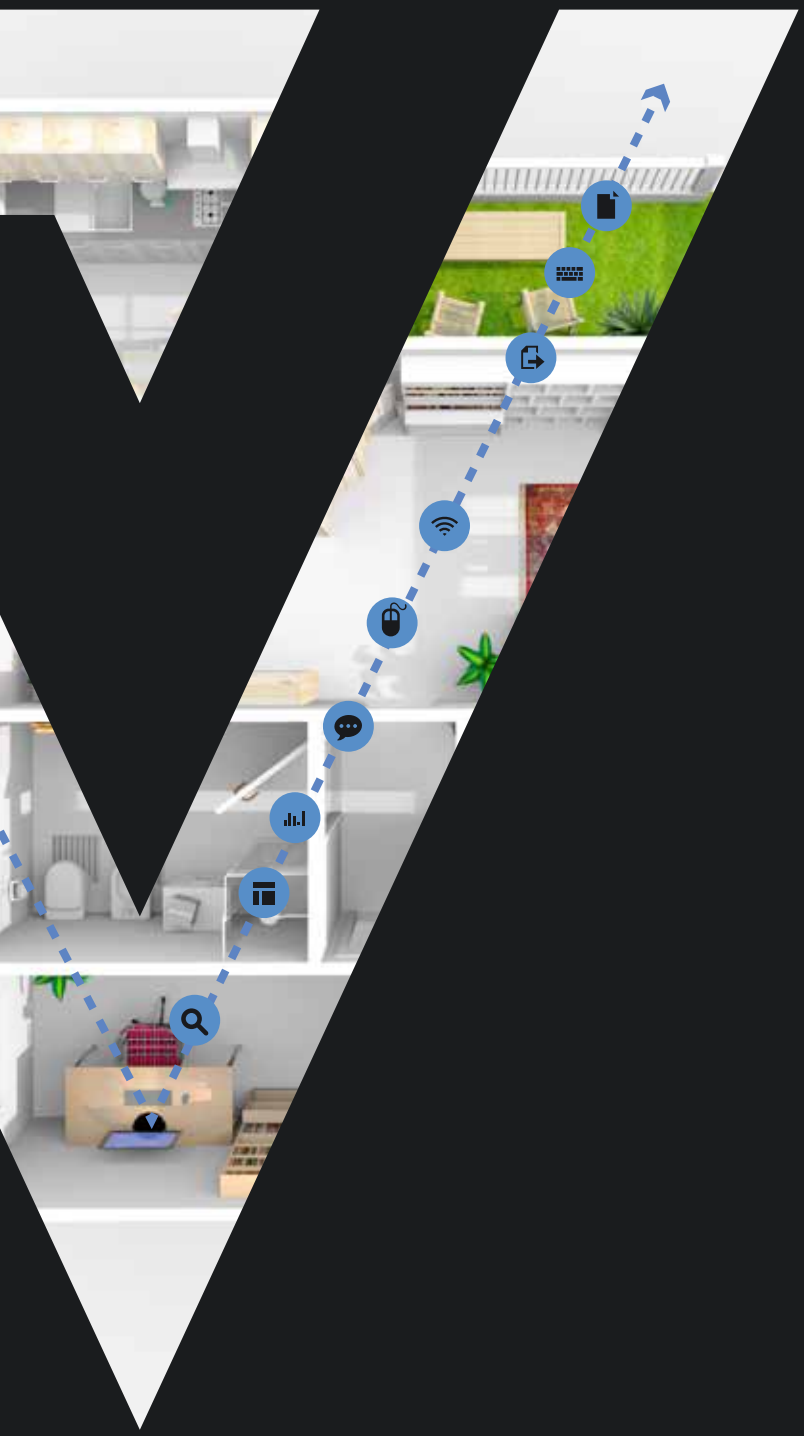


4 Steps to Monitoring Employees in a Remote Workplace

Veriato

www.veriato.com

It's a brave new world for organizations today.

The idea of maintaining a "bricks and mortar" business where every employee works solely at the office (let alone working in the same location) is no longer the norm. With 70% of employees working remotely at least one day a week[1], there is a new dynamic to how employees see the importance of the organization and its concerns around security.

While employee productivity can be a key driver in an organization choosing to utilize remote employees, not every employee is wired to work remotely. Employees can fall into the "out of sight, out of mind" category, causing a reduction in engagement. Some may feel a disconnect to the organization, due to not being around their work peers on a daily basis. This can add up to an employee solely focused on the value of the work they do, creating a sense of entitlement around both the time they dedicate to the organization and the organization's data and resources.

[1] *IWG, The Workspace Revolution: Reaching the Tipping Point (2018)*

Introduction

Working remotely comes with a fair degree of self-management and a lessened sense of accountability. This can exacerbate the risk of some very specific insider threats to the organization:

Employee Fraud – Two parts of the well-known "fraud triangle" that working remotely can either create or increase are opportunity and rationale. Remote employees can feel a sense of "being due" or being unappreciated, addressing the rationale. And, by being remote, employees can easily feel like they are able to act in a way that benefits themselves without getting caught.

Data Breach – Whether stealing data to sell or simply taking company data for personal benefit at, say, the next job, employees are responsible for 28% of all data breaches[2].

Lowered Productivity – Sometimes referred to as timecard fraud or employee wage theft, the misuse of company time for personal benefit can result in a material cost to the organization. The average employee devotes 92.3% of their "on the job" time to actually working[3], so it feels like there's not much to be concerned about. But when you apply that percentage to a 100-person company, over the course of a year, the organization is paying the equivalent of 7.5 employees to do nothing year-round. With the focus for most remote employees to find a "work-life" balance, the potential exists for the employee to easily create a "more-life, less-work" balance without the company knowing.

These threats have specific repercussions. Certainly, fraud and data breaches have the potential to thrust an organization's troubles into the headlines, but productivity – especially when a majority of employees are remote – can limit the organization's growth and negatively impact the bottom line.

---

[2] *Verizon, Data Breach Investigations Report (2018)*
[3] *US Bureau of Labor Statistics, American Time Use Survey (2017)*

To reduce risk, organizations need to monitor specific employee behavior in an effort to identify potentially threatening behavior – which includes actions that fit into any of the three categories above.

This Getting Started brief provides some high-level guidance around how to properly establish the monitoring of remote employees, including what to look for and how to appropriately respond should an issue be discovered.

STEP 1

Determine What to Measure

Depending on the threats most concerning your organization, you'll need to establish which aspects of remote behavior to monitor. For example, if your focus is employee productivity, you should be watching actions that determine whether an employee is working or not. But if you are watching for users stealing data, the focus should be on monitoring the employee's interaction with corporate data in applications and files.

Below are a few activity examples that can be measured to identify threats.

Measurement	Description	Productivity	Fraud	Data Breach
Connectivity	For organizations where users must connect to the corporate network, validating a basic connection provides a leading indication of an active employee.	✓		
Application Use	Applications relevant to each employee's role, and which apps are most used, provide context into whether they are working.	✓		
Application Activity	Just because an application is open doesn't mean it's being used. Looking deeper into whether an application is in the foreground, actively being used, or simply open in the background can help to identify true employee activity.	✓		
Application Actions	Monitoring specific actions taken within applications gives insight into what employees are doing and whether they have the organization's intention at heart.	✓	✓	✓
Data-Related Actions	Monitoring when files are copied, emailed, uploaded, and printed can identify potentially malicious actions that can hurt the organization.		✓	✓

Choosing the Right Tools

There are a number of ways to monitor employees. In some cases, log data can identify activity such as logons, interaction with file data, and web activity. SIEM solutions can assist in centralizing log data from disparate sources to simplify audits of activity. But most activity – such as use within an application - requiring the organization to invest in 3rd-party solutions specifically designed to collect activity data. User Activity Monitoring (UAM) solutions create audit trails by monitoring and recording employee activity within a session. User Behavior Analytics (UBA) solutions focus more on identifying shifts in behavior, such as an employee that never prints documents suddenly printing 100 pages a day – a leading indicator there may be an insider issue.

[1] *Verizon, Data Breach Investigations Report (2018)*
[2] *Ponemon, Cost of a Data Breach Report (2017)*

STEP 2

Determine Who to Measure

Your first instinct might be to monitor every remote employee for productivity. But, in general, organizations aren't necessarily monitoring every single employee. Instead, they identify those employees whose roles within the organization present the greatest risk. From a productivity perspective, the risk is employees who cost more per hour. From a fraud perspective, those employees access to financial information and applications. And from a data breach perspective, those employees with access to critical or externally valuable information as part of their role.

So, at a basic level, identify the roles that fall into these three categories, pointing to specific remote employees that need to be monitored.

STEP 3

Baseline Employee Activity

Establishing what's "normal" is critical when monitoring remote employees. The baseline acts as the reference point by which their productivity and well-intentioned work activity is measured. For example, an employee consistently logs on every day at 9am and actively uses a job-related application between 4 and 5 hours, but then you begin to see logons occurring later in the morning, or a reduction in the time spent in the application. You can easily assess a reduction in productivity from the change in their activity. Likewise, if an employee rarely sends large emails containing attachments and then begins doing so, it could indicate data theft. These changes in behavior are only detected if a baseline exists.

The process of baselining may be a challenge, depending on how you are monitoring employee behavior. If using log data, you'll need to manually determine what looks out of the norm – whether on an individual or group basis. If using UAM solutions, you'll at least find it easier to pull the data – for example, running a report on a given user and their logon times would quickly give you an idea of when they logon. UBA solutions are usually designed to analyze user activity to automatically generate baselines, making it easier to establish regular user behavior – and identify shifts in behavior.

Determine When and How Long to Measure

As a general rule, a baseline takes a minimum of 30-60 days. However, even a baseline of a single week's worth of work does provide some value – just with a greater margin of error in identifying deviations from the baseline.

Creating a baseline can be done at any time, keeping in mind that should a job role change for an individual, their baseline may need to be reestablished. For example, in their old role in Sales, they used a web-based CRM solution all day, never interacting with file data. But in their new role in Marketing, they interact with files, leverage cloud file syncing, and send email attachments every day. You can see how the old baseline no longer represents "normal" behavior for this employee.

STEP 4

Plan a Response

As you begin to monitor employee activity, looking for shifts from a remote employee's baseline, it's important to have a response plan ready. If you see that an employee is surfing the web and watching cat videos 20 hours a week, what is the organization's official reaction and process to deal with this. A few factors need to come into mind:

Alerts

The point of monitoring remote employees is to be made aware when they deviate outside acceptable parameters. Most solutions have some kind of alerting functionality built-in. Determine the actions that require a response (e.g., looking at a job website once isn't an issue, but spending over an hour on one is) as well as the appropriate people within the organization to be notified (e.g., HR, IT, department heads, etc.).

Maintaining Covert Monitoring

Most organizations choose to monitor in stealth and without the knowledge of their employees in order to observe natural behavior. Users who are specifically aware that they are being monitored tend to find alternative ways to carry out self-beneficial or maliciously-intended actions. Consider how you will address an issue with an employee and whether you will use the behavior data collected as part of a confrontation.

Organizations monitoring in stealth tend to lean on HR to address the issue without divulging your monitoring implementation as the source.

Consider Security-Related Threats

It's one thing to find that an employee is spending too much time on the Internet and not doing their job – that scenario requires a relatively simple response on the part of the organization. But should you find that the employee is engaging in activity that can put the organization at risk, you may need an entirely different response. These activities include:

- **Employees Considering Leaving** – Should an employee be found to be looking for a new job, the organization's response may include proactive termination or further review of monitoring detail to see if the employee has taken data, etc., in light of their plans to leave your employment.
- **Fraud** – In reviewing application use by those with access to company financial data and applications, unusual activity (e.g., using the Accounts Payable application on the weekend or late at night) may be discovered.
- **Data Theft** – Data can easily leave the organization via cloud sharing, web-based email, messaging, and more.
- **Unwitting Insiders** – Should an employee become the victim of a malware infection that includes remote access to their workstation, it's possible that you may see user activity that is the work of a cybercriminal.

Because each of these actions are far more severe and pose a greater threat to the organization, having a plan that involves HR, Security, Legal, IT, and the executive team is needed.

Keeping a Watch on Remote Employees

It should be said that the remote employee isn't automatically a risk. But by being remote, the risk potential does increase. For those organizations concerned about the possible threats that a remote employee poses, monitoring employee activity is a viable choice. Focus on the activities related to the threats the organization is concerned about. Also, consider establishing formal policies and procedures around appropriate monitoring levels, the specific activity to be monitored, who monitors it, and the actions to be taken should an indicator of misuse or threatening behavior be identified.

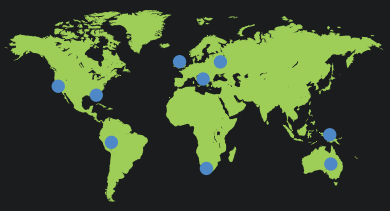
By putting monitoring in place, the organization can maintain visibility into employee productivity and activity without needing to review every action taken on a daily basis. Using technologies like UAM and UBA, organizations can proactively identify indicators that a risk may exist, heading off a potential threat.

Veriato Resources

Veriato 360 Information – Veriato.com/360
Veriato Recon Information – Veriato.com/Recon

To learn more about how Veriato can help you with employee investigation, contact a Veriato representative today.

Over 3,000 enterprises, & thousands of SMBs have placed their trust in our solutions



Our solutions are deployed in **110+ countries**

Veriato USA

4440 PGA Boulevard , Suite 500

Palm Beach Gardens, FL 33410

Veriato EMEA

3rd Floor, Crossweys House

28-30 High Street

Guildford, Surrey

GU1 3EL United Kingdom

https://plus.google.com/+Spectorsoft

https://www.linkedin.com/company/veriato

https://twitter.com/veriato

https://www.youtube.com/SpectorSoft

https://www.facebook.com/VeriatoInc/