Strangers in Your Servers:
How to Make Third-Party Work More Secure

observe it

Strangers in Your Servers: How to Make Third-Party Work More Secure

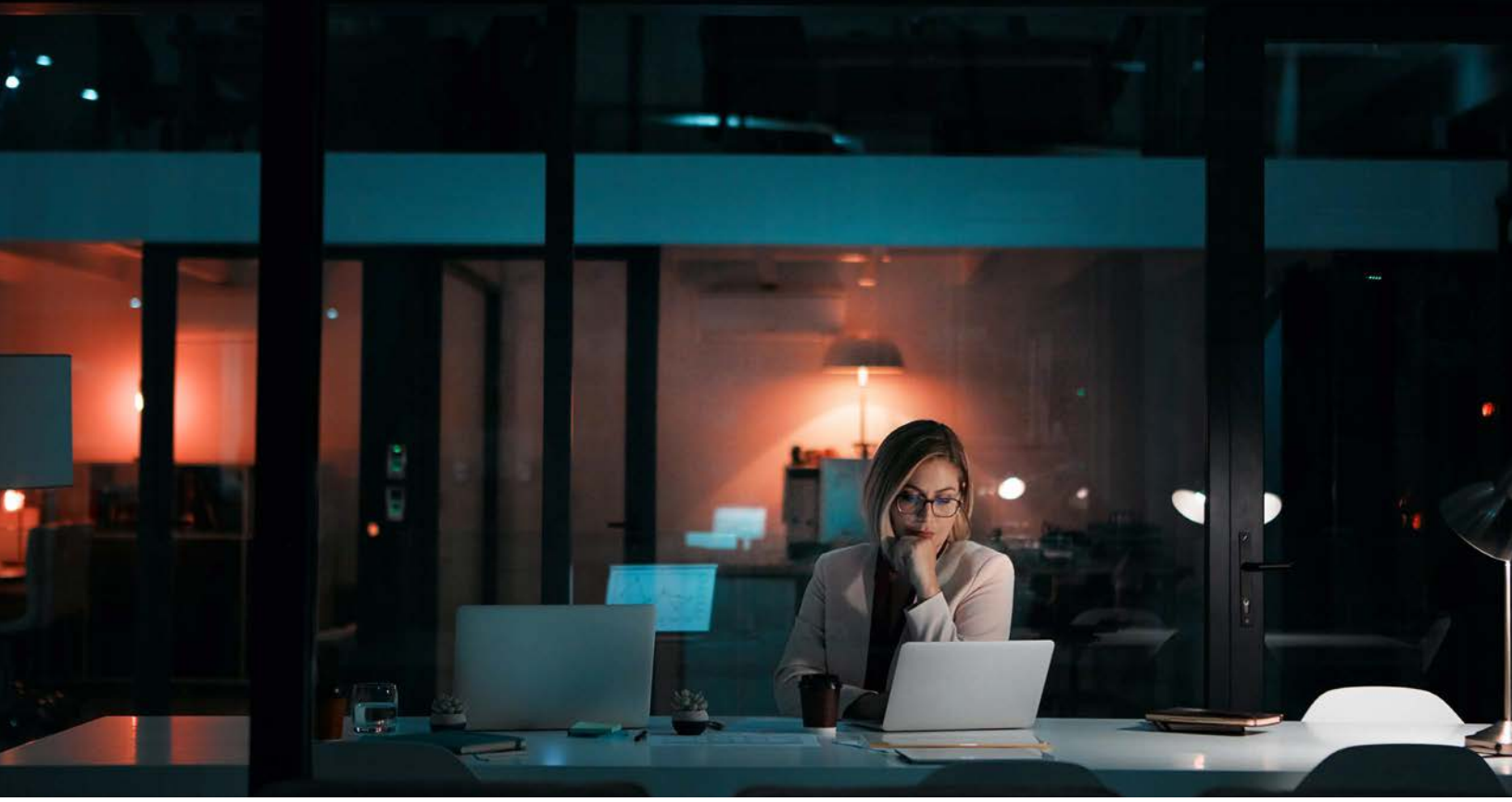
According to independent research from The Ponemon Institute, two-thirds of insider threat incidents[1] are caused by employee or third-party contractor mistakes. Yet, more and more companies are employing outside contractors and vendors to do all kinds of work, ranging from call centers, to customer service, to engineering and IT. An NPR/Marist Poll states that 1 in 5 people belong to the contract workforce, with many economists estimating that by 2028, that number may increase to half of the total workforce.

Visibility into third-party user activity has never been more important, from a cybersecurity perspective.

With no signs of slowdown in the contract economy, the organizations that employ third-party vendors need to be on high alert. Often, contractors have access to corporate resources through cloud or remote access software—even though they may not be following the same cybersecurity policies as your internal employees. These unknowns make them a big risk to proprietary systems, files, and data!

According to independent Ponemon research[3], **64% of insider threat incidents were due to employee or third-party contractor negligence**. These incidents can be caused by both intentional and unintentional insider threat actions.

1. https://www.observeit.com/cost-of-insider-threat/
2. https://www.npr.org/2018/01/22/578825135/rise-of-the-contract-workers-work-is-different-now
3. https://www.observeit.com/ponemon-report-cost-of-insider-threats/



Here's a quick review of some of the more notable, high-profile breaches caused by third-party contractors:

Universal Media Group Exposed

In 2018, a third-party engineering contractor of Universal Music Group forgot to protect an Apache Airflow server, leaving the organization's confidential AWS and database credentials exposed on the open internet — and ultimately, breached by hackers[4].

Target Breach

The infamous Target breach of 2014 was caused by credential theft from a third-party HVAC provider. The hacker used the stolen credentials to gain access to the point-of-sale system, stealing confidential customer data, including credit card numbers[5].

U.S. Government Breaches

A U.S. government contractor used to conduct background checks was responsible for two breaches in 2015, one to the Department of Homeland Security and one to the Office of Personnel Management. Both breaches resulted from credential theft and exploitation of the firm's privileged access[6].

When trusted contractors don't practice good cybersecurity hygiene, they can become unintentional insider threats to your organization, opening up major risk for both financial and reputational damages. In fact, The Ponemon Institute study indicates that credential theft — one of the top causes of the high-profile breaches cited above — is the costliest type of insider threat, at $649,000 per incident[7] on average over a 12-month period.

To learn more about how to prevent these incidents, let's explore more about the types of contractors, and what has and has not worked in terms of defending against potential insider threats.

4. https://kromtech.com/blog/security-center/contractor-for-universal-music-group-exposes-internal-credentials
5. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
6. https://www.federaltimes.com/smr/opm-data-breach/2015/06/23/contractor-breach-gave-hackers-keys-to-opm-data/
7. https://www.observeit.com/cost-of-insider-threat/

Third-Party Vendors & Contractors – Here to Stay

Many organizations employ contractors to supplement their internal teams, adding talent in specialized areas without the overhead costs of employees, such as benefits or office space. **With an estimated 57.3 million people performing contract work, contributing $1.4 trillion to the U.S. economy[8], there's no end in sight to this trend.** This is an interesting predicament from a cybersecurity standpoint, as many of these contractors cover IT services (which usually come with heightened privileged access), and business services.

Insider Threat Risks with Outsourced IT

Outsourced IT services are frequently used by companies of all sizes. With a high demand and low supply of software engineers on the job market, these contractors provide businesses with the ability to easily scale their technical workforce.

Here are just some of the functions companies may decide to outsource:

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

When an organization's internal systems are extensively accessible to remote partners, 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.

Even contractors with no nefarious motive can pose great risk to an 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 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.

8. https://blog.freelancersunion.org/2017/10/17/freelancing-in-america-2017/

Business Service Contractor Risks

Business services cover a broad swath of contractor types, but unlike third-party IT consultants, they most likely do not have privileged access to backend infrastructure or technical systems. However, they can often have access to servers and cloud services that contain confidential files or financial information, depending on their role.

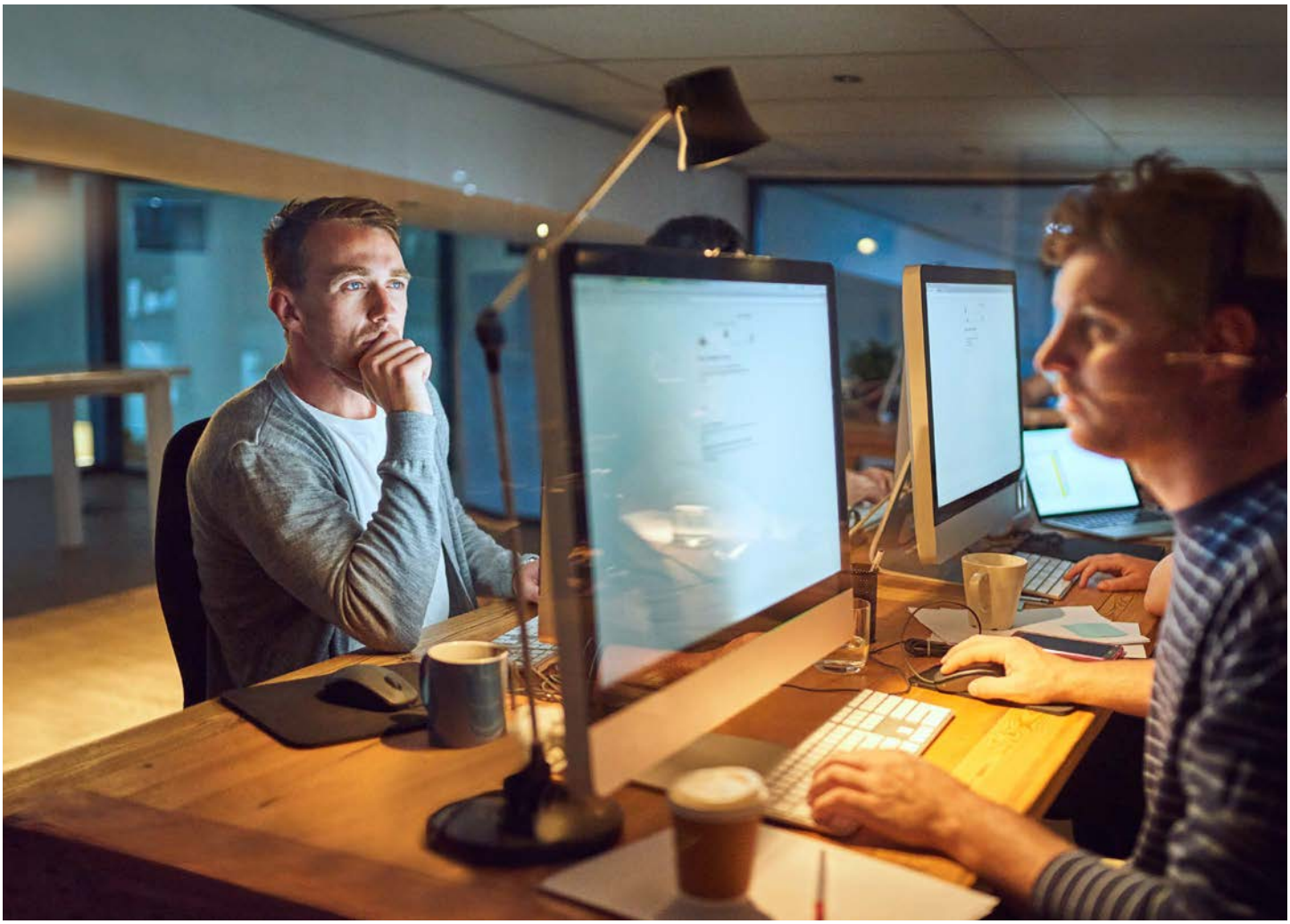
Here are just a few of the business functions companies commonly outsource to firms or consultants:

- Legal
- Business Strategy
- Accounting
- Design
- Marketing
- Public Relations
- HR
- Call Centers
- Sales
- Real Estate

Trusted third-parties in these areas often hold the keys to the kingdom — and can just as easily lose them if the right security measures aren't in place. With the rise of shared cloud services and remote VPN access, the risk of sensitive information falling into the wrong hands increases exponentially. Enforcing corporate IT policy can be difficult when there's a lack of visibility into who is accessing corporate data, when, and why.

An added challenge is the fact that contractors are managed by people across departments who may not necessarily have a strong awareness of policy themselves (for example, requiring multi-factor authentication as a cloud account security measure).

Whether a third-party vendor or contractor is focused on IT or business services, it's critical to have a strong level of visibility into their user activity on your corporate systems. Without this type of user activity monitoring in place, the margin for error or risk of insider threat is too high to ignore.



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 identity and access management (IAM) and access governance solutions to implement these access controls. However, in many cases, even those minimal privileges will still provide broad access to your organization's systems, devices, files and data.

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, these systems are focused on server and network activity alone, and not the people involved in insider threat incidents.

Another relatively common approach to insider threat management is data loss prevention (DLP). DLP tools are designed to identify, classify, and monitor data to prevent data exfiltration. The problem with DLP, however, is that these tools often take a great deal of time and resources to implement, including an extensive data classification process, which requires an in-depth audit of all data, and then fine-tuning that classification architecture year after year. They also don't consider the fact that data doesn't move itself - people, namely insiders, move data. Visibility into user activity is crucial!

Traditional DLP requires organizations to know where the data is located, and how to categorize it with the appropriate tags, policies, and rules. If employees are accessing data via software-as-a-service (SaaS) applications, sharing it with external vendors and contractors, and tapping into corporate systems with different devices, the task of knowing exactly where the sensitive data lies becomes infinitely more complicated.

Even considering other methods of internal detection, such as employee vigilance or noticeable performance degradation, **the average insider threat takes about 72 days to contain, costing organizations on average $9.55 million annually**, according to The Ponemon Institute[9]. The longer an incident takes to contain, the more these costs escalate.

The problem is simple: companies are trying to gain insight into the behavior and activity of users by looking at system log data or DLP alerts rather than actually watching what those users are doing. In many cases, the likelihood of false positives can send security teams on a wild goose chase to discover the root cause of a potential incident, when it's the users themselves who should have been monitored all along.

9. https://www.observeit.com/cost-of-insider-threat/

Comprehensive Insider Threat Management

Instead of remaining in the dark, knowing definitively – both in real time and after the fact – exactly what every user was doing during every minute that they were logged in to your IT systems could be a game-changer. Imagine taking that knowledge a step further by watching screen recording videos of every user action during every server and desktop session, and instantly finding portions of the video based on search keywords describing an action or effected resource. Finally, imagine getting immediately alerted any time a user engages in suspicious behavior.

A combination of these activities could put your organization in the best possible position to detect and prevent dangerous insider threat incidents and security breaches, whether due to malicious intent or inadvertent error. Beyond the logs and alerts, a more comprehensive, context-driven insider threat management approach is exactly what insider threat management solutions provide.

Insider Threat Management solutions generate optional video recordings of every login session—along with detailed user activity audit logs—providing unparalleled insight into what is being done on company servers.

Note: Data anonymization is possible with modern insider threat management solutions.

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 cybersecurity today.

Recorded videos of user sessions are only part of the solution.

Insider Threat Management 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 Insider Threat Management solutions 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.

Insider Threat Management Case Studies

The following are some examples of how Insider Threat Management solutions have been used to detect intruder activity on company servers:

- **The Insider Threat Management solution 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 feature. 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.

- **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.**

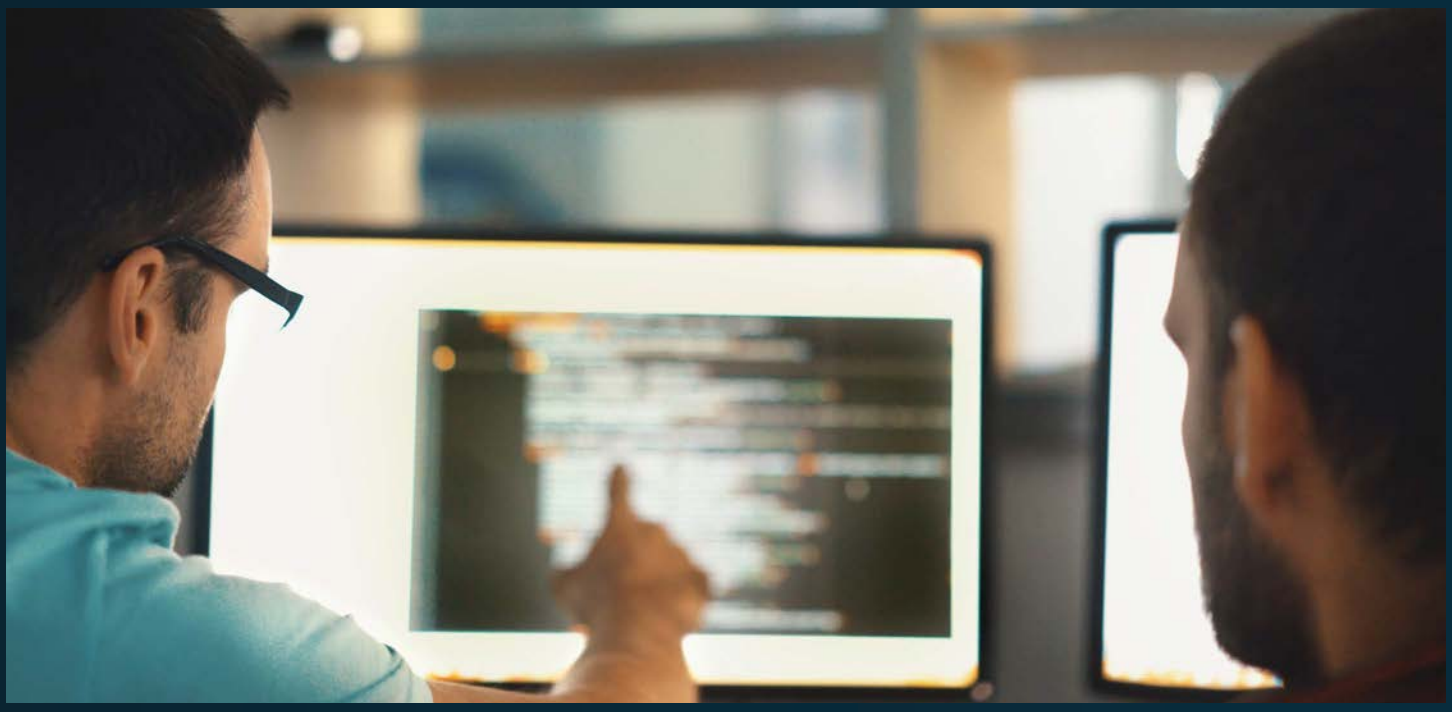
  A quick review of the screen recordings of these sessions showed obviously unauthorized activity, including extensive use of Windows Explorer to browse the files on a number of other network servers. The account was immediately disabled, and the IP address of the remote computer was provided to law enforcement 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 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 an Insider Threat Management solution 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), Insider Threat Management software also makes it easier to establish and maintain compliance with 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.



Top 5 Benefits of Insider Threat Management Software

1. Improved IT security and early data breach detection

Custom real time alerts and integration with SIEM/NMS (network management software) and DLP systems provide early warning for negligent or malicious user actions.

2. Increased visibility through 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 + context

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.

Want to experience first-hand how insider threat management software can help protect your organization against third-party insider threat risks?

Test Drive ObserveIT, today!

https://www.observeit.com/tryitnow/

observe it