observe IT
a division of Proofpoint

WHITE PAPER

Privacy and Visibility Best Practices

Insider Threat Management

Introduction

McKinsey found that approximately 50% of data breaches between 2014 and 2018 were driven by insiders. To address the risks of insider compromise, system misuse and data exfiltration, organizations want to collect user-related data in one place and with privacy in mind. With the explosion of data being collected by consumer firms and within the enterprise, multiple data privacy regulations have sprung up in the EU, multiple U.S. states and across industries.

Many of these data protection laws and privacy enforcements have identified similar strategic definitions for what information constitutes “personal data”. Additionally, they developed frameworks for how businesses and organizations are expected to protect client data and employee data, and how to collect, use, and dispose of the data. In many cases, security and privacy of personal data go together. The same regulations that stipulate the privacy needs around capturing a consumer’s data also emphasize the security goal of information around the access, manipulation, and authorized use of that data.

Table of Contents

8 General Best Practices for Data Collection

Best practices

It is challenging to figure out how to balance privacy and security. Based on our experience, it starts with collaborating with your HR, privacy, compliance and business peers to understand your work culture and compliance.

For example, if you face PCI DSS audits, then be aware of the visibility required on remote vendors and legacy applications that handle PII or personal financial information. If it's NISPOM Change 2, be aware of the visibility required on users as they interact with different classifications of data. Within ObserveIT Insider Threat Management (ITM), this starts with adapting data collection needs to your work culture and compliance environment.

Number 1 Consider the user data being collected by other systems to determine your baseline established privacy policies within your organization.

Number 2 Be transparent about the reasons for insider threat management program.

Number 3 Be clear about individuals about how any monitoring will operate.

Number 4 Review personal data regularly to check whether it is still needed for monitoring purposes.

Number 5 Put a policy in place explaining how long personal data should be kept.

Number 6 Put in place a clear well documented security and acceptable use policy. Ensure that is checked regularly, passed through HR, and kept up to date.

Number 7 Inform individuals what measures are in place to protect their data and of any significant changes that occur.

Number 8 Make sure that only staff who need to view this personal data are given access to it and are trained how to use it properly. Example: Restrict access to officers with responsibility for monitoring and equality rather than providing access to all human resources officers.

Common Privacy Recommendations

The most common questions typically asked around the data that ObserveIT Insider Threat Management (ITM) collects can be related to social media, personal financial information, as well as sensitive communications between individuals.

It is important to reiterate that no technical controls can substitute for transparent corporate security policies and strong security standards. In the realm of privacy-centric insider threat management, security and privacy policies often relate to acceptable use, access control, user right and confidentiality. The standards must implement data loss and insider threat protection and response, with user privacy at the forefront when there is no proof of wrongdoing yet.

General recommendations and best practices based on the following regulations can be seen adopted across multiple countries and multinational organizations. The collection of specific user data related to data loss, brand damage and other malicious acts by users and associated selective investigations have long been part of standard employment contracts within most corporate AUPs.

The rest of this section is based on the following Data Protection regulations:

- EU – GDPR
- U.S. – CCPA, NISPOM Conforming Change 2, PCI DSS, SOX & HIPAA/HiTech

Privacy concern 1

User's identity, job role, system, and metadata are exposed to anyone in the security team.

Administrative recommendation:

Anonymize personal data where possible, and only use information that identifies an individual where it is necessary.

Technical control:

ObserveIT ITM can obfuscate and pseudo-anonymize user data such as name, device, and relevant metadata such that security analysts are alerted about risky activity without the ability to view data that could identify a specific user. A Chief Privacy Officer or equivalent would then have to approve any request for revealing a user's data.

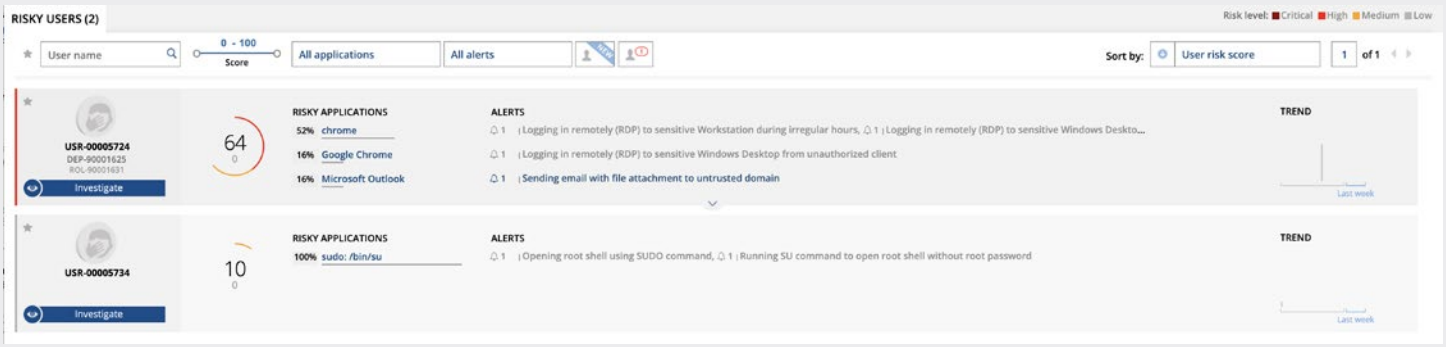

Figure 1: Anonymized risk dashboard.

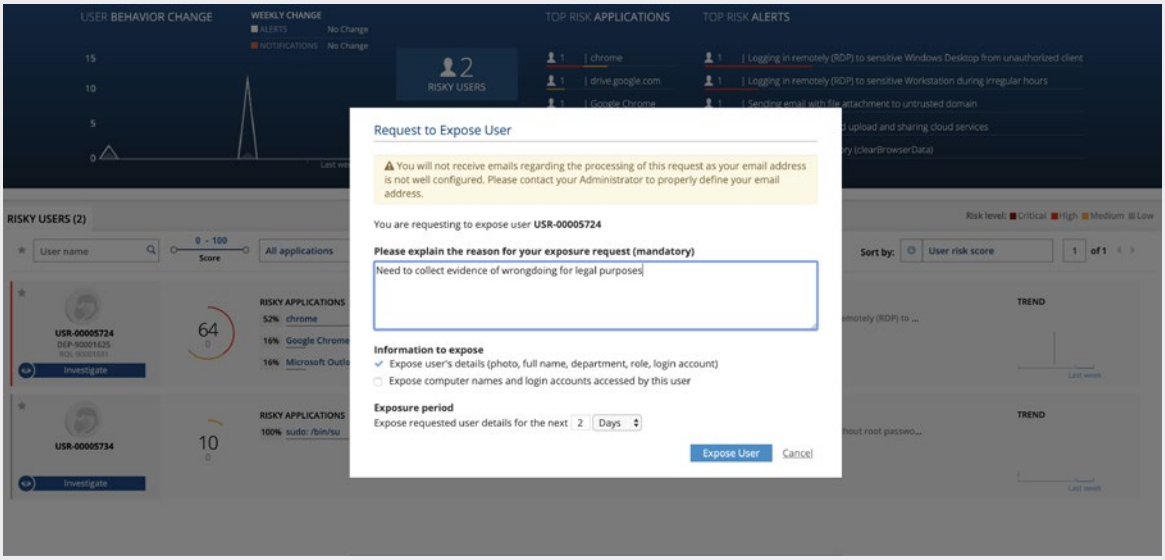

Figure 2: Exposer Request Workflow.

Privacy concern 2

Monitoring employees while they are accessing personal data on an endpoint such as financial, personal email, healthcare & social media websites or applications.

Administrative recommendation:

Exclude sensitive applications and personal data from being captured by ObserveIT.ITM. Adapt the controls based on the data protection laws in the location of user population.

Technical control:

Configure ObserveIT ITM metadata collection policies to not collect any user activity data when users access specific websites and applications. Use website categorization to assist in identifying HR, finance, healthcare, social media, personal email and other applications used for personal purposes. Modify web application exclusion lists based on user's residence to meet that country's data protection laws.

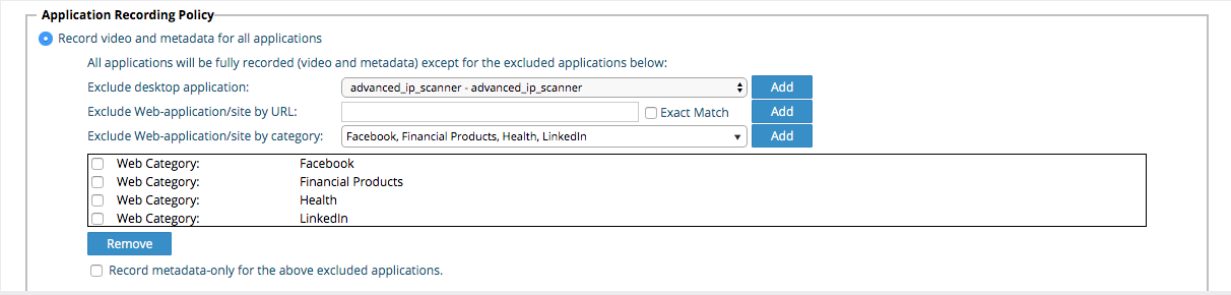

Figure 3: Application Exclusion Policies.

Privacy concern 3

Screen capture will expose personal data.

Administrative recommendation:

Use intelligent and privacy-aware screen capture of user activity. Ensure this is triggered only when a user breaks a significant acceptable use policy, instead of continuous monitoring.

Technical control:

ObserveIT policies can be configured to run in metadata-only mode for a user until that user takes an action considered severe enough to collect a visual activity replay for investigation purposes. The former metadata-only mode will only capture a textual break down of a user's session with no screen capture. Visual activity replay can be the proof of user intent as it provides the user's risky actions that caused the high severity alert and the subsequent actions immediately after the triggered alert.

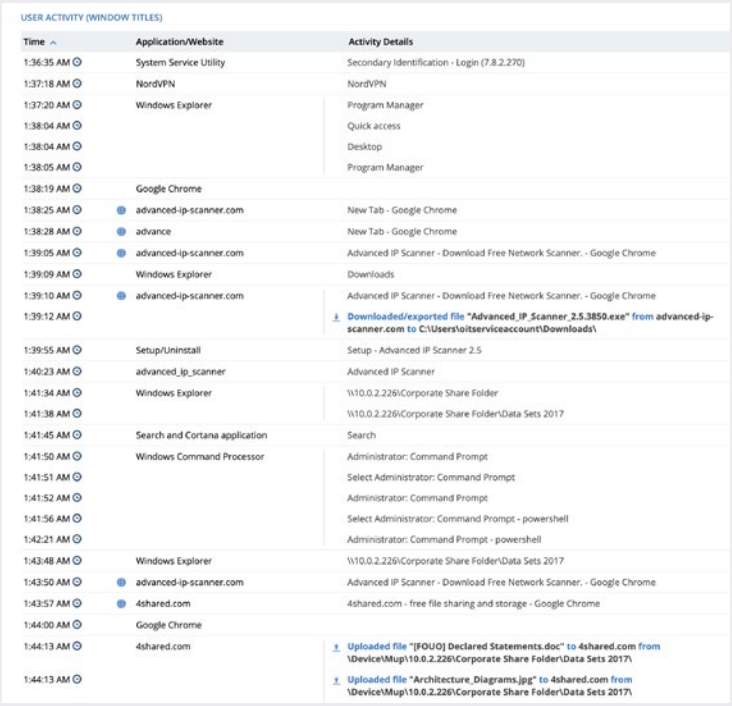

Figure 4: Metadata only in the ObserveIT Web Console.

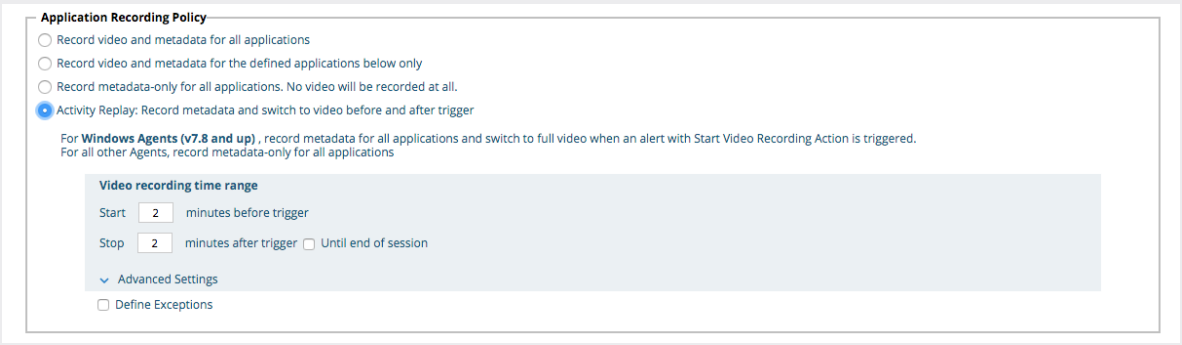

Figure 5: Visual Activity Replay.

Privacy concern 4

Ensuring fair use of access to the ObserveIT ITM web console.

Administrative recommendation:

Create console users, with the proper roles and permissions, so they only have access to the information they need within their job scope. Further protect the data collected with a master password.

Audit access, activity, and configuration changes to the ObserveIT ITM console.

Technical control:

ObserveIT ITM has granular role and permission delegation with Active Directory integration.

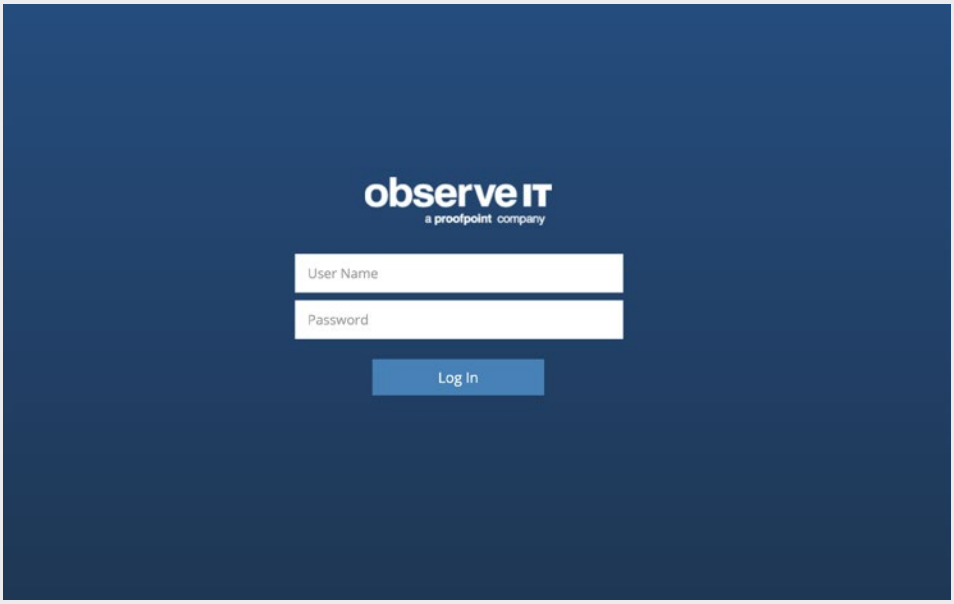

Figure 6: ObserveIT ITM Web Console login page.

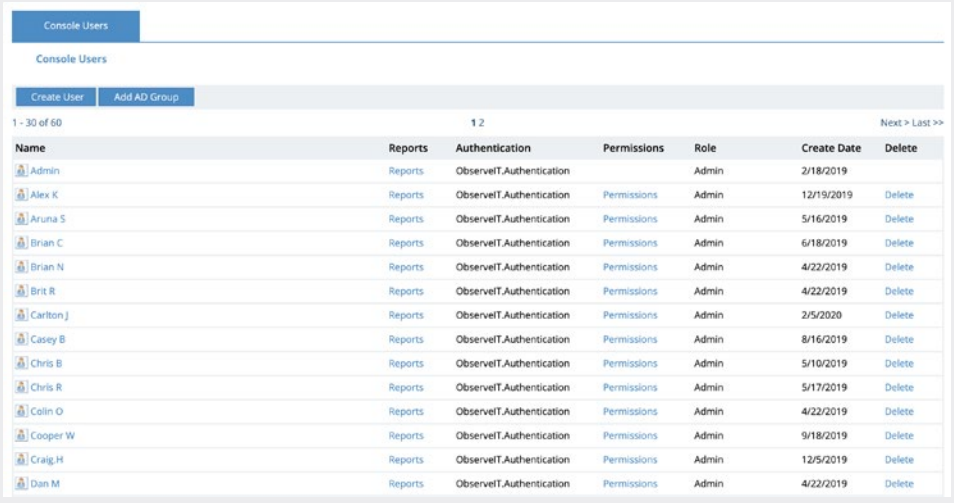

Figure 7: Granular roles and permissions can be assigned to individuals and groups.

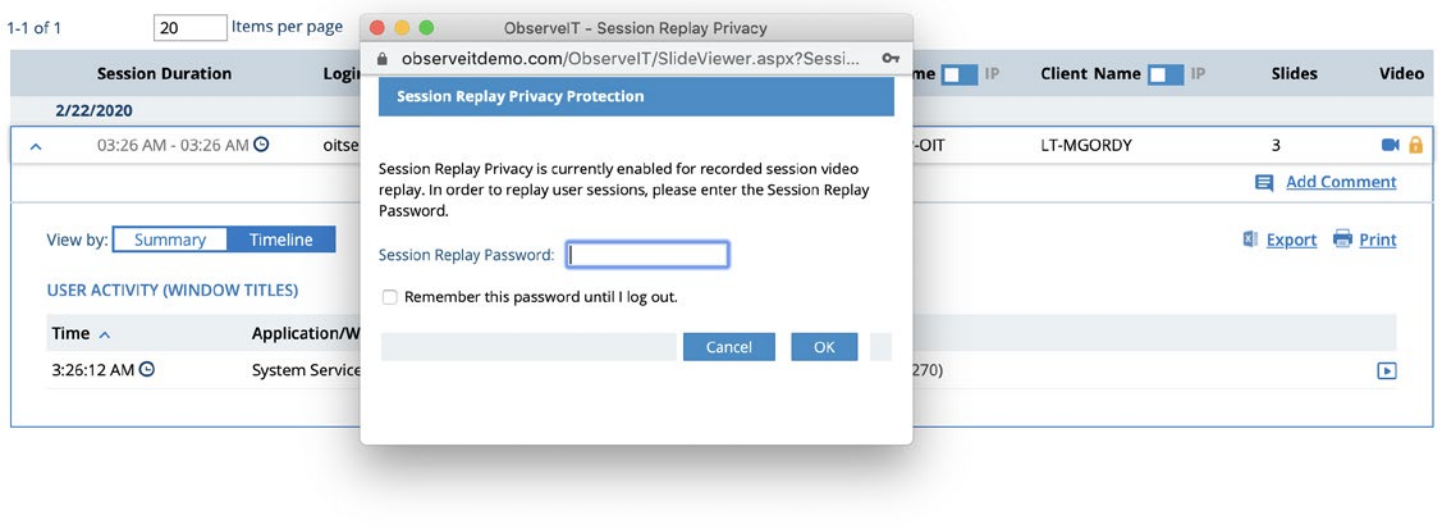

Figure 8: The Session Replay Privacy Protection assigns a master password that must be entered each time a console user wants to replay sessions.

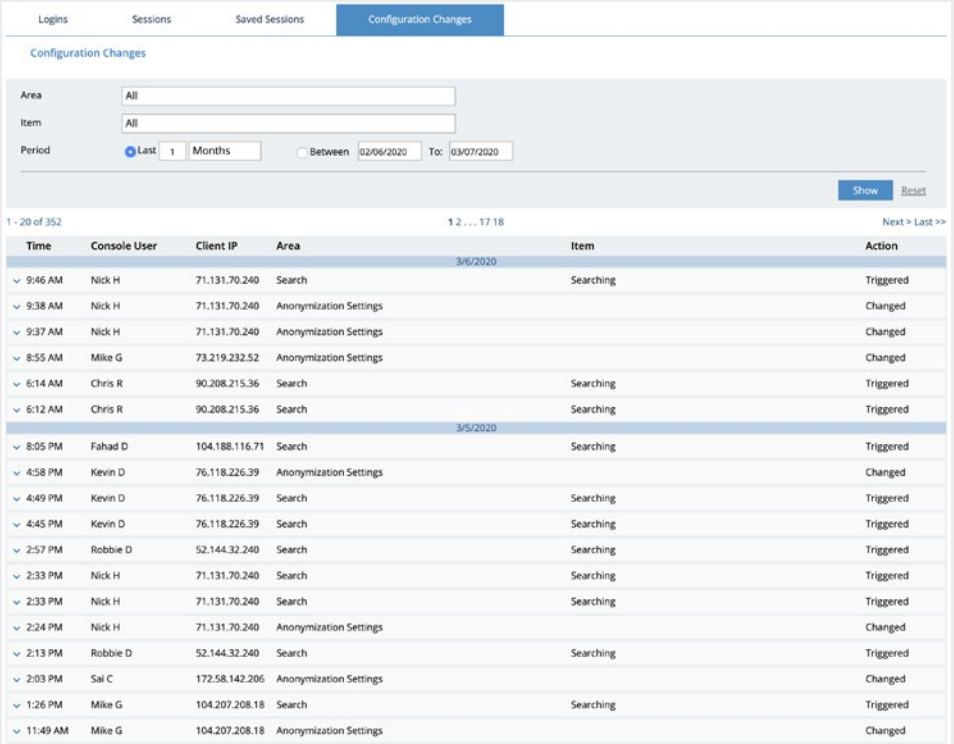

Figure 9: ObserveIT ITM is a fully self-audited solution. Audit any login, session view, export of data, or configuration change.

Privacy concern 5

Creating new sensitive data that needs to be secured.

Administrative recommendation:

Place ObserveIT ITM data in the highest level of private data classification (highly classified, top secret etc.) so that the data is protected, regulated, and secured the same way existing critical data such as PII, PHI, and financial information is stored.

Technical control:

ObserveIT data is secured at rest and in transit. The metadata and screenshots are SSL encrypted in transit between the agents, application servers and databases and can be encrypted when stored in ObserveIT ITM databases. ObserveIT ITM has redundant controls to monitor all activity that takes place on the ObserveIT ITM database and application servers. It is recommended to set up alert notifications whenever there is user access on these endpoints that is not permitted.

Privacy concern 6

Users finding ObserveIT ITM software running and tampering with the agent.

Administrative recommendation:

Unless specified for an investigation, security awareness training should be performed to let users know they are being monitored and in what fashion. Tampering safeguards, as well as explicit instructions, should be put into place to protect the ObserveIT ITM agent under the same restrictions as other security solutions that should not be tampered with i.e., firewalls, anti-virus, DLP etc.

Technical control:

ObserveIT ITM can be deployed in full stealth mode and won't show up as a running process. If the agent is displayed and attempts are made to uninstall the agent, a watchdog mechanism turns the agent back on automatically. An uninstallation password can be enabled on the agent as well as system events for tampering and DLL deletion will trigger.

Privacy concern 7

Users are not aware they are being monitored.

Administrative recommendation:

Make any privacy notice and monitoring forms easy to understand.

Technical control:

The above recommendation is an administrative control typically facilitated by security awareness training, documentation, and procedural notifications. ObserveIT ITM encourages administrators to issue real-time notifications or static messages that will notify users of the type of data, the purpose of its collection, and time-period in which data is gathered.

Summary

ObserveIT ITM works with 1,200+ organization worldwide across every major industry. Organizations are mobilizing to deal with insider threats in a privacy aware and programmatic manner. These are best practices to protect organizations data and their people from insider threats while ensuring their users' privacy until proven guilty and complying with global data protection laws.

To learn more, visit observeit.com/product/privacy.

LEARN MORE

For more information, visit **observeit.com**.