Fighting the Insider Threat

IT’S TIME TO THINK ABOUT BEHAVIOR NOT JUST DATA
Introduction

ELIMINATING THE INSIDER THREAT REQUIRES A DIFFERENT APPROACH

DLP and other traditional tools have been employed by organizations that need to control the movement of important documents and information exiting the company firewall. Many organizations, faced with the daunting task of managing the rise of the insider threat, have tried to use those tools to help stem that problem but the bottom line is they weren’t designed for that task. Each tool is an important ingredient in a smart, layered security approach but individually, they’re not designed to fight the insider threat. It’s kind of like using a butter knife as a screwdriver. It almost works, but not really.

The end result of using tools for tasks that are outside their scope can often be security that is too restrictive or wholly inadequate. For example, when a company uses DLP to restrict the way in which employees move documents they often end up sharing critical information in unsanctioned (and even riskier) ways. Or, worse than that, the flow of business-critical information screeches to a halt. In the end, neither approach works.

So, how can you keep your business running swiftly while striving to eliminate the insider threat? And how can you do it simply and without disruption?

Stopping the insider threat requires a different approach—one that recognizes the needs of the user and the security of the organization, and works with a company’s business processes rather than slowing them to a crawl.

About the Author

Daniel Velez is the senior manager for insider threat operations at Raytheon|Websense. He is responsible for the delivery and support of insider threat monitoring, investigation solutions and services to Raytheon’s customers. Prior to joining Raytheon, he served as a Senior Cyber Counterintelligence Investigator specializing in insider threat detection and investigations. He is also retired from the U.S. Navy Submarine Force, where he served duties ranging from nuclear reactor operations to strike group operations and antisubmarine warfare.

1http://www.computerlinks.de/FMS/22876.magic_quadrant_for_content_aware_data_loss_prevent.pdf

50% of enterprises use DLP1
GLOBAL CYBERSECURITY SPENDING IS AT AN ALL TIME HIGH…

In 2015, people are more connected than ever.

Everyone sitting in an office uses email, social media, the web, instant messaging—you name it. Some channels are expressly for business purposes, so IT governs and monitors them. Others are for personal use, even if they’re not officially sanctioned by the organization. A lot of that personal activity is innocent—parents communicating with children at school or making plans for later that day. It consumes some network resources, and most businesses are willing to write that off, but it brings with it the risks associated with the untrained or careless user.

On the other side of the equation are a very small number of people who present a serious insider threat.

They intentionally engage in hostile or malicious activities, often working hard to cover their tracks—as the attackers that breached Target in 2013 did. Their aim is clear: to inflict pain on IT systems and cause damage to the bottom line and reputation of an organization. Financial reports can easily show a price tag for IT systems and the hours it takes employees and consultants to fix them in the wake of an attack. It’s simple dollars and cents. But damage to the reputation of an organization and the toll it takes on customer goodwill is incalculable.

35% of enterprises report it takes weeks to fix things in the wake of a breach²

“…damage to the reputation of an organization and the toll it takes on customer goodwill is incalculable.”

²http://www.ponemon.org/blog/cyber-security-incident-response-are-we-as-prepared-as-we-think
…SO WHY ARE THERE MORE HIGH-PROFILE LEAKS THAN EVER BEFORE?

Gartner research shows that 50% of enterprises were using some type of data loss prevention (DLP) solution in 2014³. Gartner also forecasts that global cybersecurity spending will reach $76.9 billion in 2015⁴. So, it’s clear that organizations are not skimping on security.

With numerous safeguards in place, why are there so many high profile breaches? Because the solutions most organizations employ focus on the wrong thing—data.

Data is obviously important, but organizations struggle to identify all their data, classify its importance, tag it, store it in containers, and then use DLP or other tools to secure it. Despite the struggle, IT departments rely on these tools to control the movement of important documents and information exiting the company firewall—mainly because there hasn’t been a better way.

$76.9 billion in 2015

Enterprises will spend $76.9 billion on cybersecurity in 2015⁵

³http://www.computerlinks.de/FMS/22876.magic_quadrant_for_content_aware_data_loss_prevent.pdf
A solution for user activity monitoring should be simple.

It should operate in the background. Anyone authorized, even non-technical staff, should be able to immediately identify threats and behavior outside the norm. The solution should quickly identify high-risk user activity and help resource-constrained analysts, who often waste their time investigating false alarms (while the actual threats that lurk inside the organization go undetected).

At its core, a modern user activity monitoring solution should perform a number of critical functions, including:

- Protection from the network edge to the desktop
- Incident replay for forensics and investigation
- Detection of incidents even where all traffic is encrypted
- Capture of incidents that take place when a device is not connected to the network
- Ability to use policies that reflect an organization’s needs

Only 26% of enterprises have a defined insider threat management program\(^6\)

\(^6\)http://www.ponemon.org/blog/cyber-security-incident-response-are-we-as-prepared-as-we-think
\(^7\)http://www.medpagetoday.com/PracticeManagement/InformationTechnology/51074

“"A solution for user activity monitoring should be simple. ""
The “stop, block and tackle” approach of traditional data-focused tools isn’t very effective when it comes to stopping the insider threat. Organizations are often frustrated trying to force those tools to do something beyond their intended function, such as watching data movement and relying on them to stop an insider threat.

We all know there are other methods, such as content monitoring and filtering, but they also lack the context necessary to identify, analyze and react to threatening insider behavior. So, inevitably, they fail at thwarting the insider threat because they’re not designed to recognize it.

In the end, organizations will be able to do very little about insider threats if they keep the narrow focus only on data.

However, there is something very concrete an organization can do if they think more broadly and realize that insider threat is a user behavior issue.

74% of IT security professionals are concerned about insider threats from negligent or malicious employees.


“...think more broadly and realize that insider threat is a user behavior issue.”
THE RIGHT SOLUTION TO INSIDER THREAT SHOULD BE USER-CENTRIC, NOT DATA-CENTRIC

Organizations need an approach that’s simple to use, recognizes the needs of the user and supports the security requirements of the organization. Perhaps more importantly, the solution should work alongside a company’s business processes rather than getting in the way and slowing them to a crawl.

The solution is user activity monitoring, which doesn’t use the blunt force of limiting or rejecting an action. It looks at behavior and spots trends so an analyst can cut through the cacophony of alerts, determine the situation and immediately take action to stop an insider threat.

28% of IT security professionals say insider threat detection and prevention isn’t a priority in their organizations

32% of IT security professionals say they have no ability to prevent insider breach

HOW USER ACTIVITY MONITORING WORKS

Rather than attempting to stop and block unauthorized use of a USB stick, as DLP would, user behavior monitoring tells you if the controls are working and if the user is attempting to rename or obfuscate a file’s true content.

Instead of encrypting data at rest, so that only authorized persons can view and edit it, user activity monitoring lets you know if an authorized user is handling that sensitive data within the acceptable use policies of your organization.

While DLP might help you identify a privileged user attempting to make a rule change, user activity monitoring goes further by helping you determine if the privileged user should have just created that new service account on your network.

When a user’s laptop is off the company network, DLP might prevent access to your data. User activity monitoring tells you what the user did while off the network and what tools they used to try and circumvent your control.

An unauthorized user might be tripped up by DLP when trying to access a file. User activity monitoring tells you which users are using credentials that are not their own.

DLP might prevent the export of data from a sensitive web application. User activity monitoring tells you the user is taking screen shots of that web page.

DLP tries to prevent access to your systems by unauthorized users. User activity monitoring reveals that a user booted from removable media today.

MANAGING AND MITIGATING INSIDER THREATS

User activity monitoring should simplify the life of an analyst, not make it more complex. It should be easy to create and configure policies using a dashboard—in much the same way that we all create Outlook rules to direct our email to specific folders. In addition, verifying compliance should be a simple task that quickly detects and traces violations, then produces actionable, efficient results.

Create + Configure using Policies Analyst Dashboard

92% of healthcare IT decision-makers say their organizations are either “somewhat” or more vulnerable to insider threats

“User activity monitoring should simplify the life of an analyst, not make it more complex.”

11http://www.vormetric.com/campaigns/insiderthreat/2015/
USING VISIBILITY TO COUNTER RISKS

Effectively detecting, responding to andremediating the range of threatening user behavior requires a contextual view of user behavior.

That comes only from combining the best of network activity monitoring technologies with endpoint monitoring.

By applying the right remediation, implementing effective security policies, improving employee training, and targeting high-risk insiders, user activity monitoring can provide the visibility organizations need to counter the risks of inappropriate behavior.

Almost 1,000 large breaches affected more than 29 million individual health records from 2010 to 2013

1http://www.businessinsider.com/r-health-data-breaches-on-the-rise-2015-4#ixzz3XvL8tR0
FOUR QUESTIONS YOU SHOULD BE ABLE TO ANSWER

In the process of analyzing behavior, an effective breach mitigation program should help analysts answer these questions:

1. **Is trust misplaced?** The system helps determine whether a person committed the violation and moved data consciously, or whether it was an innocent error.

2. **Is a technical control not working as expected?** User activity monitoring looks at whether the movement of information happened because controls weren’t configured properly.

3. **Are employees following policies?** User activity monitoring examines whether the movement of data violated a policy. If it didn’t, an analyst would investigate whether the organization should put a new policy in place.

4. **Are policies too rigid?** If a certain type of violation has occurred several times, the system looks for a valid reason for it. Again, an analyst would investigate whether the organization should adjust or rewrite the policy.

Can you or your analysts answer these questions?

Getting a decent grade isn’t the point here. If you’re lacking on even one question, your breach mitigation program isn’t adequate—and could end up completely broken.