Windows Server 2012 R2 Certified

observe it

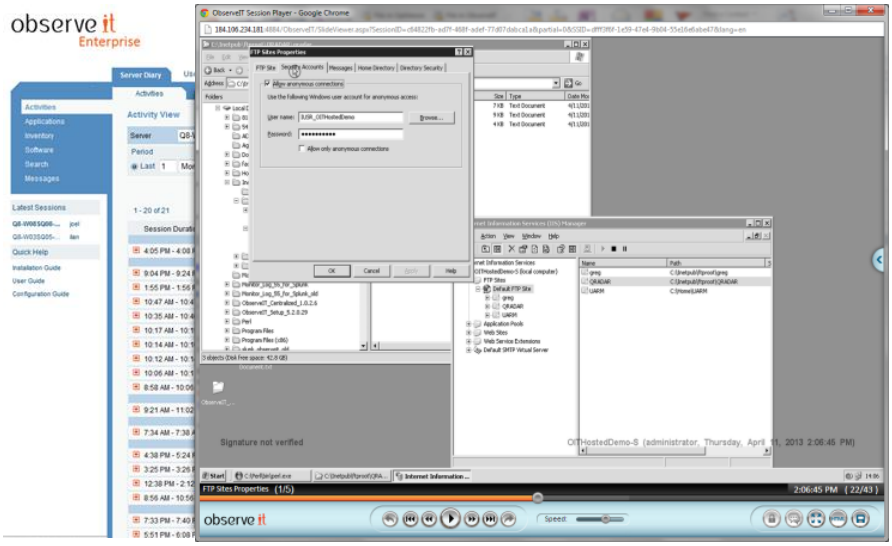
MONITORING USER ACTIVITY IN WINDOWS ENVIRONMENTS

ObserveIT monitors all user activity on Windows servers and desktops. The system generates video recordings, user activity logs and real-time alerts. The result is a complete solution for identifying and managing user-based risk.

VIDEO REPLAY AND ACTIVITY ANALYSIS

Playing back a user session shows exactly what occurred on screen during the session. Playback speed is adjustable. On the right side of the player window is an activity summary panel, which lists every action performed during the session. Clicking an action in the list jumps directly to that portion of the video – just like navigating chapters on a DVD.

However, ObserveIT goes far beyond simply recording the on-screen activity to video: the software transcribes every session into an easy-to-read user activity log so that watching the video isn't necessary to know what the user did. Clicking on any particular event in the log launches the video playback from that exact moment. This activity analysis is also used to generate real-time user activity alerts and reporting.

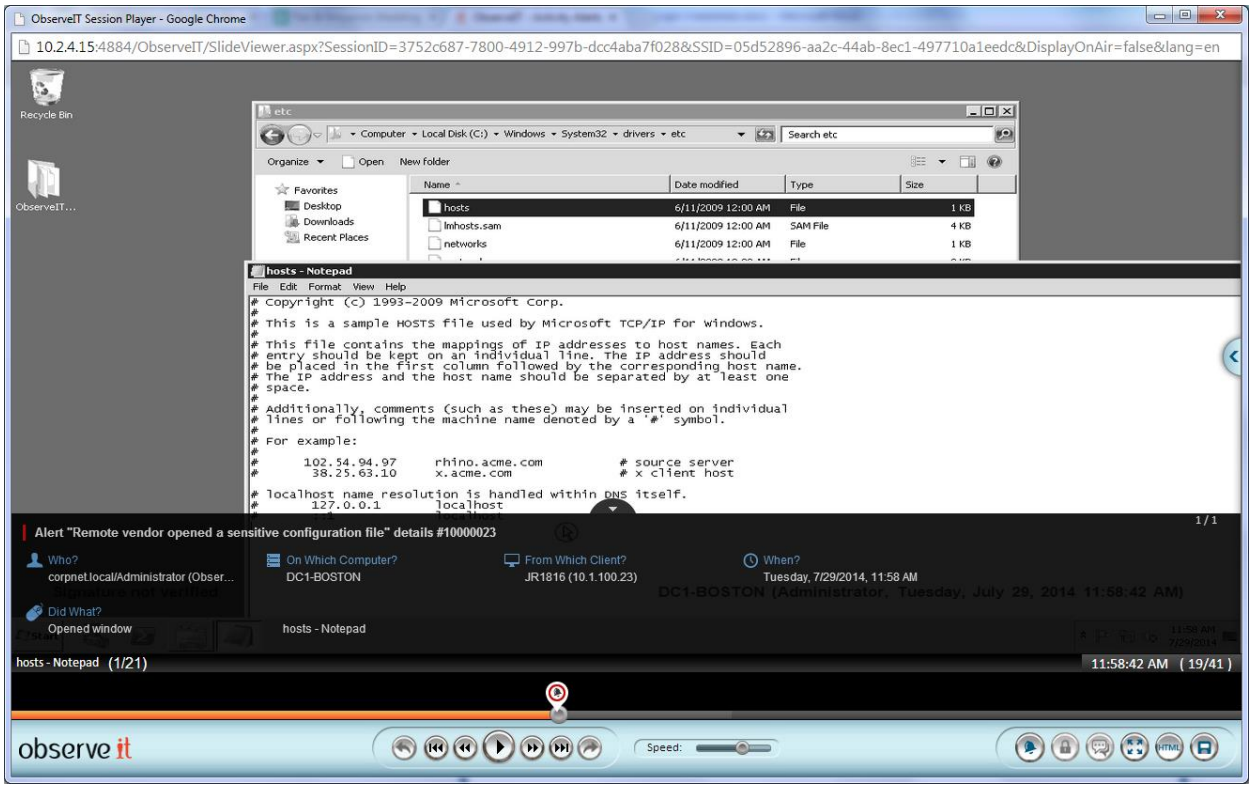


REAL-TIME USER ACTIVITY ALERTS

When user-based attacks occurs, every second counts. The longer a threat goes undetected, the more damage a company will incur in terms of both financial costs and brand reputation. Without the ability to monitor user activity in real-time, companies will continue to suffer from undetected user-based threats for extended periods of time.

ObserveIT's user activity analytics instantly alert IT security teams to abnormal, suspicious or malicious user activity. The fully-customizable alerts are integrated throughout the system, and are even overlaid into session replay.

Furthermore, each alert can be assigned a notification policy which designates who gets notified and at what frequency.



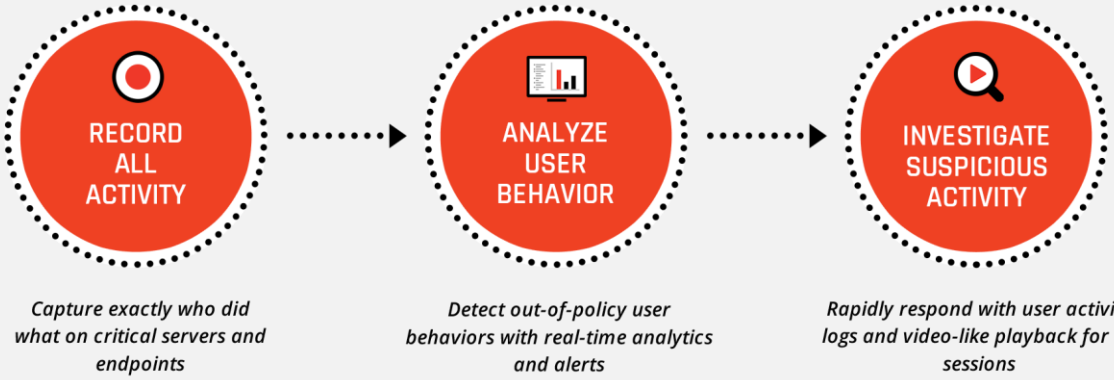
Alert details are overlaid in the session player, at the moment in the video that the alert was generated.

KEYWORD-BASED ACTIVITY SEARCH

ObserveIT captures detailed session activity data and makes it immediately available for alert generation and free-text keyword searching. Administrators, IT security officers and auditors can search for specific mouse or keyboard actions matching:

- names of applications run
- titles of windows opened
- URLs accessed via browsers
- text typed, edited, pasted, selected, auto-completed, etc.
- checkboxes and radio buttons clicked
- commands and scripts run in the CMD console

Every resulting search hit is linked directly to the portion of the video where that action occurred. This makes it incredibly easy to find the exact moment that any particular action was performed from among thousands of hours of user activity!



ZERO-GAP MONITORING, ANALYSIS, ALERTING AND INTERVENTION

ObserveIT monitors, records and analyzes all user activity in every application, Web page and window, over any connection method (Remote Desktop, Terminal Services, GoToMyPC, LogMeIn, PC Anywhere, local login, etc.). ObserveIT also records Windows sessions running as Citrix published applications, in Citrix virtual desktops and VMware environments, as well as stand-alone Windows, Unix and Linux desktops and servers. Addressing a major security gap in most organizations, ObserveIT even generates user activity logs and screen recordings for commercial, legacy, bespoke and cloud apps, including those with no internal logging facilities of their own.

Administrators can watch live sessions and can even lock a session and user account from within ObserveIT if they wish to immediately stop a suspicious or dangerous activity. This is particularly useful in the event that the system generates a real-time alert: the administrator receiving the alert can view all activity occurring in the live session screen, rewind to see the actions that led up the alert and take immediate action to cease any undesirable activity.

Additionally, the recordings and resulting user activity logs are valuable for root cause analysis, ad hoc IT forensics and regulatory compliance audit reporting. Reports can be customized to specific business needs and can be scheduled or run on demand.

LOW RESOURCE REQUIREMENTS

ObserveIT utilizes ultra-efficient data storage, requiring less than 250GB/year for a high-usage, 1000-server environment. The local agents have a minimal footprint of 1%-2% CPU utilization, 10 MB RAM during session and 0% CPU when users are inactive.

OBSERVEIT FEATURE HIGHLIGHTS

- **Screen capture recording** *plus* **video activity analysis** for searchable, text-based logging of all user activity
- **Real-time alerts** provide immediate awareness of suspicious, dangerous and out-of-policy behavior
- **Advanced keylogging** enables keyword searching to instantly find any on-screen mouse or keyboard action
- **Records actions in *all* system areas and *all* apps –** zero-gap recording of all commercial, legacy, bespoke and cloud apps plus all system areas
- **Supports all connection methods**, including local login, Remote Desktop, Terminal Services, PC Anywhere, Citrix, VMware, VNC, Dameware, etc.
- **SIEM, NMS** and **IT ticketing system** integration for better security and easier investigations – including direct links to session replay and user activity logs
- **Privileged User Identification**, without requiring password rotation or check-in/check-out
- **Threat detection console** detects and pinpoints suspicious activity
- **DBA Activity Audit** monitors and audits all SQL queries executed by DBAs against production databases
- **Pre-built and customizable audit reports** can be exported to Excel or XML, or scheduled to run automatically for email delivery

TRUSTED BY 1200+ CUSTOMERS

ING — *Auditing and compliance*

Coca-Cola — *Third-party monitoring*

UPS — *Privileged user monitoring*

SIEMENS — *Rapid incident response*

OBSERVEIT

IDENTIFY AND MANAGE USER-BASED RISK

Start monitoring in minutes, free:
www.observeit.com/tryitnow