

4 Benefits of User Activity Monitoring in Managed Environments



Table of Contents

Introduction	3
Implement Least Privilege and User Activity Monitoring	4
Case #1: Operational Efficiency	5
Case #2: Security	6
Case #3: DaaS / VDI	7
Case #4: Lack of Audit Trails	8
Conclusion	9

Introduction

The foundation of any organization is the concept of trust. IT, employees – even outsourced service providers – are all trusted to have varying levels of access to your organization's networks, systems, resources, and data. As long as they do as they are supposed to, everything will be just fine. But that's not always the case.

It's not just about trust from a security perspective – it's about trusting that employees are working, that changes to systems are being documented, as well as that system security and data integrity are being maintained.

With external threats, data breaches, and remote working at an all-time high, organizations cannot simply blindly trust employees in this dangerous mix. But IT's schedule is already filled with meetings, fires to fight, and projects to complete, all at a time where the actions of employees, contractors, and service providers is quickly growing farther away from IT's reach.

So how can organizations extend their reach and regain the visibility, context, and accountability needed?

Implement Least Privilege and User Activity Monitoring

Least privilege was defined best by the United States Department of Defense. The Department of Defense knows very well the ramifications of allowing users to run with excess privileges, as well as the benefits of having a user to run with limited privileges on their desktop. The Department of Defense defines the Principle of Least Privilege as:

“[The Principle of Least Privilege] requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.”

User Activity Monitoring (UAM) provides an organization an ability to record, document, audit, and review user activity on physical, virtual, and published desktop environments. By recording actions and capturing screenshots, specific activity can be quickly identified and replayed like a video.

Tie all of this together with Netwrix Auditor platform that enables **complete visibility** into both security configuration and data access within the entire IT infrastructure by providing actionable audit data about who did what, when and where and who has access to what.

To bring the value of UAM to light, we'll briefly cover four use cases where UAM provides both IT and the organization with tangible benefits.

Case #1: Operational Efficiency

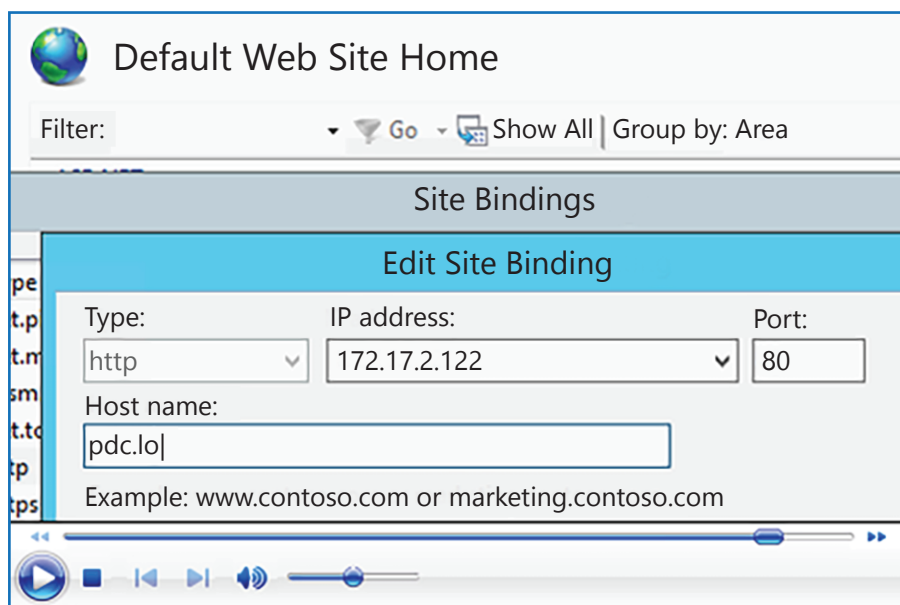
The only constant in IT is change. Whether it's a problem with one of your organization's Exchange servers or a single user's workstation, when something goes wrong, the very first question is usually "What changed?" And regardless of whether there's intent to hide self-blame, the person who should be citing the actions performed leading up to the problem, usually responds with a rather unhelpful "nothing." Sound familiar?

With 52% of IT and Security professionals making changes weekly that impact system availability¹, it's easy to understand why your IT organization finds itself frequently in situations where operational efficiency is impacted.

So, how is your organization supposed to keep operations running efficiently when they can't tell what's changing and who is making those changes?

The Value of UAM

What's needed is an ability to review activity on a given server or workstation at, or around, the time in question to identify how a problem may have been introduced. UAM captures and documents those actions, allowing support staff to replay the pertinent actions by privileged and non-privileged users alike, leading up to an application or system no longer functioning. This not only empowers IT to quickly identify the problem, but also the solution (as the original configuration settings would be documented within the video playback).



¹ Netwrix 2014 State of Changes Report

Case #2: Security

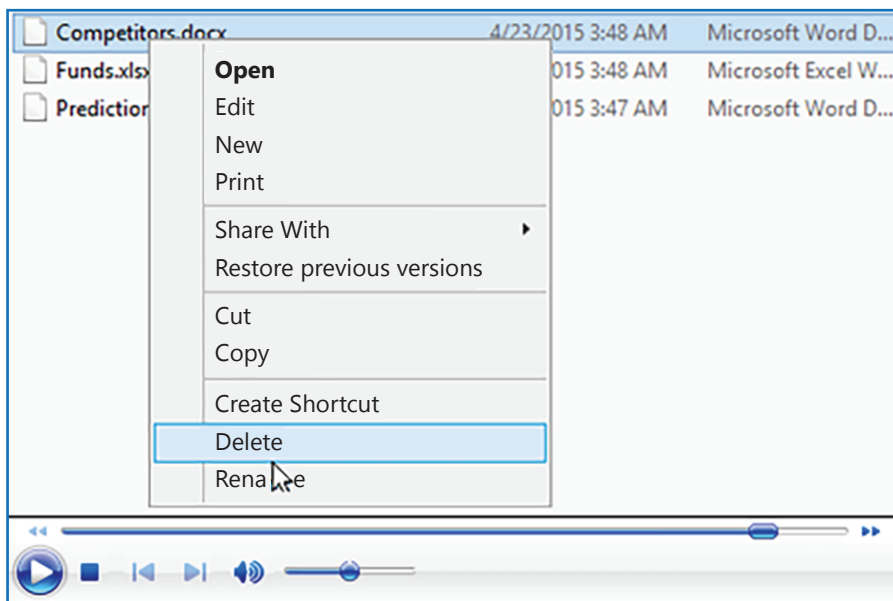
According to the Verizon 2014 Data Breach Investigations Report, 88% of insider threats are privilege misuse. Think about that – users (IT included) utilizing the privileges they've been given, accessing the applications and systems they normally do, with the only change being that they are now using them with self-serving, malicious intent.

Now add the external hacker to the mix, with 30% of them targeting IT admins and 40% of them targeting contractors². Why? For the obvious reason, of course: Those accounts have access to sensitive systems, applications, and data.

It's going to be difficult at best to tell when a user action is performed with the company's best intentions at heart. **So, how can an organization tell the difference?**

The Value of UAM

The answer is context. That is, if you want to determine if a simple user action of looking at, say, a customer record is malicious or not, you'd need to look at the actions performed before and after the action in question to see either what promoted them to perform the action, or what they did with the data accessed. UAM gives you the ability to not just pinpoint and review a specific action, but to review the activity around that action to gain context.



² Thycotic 2014 Black Hat Hacker Survey


Case #3: DaaS / VDI

Using an on-premises Virtual Desktop Infrastructure or a cloud-based Desktop as a Service platform provides organizations the ability to utilize remote workers while still retaining centralized control and simplified management of their working environment. It also creates an environment where an organization has less visibility into what remote workers are doing.

With 51% of users thinking it's acceptable to take company data when they leave the organization³ and with 57% of employees wasting an hour or more of company time on personal tasks⁴, along with concerns around operational efficiency and security in a DaaS or VDI environment, **how can you gain visibility into what employees are really doing.**

The Value of UAM

Visibility is only gained through an ability to actually see what the user, IT pro, or service provider is doing. In a traditional work setting, you can walk up and see what they are working on – something you obviously cannot do remotely. UAM provide the visibility necessary by providing the ability to review and replay user activity quickly.

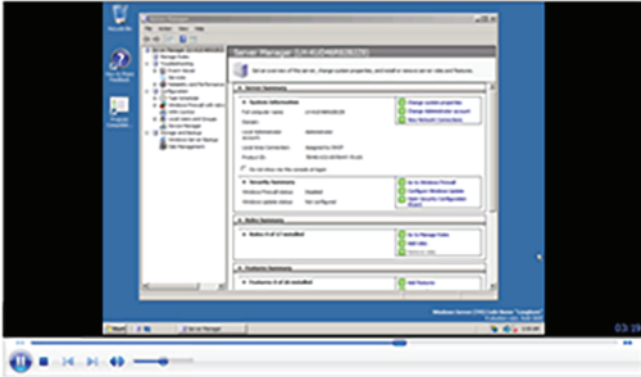


Activity Records

Generate a summary of video records

Date 9/25/2014

Computer	User	Start Time	End Time	Duration
PDC.netwrix.demo	Netwrix\Administrator	9/25/2014 4:12 AM	9/25/2014 4:17 AM	00:05:15
PDC.netwrix.demo	Netwrix\Administrator	9/25/2014 4:07 AM	9/25/2014 4:08 AM	00:01:16



³ Symantec What's Yours Is Mine: How Employees are Putting Your Intellectual Property at Risk Report

⁴ Salary.com 2014 Wasting Time at Work Report

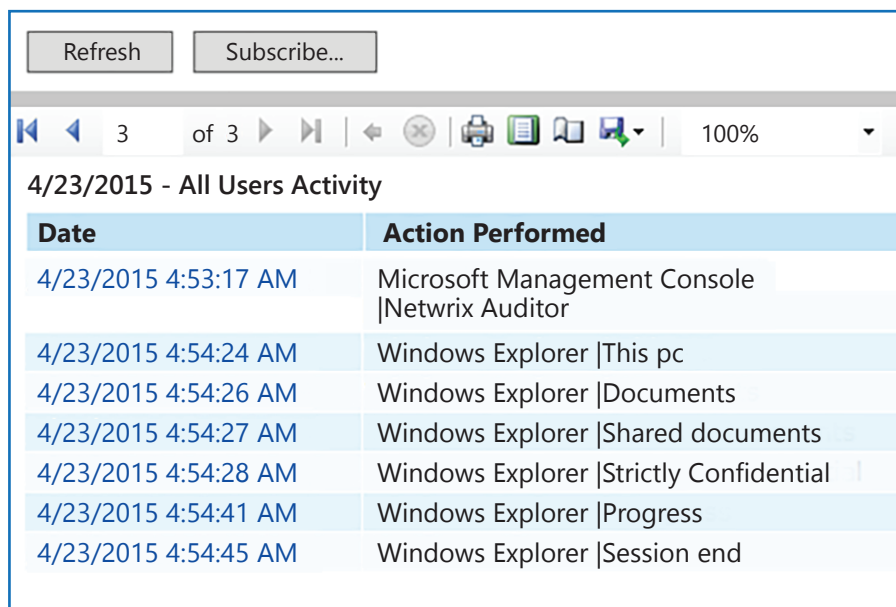
Case #4: Lack of Audit Trails

Most systems provide some degree of event logging to serve as an audit trail of actions performed. Security, Operations, and Compliance all rely on IT's ability to know what happened. But many critical applications produce no log data, leaving IT with no audit trail.

With security and compliance mandates requiring an ability to audit logs, how can you create a trail when none exists?

The Value of UAM

Because UAM records every action within every application, saving pertinent metadata about the user, application, and timeframe involved, it becomes the audit trail needed. By making this metadata searchable, and tying it to re-playable video, UAM creates the ultimate audit trail for auditors to not only see actions, but understand why those actions happened and what occurred before and after the event in question.



The screenshot shows a web interface with a 'Refresh' and 'Subscribe...' button at the top. Below is a video player control bar showing '3 of 3' and '100%' zoom. The main content is a table titled '4/23/2015 - All Users Activity' with two columns: 'Date' and 'Action Performed'.

Date	Action Performed
4/23/2015 4:53:17 AM	Microsoft Management Console Netwrix Auditor
4/23/2015 4:54:24 AM	Windows Explorer This pc
4/23/2015 4:54:26 AM	Windows Explorer Documents
4/23/2015 4:54:27 AM	Windows Explorer Shared documents
4/23/2015 4:54:28 AM	Windows Explorer Strictly Confidential
4/23/2015 4:54:41 AM	Windows Explorer Progress
4/23/2015 4:54:45 AM	Windows Explorer Session end

Conclusion

With users, IT, contractors, and service providers all having their hands on systems, applications, and data, and doing so from literally anywhere in the world, UAM gives organizations the visibility and context required to understand what's changing, who's doing it, and how it's impacting the organization's security and efficiency – regardless of the application used and whether logs are lacking or not.

About Netwrix Corporation

Netwrix Corporation enables transparency of managed environments helping your MSP business increase customer revenue and add differentiated services that show more value to your customers. Designed with increased operational efficiency in mind, Netwrix software allow fast deployment and easy integration with your existing systems and platforms.

Learn More: www.netwrix.com/msp

**Netwrix Corporation, 300 Spectrum Center Drive,
Suite 820 Irvine, CA 92618, US**



netwrix.com/social

Toll-free: 888-638-9749

Int'l: +1 (949) 407-5125

EMEA: +44 (0) 203-308-3023