

observe *it*

people audit

ObserveIT User Activity Monitoring software meets the complex compliance and security challenges related to user activity auditing.

ObserveIT acts like a security camera on your servers, generating audit logs and video recording of every action the user performs. ObserveIT captures all activity, even for applications that do not produce their own internal logs. Every action performed by remote vendors, developers, sysadmins and business users is tied to a video recording, providing bulletproof forensic evidence.

ObserveIT is the ideal solution for 3rd Party Vendor Monitoring, and PCI/HIPAA/SOX/ISO Compliance Accountability.

ObserveIT Highlights

Filling the gap - Auto-generation of logs for apps that don't have their own logs!

Log clarity - Human-readable logs instead of technical system logs

Video replay - Each log entry is tied to a video that replays the user actions

Complete coverage - All apps, all users, all protocols, Win/Unix/Linux, remote/local, servers/desktops



What does ObserveIT record

- Login to application
- Delete file
- Change password
- Start SAP transaction
- View Customer Detail page in CRM
- Open specific URL
- Access shared folder
- Edit system files
- Change OS settings
- Send Email
- Run a query on SQL Server or Oracle Database
- Download file from the internet
- Capture a printscreen image
- Send files to FTP Server
- Open Visual Studio to change source code
- and more...

See exactly what users are doing!

Market Challenges

No silver bullet for PCI compliance
In 2010, the PCI Security Standards Council released new versions of the three standards we manage: PCI DSS, PTS and PA DSS... As we enter this critical implementation phase of our security journey, there are a few items I'd like you to keep in mind: Technology is just a part of the solution.
As reported in SC

Source code stolen from U.S. software company via India branch
Software vendor Jolly Technologies reports that an insider at it overseas R&D center in Mumbai stole portions of the source code and confidential design documents relating to one of its key products.
As reported in InfoWorld

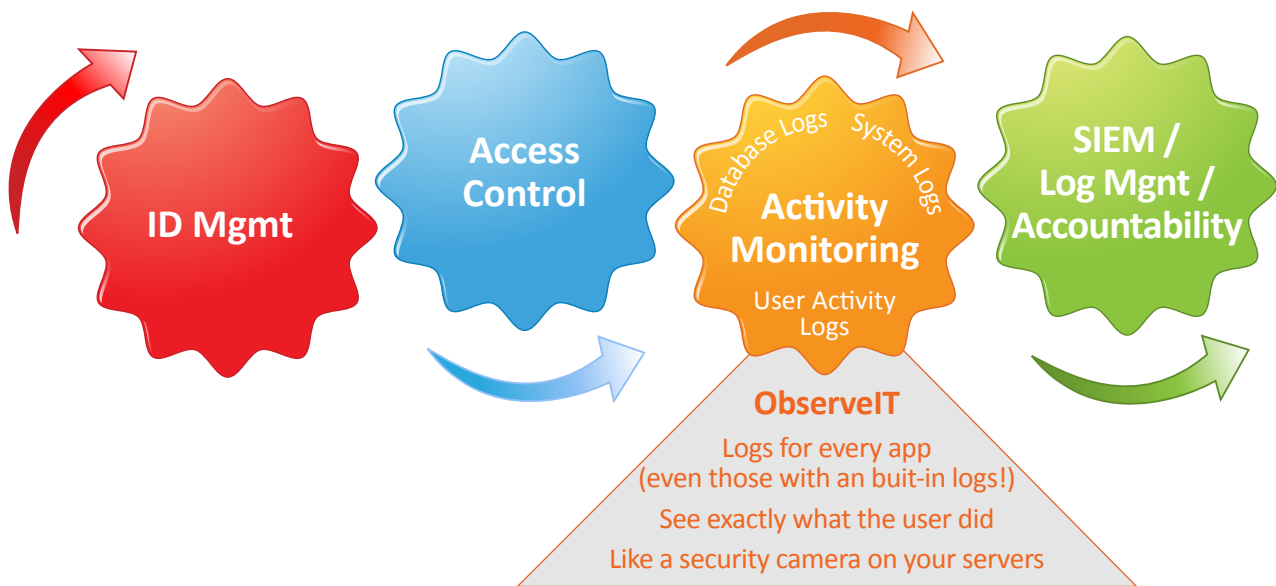
Healthcare Compliance Gotchas
Doing the basics to comply with HIPAA and PCI isn't always sufficient to keep data safe... Healthcare companies have obvious high-risk areas to watch when it comes to ensuring the safety of personal health data.
As reported in InformationWeek

System Change "Time Bomb" Planted by Disgruntled Employee
Farrise Mae reports that a contract employee, knowing that he would soon lose his job, made a change to critical Unix config settings which would only take effect weeks after his departure. If undetected, the script would have shut down the company's operations.
As reported in COMPUTERWORLD

Former Bank Contractor Charged in Fraud Scheme
Bank of New York reports that a sub-contractor computer technician has stolen over SIM by using identity theft of employee data.
As reported in The New York Times

Blind Spots
You can only audit what your logs provide!
Many apps have no logs
System logs are too technical

Where ObserveIT fits in



Accountability audit reports are only as good as the logs that they collect. Database and system monitors are not enough. **If your apps don't log it, your audit won't show it!**

ObserveIT fills this gap by generating **logs for every app**, even those with no internal logs.

And these logs add bulletproof evidence, via ties to **video replay**.

“With so many privileged vendors accessing our servers, it can be difficult to keep an eye on who's doing what.”

Isaac Milshtein, Pelephone



Solution Benefits

Generate logs for apps with no logs - Cloud apps and legacy apps are notorious for being tough to audit. ObserveIT gives full transparency of cloud and legacy app activity, even when these apps have no internal logs built in.

Bulletproof legal evidence - Reduce the risk of misaligned client-vendor interests by capturing bulletproof legal evidence of all vendor activity. Video replay can be used during litigation or to eliminate the need for legal action.

Compliance Accountability - Know exactly what 3rd party vendors are doing on your servers. Improve security and ensure transparent billing validation.

Compliance Report Automation - Track every access to corporate servers and databases, with detailed usage reporting and total application coverage.

Managed Services Monitoring - Transparent accountability reporting of all outgoing support sessions provides provable SLA validation and decreased support costs.

Root Cause Analysis - Achieve fast troubleshooting when you discover the root cause of system config changes. Establish business intelligence with focused navigation and video playback.

Who Benefits from ObserveIT?

- Compliance Officers can incorporate ObserveIT in their reporting process
- IT Managers can streamline troubleshooting
- ISVs can integrate ObserveIT into their software products, to add screen recording functionality
- Managed Services providers can embed ObserveIT into their IT service offerings, to strengthen reliability and SLA

PCI Compliance Highlights

- **PCI 10.2** – Generate audit logs (Even for apps that do not have built-in logging!)
- **PCI 10.3** – Visual audit guarantees sufficient coverage and clarity of user actions
- **PCI 10.1** – Capture Named-User credentials without the need for complex password vault management

ObservelT's Unique Advantage:

Logs that fill accountability gaps, tied with bulletproof video playback

ObservelT lists every user session



Windows Session: Metadata + Video

ObservelT captures Window title, Application name, files opened, URL accessed, UI element selection and text entry

Activity View

Server: MASTER-DC2

Up to: January 2010

Filter by user: All

Results: 1 - 12 of 12

Session Duration	Login	User	Server	Client	Slides	Video
5:34 PM - 8:38 PM	Administrator	noam	MASTER-DC2	(local)	1366	[Video]
5:13 PM - 5:13 PM	Administrator	noam	MASTER-DC2	(local)	2	[Video]
8:49 PM - 8:50 PM	Administrator	noam	MASTER-DC2	(local)	19	[Video]
8:01 PM - 8:35 PM	Administrator	noam	MASTER-DC2	(local)	118	[Video]

ObservelT - Login (4.0.3.0)

Program Manager (2)

Group Policy Management (3)

New GPO

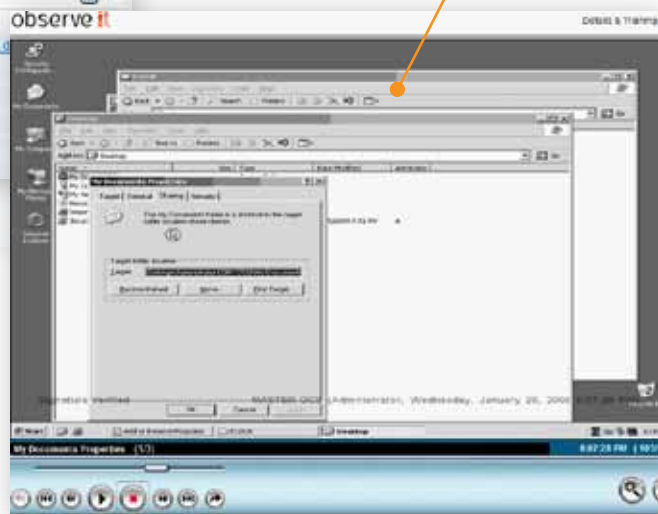
Group Policy Object Editor (2)

Group Policy Management (3)

New GPO

Group Policy Object Editor (2)

Exact video playback



Within each session, details of every action taken



Unix/Linux Session: Metadata + Video

ObservelT captures shell logins, including all command line activity and system calls. (If user types "rm*", ObservelT captures each file name that is deleted.)

Session Duration	Login	User	Server	Client
11:57 AM - 11:57 AM	Administrator	n/a	solarism1	Client

chmod

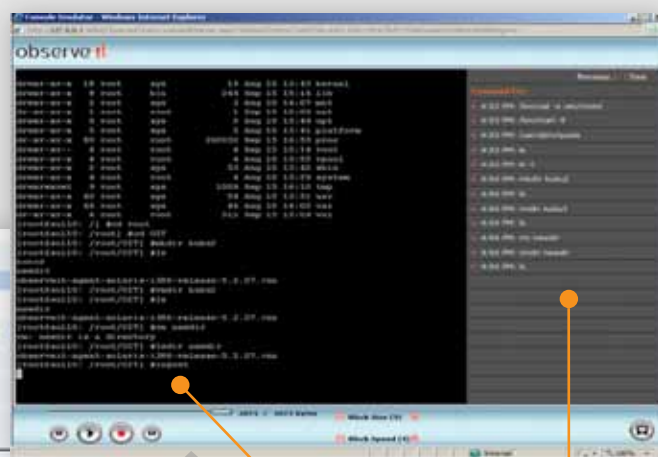
11:22 /bin/chmod a+x /tmp/session

Time	Process ID	Function	Params
11:23 PM	6995	EXEC	chmod a+x /tmp/session
11:23 PM	6995	CHMOD	/tmp/session

rm

11:35 /bin/rm -f /tmp/session

Time	Process ID	Function	Params
11:35 PM	6996	EXEC	rm -f /tmp/session
11:35 PM	6996	UNLINK	/tmp/session



List of each user command

Exact video playback of command prompt screen

For each command, a detailed list of system calls

ObserveIT Feature List

“Not only was ObserveIT able to record every single user session on the servers, the recordings are also fully indexed, allowing me to zoom in on areas of interest.”

Robert Ng, Siemens

Generate Logs for Apps that have no logs - Detailed log for all apps, even those that have no internal logs, including Cloud apps (ex: salesforce.com), legacy apps (ex: customized ERP) and commercial software (ex: Excel, SQL query tools).

Record and Replay Windows, Unix and Linux Sessions - Exact video playback of every session, including mouse movements, UI interaction, command line interaction, text entry and underlying system calls. Simple playback and navigation of recordings.

Privileged User Identification - Add additional level of system access control for sensitive resources. Require shared-id users (ex: administrator) to add secondary login credentials. Manage users locally or tie in to AD.

Intelligent Metadata Text Log - Captures details about each user action: Application name, User name, Server, Window title, File or Resource accessed, underlying system calls. Interactive drilldown and fast navigation eliminates the need to replay hours of video to find what you need.

Policy Messaging - Send policy and status updates to each user exactly as they log in, ensuring that corporate standards are understood and acknowledged.

Real-time Playback - Session recordings are immediately available once session begins. View session activity "on the air", while users are still active.

API Interface - Control the ObserveIT Agent via scripting and custom DLLs from within your corporate applications. Trigger recording activity based on process IDs, process names or web URLs.

Report Generator - Use our pre-built audit reports, or create your own custom reports. Schedule reports to run automatically for email delivery, or run ad-hoc and export to Excel or XML.

Complete Coverage - Agnostic to network protocol and client application. Captures all remote and console sessions: SSH, Telnet, Terminal Services, Citrix, Remote Desktop, PC-Anywhere, VMware, VNC, Dameware and more.

System Monitor Integration - Instant replay from within network management (SCOM, Unicenter, Tivoli, OpenView and more). Real-time alerts on any user action (file access, network share, registry edit, URL access).

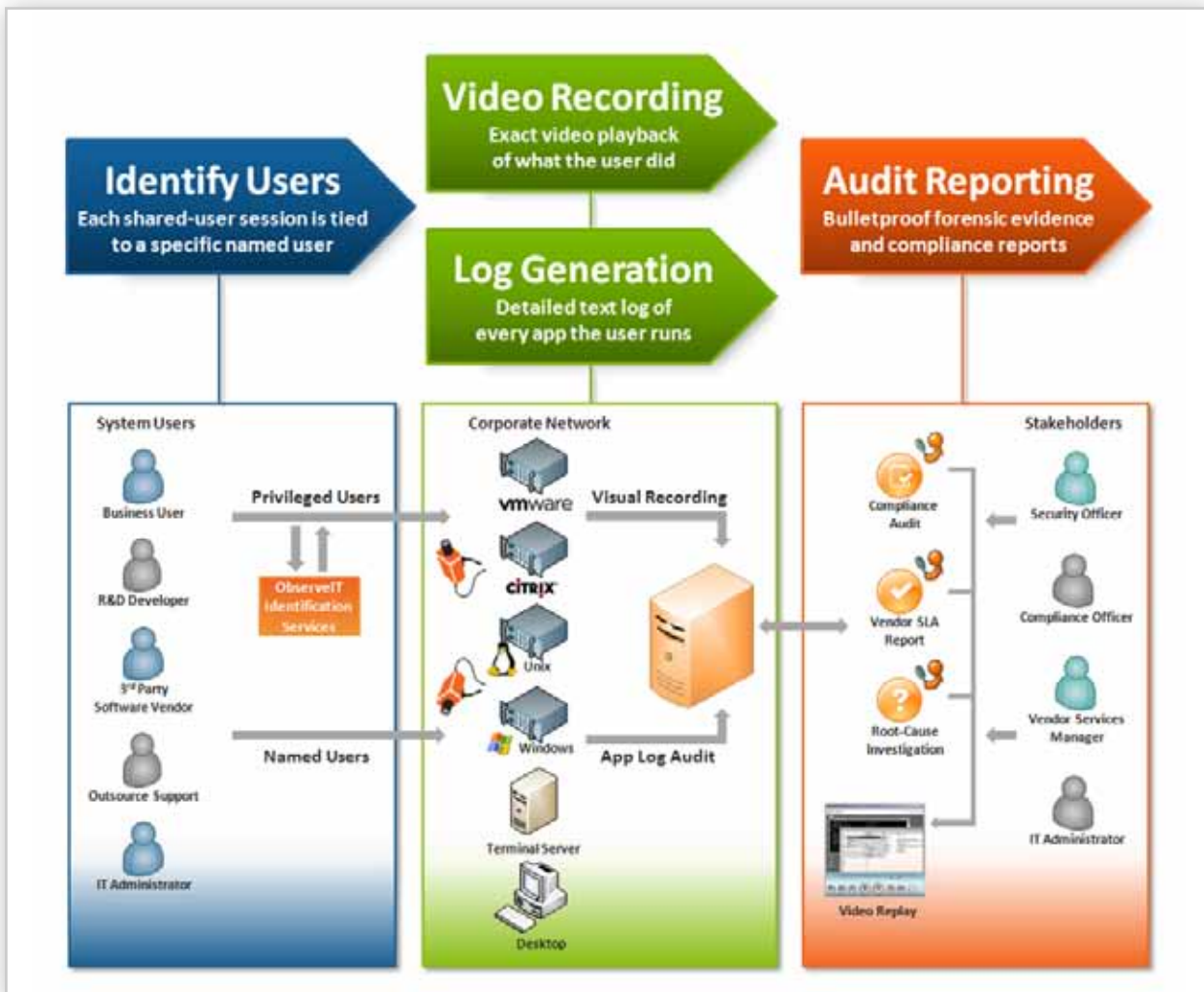
Robust Security - Agent-Server encryption, Digital Signatures and Watchdog mechanism ensure the highest security and reliability.

Recording Policy Rules - Granular include/exclude policy rules to set recording rules per server, user/user group or application.

Pervasive User Permissions - Granular permissions and access control affects all content access, satisfying all regulatory requirements.

Small Footprint - Ultra-efficient data storage: Less than 250GB/year for high-usage, 1000 server environment. Minimal Agent CPU utilization: 0% CPU when no console active, 1%-2% CPU, 10 MB RAM during session).

How ObserveIT Works



Identify: ObserveIT identifies all remote and terminal users

As soon as a user starts a session (using any connection protocol), ObserveIT identifies the precise user id. Shared users (ex: 'administrator') must provide secondary credentials of a specific named user.

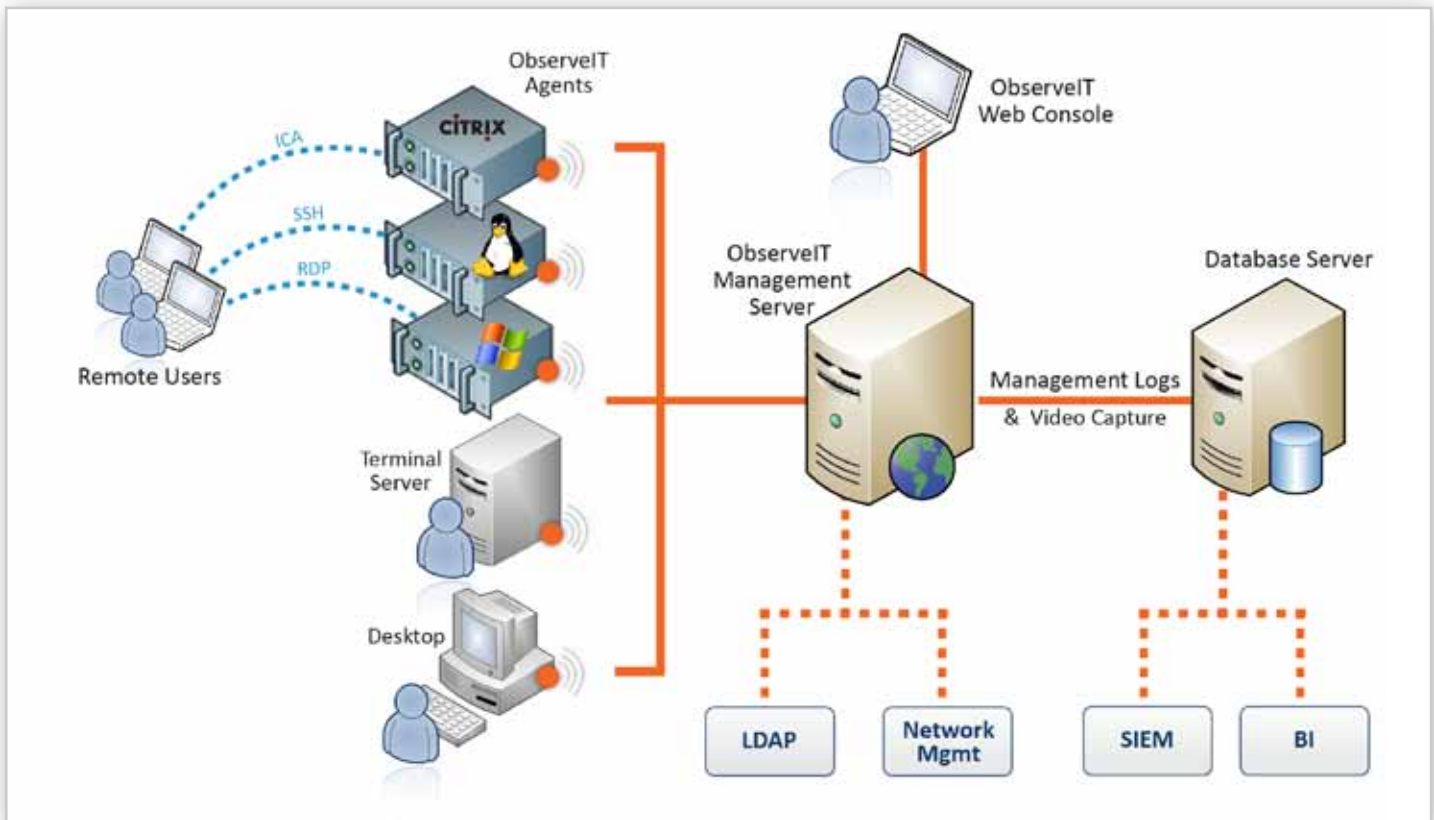
Record: Generating logs and capturing video

ObserveIT captures a detailed textual log plus video recording of every user action. Logs are generated for every application, even those that don't have their own internal logs. These logs avoid the technical mumbo-jumbo of typical system logs, instead showing exactly what the user did (and not just the underlying results). Details include the files opened, windows viewed and specific UI activity, which are then tied to precise video that delivers precise forensic evidence.

Report: Pre-built and customizable compliance audit reports

Access the audit recordings any way you wish. Automated canned reports sent via email, periodic and customized reports, textual summaries and full video replay are at your fingertips.

ObserveIT Architecture



The ObserveIT Agent is installed on each monitored server. The Agent captures data (screenshot and metadata) for every user action. Metadata includes info on the state of the operating system and the application program being used, which allows ObserveIT to precisely identify what the user is doing. By default, the Agent communicates with the Management Server via HTTP POST (TCP port 80). All content is encrypted. The Agent architecture includes a Watchdog service to prevent it being shut off.

The ObserveIT Management Server is an ASP.NET application in IIS that collects all data delivered by the Agents, where it is analyzed and sent to the Database Server to be stored and indexed. The Management Server communicates with the Agents for configuration update. It also can integrate easily with AD for user validation, with SIEM to link video replay from within textual log file listings, and with Network Management systems to allow for system alerts and updates based on user activity.

The ObserveIT Web Console is an ASP.NET application in IIS that serves as the primary interface for accessing information (video replay, reporting, etc.) in ObserveIT. It is also used for configuration and administration tasks. Config data is also stored in the Database Server. The Web Console includes granular policy rules for limiting access to sensitive data.

The Database Server is a Microsoft SQL Server database that stores all configuration data, metadata and screenshots captured by ObserveIT Agents. Both the Management Server and Web Console apps connect via standard TCP port 1433.

Each of the three server applications can be installed on a single machine, or distributed for performance and security considerations.

Who's Using ObserveIT

Manufacturing

Financial

Telecommunications

IT Services

Healthcare/Education/Gov't

observe **it**
people audit

*Like a Security Camera on
Your Servers.*