The Hidden Threat to Digital Enterprises

Insider born data breaches and attacks are rising faster than external attacks

Security professionals are awakening to the fact that they have been spending 100% of their effort on about 50% of the problem. The $120B security industry has long focused on defending organization's assets from outside threats - hackers and state actors trying to slip past their defenses.

What the industry has largely missed is the fact that internal actors are to blame for an increasing number of data breaches. According to Verizon's 2017 Data Breach Investigations Report, 25% of breaches were attributed to people inside the compromised company. That's an increase of about 12% compared to 2014.

The financial services and healthcare sectors are especially vulnerable. According to the 2017 IBM X-Force Threat Intelligence Index report, there were more insider-born attacks (58%) than outsider attacks (42%) on financial services companies in 2016. And, healthcare industry is the second biggest victim of cybercrime, with Insider and Privilege Misuse, Physical Theft and Loss, and Unintentional Actions accounting for 81% of the breaches, as per the latest Verizon 2017 Data Breach Investigation Report. Insiders have the trusted access and expertise to steal valuable corporate information and cause the most harm to the organization. To make matters even more complicated, many insiders are acting innocently and don't realize they're causing harm.

Most security products, whether it is a firewall or an anti-virus, endpoint encryption or web gateway, patch management or intrusion prevention system - focus on stopping bad guys trying to come in from the outside or access information they are not authorized to access. Now CISOs, security administrators and vendors must devote just as much time and resources, if not more, to battling the insider threat. While people and processes play a critical role, security teams are looking to improve their security incident and insider breach investigation capabilities through new technologies and innovations that deliver greater effectiveness. They need to be able to detect, investigate and manage insider threats, with complete user-data visibility, to quickly contain the business impact to their organization.

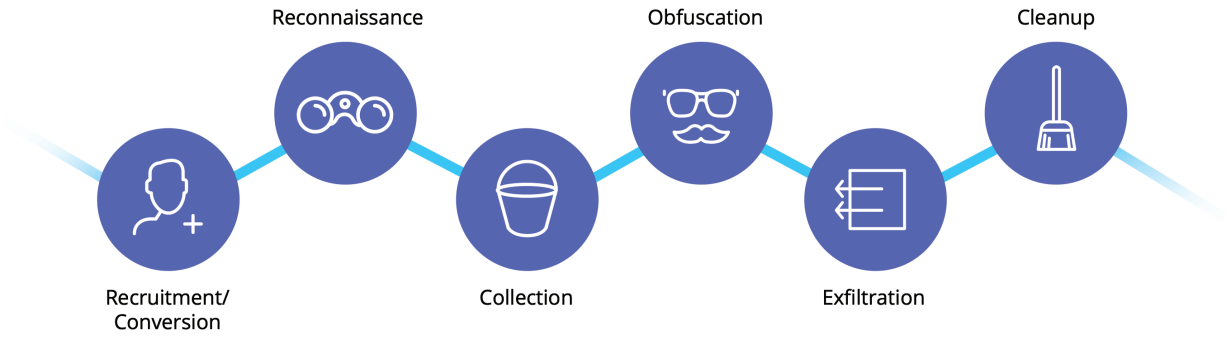
What types of data are put at risk by insiders? Pretty much everything a company cares about: personally identifiable information (PII), protected health information (PHI), intellectual property (IP), confidential business information (e.g. M&A plans), HR information, not to mention brand reputation.

When you think of an insider threat, you may picture the disgruntled ex-employee who steals data on his way out the door, or even a current employee selling confidential information to outside actors. But, not all insider threats are malicious. There are well-meaning employees who are just trying to get their work done and accidentally share sensitive information with somebody they shouldn't. Or, they knowingly bypass established data security policies. Dell's End-User Security Survey 2017 report found these employees are not acting maliciously. They simply ignore information sharing policies when they believe doing so will help the company, or help them be more effective in their jobs. In fact, nearly 80 percent expressed frustration over how their company's security policies hurt their productivity levels. Finally, reduced loyalty between a company and an employee also plays a role in employees feeling entitled to company's data.

Lately, our news have been full of examples of insiders taking organization's sensitive data: the Waymo-Uber case, Pfizer executive IP theft, defense contractor stealing national secrets, etc. Well publicized cases of Edward Snowden and Chelsea Manning highlight that even the CIA, the NSA and the FBI have all had serious insider-threat incidents leading to major damage to US national security. The fact is that organizations around the world share a very large problem, and the security industry is only now just waking up to it.

The Insider Threat Kill Chain

In a typical insider threat kill chain, it all starts with the **Conversion** stage when an employee becomes the insider. Whether becoming disgruntled for reasons such as being passed over on for a promotion or due to external recruitment efforts, coercion, or similar factors. The employees' sentiment changes and they start planning for malicious activities, in most cases eventual data theft and exfiltration.



The Insider Threat Kill Chain

Next comes the **Reconnaissance** stage. The insider surveys the environment for valuable data and determines where it "lives." It may already exist on the employee's endpoint or located on an accessible network share, SharePoint folders or in company's cloud share locations like Box or Google Drive. A company's customer contacts, source code and other intellectual property are all prime targets.

During the **Collection** stage, the insider focuses on accumulating this valuable data for future exfiltration. Sophisticated insiders try to stay under the radar by copying smaller sets of data at a time, giving their folders innocent-sounding names, working outside of normal hours, etc.

Prior to exfiltration, sophisticated insiders typically hide the data to be exfiltrated by converting it into less obvious or more difficult to inspect formats, like renaming files, ZIP'ing them or using encryption, hence this stage is called **Obfuscation**. Most basic DLP rules would prevent a user from copying 15,000 files to a USB drive or uploading plain text PII or PHI to a personal cloud share. However, DLP rules fail when company secrets are packaged in an encrypted archive.

The **Exfiltration** stage is straightforward: whether using a removable media, email, cloud storage or an FTP, whether fast or slow, whether obfuscated or not - data is leaving the organization.

Finally, the **Cleanup** stage. Most insiders spend at least some time covering their tracks by, at a minimum, deleting the cache of sensitive information they have accumulated in the Collection stage.

To make the entire process more complex and difficult to detect, sometimes there are mini-loops within the overall kill chain, where an insider tests exfiltration on a small data set, while planning for a larger exfiltration.

Changing Winds

Various traditional security vendors have started marketing or repositioning their existing products towards this newly recognized threat:

- **DLP** is focused on blocking unauthorized data actions, such as exfiltration, but does not have visibility into information creation and usage. Also, DLP requires configuration of complex rules, which is akin to trying to predict the future. You have to ask yourself questions like "what is it that I care about that should not be shared externally?" Coming up with the perfect answers upfront is virtually impossible.
- **UEBA** is only as good as the sources and quality of the data that is fed to it. It is designed to find anomalies, either caused by malware or malicious insider, but is often blind to what's happening on the endpoint itself. Or, if the data access appears to be 'normal' by a 'trusted' insider.

- **SIEM** wasn't built for insider threat detection in mind. It is a system/event log aggregator and parser with some intelligence and rule-engine built on top of it. It is still a needed component in the enterprise security ecosystem, but it is not an insider threat platform by itself.
- **EDR** is focused only on detecting malware that passed through other defenses and has no visibility on the information content level.
- **Endpoint security/AV** attempts to block external attacks via malicious executables.

Cobbling together a security system built out of these multiple parts that were not designed to focus on the insider threat has proven to be ineffective. We need new technology and an innovative platform that is purpose-built to address insider threat detection and investigation.

Introducing Insider Detection and Investigation

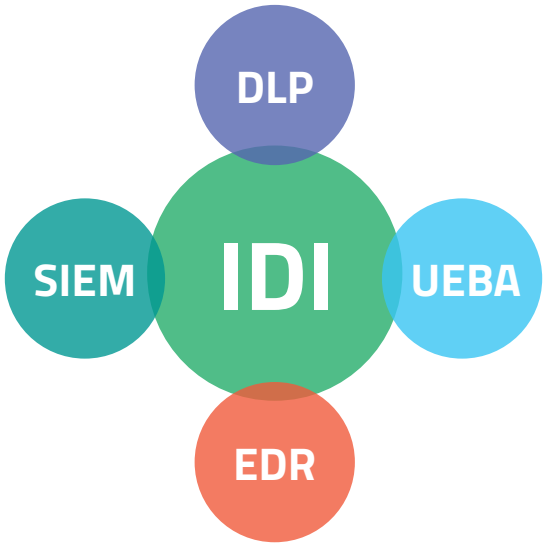
Yes, it is interesting to know that file XYZ was uploaded to DropBox. But it's much more useful to have real-time insight that file XYZ, containing 24,000 credit cards numbers, including a specific credit card number 1234-4444-5555-0987, was uploaded to a specific Dropbox location, using Google Chrome, by user "Bill", from BillSMacPro machine, at 10:05pm on July 4th, 2017. That information attribution is critical for today's environment.

Insider Detection and Investigation (IDI) isn't something that is run on an infrequent static schedule. Rather, it provides real-time continuous tracking of all activity at the data-element level. In other words, IDI provides unique context into how data is created, accessed, moved and shared.

Having a purpose-built IDI product enables you to focus on detecting insiders throughout every step of the insider kill chain, when DLP, endpoint security and other solutions are unable to.

Of course, not every stage of every insider-driven exfiltration can always be detected. However, even if the insider suspicious activity was detected during one of the later stages of the insider kill chain (e.g. Cleanup), the solution should allow you to walk it back using the digital breadcrumbs in hand. Furthermore, by modeling behavior and putting seemingly disconnected moments together, it should be possible to predict the insider's next step and even its timing. For example, if stages 2, 3 and 4 already happened, then the likelihood of exfiltration happening is extremely high. This should alert the security ops team to immediately take an action to prevent further damage and loss of data.

Insider Threat Needs a Purpose-built Solution



Focus on the Data

Even the most capable security system cannot prevent every attack. That's why your security framework needs to include some combination of technologies that provide you with a real-time visibility into your data and its usage.

ThinAir isn't another silver bullet replacing all other security tools. SIEM and similar tools provide you with extensive and relatively easy to use search capabilities. But do you go to Google for the sake of searching or for the long list of results? No, you want the answer. That's why ThinAir provides you with the computed answer (similar to WolframAlpha or Google's knowledge graph), rather than with the long list of possible results. It can also help orchestrate other security tools like firewalls and DLP products to respond to insider actions.

Real-time continuous nature of data-element level visibility is hard to underestimate as well. In a recent Stanford University article, Clifton B. Parker states that "...people change over time, background checks do not really provide measures of an individual's character, only his or her current state of mind". If your insider threat detection product isn't continuous, you will get "snapshots, not portraits" of your employees and thus likely miss the Conversion stage on the insider kill chain.

No Rip-and-Replace

If you already spent time and money implementing DLP or another endpoint protection software, emergence of IDI doesn't mean you should now uninstall it from your users' desktops and laptops. Your primary objective should be two-fold: implement the technologies that will further strengthen your security posture, and do so without interrupting your users as they try to get their work done every day.

We designed ThinAir to provide you with complete visibility, insight, and chain of custody over your most important digital assets - your information - without changing the way your users interact with it. Just as important as its capabilities, is how seamlessly ThinAir integrates with, and enhances, the effectiveness of your current security systems.

Overall, IDI is a pivotal part of the insider threat prevention strategy. At the same time, you should of course continue investing in employee training and deterrent measures, separation of duties, least privilege policies, and conduct regular access and data policy reviews.

Insider threat mitigation needs to be a high priority in enterprise security programs across all organizations in every sector. Healthcare, Finance, Technology and Public Sector organizations are reaching an inflection point with insiders becoming the major threat actor in most data breaches, motivated by financial and espionage reasons. In the federal space, insiders have already become the major source of sensitive and secret information loss.

Every organization should review their security program and consider an **Insider Detection and Investigation** platform to improve their security incident and insider breach investigation capabilities.

About ThinAir

THINAIR SIMPLIFIES INFORMATION VISIBILITY AND SECURITY ENABLING INSIDER THREAT DETECTION AND INVESTIGATION IN 90 SECONDS

ThinAir answers sophisticated questions about information creation, consumption and communication through easy to use search and analytics, tracking and reporting. We continuously track and record information interactions across the entire enterprise, empowering security and IT professional to have instant data-element level visibility in real time and historically, even if the evidence has been tampered with or destroyed.

ThinAir participated in Y Combinator's W15 class and is built by a team from Palantir, Dropbox, Microsoft, Apple, Juniper, Symantec, Cisco and former members of the NSA and U.S. Department of Defense.

"Security teams seeking continuous data-element visibility to enable rapid detection and investigation of insider threats should take a close look at ThinAir's purpose-built solution"

ENTERPRISE STRATEGY GROUP, JULY 2017

THINAIR

Learn more at:
www.thinair.com
testdrive@thinair.com

HIPAA

AICPA SOC 2