking Option, installed on each PC
- CWAT Anti-Theft Option, installed on each PC

\*Included in OPDC Pro together with eDRM functions

### **Software Security Assurance Practices**

The product cycle of CWAT complies with the Information Security Management System (ISMS) standard.

## 2. Feasibility Assessment

### 2.1. Installation and Support Requirements

CWAT is capable of being installed on 12,000 machines simultaneously with no operational impact or performance degradation. CWAT includes separate network and PC monitoring components, which allows for real-time detection and immediate automatic response by each component to data extrusion actions. Because each component has its own detection and response capabilities, and because the system maintains monitoring logs that provide proof of data extrusion actions, they place no burden on network operating resources. Once installed, the software requires minimal additional support other than routine administrator functions and report monitoring.

### 2.2. Network Loading

Centralized monitoring and control components provide for centralized management of data extrusion prevention policies, and optimal time distribution to the separate monitoring components facilitates operations management. Data extrusion prevention policies are stored on the PC along with the monitoring component, which provides the same detection and automatic response capabilities when PCs are taken off the network as when they are on the network. An artificial intelligence engine studies and learns normal PC operation patterns so it can detect abnormal behavior associated with operations and data extrusion attempts that would not be detected by organization-specific policy settings.

There are three major files to be communicated between the central manager and the agent;

(1) Security policies and various configurations configured on the server which will be deployed to the agent. Configuration communications between the central managers are limited to those required at initial deployment, and then only when policies or configurations are modified. After the initial deployment, only updated policies will be sent to the agent to minimize the network load. The file size is dependant on the number and size of policies created and the number of registered nodes and users on the server. As an example;

1 policy = 1-5KB

1 node = approx. 2KB

1 user = approx. 1 KB

(2) Alert logs to be sent to the server when a policy violation is detected by the agent. Policy violations are communicated whenever a policy violation occurs.  
1 alert log = 3KB average. (1KB–8KB)

(3) Audit logs accumulated on the agent to be collected to the log storage server.  
Routine communications are made at the interval specified at the log storage server.  
Audit log on a PC/day = 1MB-10MB

### 3. Compliance with Technical Requirements

CWAT has been designed as a total enterprise solution to detect, report and prevent the threats imposed by insider threats. To meet the typical requirements defined by organizations, the following table provides a side-by-side comparison of technical requirements and CWAT capabilities.

Requirement	CWAT Capabilities
The tool should operate in a controlled environment with access restrictions applied to the data gathered, the tools operation, and the tool's software elements. Some of the features may include the ability to ensure Confidentiality and Integrity of the software elements through self-protection mechanisms and access controls to limit the users to an identifiable select group. Additionally, the tool should protect the gathered information from unauthorized access and control its availability to select groups. All communications should be encrypted.	CWAT assures and operates in a controlled environment with access only through the dashboard - the central management monitoring point called Organization Monitor, or OM. Operation of the product may be chosen to be stealth or visible. Confidentiality and integrity is assured through self-protection capabilities and through policy setting. Audit logs collected and sent to the dashboard (OM) are encrypted.
The tool should be scalable to the target community with a deployment, management, and information gathering capability managed from a single manager.	CWAT is scalable solution and one OM can manage and collect information from up to 12000 hosts (PCs).
The collected data should induce both host and user information. The information may include descriptive data such as: local/network account users and groups; operating systems; time reference; user ID; and the specific type of activity and the user's actions during the monitored period.	CWAT alert logs include host names, IP addresses, MAC addresses, and logon user names. The information includes local/network account users and groups, time reference, user ID, file operations, application operations, used external/media devices, and internet access. For example, in case of unauthorized copy of data to a USB drive, identified will be the process name, file name, device name, device type, etc.

Requirement	CWAT Capabilities
<p>The tool should provide for self-preservation to include a capability to self-report, to self or operator restart/reinstall for all portions of the system.</p>	<p>CWAT provides a capability to self-report (to show descriptive error messages). It has the capability to work independently; with or without operation with the OM. The Host agent will enforce a policy even if the terminal is disconnected from the network.</p>
<p>The tool should create, maintain, and archive customizable audit logs for all activities to include user, network, system, and tool actions. Typical collected data includes elements such as: user ID, type of activity, timestamp, unique device ID, process ID, thread ID, and workstation ID.</p>	<p>CWAT creates, maintains, and archives customizable audit logs for all activities to include user, network, system, and tool actions. The logs consists of (1) alert logs, which describe policy violations, (2) audit logs, which describe daily activities, and (3) system logs, which describe CWAT actions. The alert and audit logs include user ID, type of activity, time stamp, unique device ID, process ID, and workstation ID.</p>
<p>The tool should provide for customizable alarm generation and notification to the operator.</p>	<p>CWAT provides for customizable alarm generation to let the administrator define three levels of urgency and notification to the operator by executing other programs or sending email to specified addresses when a policy violation occurs and if the operator is not in front of the OM monitor.</p>
<p>User analysis is expected to be based on configurable thresholds, indicators, and pre-defined templates of user-based anomalies and create subject behavior profiles using defined behavior patterns.</p>	<p>The user analysis is based on comparing the new event with statistics of the accumulated past events and grading it. CWAT's artificial intelligence engine profiles the user behaviors by checking power on/off, application operations (start, exit, install), file operations (print, write, update, rename, copy), external device connections , e-mail activities, and web activities.</p>
<p>The tool should provide for host machine screen captures and replay those screen captures in a video or movie format.</p>	<p>CWAT provides for host machine screen captures whenever a policy violation occurs on the host; the format is convertible to a video or movie format.</p>

Requirement	CWAT Capabilities
For follow-on investigation purposes the tool should have the capability to capture, via industry approved methods, forensic data.	The screen captures at time of the occurrence of the illegal operation and the information from the logs can be used as forensic evidence.
The tools should provide conversion of collected user data into actionable information on specific user activities.	CWAT provides tools to collect host activity logs, and export the logs to log analysis tools and will provide graphs, charts, etc.
There should be an operator-friendly display method that facilitates the decision process, provides real-time actionable information, alerts on behavior activities, and controls the interaction (refresh rate, bandwidth, etc.) between all components.	The Console (OM) is the central display and interaction point for the gathered data; the alerts indicating policy violations are sent by the Host (OPDC) in each terminal, system configurations are done at the Console (OM), and audit logs are collected at the Console (OM). The Console (OM) reflects the decision process and facilitates it by showing detailed policy setting screens. The alerts sent by the Host (OPDC) to the Console (OM) provide real-time actionable information, such as sending message to the terminal, freezing the terminal, or forcing out the user from the terminal.
Information gathering and assessment capability should include gathering, displaying, and alerting the operator based on parameters and templates that consist of both pre-defined and operator-configured actions.	The Console (OM) gathers, displays, and alerts the operator based on parameters, which are set in the Console (OM) at the CWAT console screen. Pre-defined actions are taken at the Host (OPDC) side and operator-configured actions are taken at The Console (OM).
The tool should correlate and normalize the gathered data, allowing attribution of activities to specific users.	The Console (OM) sorts the gathered data, such as alert and audit logs, allowing attribution of activities to specific users.
The tool should make available operator configured, filtered, decision information for electronic interaction (i.e. data mining and keyword searches), electronic exchange (import/export) through industry standards (CSV, OBDC, XML, etc.), as well as through customized and template reports and alerts.	The Console (OM) makes available operator configured, filtered, decision information for electronic interaction, such as sorting, electronic exchange (import/export) through industry standards (CSV and XML), as well as providing an exporter for customized reports and alerts. Additional specific templates can be easily defined.

Requirement	CWAT Capabilities
The tools should be capable of supporting a large number of operating systems in government and industry.	CWAT's Host agent (OPDC) can be installed on Windows 2000, Windows XP, Windows 2003, and Windows NT4 (SP6a) to monitor and control the users behaviors. For the clients with the other operating systems, CWAT network monitoring module (SDC) monitors and controls network packets.
The tool should be compatible with and not interfere with other approved CND tools (i.e. Anti-Virus, Anti-Spyware, and Host-Based Security System (HBSS)).	CWAT is compatible with and do not interfere with other approved CND tools, and updates are continuously developed to add compatibility with other tools.
The tool should identify and associate the data with the user account information.	CWAT identifies and associates the data with the user account information by registering the monitored users on the Console (OM) and delivering the information to the Host (OPDC). Also, CWAT supports importing Windows Active Directory users to CWAT user account information.
The operational characteristics of the tool should include the ability to install and operate without the user's knowledge or being flagged by existing host-based CND tools (i.e. Anti-Virus, Anti-Spyware, and Host-Based Security System (HBSS)). At a minimum, it must “hide” indications of its presence from the user.	CWAT's Host (OPDC) has operational characteristics including the ability to install and operate without the user's knowledge or being flagged by existing host-based CND tools by using the capability of adjustments to such tools. CWAT silent installation enables the organization to install the host agent without letting the user know. CWAT's Host (OPDC) also can hide its presence (the process, program files, or registry keys) from the user and protect itself from being stopped or uninstalled.
The tool’s operational impact to the users system, in terms of input-output performance, system usability, and functionality, must be negligible.	CWAT's operational impact to the users system, in terms of input-output performance, system usability, and functionality, is negligible.
Information and data must be protected and preserved using industry standard and business best practices to ensure the security and traceability of the user's actions.	CWAT protects and preserves information and data ensuring the security and traceability of user's actions by preventing policy violations and providing alert/audit logs.

Requirement

CWAT Capabilities

The tool should monitor and report all available system data on software and hardware activities associated with system configuration changes, installation, modification, and removal.

The host sensor (OPDC) monitors and reports all available system data on software and hardware activities associated with system configuration changes, application installation, and application removal; CWAT monitors changes such as devices added as well as software that is installed/uninstalled.

The tool should gather user account data that identifies and tracks specific user's actions. The type of data includes local user account modification information, user name, and the user's activities.

The host sensor (OPDC) gathers user account data that identifies and tracks specific user's actions, such as policy violations. The type of data includes local current user account, user name, and the user's activities.

The tool should capture and report on the underlying Operating System actions associated with inherent features such as cut/copy and paste, drag-and-drop, and Command Line sessions

The host sensor (OPDC) is capable of logging the activities on OS as audit logs. Regarding the Command line session, execution of the Command Prompt window can be monitored.

For all web and Internet connections, the tool should be capable if gathering data, and replaying the activities, for potential misuse through mobile code, such as Java and ActiveX and web browser window actions. The collected data will be sufficient to rebuild the session to include the associated URL of any visited web page(s).

The network sensor (SDC) gathers data and is capable of tracking the network activities. The host sensor (OPDC) gathers data including the URLs according to the Web access policies.

The tool should be capable of analyzing encrypted sessions before encryption or after decryption.

While the CWAT network sensor (SDC) does not analyze encrypted sessions, the host sensor (OPDC) analyzes the data before being sent even if encrypted.

The tool should be able to distinguish and capture traffic associated with numerous data on services, ports, and protocol use. Some examples are Voice-Over-IP, TLS, SSL, Rlogin, Xwindows, NNTP exchanges, SNMP exchanges, DNS exchanges, RPC Peer-To-Peer, IMAP, POP, SMTP exchanges, IRC sessions, Instant Messaging, Telnet and FTP.

CWAT network monitoring function provided by SDC supports TCP, UDP and ICMP. It monitors network traffic according to the port numbers specified, the range of IP address (from/to), or keywords (for plain text message only).

Requirement

CWAT Capabilities

The tool should be able to capture the use of removable, writeable media, regardless of the Operating System format. Additionally that information will be transferred to a repository (log) and contain specific information associating the media with the information placed on or removed from that media.

CWAT's removable device policy monitors removable/writable media such as DVD, CD, USB, MO, IDE, FD, and everything not listed here will be monitored as others. Use of these devices will be logged with device name, device type, process name, file name, user name, IP address, and location.

The tool should be able to capture the transmission of files and messages through network connections. The network connections, at a minimum, include dial-up modems, Ethernet, and wireless.

CWAT monitors file upload as well as outgoing emails on the network connections, such as Ethernet, wireless, and dial-up modems.

For any file operation the tool should record associated file attributes and user actions.

CWAT records Time, IP address, User name, Location of activity performed, Process name, File name, etc.

The tool should be able to capture the use of detachable devices such as, fire-wire (IEEE 1394) devices (e.g. PDA, printers, etc.), infrared devices, EVDO, WiFi, Bluetooth, parallel port devices, serial port devices, and USB media and devices (e.g. thumb drives, PDA, digital camera, MP3 players).

CWAT can monitor the detachable device connection by the category of PCI, USB, RS-232C, Printer port, IEEE1394, SCSI, IDE, LAN I/F, Modem, Infrared light/Bluetooth. Also any other detachable devices can be captured.

The tool should monitor and capture actions associated with the use of input/output devices commonly attached to hosts (i.e. keyboard strokes and mouse movements).

CWAT monitors the specified keyboard strokes, and execution of executable files by use of a mouse.

The tools should be able to monitor printer activity to include such information as Printer Name, Job ID, printer location, printed document name, source machine information and printed data information, such as text and graphics.

CWAT monitors printer activity to include connections, use for specific files, printed time, host name used for printing, IP address of the terminal used for printing, MAC address of the terminal used for printing, logon user name, domain name, Printer Name, printed document names, and printed file size.