WHAT'S NEW IN OBSERVEIT 6.7

ObserveIT 6.7 introduces a comprehensive solution to Identify and Eliminate Insider Threats.

A new Insider Threat Library (ITL) significantly increases the out-of-the-box value by providing greater visibility to user risks and intents, with virtually no setup time.

Alerts are now more accurate, leveraging newly-collected metadata such as website categories and file print detection, and are triggered only for the relevant group of users - whether administrators, everyday users, remote vendors, or terminated employees.

With ObserveIT 6.7, you can efficiently manage large sets of alert rules, integrate data from your HR systems, and better protect employee privacy by anonymizing personal user information in the ObserveIT console.

And last but not least – the Mac agent is now available (as Beta), so you can start observing your Mac users too!

MAJOR PRODUCT ENHANCEMENTS IN 6.7

Increase value and reduce alert noise with a rich and optimized alert rule library

- ✓ Insider Threat Library (ITL) – 180 out-of-the-box alert rules
- ✓ Rules are mapped to privileged or everyday users, remote vendors, terminated employees, and so on
- ✓ Ability to assign a different risk level for each specific user group

Efficient alert rule management

- ✓ Group alert rules by Categories
- ✓ Create lists of users or keywords and reuse them in alert rules
- ✓ Easily assign alert rules to multiple user lists with a specific risk level per List
- ✓ Bulk alert rule actions – delete or activate multiple alert rules at once

Increase visibility to user activity and risk

- ✓ Website Categorization – know when users visit illegal, phishing, harmful sites, etc. (more than 28 billion indexed URLs).
- ✓ Print job monitoring – track any file printing sent either to a local or network printer
- ✓ New graph in the Dashboard helps you to understand user risk and behavior trend over a specified period of time.

Better protect employee privacy

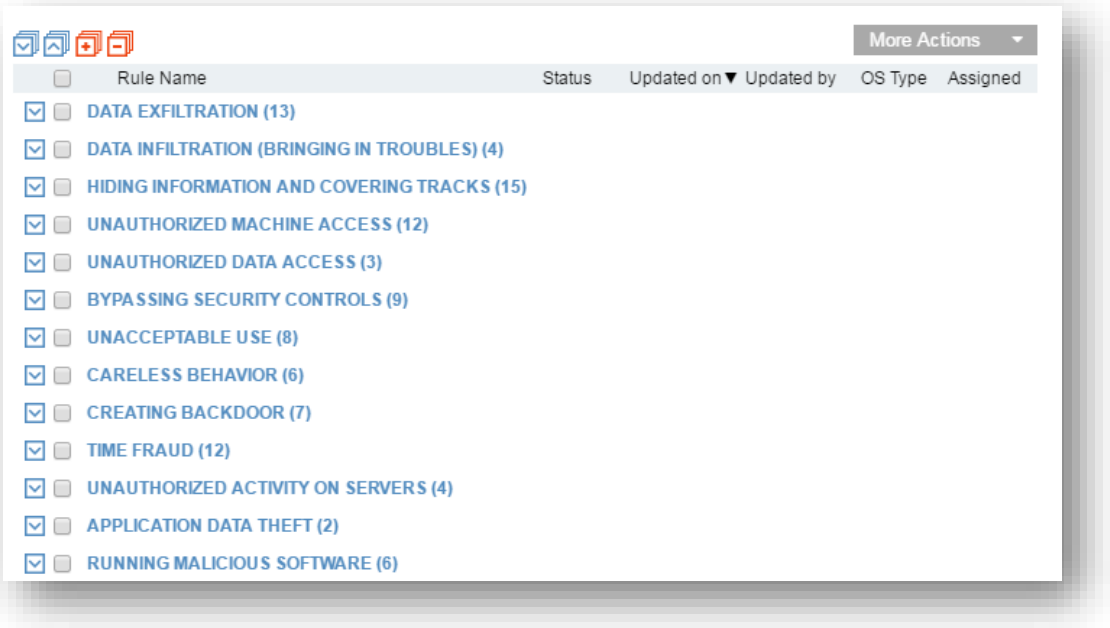
- ✓ Anonymize users and personal information in the Dashboard and Web Console
- ✓ Integrate with HR lists (e.g., terminating employees) and manage them privately

Expand to more platforms

- ✓ *New* Mac agent (Beta)
- ✓ Windows 10 support (including Edge Browser)
- ✓ Ubuntu 16.04 support
- ✓ RHEL 7.2 support

COMPREHENSIVE INSIDER THREAT LIBRARY

ObserveIT 6.7 introduces a fully renovated Insider Threat Library (ITL) for detecting over 180 risky user scenarios out-of-the-box. The rules are already active, grouped into Categories for ease of management, and already assigned to specific user Lists with an appropriate risk level.



Insider Threat Library – comprehensive coverage of common risk categories

The new Library takes advantage of newly available metadata such as Website Categorization. For example, to detect users visiting Job Searching or Phishing sites, you don't need to manually list those websites; ObserveIT will categorize the visited sites for you in real-time.

Privileged Users and Everyday user lists are prepopulated based on common Active Directory groups. You can modify these lists, and easily create or populate other lists (such as, Remote Vendors, Terminating Employees, and so on) by assigning individual users or Active Directory groups to the lists.

Other "General" lists are either prepopulated (e.g., list of Hacking Tools process names) or empty (e.g., list of sensitive file names), allowing you to simply add or edit items to fine-tune the Library for detecting your specific insider risks.

You can activate/inactivate library rules, create new user lists, assign specific rules to these lists, and even duplicate and change specific alert rules according to your specific needs.

Full Import/Export capabilities are available, allowing you to migrate all your library changes between various environments, and to easily deploy new library content that is available.

The following Security Categories are provided as part of the ObserveIT Insider Threat Library:

- ✓ APPLICATION DATA THEFT
- ✓ BYPASSING SECURITY CONTROLS
- ✓ CARELESS BEHAVIOR
- ✓ COPYRIGHT INFRINGEMENT
- ✓ CREATING BACKDOOR
- ✓ DATA EXFILTRATION
- ✓ DATA INFILTRATION (BRINGING IN TROUBLES)
- ✓ HIDING INFORMATION AND COVERING TRACKS
- ✓ INSTALLING/UNINSTALLING QUESTIONABLE SOFTWARE
- ✓ PERFORMING UNAUTHORIZED ADMIN TASKS
- ✓ RUNNING MALICIOUS SOFTWARE
- ✓ SEARCHING FOR INFORMATION
- ✓ TIME FRAUD
- ✓ UNACCEPTABLE USE
- ✓ UNAUTHORIZED ACTIVITY ON SERVERS
- ✓ UNAUTHORIZED DATA ACCESS
- ✓ UNAUTHORIZED MACHINE ACCESS
- ✓ USING UNAUTHORIZED COMMUNICATION TOOLS
- ✓ IDENTITY THEFT
- ✓ IT SABOTAGE
- ✓ PERFORMING PRIVILEGE ELEVATION
- ✓ PREPARATION FOR ATTACK
- ✓ SHELL ATTACK
- ✓ UNAUTHORIZED SHELL OPENING
- ✓ SYSTEM TAMPERING

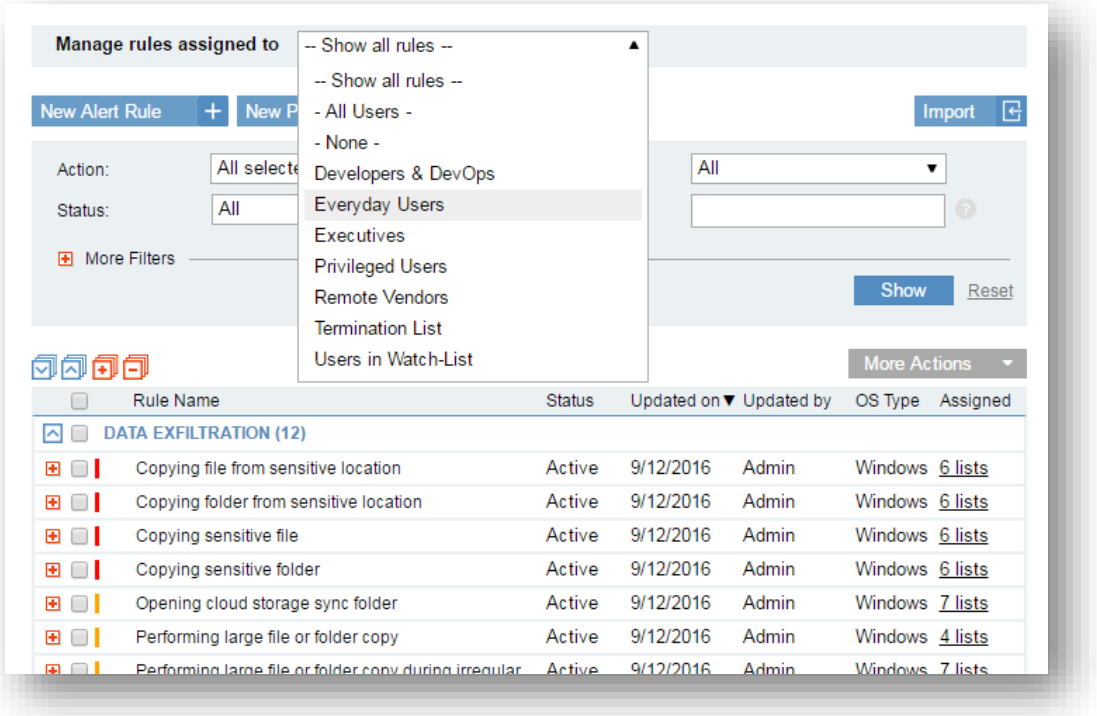
Following is a sample of some of the Windows alert rules that are provided as part of the ObserveIT library:

ALERT RULE CATEGORY	ALERT RULE
✓ DATA EXFILTRATION	▪ Printing large number of pages during irregular hours ▪ Printing sensitive documents ▪ Copying sensitive file or folder ▪ Performing large file or folder copy during irregular hours ▪ Uploading or sharing files via cloud storage services
✓ HIDING INFORMATION AND COVERING TRACKS	▪ Running steganography tools ▪ Clearing browsing history
✓ PERFORMING UNAUTHORIZED ADMIN TASKS	▪ Running Command Line Shell programs as Administrator
✓ RUNNING MALICIOUS SOFTWARE	▪ Running hacking or spoofing tools
✓ CARELESS BEHAVIOR	▪ Storing passwords in clear text ▪ Browsing Phishing sites
✓ APPLICATION DATA THEFT	▪ Executing sensitive SQL commands in DBA tools
✓ DATA INFILTRATION (BRINGING IN TROUBLES)	▪ Connecting USB Storage Device ▪ Browsing harmful, risky or contaminating sites
✓ BYPASSING SECURITY CONTROLS	▪ Accessing the Darknet using TOR (The Onion Router)
✓ PERFORMING UNAUTHORIZED ADMIN TASKS	▪ Running Windows management tools
✓ SEARCHING FOR INFORMATION	▪ Searching data on hacking or spoofing
✓ TIME FRAUD	▪ Browsing job searching sites ▪ Browsing various counter-productivity sites
✓ UNACCEPTABLE USE	▪ Browsing Gambling/Adults/Illegal-Drugs sites

EFFICIENT ALERT RULE MANAGEMENT

ObserveIT 6.7 allows you to manage a large set of rules efficiently:

- Manage alert rules by expanding/collapsing categories allowing you understand your risk coverage in each risk category and to locate rules quickly.
- Quickly understand which alert rules are assigned to which users, with their assigned risk level.
- Understand which alert rules are not yet assigned to specific users – and easily assign them.
- Perform bulk actions on a large set of rules, for example, activate, inactivate or delete multiple alert rules simultaneously.
- Re-use common lists across multiple rules, such as, lists of sensitive file names or lists of keywords.
- Import/Export alert rules including the lists that are used by the rules.



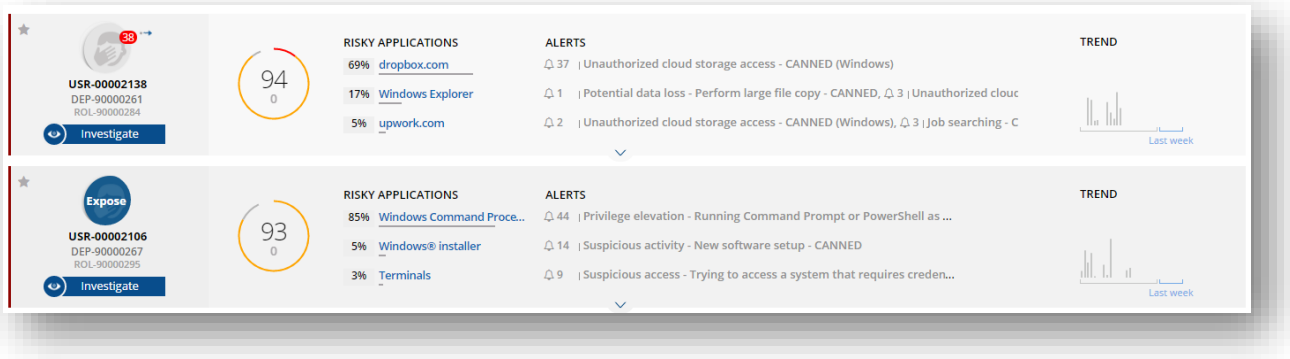
Viewing all alert rules assigned to a specific user group

PROTECTING USER PRIVACY: ANONYMIZING USER DETAILS

ObserveIT 6.7 addresses new privacy laws in Europe, helping you to comply with privacy regulations and concerns worldwide, by configuring ObserveIT to work in Anonymization mode.

In Anonymization mode, all personal user information in the Dashboard and the Web Console is encoded – so there is no way to tell the name of the user, the role or department, or see the user's personal photo. In addition, computers that are accessed and login accounts being used are anonymized.

As a result, a Security Analyst or an Investigator using the system, can still get detailed visibility to the risky users including their alerts and activity, but without their personal identity being exposed.

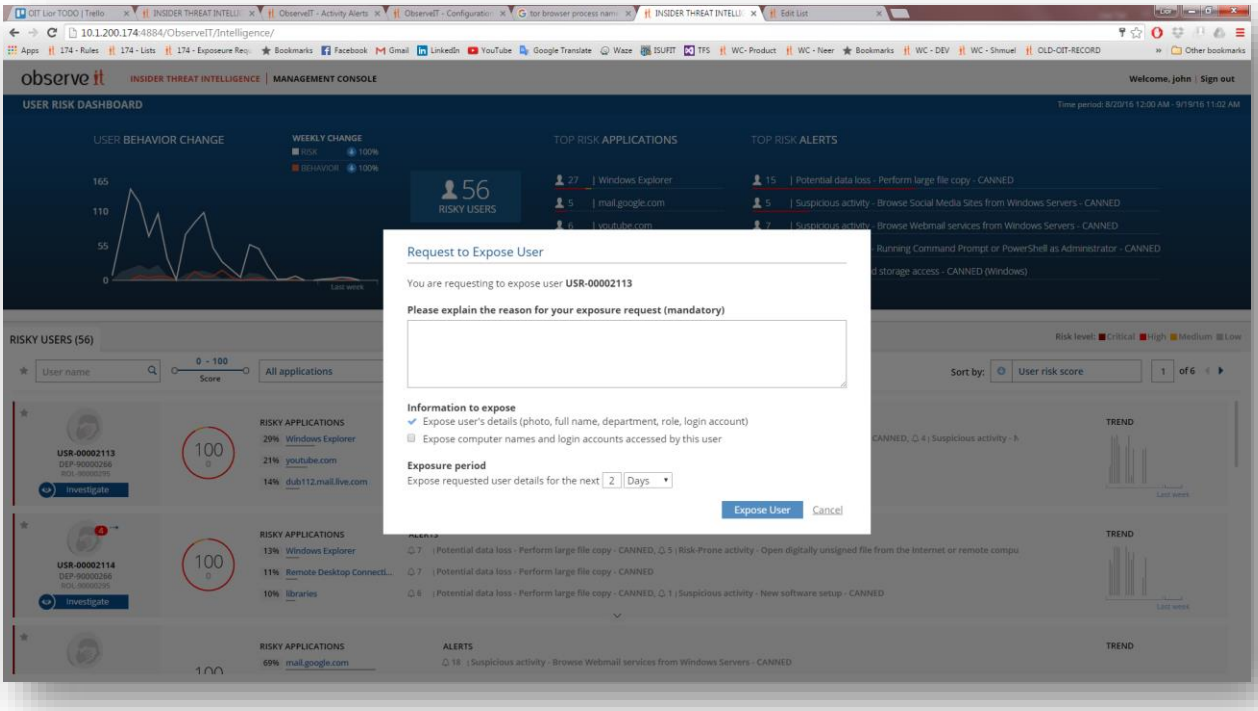


Anonymized users in the ObserveIT Dashboard

If there is a need to expose user details during the investigation process, an Exposure Request is submitted, and the request is reviewed and approved (or rejected) by an authorized administrator acting as the Privacy Officer.

ObserveIT supports the full process of submitting exposure requests, approving or rejecting them - including notification emails sent to the requester or the approver correspondingly. The Privacy Officer can review all historical requests, and cancel active requests if needed.

In addition, exposure requests have an expiration date; once expired – the user becomes anonymized again.



Form requesting to expose user details in an anonymized ObserveIT Dashboard

In addition, it is possible to exclude certain users or groups from being anonymized (e.g., Remote Vendors) and allow high rank individuals (e.g., the CISO) to view data in the clear (i.e., not anonymized).

INCREASE VISIBILITY: WEBSITE CATEGORIZATION

ObserveIT 6.7 provides high visibility into your employees' web browsing habits. Using a world-leading URL Filtering technology, ObserveIT can automatically categorize any visited website and alert when browsing phishing, harmful, counter-productive websites, or websites that are not allowed by policy or are suspicious for specific individuals.

Examples of risky scenarios:

- Everyday employee (not an administrator) browsing websites discussing sniffing or hacking techniques
- Employees accessing cloud storage or cloud transfer sites
- Display a blocking message to the user when accessing a malicious or a phishing website
- Using servers for non-work-related tasks such as P2P services, social media, watching online videos, etc.
- Searching data on Darknet, illegal drug sites, violence, or any other legal-sensitive websites
- Employees wasting time in gaming, gambling, sports or news websites

You don't need to know these websites in advance. ObserveIT has over 28 billion indexed URLs that are updated on a daily basis to keep you up-to-date with new websites and new security risks.

Website Categorization is provided with no extra fee and supports flexible deployment modes whether your server can access the internet directly or via a protected proxy.

Note that even if you have a Web Filtering solution deployed in your organization, ObserveIT Web Categorization capabilities can help you detect unacceptable use amongst those websites that you still allow employees to access.

Built-in Website Categories include the following:

Malicious, Infected/Malicious, Phishing, DDNS Services, Remote Proxies, Copyright Sensitive, Legal-Sensitive, Adults, Illegal Drugs, Gambling, Search Engines & Portals, Job Searching, Downloads, Music, News, Sports, Gaming, Shopping, Social Media Site, Streaming, Storage, Counter-Productivity, Web Mail, Chats, Instant Messaging, P2P, Ads.

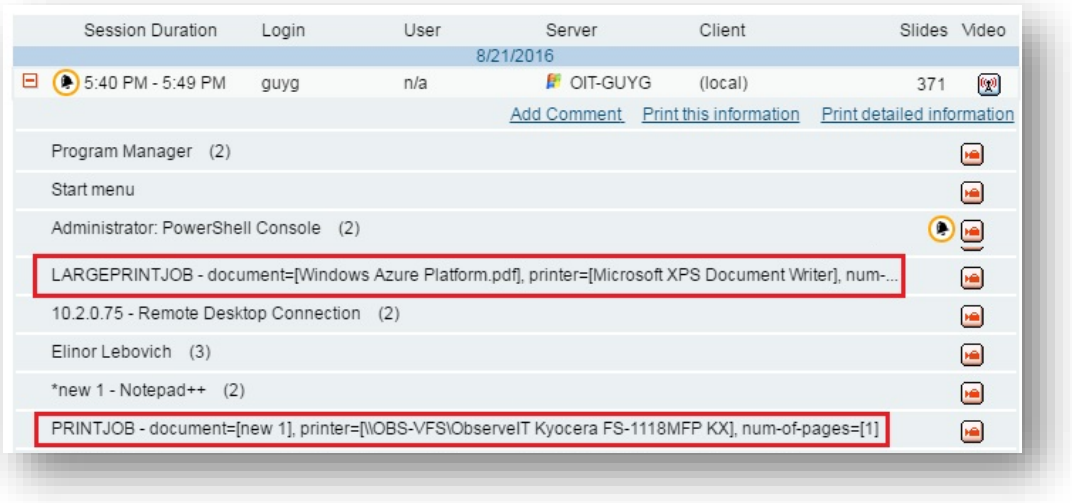
INCREASE VISIBILITY: PRINT JOB MONITORING

Printing documents is a common way to exfiltrate company data. ObserveIT 6.7 can monitor any print job that is sent to the printer, by providing the following information:

- Details about the user/computer who printed the file
- Name of the document being sent to the printer
- Printer name, including manufacturer's name
- Number of pages sent to the printer
- Whether a large number of pages (10 or more) were sent to the printer

Both local and network printers are supported.

Similar to any other user activity in ObserveIT, you can search for printing activity, create alerts and reports, and export print job activities to your favorite SIEM.



Printing activities captured and displayed in the Server Diary

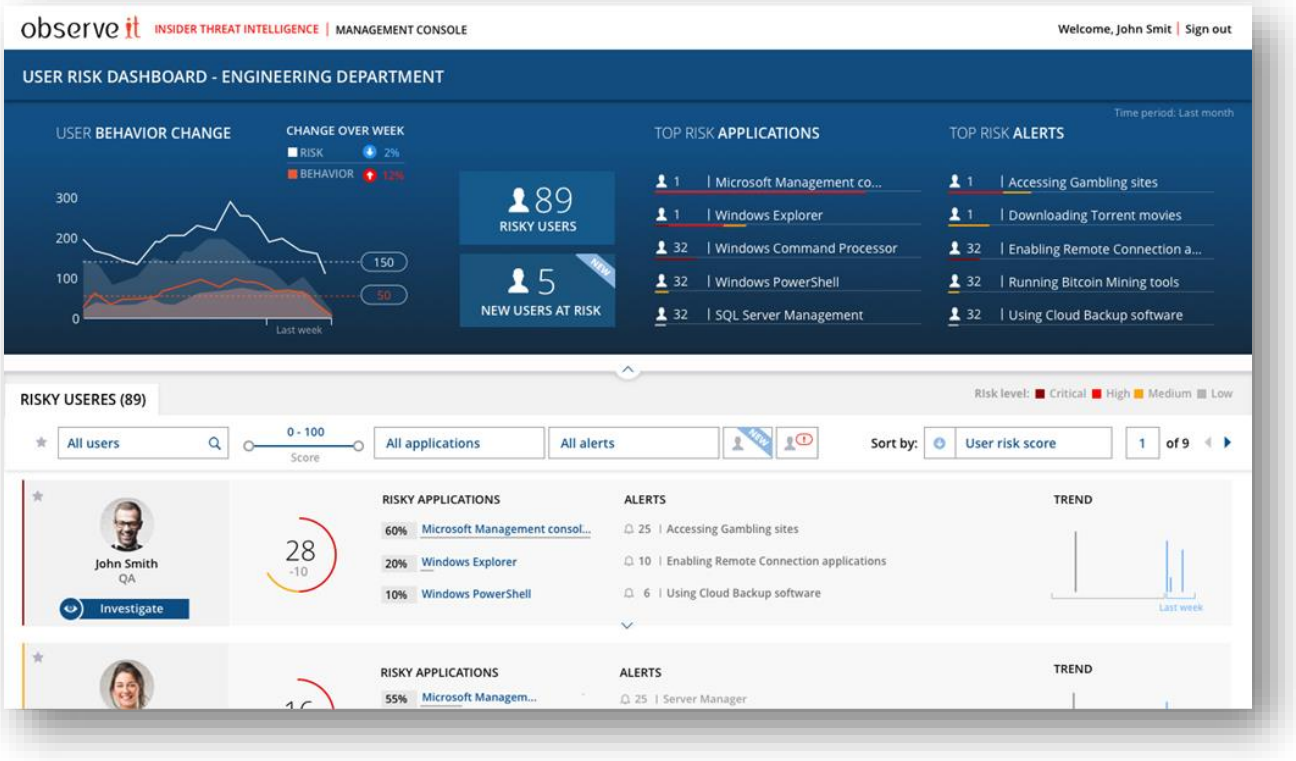
USER RISK AND BEHAVIOR TREND GRAPH

A new graph in the User Risk Dashboard allows you to track your overall risk and behavior trends over a period of time.

The graph shows the number of alerts that were triggered each day (white line), the number of out-of-policy notifications displayed to users each day (orange line), and the number of users involved in those alerts and notifications (area graphs).

You can quickly tell whether the risk has increased or decreased overtime, compare to last week's average, and see how policy notifications reduce the overall risk.

Similar to all other data in the Dashboard, the information presented in the graph is restricted to what the specific console user is permitted to see.



ObserveIT Dashboard with user risk and behavior trend graphs

LISTS

ObserveIT 6.7 introduces a new List module allowing you to easily manage two main types of lists:

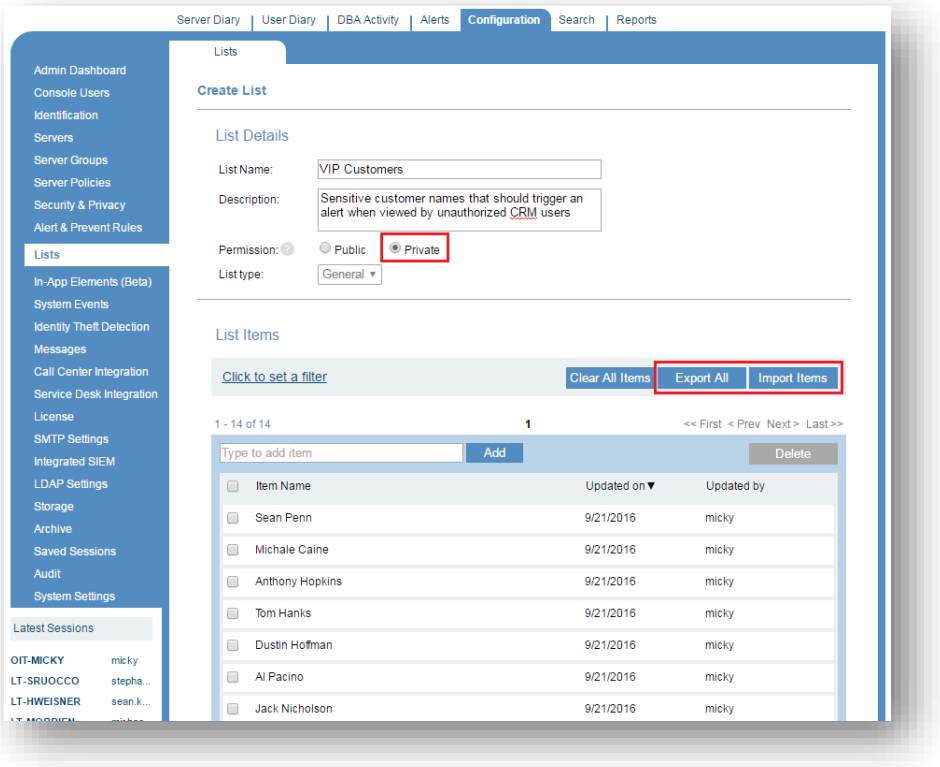
- **User lists** – lists of users and/or Active Directory groups that can be used for alert rule definition or assignment. For example: Everyday users, privileged users, remote vendors, terminating employees, etc.
- **General lists** – lists of any keywords that can be used for alert rule definition. For example: VIP customers, politically exposed patients, work violence keywords, sensitive application names, allowed IP prefixes, etc.

Lists can be reused across multiple alert rules allowing you to manage them from a single location without the need to update multiple alert rules.

Lists enable integration with HR data that is available in your organization, hence providing richer content for the detection and investigation process.

All lists can be exported and imported as a comma-delimited format file (CSV), so for example, you can simply export your current "Employee watch-list" from your HR system and import it into your list in ObserveIT.

As list content can be sensitive, ObserveIT 6.7 allows you to protect the content of the list by setting the list to be private. The content of private lists can be viewed only by the user who made the list private.



Private list of sensitive VIP customers that was imported from an HR system

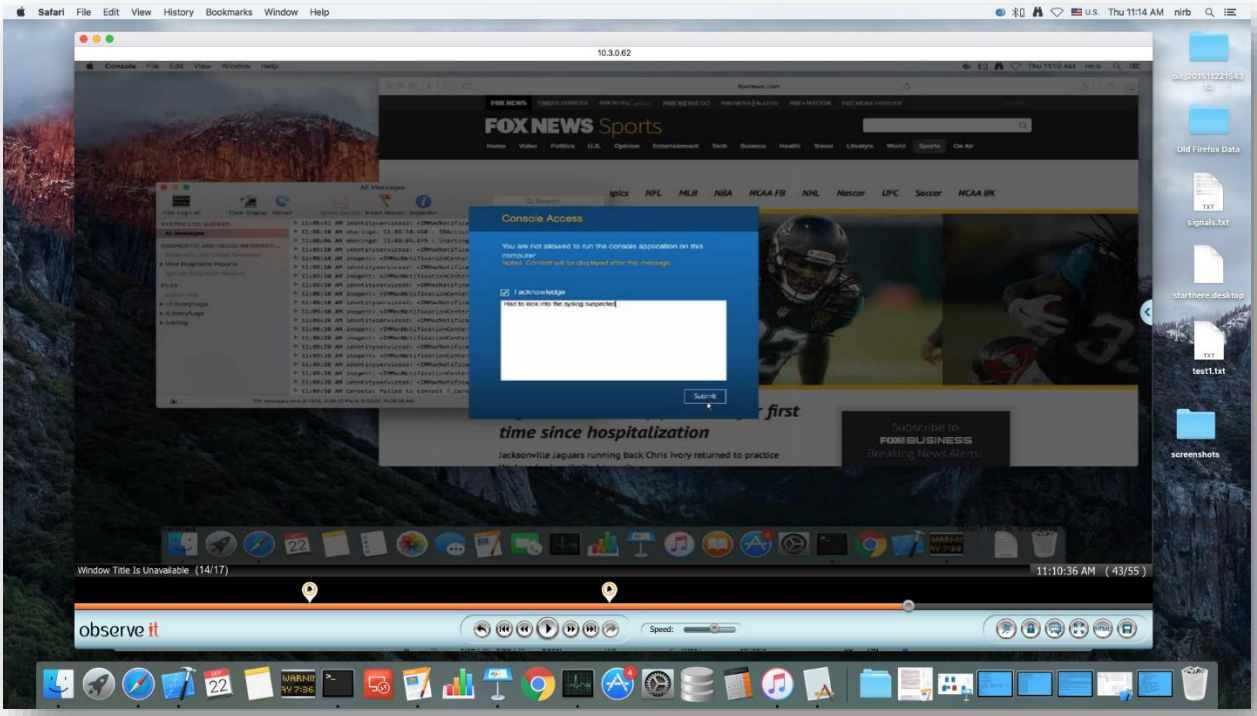
MAC AGENT (BETA)

To complete our enterprise coverage for endpoint monitoring, ObserveIT 6.7 introduces a new agent for Mac with full recording capabilities, including:

- Video and metadata recording
- Configurable recording policies (include/exclude users, applications, or URLs)
- Record when agent is offline
- Recording notification message
- Out-of-policy notifications (warning and blocking messages)
- Health monitoring – know if the agent is offline or has been tampered with

All the metadata that is collected from the Mac is searchable, reportable, can be alerted on, and can be exported to your favorite SIEM.

Risky activity that is performed on the Mac is consolidated with other risky activities from the same user, providing a unified risk score for the user and a user-centric view in the User Risk Dashboard.



ObserveIT Video Player running on the Mac and playing a recorded Mac session with a Blocking Message

NEW PLATFORMS

The following new platforms are now supported by ObserveIT 6.7 agents:

- Windows 10 (including Edge Browser)
- RHEL 7.2
- Ubuntu 16.04