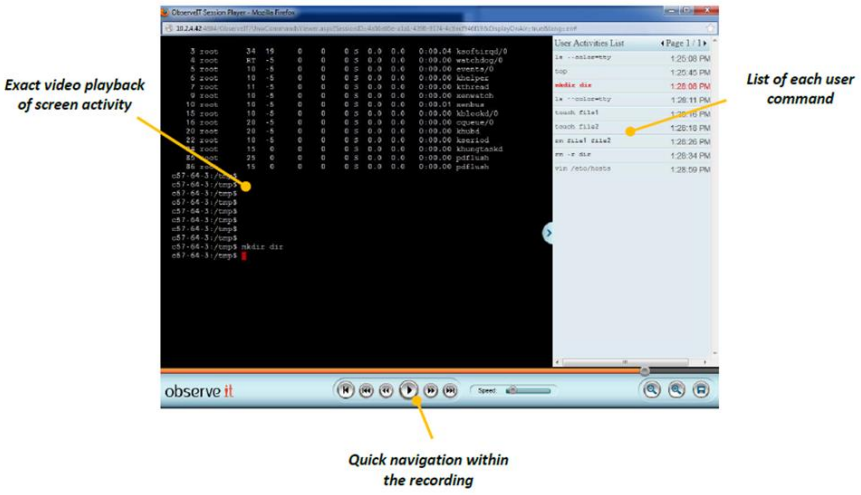
MONITORING USER ACTIVITY IN UNIX/LINUX ENVIRONMENTS

ObserveIT monitors all user activity on UNIX and Linux 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 the command summary panel, which lists every command executed during the session. Clicking a command in the list jumps directly to that portion of the video – just like navigating chapters on a DVD.

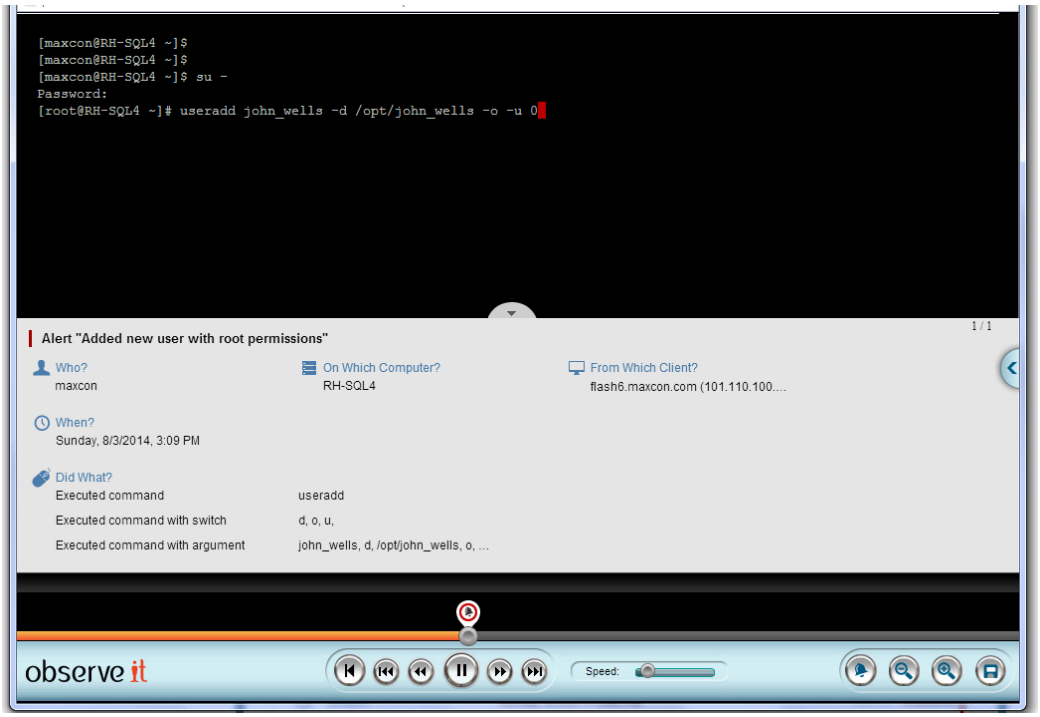


However, ObserveIT goes far beyond simply recording the on-screen activity to video: the software transcribes every session into an easy-to-read user activity log so that watching the video isn't necessary to know what the user did. Clicking on any particular event in the log launches the video playback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

REAL-TIME USER ACTIVITY ALERTS

When user-based attacks occur, 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.

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.



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

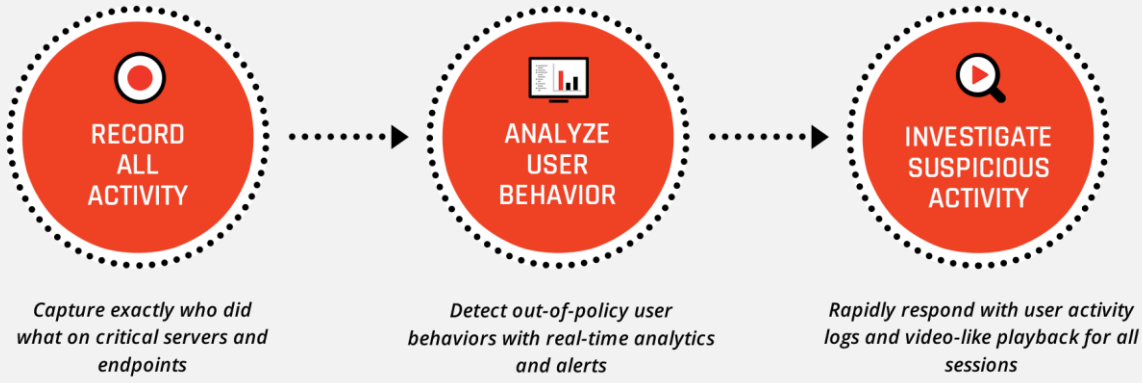
KEYWORD-BASED ACTIVITY SEARCH

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 user actions, using keywords matching:

- user-executed commands
- script-executed commands
- underlying system calls
- names of files/resources affected
- all keyboard keystrokes
- all terminal screen output

This means that every file create, delete, open and permission change, process creation and link creation is captured and searchable. For example, if the user runs an alias command or script that includes system calls to delete files and change user permissions, this info will all be captured. Likewise, ObserveIT captures every file and resource affected by each user command (e.g., if the user typed *rm *.txt*, ObserveIT will capture the actual name of each deleted file).

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 an action was performed from among thousands of hours of recorded user activity.



ZERO-GAP RECORDING, ANALYSIS, ALERTING AND COMPLIANCE

ObserveIT records and analyzes all user activity over any login protocol (SSH, Telnet, rlogin, xterm, direct console login, etc.), including all application usage, all commands, the system calls triggered by user commands (e.g., every permission change, process creation and link creation is fully exposed), and the resources affected (e.g., the exact name of each file touched). All of this data is available in user activity logs for the purposes of analysis, alert generation, reporting and search.

To address regulatory compliance requirements, ObserveIT provides the critical ability to track all administrator activity on sensitive servers, including the ability to identify the individual users logging in as root, or changing permission levels to root (or other privileged accounts) during a session. The system can generate alerts for the most dangerous administrator actions, such as *sudo -i* or *sudo su* or even running a specific command with root permissions. Additionally, user activity recordings and logs are valuable for root cause analysis, ad hoc IT forensics and detailed user activity reporting. These reports can be customized to specific business needs and can be scheduled or run on-demand.

Beyond Unix/Linux environments, ObserveIT can also record sessions in Windows servers and desktops, as well as Citrix published applications, Citrix virtual desktops and VMware environments.

TAMPER PROOF

Unlike simple Unix/Linux utilities that log user actions, there is no way for users (even root users) to shut down the ObserveIT recording agent without terminating the entire session. The agent embeds itself into any shell derived from a login process. Because this mechanism is connected to both the shell and the auditing process, it is

impossible to disable or tamper with the agent without closing the shell.

All session data sent by the agent to the ObserveIT server can be encrypted before transmission using industry-standard SSL. In the event that agent-server communication is temporarily lost, data is cached locally until the network connection is restored.

UNIX/LINUX PLATFORM COVERAGE

- AIX 5.3 (TL10 or higher) 32-bit/64-bit
- AIX 6.1 32-bit/64-bit
- AIX 7.1 32-bit/64-bit
- Debian 6 and 7 (64-bit only)
- HP-UX 11.23/11.31, Itanium (64-bit)
- Oracle Linux 5.0-5.10 i386/x86_64
- Oracle Linux 6.0-6.5 i386/x86_64
- RHEL/CentOS 5.0-5.10 i386/x86_64
- RHEL/CentOS 6.0-6.5 i386/x86_64
- SLES SuSE 10, SP2-SP4 i386/x86_64
- SLES SuSE 11, SP2-SP3 i386/x86_64
- Solaris 10, updates 4-11; x86/x64 or Sparc
- Solaris 11, update 1; x86/x64 or Sparc
- Solaris 9, update 9; Sparc
- Ubuntu 10.04 LTS i386/amd64
- Ubuntu 12.04 LTS i386/x86_64