WHAT'S NEW WITH OBSERVEIT:
INSIDER THREAT MANAGEMENT VERSION 6.5

ObserveIT's award-winning insider threat management software combines user monitoring, behavioral analytics, and now policy enforcement and dynamic forensic recording. **ObserveIT Insider Threat Management 6.5** enables you to change employee behavior across your enterprise through policy notification and enforcement.

Nearly all security incidents stem from people - whether it's getting infected, misbehaving, or making innocent mistakes. There is no patch for people. A lack of a security awareness accounts for the majority of risks; as they stem from unintentional insider threat or negligent employee behavior. People often forget what they hear during employee on-boarding, training, and quarterly company policy updates.

ObserveIT Insider Threat Management 6.5 educates and changes employee behavior through policy notification and enforcement. ObserveIT allows you to centrally manage and enforce security policies through real-time user notifications and in context of their activity.

Major product enhancements in 6.5 are (detailed below):

- Increase security awareness by educating employees with policy notifications
- Prevent unauthorized and malicious activity with policy enforcement
- Double library of Package Analytics to detect known patterns of risky behavior
- Dynamic forensic video recording for high-risk activity

Additional new features include:

- FIPS Compliant Agent
- Tamper-proof Windows Agent
- Massive database scalability and performance improvements

POLICY NOTIFICATION: INCREASE SECURITY AWARENESS AMONG EMPLOYEES

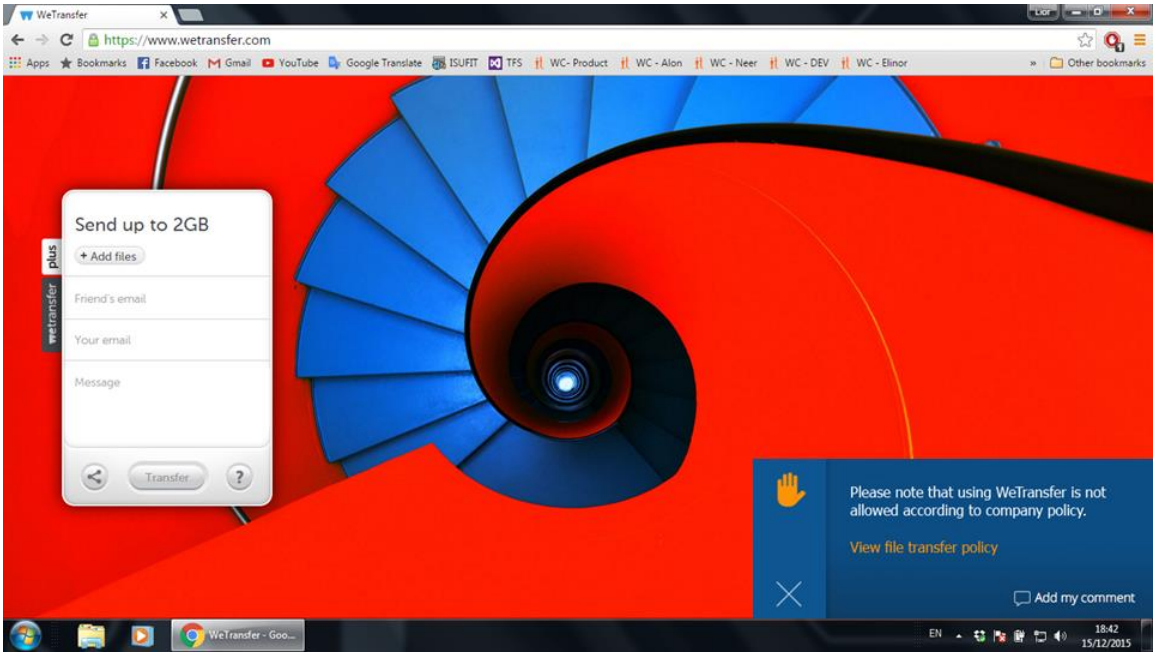
ObserveIT 6.5 introduces new policy notification capabilities. Using the full flexibility of the ObserveIT Activity Alert Rules, you can easily define your company policies and security regulations and enforce them by posting a specific, detailed notification message in real-time to any user violating these rules. The notification message can be triggered each time the rule is violated, or alternatively only once per user session.

There are 2 types of policy notifications:

Warning Notification

This notification message automatically disappears after a few seconds so there is no impact on end user productivity. Customers can choose to have the notification branded with their company logo, or leave it generic (see example below).

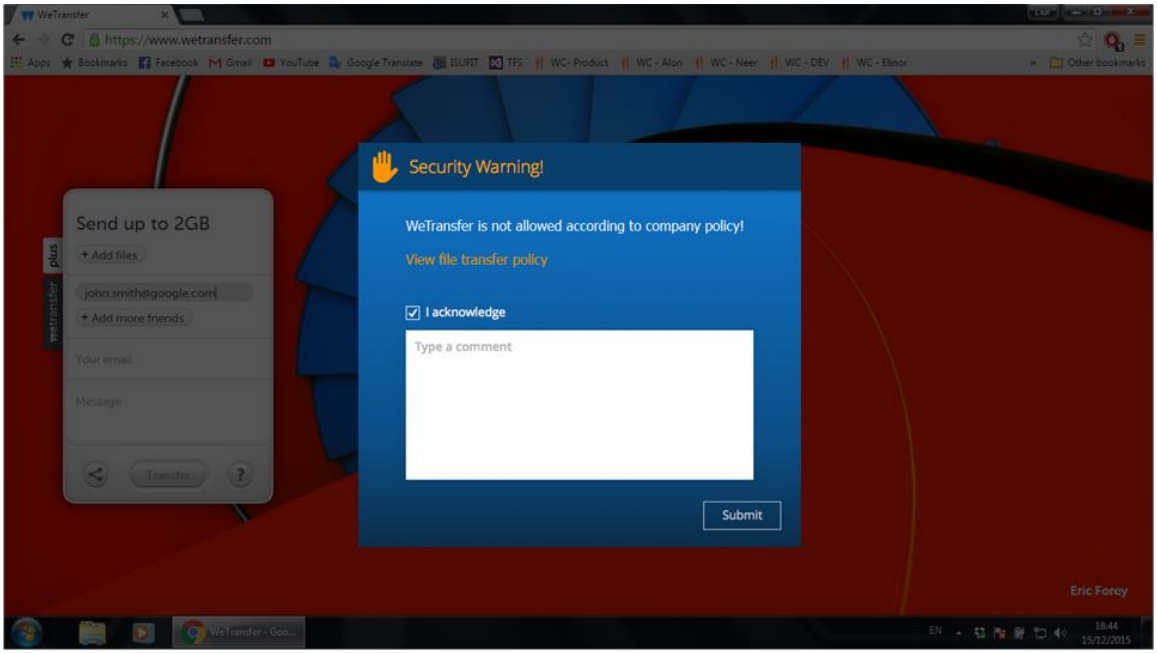
Once the notification is displayed, the user can click to view the policy/security requirements directly from the message itself and have the option to provide a comment explaining their misbehavior or to acknowledge the message.



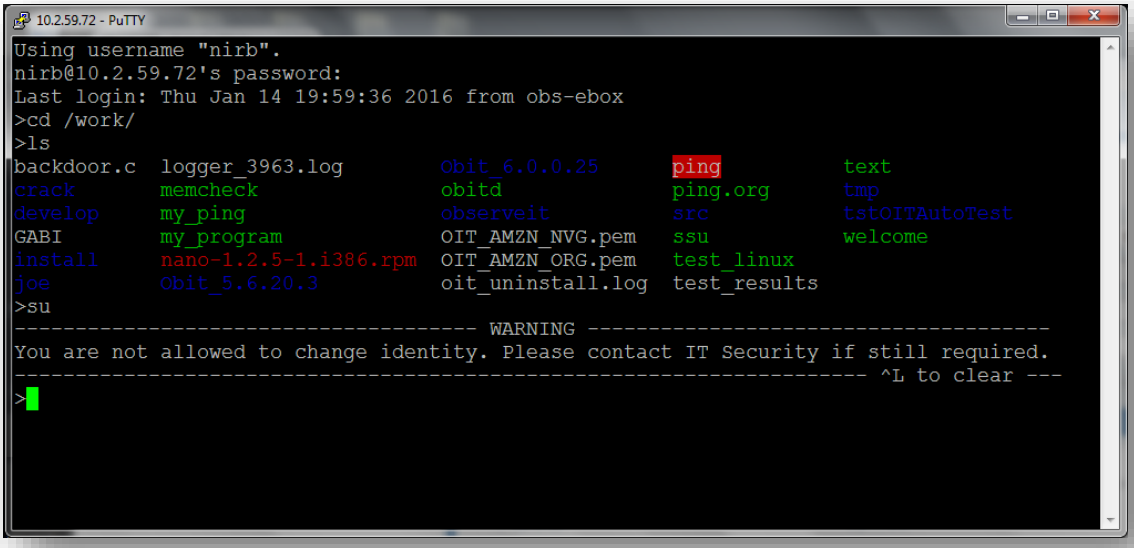
Blocking Message

This notification message blocks users from whatever they were doing – forcing them to review the message, acknowledge it, and provide their comment (optional, based on configuration) before they can continue with their work. Again, the policy/security requirements are available directly from the message.

All text messages including the window title and logo are configurable.



For Unix/Linux, policy notification is applied by writing the real-time notification message text directly to the terminal output. Users become aware of the security/policy violation message and can keep on with their work. The text is *not* added as input to the currently running command – hence there is no impact on any interactive or back processes. A simple clear command (^L) will clear the text message.



Every end-user notification message also triggers an alert that notifies security specialists about the incident and updates the user's risk score – consistent with all other alerts.

Below are some commonly requested policy notification use cases supported with ObserveIT 6.5:

- Accessing Cloud Storage or Backup sites that are not allowed by policy
- Connecting USB Storage Devices (including mobile phones)
- Running suspicious hacking or monitoring tools
- Using sensitive administration tools or configurations, such as Registry Editor, Microsoft Management Studio, PowerShell, Firewall settings, etc.
- Browsing websites with unauthorized content (e.g., gaming, porn, movies, p2p, downloads, etc.) or sites with potential security risk (i.e., low ranking sites)
- Attempting to gain higher user privileges (e.g., su, sudo, running application as Administrator)
- Trying to access another computer remotely or trying to log in from outside the organization

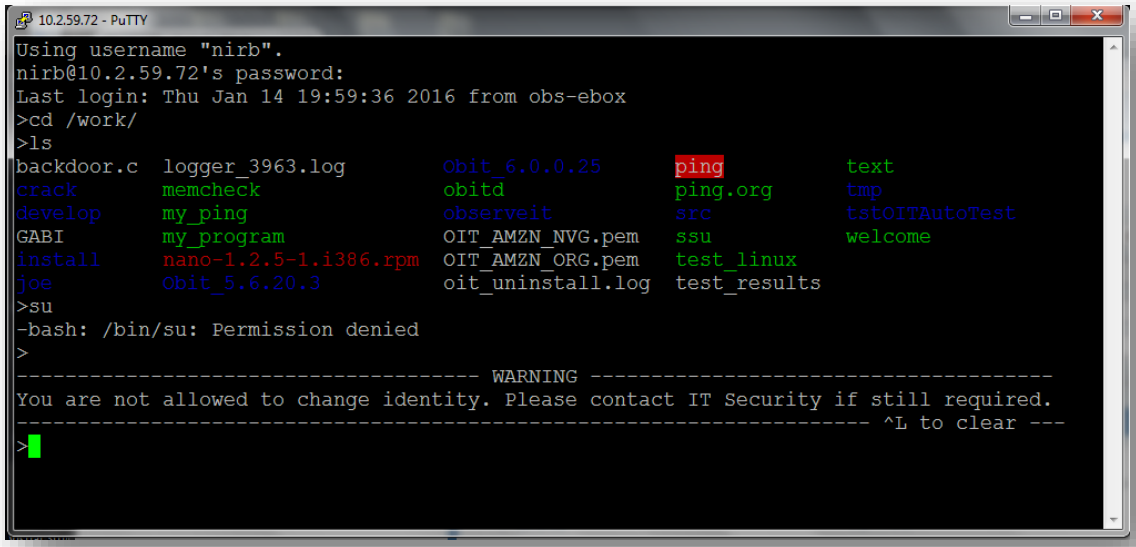
POLICY ENFORCEMENT: PREVENT MALICIOUS OR UNAUTHORIZED ACTIVITY

ObserveIT 6.5 can stop unauthorized Linux commands from being executed based on flexible Prevention rules defined by customers.

Prevention rules are based on:

- User identity (login account, secondary identification, Active Directory group membership, etc.)
- Command names (e.g., su, sudo, rm) combined with specific command line arguments and switches
- Computer details (computer name, IP address, Operating System and more)

When a Policy Enforcement rule is triggered, the end user gets the standard operating system “Permissions denied” message together with an optional message configured by security administrators.



USER BEHAVIOR CHANGE: TRACK POLICY VIOLATIONS AND NOTIFICATIONS

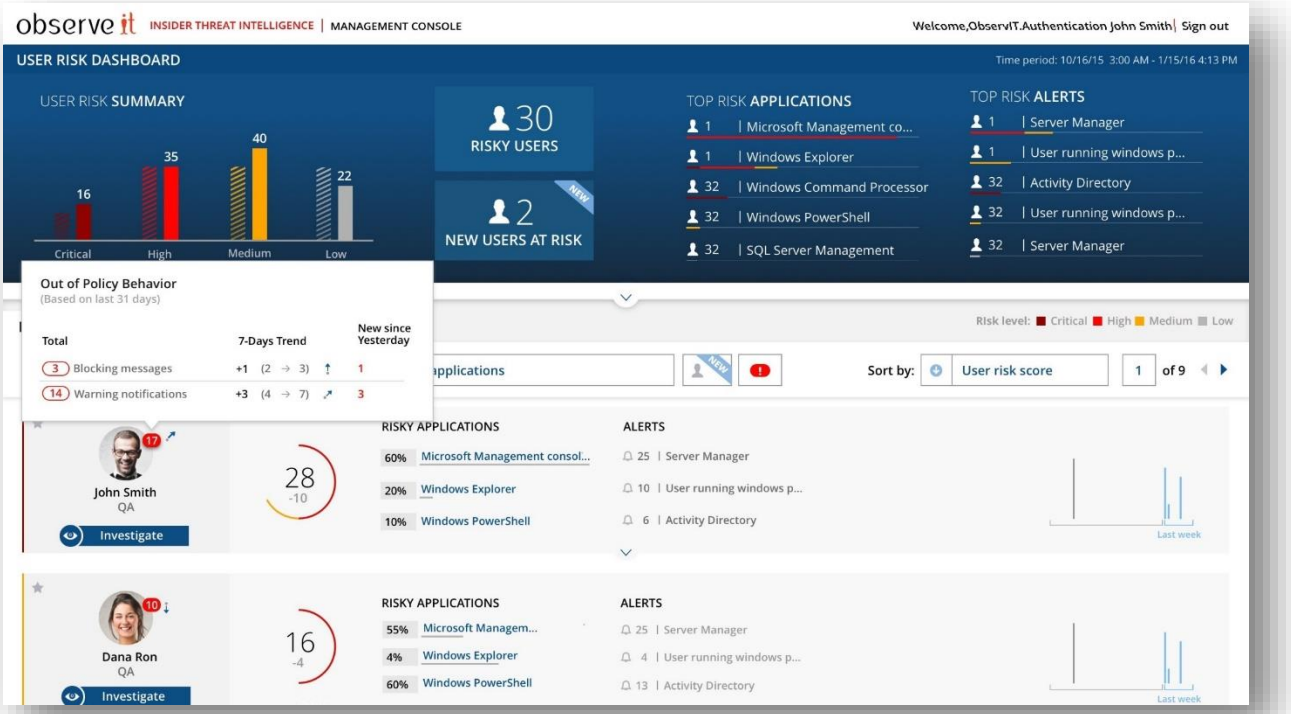
The ObserveIT 6.5 User Risk Dashboard provides Security Analysts and Investigators with an easy way to track users that have experienced any type of policy notification or enforcement as a result of violating company policy or security rules. It also can quickly pinpoint the users with the highest number of policy violations, as well as those who are not improving with time.

As seen below, a red tag with the number of out-of-policy notifications is displayed next to the risky user’s photo. A trend arrow to the right of the red tag indicates whether or not the user behavior has improved with time. For more details, a tooltip shows extra information about the types of violations involved so analysts can drill down to view full details of any incident including playing the video recording.

The detailed information inside the tooltip helps analysts to quickly learn about the change in user behavior by providing the following metrics:

- **Total count:** Breakdown notification count by the type of out-of-policy behaviors, whether Warning Notification, Blocking Message, or Denied Access.
- **7-day Trend:** Compare the number of notifications during the last 7 days with the number of notifications during the 7 previous days.
- **New since Yesterday:** Show the total number of notifications that occurred since yesterday.

The risky user list can be filtered and sorted according to the number of out-of-policy notifications and behavior trends – providing an easy way to identify those users who constantly violate security policies and those who keep ignoring them despite being warned or even blocked.

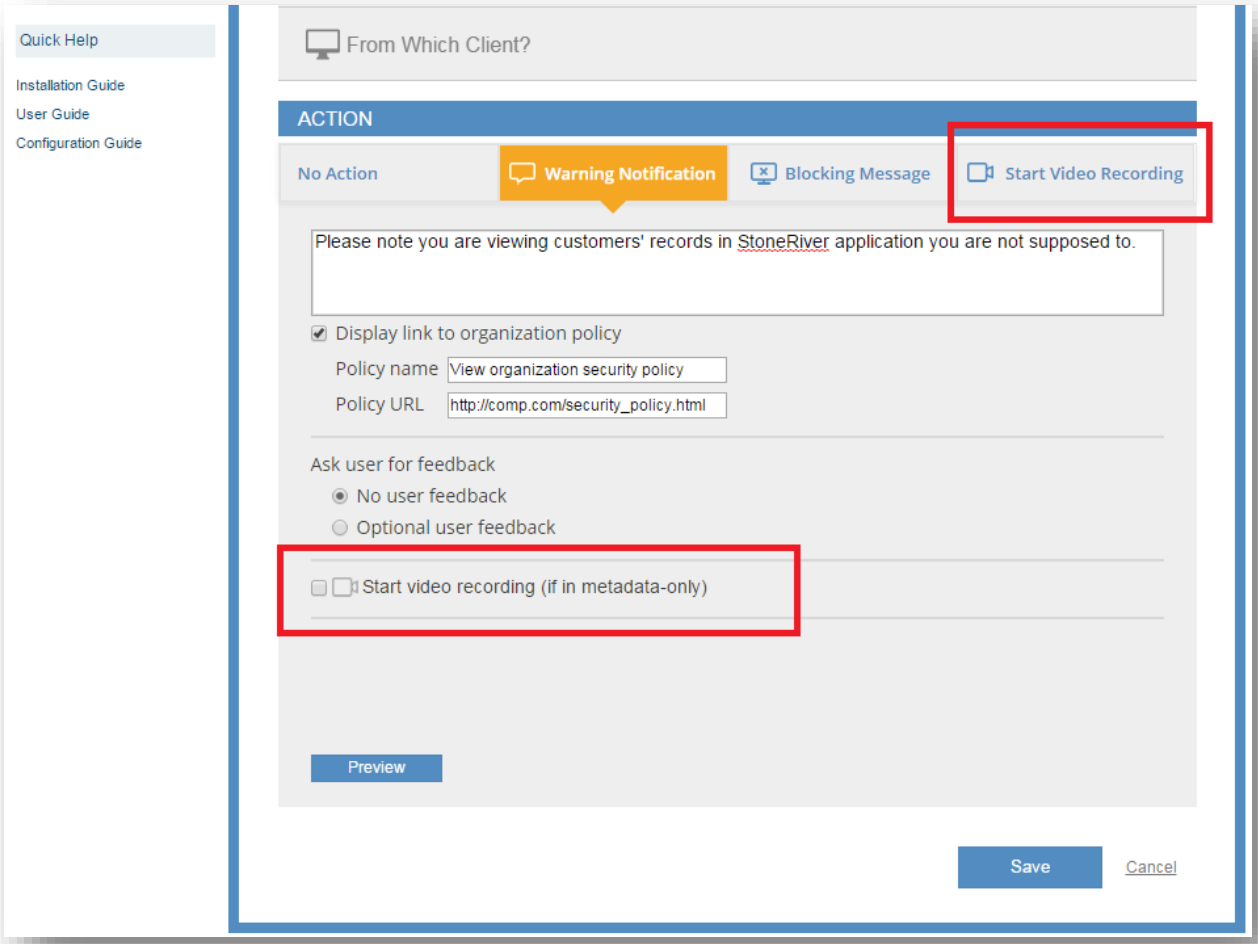


Dynamic Forensic recording: Determine intent of high risk activity

ObserveIT also helps to protect end-user privacy and reduce storage requirements by providing a new capability for activating video recording **only when a specific alert is triggered**.

Setting the recording policy to 'metadata only' will provide ObserveIT with all the activity data required for analyzing user behavior – without disclosing any sensitive data that might appear on the user screen.

A new "Start video recording" action in the Alert/Policy Rule will add video recording until the end of the user session once the security incident occurs and the alert has been triggered.

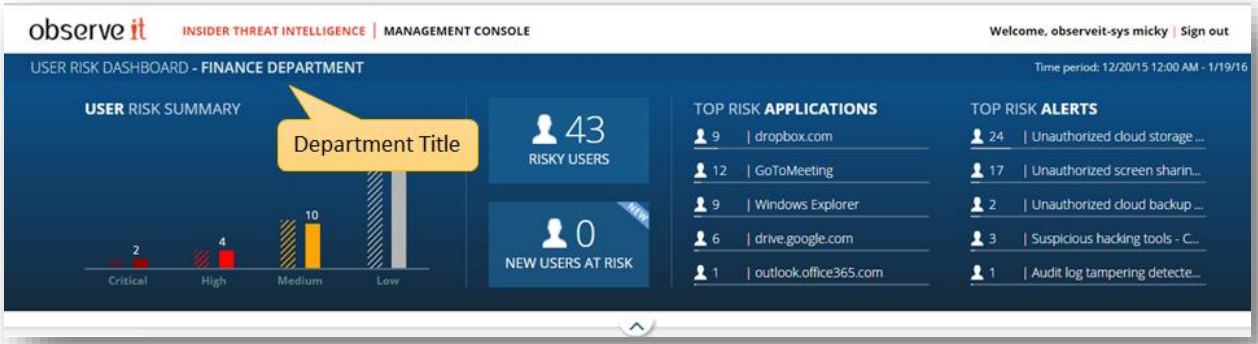


DEPARTMENT LEVEL RISK MANAGEMENT VIA GROUP BASED PERMISSIONS

ObserveIT 6.5 allows large organizations to manage the risk of their employees in separate departments or groups – each owned by a dedicated security team member or manager.

The monitored users of each department are configured based on Active Directory Groups/Users ensuring full segregated permissions across the product – including all risky user data, risk summary statistics, session recordings, alerts and reports.

In addition, you can set a title for the department or group. The title will be displayed in the User Risk Dashboard's header helping security staff members to quickly understand the scope they are viewing.



DETECT POTENTIAL DATA LEAKS WHEN COPYING FILES OR CONNECTING USB DEVICES

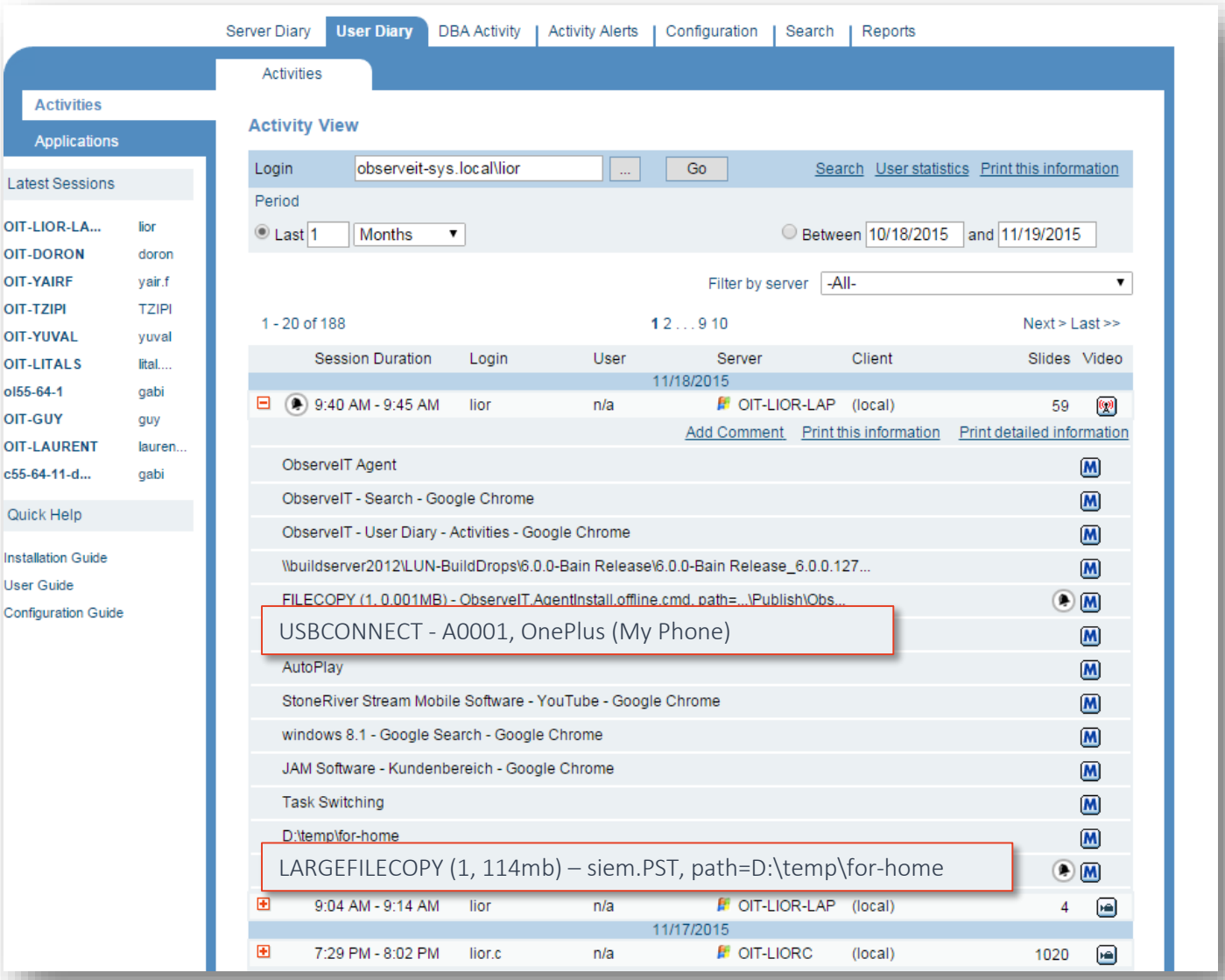
ObserveIT 6.5 enriches the recording metadata by capturing new user activity, including a potential data leak:

If there are attempts to move files (or folders) by copying them to the clipboard or dragging them with the mouse, ObserveIT immediately captures the names of the files as well as their source location and size. Thresholds can be defined to indicate a LARGE file copy based on the number of files being copied and/or their total size.

If the user connects any USB Storage device (including mobile phones), ObserveIT immediately captures the device description (i.e., model and manufacturer) and the mapped drive letter. Note that non-storage USB devices such as USB keyboard or mouse – are not recorded to avoid unnecessary noise.

This new metadata is fully integrated across the product, allowing customers to detect and deter any out-of-policy behavior or risky activity of their employees with regard to file copying and data exfiltration through USB Storage Devices.

Users can define alerts when sensitive files are being copied, pop up a blocking message when a USB Storage Device is connected, generate reports, search for specific files being copied, and export the new metadata to their favorite SIEM system.


Server Diary
User Diary
DBA Activity
Activity Alerts
Configuration
Search
Reports
Activities
Activities
Applications
Latest Sessions
OIT-LIOR-LA... lior
OIT-DORON doron
OIT-YAIRF yair.f
OIT-TZIPI TZIPI
OIT-YUVAL yuval
OIT-LITALS lital....
oI55-64-1 gabi
OIT-GUY guy
OIT-LAURENT lauren...
c55-64-11-d... gabi
Quick Help
Installation Guide
User Guide
Configuration Guide
Activity View
Login observeit-sys.local\lior
Go
Search
User statistics
Print this information
Period
Last 1 Months
Between 10/18/2015 and 11/19/2015
Filter by server -All-
1 - 20 of 188
1 2 . . . 9 10
Next > Last >>
Session Duration
Login
User
Server
Client
Slides
Video
11/18/2015
9:40 AM - 9:45 AM lior n/a OIT-LIOR-LAP (local) 59
Add Comment
Print this information
Print detailed information
ObserveIT Agent
ObserveIT - Search - Google Chrome
ObserveIT - User Diary - Activities - Google Chrome
\\buildserver2012\LUN-BuildDrops\6.0.0-Bain Release\6.0.0-Bain Release_6.0.0.127...
FILECOPY (1, 0.001MB) - ObserveIT.AgentInstall.offline.cmd, path=...\Publish\Obs...
USBCONNECT - A0001, OnePlus (My Phone)
AutoPlay
StoneRiver Stream Mobile Software - YouTube - Google Chrome
windows 8.1 - Google Search - Google Chrome
JAM Software - Kundenbereich - Google Chrome
Task Switching
D:\temp\for-home
LARGEFILECOPY (1, 114mb) – siem.PST, path=D:\temp\for-home
9:04 AM - 9:14 AM lior n/a OIT-LIOR-LAP (local) 4
11/17/2015
7:29 PM - 8:02 PM lior.c n/a OIT-LIORC (local) 1020

DOUBLED PACKAGED ANALYTICS AND ADDED IMPORT/EXPORT ABILITY

UPDATED OUT-OF-THE-BOX DETECTION RULES

ObserveIT 6.5 Packaged Analytics has been enriched with additional and improved out-of-the-box detection rules. It includes:

- 40 new rules - most of them are active by default and require no additional configuration.
- New rules addressing data leak detection capabilities of USB insertion and copying large files.
- New sample rules demonstrating the usage of soft and hard preventive actions.

All rules have been categorized into one of the following security categories to help navigation and management:

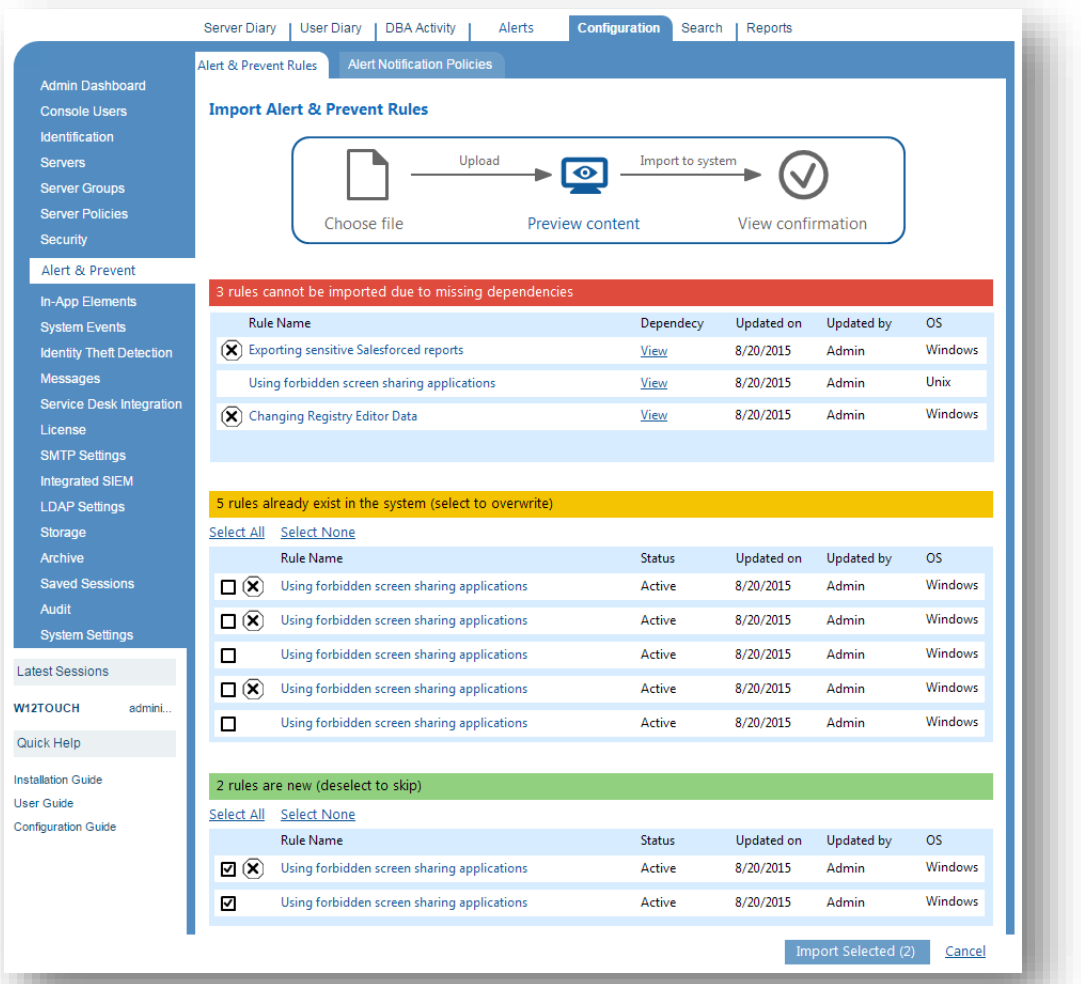
- Account compromise
- Backdoor detected
- Information seeking
- Malicious activity
- Potential data loss
- Privilege elevation
- Suspicious access
- Suspicious activity
- Suspicious SQL activity
- System tampering
- Unauthorized access

IMPORT & EXPORT OF DETECTION RULES

ObserveIT 6.5 introduces Import & Export capabilities for Alert and Policy Rules and their related actions, allowing customers to:

- Enjoy recent updates of ObserveIT Packaged Analytics (Detection Library) without needing to upgrade their system to the latest version.
- Easily migrate alert, policy, and prevention rules between staging or other environments (e.g., from POC to UAT to Production).

Exporting rules is done by simply selecting the rules you wish to export and providing the location for the export file. Importing rules is managed by a straightforward wizard notifying you in advance about any potential conflict or missing data on the target environment, so that you can quickly address it.



SECURITY AUTOMATION AND SCALE MANAGEMENT

As in every ObserveIT release, ObserveIT 6.5 adds Security Automation and Scale Management features for large-scale enterprise deployments with multiple Desktops and Servers.

- **Improved database scalability and performance, including:**
    - Dramatically reduced Archive process time - by up to 70%
    - Leverage SQL Server Enterprise Edition® capabilities such as data partitioning and compression
    - Reduce Unix/Linux meta-data storage size by order of magnitude

- **FIPS Compliant Agent:**
    - Both Windows and Unix/Linux agents now comply with the FIPS security standard and can be deployed on any supported FIPS-enabled machine.
    - TLS protocol is supported for communication between the agent and the application server
- **Tamper-proof Windows Agent that cannot be killed due to enhanced watchdog mechanism**