REMOTE VENDOR MONITORING E-BOOK

Strangers in Your Servers:

Make Working with IT Contractors More Secure

Nearly 90% of data breaches are accomplished via remote access to a company's systems. Yet, third-party service providers are routinely given wide-ranging remote access privileges – and companies have no idea what these vendors are actually doing once they are logged in. There is a better way to keep track of what these vendors do: User Activity Monitoring.

observe it

Two research reports have clearly indicated that the most common avenue used for data breaches is a remote access service providing privileged entry to corporate resources: Verizon reports that remote access accounts for 88% of data breaches,[1] while Trustwave reports that 76% of data-breaches investigated were due to exploitation of remote vendor access channels.[2]

> *"As soon as vendors discoverd that all actions are being recorded, it became much easier to manage them."*
>
> *Moti Landes,*
> *IT Infrastructure Mgr & IT Div. CISO*
>
> Coca-Cola

A quick review of some high-profile remote access breaches:

- Hackers swiped the credit and debit card information of up to 40 million Target customers via the remote login account of an HVAC sub-contractor.[3]
- Romanian hackers stole consumer credit card data from Subway computers via remote desktop access software over a period of three years, enabling them to ring up over $3 million in fraudulent charges.[4]
- Hackers entered Sony's PlayStation network by remotely taking over the PC of a system administrator and compromising the personal information of 77 million user accounts.[5]
- Using remote access vulnerabilities, the systems at South Carolina Department of Revenue were compromised, allowing state tax data belonging to 6.4 million consumers and businesses to be compromised.[6]

Your company's servers hold vital and sensitive information, yet they are constantly exposed to both internal privileged users and external third-party contractors. Once these privileged users have gained access to the servers, most IT security managers have no idea what these users are up to. Even companies that have invested in IAM, SIEMs and other log analysis tools still don't know most of what users are actually doing while logged in to servers. In fact, only 1% of breaches are discovered by the victimized organization's log analysis and/or review process (more about this below).[2]

> *"Once these privileged users have gained access to the servers, most IT security managers have no idea what these users are up to."*

The IT Contractor – An Integral Part of your Business that is here to Stay

"We enjoy showing off to our customers that every user action is recorded. This increases confidence all around."

Rick Beecroft,
Area Manager, Americas &Pacific Rim

Bellin Treasury

It's undeniable that remote contractors and their employees have become an integral part of day-to-day IT operations in most organizations. Internet-based remote access systems are critical for numerous business function providers, including:

- Outsourced software developers and QA teams
- Outsourced software application configuration/customization consultants
- Outsourced database administrators
- Managed service providers responsible for servers, network equipment (firewalls, routers, switches, etc.) and even entire data centers
- Managed service providers responsible for employee desktops (operating systems, user permissions, software applications)
- Outsourced employee technical support and helpdesk services

When an organization's internal systems are so extensively accessible to remote partners (whose employees are usually total strangers to the organization), there is dramatically increased risk that unauthorized users will exploit their access privileges to find an avenue into company servers, databases, control systems and other sensitive resources.

Furthermore, even contractors with no nefarious motives at all still pose great danger to the organization: mistakes made while deploying code, configuring systems or assigning user permissions have the potential to reduce the performance of business-critical systems, destroy data or open huge security holes. The chances are also much greater for privileged user credentials to be stolen by third-party hackers and data thieves without a contractor's intent or knowledge.

The bottom line is that having IT vendors with access to sensitive internal systems is a fact of modern corporate life, despite the tremendous danger that this reality imposes on the organization. The question is: How can organizations leverage the business and economic benefits of remote vendors, while mitigating the associated threats? Let's begin to answer this question by exploring how companies are addressing the risks today.

"Even contractors with no nefarious motives at all still pose great danger to the organization."

How are Organizations Protecting Themselves Today?

Well-known security best practices dictate that all users – external contractors and employees alike – should only have the minimum privileges they need to get their jobs done. Companies typically use IAM and access governance solutions to implement these access controls. However, in many cases, even those minimal privileges will still have to provide broad access to your organization's systems, devices, files and data. These conditions are only getting worse, as both the amount of sensitive data collected, and the number of people who need legitimate access to it, are skyrocketing.

"ObserveIT gives us the confidence of allowing admins and remote vendors to do their work, while ensuring that our data is secure and audited. We also use the product to document IT processes & installations."

Mr. Simon Thunder, Head of IT

Premier League

This prevention-based approach isn't sufficient, as once users with legitimate credentials gain access, companies have little or no idea what they are doing.

A commonly used approach to attempt to detect unauthorized access to IT resources is **log analysis**, often using a security information and event management **(SIEM) system**. Companies using a SIEM or log analysis system are certainly better positioned to handle cyber-attacks than those companies not using SIEM. However, the fact is that only 1% of data breaches are discovered by the victimized organization's log analysis and/or review process.[2]

Even including other instances of internal detection, such as employee vigilance or noticeable performance degradation, only 16% of attacks and breaches are detected by the victimized organization itself, with hackers enjoying an average of 174 days within the victim's environment before detection occurred by a third party.[2] The costs of cyber-attacks escalate rapidly if not promptly resolved; studies shown a positive relationship between the time to contain an attack and the organizational cost.[7] Clearly something isn't working.

The problem is simple: companies are trying to gain insight into the behavior and activity of users by looking at system log data rather than actually watching what those users are doing.

"Only 1% of data breaches are discovered by the victimized organization's log analysis and/or review process."

The Solution: User Activity Monitoring and Analysis

> *"ObserveIT directly minimizes the risks associated with employee and third-party vendor activity over a full range of applications and environments. Its full video recording and direct-access keyword search are amazing and unique."*
>
> *Diego Hernan Pizolli, CISO*
>
> *Telecom Argentina*
>
> TELECOM

What if your organization could know definitively – both in realtime and after-the-fact – exactly what every user was doing during every minute that they were logged in to your IT systems? What if you could watch screen recording videos of every user action during every server and desktop session? What if you could instantly find portions of the video based on search keywords describing an action or effected resource? What if you had a solution that immediately alerted you any time a user was engaging in suspicious behavior?

The answer to the above questions is that your organization would be in the best possible position to detect and prevent dangerous incidents and security breaches, whether due to malicious intent or inadvertent error. This is exactly what User Activity Monitoring and Analysis provides.

Use Activity Monitoring systems generate video recordings of every login session–along with detailed user activity audit logs—providing unparalleled insight into what is being done on company servers. Whereas standard IT logs collect data on server and network activity, user activity recordings focus on what users are doing in every application: commercial, bespoke, legacy, cloud and operating system. *This user-focused monitoring and analysis capability fills a major void plaguing cyber security today.*

Recorded videos of user sessions are cool, but they are only part of the solution. User Activity Monitoring solutions must also generate textual activity logs of everything done by users while logged into company servers. These can be easily reviewed and searched using keywords, as they contain the names of applications run, windows opened, system commands executed, check boxes clicked, text entered/edited, URLs visited and nearly every other on-screen event. Whether by manual daily review, summary reports or customizable activity alerts, the important clues to most illicit server-based activity can be easily identified.

To extend the benefits of User Activity Monitoring from forensic (reactive) to detective (proactive), behavioral analysis is required. User behavior analysis builds upon user activity recording and adds the analytics required to rapidly detect changes in user behavior associated with breaches.

> *"This user-focused monitoring and analysis capability fills a major void plaguing cyber security today."*

Let's Get Real

The following are some examples of how User Activity Monitoring and Analysis systems have been used to detect intruder activity on company servers:

- The User Activity Monitoring system generated a real-time alert when a privileged user account was used to log in to a Unix server on a weekend. The on-call NOC security officer who received the alert immediately began watching the session in real-time using the session recording system. When he saw the logged-in user preparing to upload files via FTP to an IP address outside the network, he immediately terminated the session and notified the company's CISO.

"Implementation has been dictated to prevent problems with third parties having access to our IT system."

Przemysław Jasiński
IT Department Manager
Elektrotim

- A daily user activity report of a remote vendor included a number of logins to a Windows server from an account that had not been used for months. A quick review of the screen recordings of these sessions showed obviously unauthorized activity, including extensive use of Windows Explorer to browse the files on a number of other network servers. The account was immediately disabled and the IP address of the remote computer was provided to law enforcement authorities for further investigation.

- A weekly user activity summary report of applications run on a company's servers included instances of TeamViewer, a remote control application having no business on a company server. An immediate investigation with User Activity Monitoring revealed that a newly-hired IT administrator installed TeamViewer on a server which stored customer credit card information and enabled the software to provide full control of the machine from any outside computer. Confronted by authorities with the video showing his actions, the administrator admitted that he planned to sell access to the computer to a hacker group.

In summary, deploying User Activity Monitoring and Analysis makes any organization extremely capable of detecting questionable, dangerous or abusive remote (and internal) user activity. Beyond better data breach detection and response capabilities (via faster ad hoc forensic analysis), User Activity Monitoring also makes it easier to get compliant and stay compliant with security aspects of government and industry regulations (e.g., PCI, HIPAA, NERC, FISMA), while reducing overall security auditing costs. Most auditor requests can now be answered instantly by searching for user actions or watching a portion of a recorded session video—without the need for complex machine data research and analysis.

"In summary, deploying User Activity Monitoring and Analysis makes any organization extremely capable of detecting questionable, dangerous or abusive remote user activity."

observe it

Top 5 Benefits of User Activity Monitoring and Analysis

User Activity Monitoring provides a wide range of benefits to any organization, with the security and contractor monitoring advantages at the top of the list:

1 Improved IT security and early data breach detection

Custom realtime alerts and integration with SIEM/NMS systems provide early warning of both human error and malicious actions.

2 The ultimate in remote vendor monitoring

Review and search remote vendor activity to ensure that vendors are meeting their obligations and posing no risk to the organization.

3 Easier compliance accountability

Monitor and audit local and remote user activity to satisfy PCI, HIPAA, SOX, FISMA and ISO 27001 security requirements.

4 Greater IT efficiency

Easily conduct root cause analysis and forensics investigations, plus enjoy effortless documentation of all IT activity on monitored servers.

5 Deterrence

The behavior of your remote vendors (and employees) changes dramatically when they know their actions are being monitored and reviewed.

About ObserveIT

ObserveIT is an enterprise-class User Activity Monitoring and Analysis solution. The solution records server and desktop sessions on UNIX, Linux and Windows computers, accessed locally or remotely. ObserveIT works on-premises and in cloud environments, natively integrated with leading cloud providers such as Amazon and IBM. ObserveIT generates both videos and keyword-searchable activity logs of every user action in every application and system area, as well as real-time user behavior alerts. Hundreds of companies worldwide, including dozens of Fortune 500 companies, use ObserveIT daily to help them protect corporate data and other IT assets, monitor privileged users and remote vendors, increase the efficiency of IT processes and achieve and maintain regulatory compliance. Learn more at www.observeit.com.

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

[1] Verizon 2012 Data Breach Investigations Report, March 2012
[2] Trustwave 2012 Global Security Report, February 2012
[3] Gizmodo: Last Month's Massive Target Hack Was the Heating Guy's Fault, February 2014
[4] Ars Technica: How hackers gave Subway a $3 million lesson in point-of-sale security, December 2011
[5] NBC News: Hackers stole personal data from PlayStation Network, April 2011
[6] The Island Packet: How hackers stole South Carolinians' tax-return data, November 2012
[6] Ponemon Institute: 2012 Cost of Cyber Crime Study, October 2012