




3 Steps to Spotting Insider Threats



The biggest challenge to spotting a threat is knowing what to look for.

Your employees have access to your organization's most valuable data - customer detail, intellectual property, personally identifiable information (PII), vendors lists, bank accounts, financials, and more.

When an employee no longer has the organization's best interests at heart and shifts their loyalty to themselves, they begin to look for ways to take advantage of company data, assets, resources, and money. This can happen because they're looking for a new job, are having financial difficulties, are experiencing personal issues, or simply have a sense of entitlement.

The greatest challenge for most organizations who are trying to identify insider threats, is visibility into employee behavior and actions. Without it, you lack context to understand whether activity is beneficial or harmful to the organization.

Veriato provides contextual user activity detail and screen recordings needed to investigate whether employee activity is appropriate, sanctioned, and well-intended. By logging all user activity and capturing screen detail for video playback, Veriato creates an indisputable audit trail that can provide context around what transpired, who did it, and, in many cases, why - all making your investigative efforts materially easier.

Introduction

Organizations focused on security threats tend to focus on the external attacker. Solutions used to secure the perimeter, endpoints, email, and data are put in place. While absolutely necessary, they organizations lack the ability to equally protect against the insider – the employee that puts the organization at risk through either malicious intent or negligence.

For example, data breaches are caused by insiders 28% of the time¹ - a staggering number, considering the other 72% is made up of external attackers leveraging automation, scripting, and other technologies to steal data, which only makes their job easier (and, therefore, creates opportunistic breaches). The insider, on the other hand, is someone who needs to personally perform the threat action, demonstrating the importance of the 28% number. The average data breach costs approximately \$3.82 million². Fraud is another great example of an insider threat – one that costs organizations an average of \$130K.

In either case, it takes months to discover the threat action – for example, the median duration of a fraud scheme is 16 months before it's discovered. The reason is that employees committing an internal threat action are performing the very same actions they use when doing their job appropriately.

So, what's needed is a means by which organizations can proactively spot insider activity before it hurts the organization, as well as an ability to investigate actions reactively to pinpoint when a threat action was taken, by whom, and what specifically was done.

This Getting Started brief provides some high-level guidance around the steps necessary to spot insider threats both proactively and reactively. While not exhaustive, it does lay the groundwork for you to begin planning and rolling out an insider threat program, complete with desired solutions.

¹ Verizon, *Data Breach Investigations Report (2018)*

² Ponemon, *Cost of a Data Breach Report (2017)*

Define “Insider Threat”

It’s not as simple as saying you’re looking for a “malicious insider”. You need to first define what means within your organization. There are a number of employee-related threats to the productivity, security, and profitability of an organization – each one gaining varying degrees of attention of IT, HR, Legal, and Executive teams.

So, within your organization, you need to determine which of the following insider threats are of concern, and whether that concern warrants analyzing shifts in employee behavior proactively, and/or monitoring employee activity to spot or investigate current threats.

- 1 Unproductive Employees** – Employees are the lifeblood of your organization. And the loss of focus on productive work can quickly translate into a material cost to the business. The simple act of each employee wasting an hour a week surfing the web can cost you. In a 100-person company, if each employee wasted an hour weekly, this equates annually to 2 and a half employee’s time normally put into work-related activities. In essence, you’d be paying for 2.5 employees to do literally nothing work-related all year.
- 2 Harassment / Discrimination Complaints** – An employee acting inappropriately in the workplace have serious financial repercussions. The EEOC reports that over 84,000 harassment and discrimination charges occurred in 2017 with damages in excess of \$355 Million.
- 3 Corporate Fraud** – According to the Association of Certified Fraud Examiners (ACFE)³, the median loss from fraud is \$130,000, taking 16 months to be discovered. With 85% of perpetrators being first-time fraudsters,
- 4 Insider Data Theft** – Data breaches are perpetrated by insiders 28% of the time¹. With an average breach size of a little over 24,000 records² and an average cost/record of \$1412, the average cost of a data breach is slightly under \$3.4 Million².

- 5 **Negligence** - The simple act of leaving a database exposed to the Internet or losing a laptop outside the office can have serious material repercussions.
- 6 **Unwitting Participants** - The innocent clicking of a malicious email attachment can infect a machine with malware, giving an external attacker a foothold within your organization, making the employee an unintentional accomplice to data breaches, ransomware attacks, espionage, and more.

Each of the threats listed above ultimately cost the organization. While most organizations focus on data breaches (because of the alignment with externally-based data breach attacks), all six are relevant threats to your business. But, don't just stop at choosing from the scenarios; dig into each one, developing scenarios specific to your business - this will become very important when you plan out your execution strategy.

As you develop your threat scenarios, keep in mind that what's important to the insider may not be important to the organization. Take the simple example of a list of vendors used by a manufacturing company. The organization may not see the list as something proprietary and worth protecting, but that list could be used by someone seeking to start a competing business. So, think about how an employee's actions (or inactions) can harm the business, and build your resulting list of detailed insider scenarios that define what "insider threat" means to your organization.

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

Monitor Leading Indicators

For most insider threat actions, there are common leading indicators - particularly in cases where the insider's actions are malicious in intent. Insiders don't just wake up one day and decide they're going to defraud the company; there are circumstances surrounding the action, as well as shifts in communications, behavior, and actions preceding it. As an example, the ACFE found that in 85% of fraud cases, at least one of 23 behavioral "red flags" were displayed by the perpetrator before they committed fraud³.

The following list of leading indicators include some of the ACFE's red flag behaviors and may apply to more than one of the previously mentioned insider threat scenarios.

- 1 Personal Issues** - Problems at home can be the source of insider activity. Changes in home finances, living beyond their means, divorce, depression, addiction, and legal problems all can put an employee in a situation where their priority - and therefore, their loyalty - shifts to themselves, looking for a way out of the situation.
- 2 HR Issues** - Work-related problems can also indicate an employee isn't happy with the organization. Employee that are written up for performance issues, have been passed up for promotion, or have been in violation of corporate policies/procedures are insider candidates.
- 3 Arrival/Leaving Times** - People are creatures of habit. They come to work and leave at the same time every day. So, if an employee that never comes in on the weekends suddenly does, it's cause for concern.
- 4 Communications** - An employee that has the company's best interests generally uses words like "we" and "us" and has a positive tone towards the company. One whose interests have shifted to themselves will have a shift in tone and words - their outlook on the company will be more negative, and the presence of "I" and "me" words will be more prevalent.

³ ACFE, *Report to the Nations (2018)*

- 5 **Looking for A New Job** – Someone existing the company is one of your greatest risks, as more than half of employees take information with them when they leave the organization. Repeat visits to job websites, as well as the receiving of job search notifications in company email are clear indications that someone is considering leaving.
- 6 **Searches on The Internet** – Tied with personal issues, web searches can reveal what an employee is thinking about. Searches for debt consolidation, marriage counseling, addiction, guns, etc. all can indicate potential problems for the organization.

There are a number of ways you can monitor for these indicators:

- ✓ **HR** – Human Resources is one of the greatest sources of intel about employees. They are aware of personal and personnel issues. They can provide IT with guidance around which employees pose a present risk to the organization.
- ✓ **User Behavior Analytics (UBA)** – HR's intel isn't enough to pinpoint an insider. UBA solutions monitor and analyze each employee's behavior, comparing current and past behavior and communications, looking for anomalies that may indicate a potential threat. Alerts can be sent so that HR, IT, and any other appropriate teams can respond.

Veriato Recon

With Veriato's UBA solution, Veriato Recon, 30 days of detailed user activity data and screen recordings is also collected. So, should an employee's behavior indicate a potential threat to the organization, their activity data can be unlocked, reviewed, and replayed to see if threat actions have already taken place.

Look for Active Indicators

Most insider threat actions involve activities that are a part of the employee's job function. For example, if an employee works in the finance department, the threat action may involve creating a vendor and cutting them a check – something they do regularly. So, it's difficult at best to identify active indicators of a threat without some guidelines around how to look for anomalies. The following list is by no means exhaustive but will give you some ideas of what to be looking for.

- 1 Unusual Logon Times** – Employees don't want to be caught, so coming in early and leaving late can be indicative of a problem. Additionally, multiple successive logons could indicate a nervous employee unsure about committing a threat action.
- 2 Abnormal Application Use** – There are a number of examples of potentially threatening application use. Using a particular function repeatedly (such as exporting data or running reports) could indicate data exfiltration. Using a browser actively in the foreground for an extended duration of time could indicate an employee wasting time browsing the Internet. Or simply using an application at an odd time of day, day of week, or day of the month (e.g. a payroll application that's only used twice monthly to issue paychecks being used several times in one week) can indicate inappropriate use.
- 3 Excessive Printing** – Employees can steal data “the old-fashioned way” by simply printing reports, screen captures, etc. While an inefficient method of data transfer, it's still effective in its ability to take data out of the organization. Printing that's either beyond an establish threshold (e.g. a number of pages per day) or is abnormal for a given user indicates potential misuse.
- 4 Abnormal Access of Sensitive Data** – Assuming the employee in question has permissions to access sensitive data, this is more about is it out of the ordinary. For example, accessing a project that hasn't been touched in a year, or accessing it after hours.

- 5 **Copying of Sensitive Data** – The saving of data to a USB stick, copying to a folder that syncs with the cloud, uploading directly to a website, or attaching to webmail are all examples of data leaving your organization.
- 6 **Communications** – Any conversations via corporate or personal email, web browser-based email, chat applications, even messenger within Facebook all provide context around why an employee is performing an action. Seeing a web-based chat that includes “I’ll bring the USB stick, you bring the money. 10pm tonight” probably gives you a good idea the employee is up to no good.
- 7 **Creating Backdoors** – Employees fearful of being fired who wish to come back into applications and systems they manage may create backdoor accounts to regain access once they’ve been fired. This can include an IT employee creating user accounts or a non-IT user installing remote control software on their workstation to connect to it after they’ve left your employment.

There are a number of ways you can monitor for these indicators:

- ✓ **User Activity Monitoring (UAM)** – Because nearly every action will take place on the employee’s computer, it’s imperative to UAM recording the actions of high-risk employees (which are either those you deem high-risk do to the nature of their role within the organization, or those that have triggered leading indicators by HR or a UBA solution). By having a solution on the employee’s endpoint, you record every action they perform regardless of application and without the need for external audit trails. UAM also empowers you to search through, identify, and playback activity before and after the event in question, providing context around a suspect action.
- ✓ **Security Information Event Management (SIEM)** – SIEM solutions act as aggregators of information from disparate systems and applications, providing a single view of all auditable data. They, generally, cast a wider net than UAM because of the variety of data sources, but usually lack the visibility into every user action, because they are limited to only collecting from systems and applications that provide an audit trail.

Veriato 360

With Veriato’s UAM solution, Veriato 360, records every user action performed on their computer, complete with screen captures. It provides unmatched visibility into an employee’s actions, leaving no activity hidden from its view. Activity can be reported on, generate alerts, searched, reviewed, and replayed as needed to identify, document, and intelligently respond to threat actions.

Spotting Insider Threats

The three steps covered in this paper provide high-level direction around the work necessary to spot an insider threat. While requiring solutions to accomplish most of the work, what makes your ability to spot threats successful is the defining what you see as a threat to the organization and defining the specific actions that need to be carried out.

By following the 3 steps above, and through the use of UBA and UAM solutions, you can rest assured you have the appropriate tools in place to reduce the risk of insider threat as much as is possible, and have the detail you require should you need to respond to an already occurred threat action.

Veriato Resources

Veriato 360 Information - Veriato.com/360

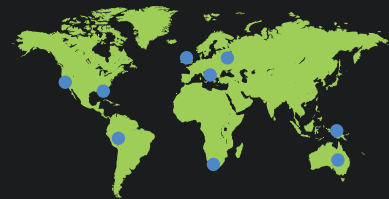
Veriato Recon Information - Veriato.com/Recon



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, Crossways 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/>