

observe *it*

people audit



Aufzeichnen und Wiedergeben von allen Windows und Unix User Sessions

Wie eine Sicherheitskamera auf Ihren Servern

ObserveIT ist die einzige Unternehmenslösung, die Windows und Unix User Sessions aufzeichnet und alle Zugriffsmethoden unterstützt - ohne irgendwelche Änderungen in der Architektur.

- ▶ *Vollständige Videowiedergabe jeder User Aktion*
- ▶ *Zeichnet alle remote und Konsol Windows und Unix Sessions auf:
RDP, ICA, VMWare, SSH, Telnet und mehr*

Umfassende Softwarelösung für:

- *Monitoring von firmenexternen Dienstleistern*
- *Sicheres Compliance Auditing von allen User Aktivitäten*
- *Ursachenerkennung bei Fehlerbehandlung*



ObserveIT Vorteile

Rechtssicherer Nachweis - Verringert das Risiko von missbräuchlichen Aktivitäten durch das Erfassen rechtssicherer Nachweise von allen Aktivitäten einer Fremdfirma. Videoaufzeichnungen können als Beweise benutzt werden.

Erhöhte Eigenverantwortung - Videoaufzeichnungen dokumentieren alle Aktivitäten externer Mitarbeiter und ermöglichen Ihnen, Abhängigkeiten zu reduzieren. Beseitigen Sie das 'Mysterium' und wissen Sie, was sie tun. Verbessern Sie die Flexibilität bei Vertragsbeendigungen, -anpassungen oder beim Festlegen von SLA-Erwartungen.

Verbessern der internen Kenntnisse - Eine indizierte Datenbank von User Session Aufzeichnungen wird ein bewährtes Repository für den Geschäftsbetrieb.

Verbesserte Kommunikation - Reduzieren sie die Notwendigkeit von verbalen Beschreibungen und Email-Erklärungen: 30 Minuten Video erklären mehr als Stunden von Training, Telefongespräche und Emails.

Erweitern Sie die System Management Infrastruktur - Verbinden Sie eine präzise Videowiedergabe mit jedem textlichen Logeintrag in Ihrem System Management.

Sofortige Compliance für neue Applikationen - Jede neue Applikation wird automatisch überwacht und ist für Compliance Auditing bereit. Es ist nicht notwendig, Code oder Konfigurationen zu ändern, um die Log-Anforderungen zu erfüllen.

Aufzeichnung wird angezeigt - Über die Aufzeichnung der Bildschirmaktivitäten wird der User mit einem Hinweis in Kenntnis gesetzt. Dies erhöht den Präventionseffekt bei den Mitarbeitern und erfüllt die gesetzlich strengen Vorschriften über den Umgang mit personenbezogenen Daten.

- ▶ Remote Fremdfirmen Auditing
- ▶ Sichere Compliance
- ▶ Sofortige Fehlerdiagnose

ObserveIT's einzigartiger Vorteil: Video + Metadaten Intelligenz auf Fingertip

ObserveIT listet jede User Session auf



Windows Session: Metadata + Video

ObserveIT erfasst Window Titel, Applikationsname, eröffnete Dateien, abgerufene URLs, UI Element Auswahl und Texteingabe

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 Icon]
5:13 PM - 5:13 PM	Administrator	noam	MASTER-DC2	(local)	2	[Video Icon]
8:49 PM - 8:50 PM	Administrator	noam	MASTER-DC2	(local)	19	[Video Icon]
8:01 PM - 8:35 PM	Administrator	noam	MASTER-DC2	(local)	118	[Video Icon]

ObserveIT - Login (4.0.3.0)

Program Manager (2)

Group Policy Management (3)

New GPO

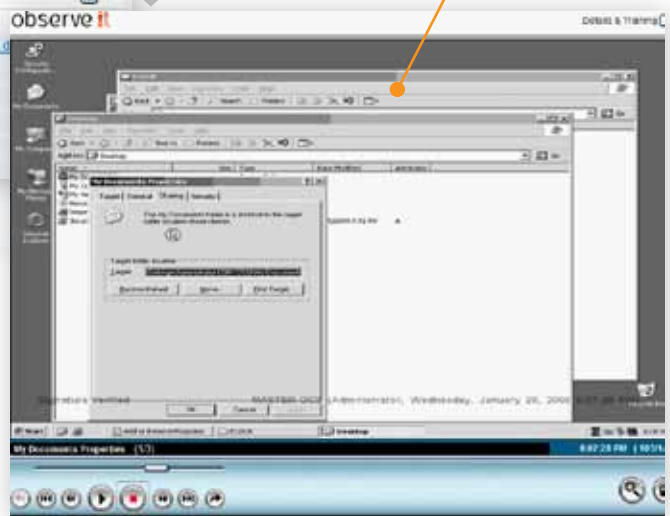
Group Policy Object Editor (2)

Group Policy Management (3)

New GPO

Group Policy Object Editor (2)

Exakte Videowiedergabe



Innerhalb jeder Session, Details von jeder ergriffenen Aktion



Unix Session: Metadata + Video

ObserveIT erfasst Shell Logins, inklusive aller Command Line Aktivitäten und System Calls. (Wenn der User "rm" eingibt, erfasst ObserveIT jeden Dateinamen, der gelöscht wurde.)

Session Duration	Login	User	Server	Client
11:57 AM - 11:57 AM	Administrator	n/a	solarsvm1	Client

chmod

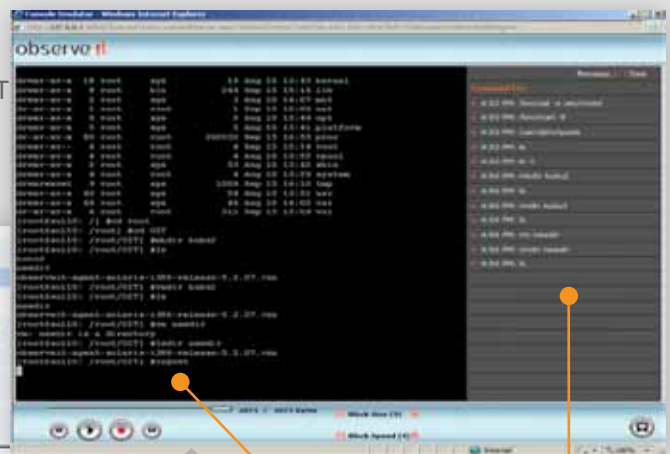
11:22 /bin/chmod a+x /tmp/session

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



Listet jeden User Befehl auf

Für jeden Befehl, eine detaillierte Liste der System Calls

Exakte Videowiedergabe vom Command Prompt Screen

Hauptmerkmale

Aufzeichnen & Wiedergeben - Exakte Videowiedergabe von jeder Windows und Unix Session, inklusive Mausbewegungen, UI Interaktion, Texteingabe und Befehlszeile.

Intelligente Metadaten mit jeder Session - Es ist nicht notwendig, stundenlang Videos abzuspielen, um zu finden, was Sie benötigen. Interaktiver Drill-down - nach User, Server, App Name, Datei oder benutzte Ressource, zugrunde liegende System Calls und mehr - führt Sie direkt zur Wiedergabe der richtigen User Aktion.

Real-time Wiedergabe - Sehen Sie sich Session Aktivitäten "auf Sendung" an, während User noch aktiv sind oder spielen Sie jederzeit historische Aufzeichnungen ab.

Privilegierte User Identifikation - Verbinden Sie Usernamen mit jedem anonymen 'Administrator' Login. Fügen Sie eine zusätzlichen Kontrollebene für Systemzugriffe für sensitive Ressourcen hinzu.

Vollständige Abdeckung - ObserveIT ist tolerant gegenüber Netzwerkprotokoll und Client Applikation. Erfasst Unix und Windows Sessions via: SSH, Telnet, RDP, Terminal Services, Citrix, VMware, VNC, PC-Anywhere, Dameware und mehr.

System Monitor Integration - Sofort-Wiedergabe vom System Management heraus (SCOM, Unicenter, Tivoli, OpenView, etc.). Real-time Alarme bei jeder User Aktion (Dateizugriff, Netzwerkfreigabe, Registry Edit, URL-Zugriff und mehr)

Unternehmensweit

Robuste Sicherheitsarchitektur - Agent-Server Verschlüsselung, Digitale Signaturen, tiefgreifende User Berechtigungen und System Watchdog-Mechanismen gewährleisten sichere Umgebungen.

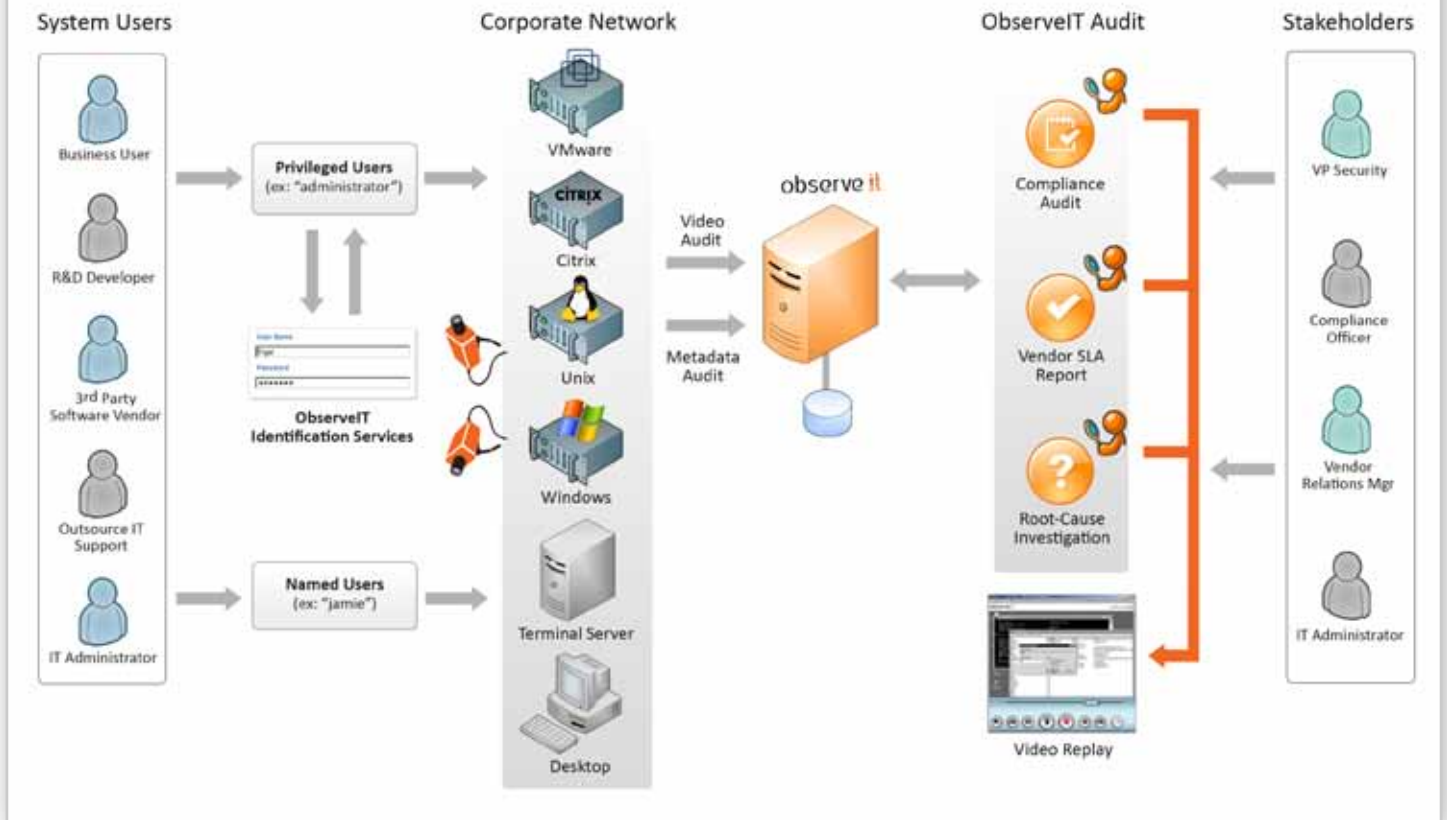
AD Policy, Event-gesteuerte Regeln - Eine flexible Regelmaschine ermöglicht den Einschluss/Ausschluss von Active Directory User und User Group Regeln. Event Regeln können per benutzte Applikation/Ressource genutzt werden.

Kleiner Ressourcenbedarf - Hocheffiziente Datenspeicherung: weniger als 250GB/Jahr für eine intensiv benutzte 1.000 Server Umgebung. Minimale Agent CPU Benutzung: 0% CPU, wenn keine Konsole aktiv ist, 1%-2% CPU während der Session.



Wie ObservelT arbeitet

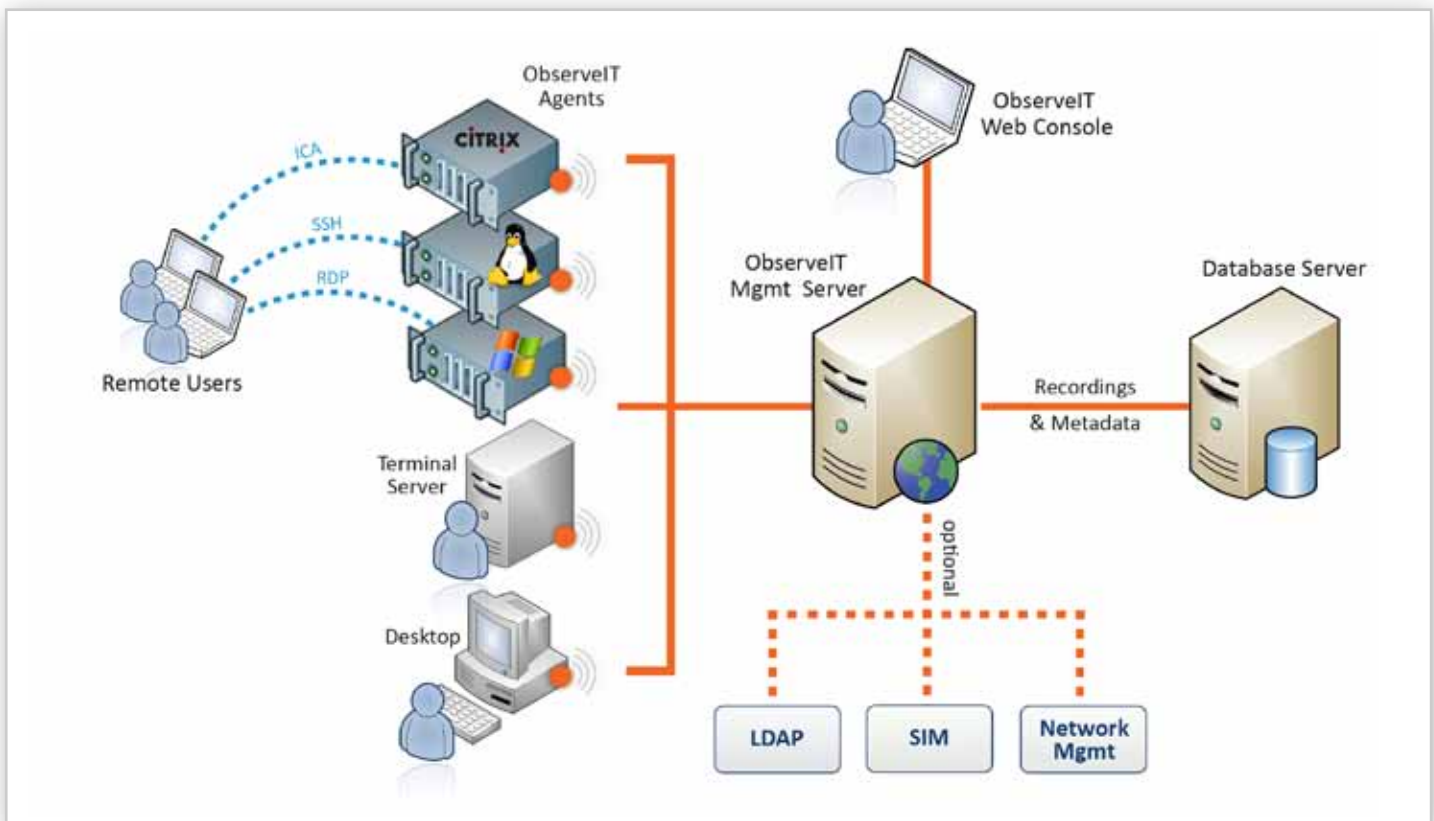
- 1 Remote und Terminal User greifen auf Ihre Server zu.
- 2 ObservelT zeichnet jede User Aktion auf.
- 3 Sie können alle User Sessions durchsehen, prüfen, suchen und wiedergeben.



Warum ObservelT einsetzen

- ✓ **Remote Auditieren von externen Mitarbeitern: Keine Schuldzuweisung!**
 Sie wissen genau, was die Mitarbeiter von Fremdfirmen auf Ihren Servern tun.
- ✓ **Sichere Compliance: Auditieren von Personen, nicht nur Applikationen**
 Detaillierte und automatisch gelieferte Audit Reports bieten unangreifbare Nachweise für jeden Zugriff auf Ihre Unternehmensserver und Datenbanken.
- ? **Schnelle Fehlersuche: Besiegen Sie den den "Uups Faktor"**
 Finden Sie schnell den Grund jeder Konfigurationsänderung - mit detaillierter Suche und Video-wiedergabe von User Sessions.

ObserveIT Architektur



Der ObserveIT Agent ist auf jedem überwachten Server installiert und erfasst Daten (Screenshots und Metadaten) für jede User Aktion. Metadaten enthalten Informationen über den Betriebssystemstatus und des benutzten Anwendungsprogramms, die es ObserveIT ermöglichen, exakt zu erkennen, was der User tut. Standardmäßig kommuniziert der Agent mit dem Management Server über HTTP POST (TCP Port 80). Jeglicher Inhalt ist verschlüsselt. Die Agent Architektur enthält zur Vermeidung von Störungen einen Watchdog Service.

Der ObserveIT Management Server ist eine ASP.NET Applikation im IIS, die alle von Agents gelieferten Daten sammelt, analysiert und zum Datenbank Server sendet, der sie speichert und indiziert. Der Management Server kommuniziert mit den Agents für Konfigurationsänderungen. Er kann leicht mit LDAP für User Berechtigungen integriert werden, mit SIM, um Videowiedergaben mit textlichen Logdateilisten zu verbinden und mit System Management Systemen, um Systemalarme und Updates zu ermöglichen, die auf User Aktivitäten basieren.

Die ObserveIT Web Konsole ist eine ASP.NET Applikation im IIS und die primäre ObserveIT Benutzeroberfläche zum Zugriff auf Informationen (Videowiedergabe, Reporting, etc.). Sie wird auch für Konfigurations- und Administrationsaufgaben benutzt. Konfigurationsdaten werden im Datenbank Server gespeichert. Die Web Konsole enthält detaillierte Policy Regeln zum Begrenzen von Zugriffen auf sensitive Daten.

Der Datenbank Server ist eine Microsoft SQL Server Datenbank, die alle Konfigurationsdaten, Metadaten und von ObserveIT Agents erfassten Screenshots speichert. Der Management Server und die Web Console kommunizieren via Standard TCP Port 1433.

Alle drei Server Applikationen können auf einer einzigen Maschine oder zum Zweck von Performance- oder Sicherheitsbetrachtungen verteilt installiert werden.

Wer benutzt ObservelT

Manufacturing	Financial	Telecommunications
      	         	      
IT Services	Healthcare/Education/Gov't	
     	     	

observe **it**
people audit

*Wie eine Sicherheitskamera
auf Ihren Servern.*