ENHANCED DATA PROTECTION AGAINST THREATS INSIDE THE PERIMETER

WHAT IF you could enhance your ability to detect and respond to insider attacks proactively, without negatively impacting workflow and without adding to the seemingly endless barrage of noisy, low priority alerts.

The financial and reputational effects of a data leak on an organization are well known. Around the world, organizations are increasingly aware that 'building a wall' to keep the barbarians outside of the gate is no longer sufficient; there are very real threats emanating from both malicious and accidental insiders.

An effective insider threat program requires a mix of people, process, and technology. Over-reliance on, or neglect of, any of these three pillars has significant negative impacts on the ability of an organization to effectively identify and react to insider incidents before they become damaging (and with increasing frequency publicly known) attacks. The good news is that a sound technology foundation - investment in solutions designed specifically to deal with insider threats - minimizes the impacts on people and processes.

Veriato provides the ability to detect meaningful shifts in insider behavior through evaluation and analysis of critical technical and psycholinguistic indicators, in combination with the creation of a context-rich system of record of the human activity that is occurring in the time before, during, and after anomaly detection.

How Veriato™ Delivers Value

Veriato's User Behavior Analytics is designed to cut through the noise and deliver meaningful alerts. Through a combination of machine learning and statistical analysis, Veriato identifies normal behavior for the people and groups in your organization. When a deviation from normal data access and / or movement is detected, a detailed alert is triggered. Rather than using a simple "is allowed / is not allowed" rule based approach or alerting on activities, Veriato applies an intelligent analytical layer that reduces the number of alerts, allowing you to prioritize what is truly important.

Many User Behavior Analytics solutions stop there, but Veriato also delivers investigation efficiency by creating a detailed, context-rich and easily understood record of actual user activity. From one console, the Veriato solution reduces the time and staff required to investigate alerts.

One of the central challenges when dealing with insiders is improving security without negatively impacting the ability of your employees to do their jobs. The Veriato solution rapidly detects elevating insider risks and attacks, but doesn't interfere with business workflow.

Veriato™ Insider Threat Solution:

Persistent Detection - Forensic Grade Investigation

Veriato is built to detect the unknowns within your perimeter. Our solution conducts constant reconnaissance within the online and communications fabric of your company. It focuses on the actions and behavioral patterns of people at the point of intersection with organization resources and watches for meaningful deviations from the norm that suggest threat. Because an attacker, no matter how sophisticated, will cause a deviation from normal patterns.

Veriato analyzes technical indicators - the ways insiders interact with, and move, data. We also focus on psycholinguistic indicators, machine reading content to cull early warnings of insider behaviors through insight into emotional state and attitude, without requiring human review of employee communications. When further investigation is needed, Veriato delivers forensic grade results, acting as a clear system of record of insider activity for use in interdiction, response, and when needed, as evidence.

Common Use Cases

DATA LEAK

Protecting company and customer data is the top security priority for organizations. Insiders carried out 60% of cyber attacks[1], and insider-related breaches drove about 80% of data breach losses in 2015. Employees require access, but that access creates risk of both inadvertent and malicious data leaks. Veriato employs behavioral analysis to identify access to, and movement of, data outside of normal work patterns. Comprehensive insider activity monitoring detects dangerous actions and provides unmatched visibility into exactly what is happening - visibility needed for effective reaction and response.

IP THEFT BY DEPARTING EMPLOYEES

The 'High Risk Exit Period', comprised of the 30 days prior to notice of resignation or termination, is the most common time for critical data to be taken by insiders. 59% of employees who leave an organization say they take sensitive information with them[2]. Organizations should review departing employees' online activity, but few do so effectively without purpose-built solutions that enable this practice. Veriato creates a system of record of employee activity that perfectly aligns to this need, providing a single pane of glass capability to accurately assess and react to the risk to data security posed by departing employees.

WORKPLACE INVESTIGATIONS

Inappropriate workplace behavior can have profound negative impacts on morale and productivity, disputes between co-workers or management and employee create significant distractions that jeopardize the team's mission, and lack of clear documentation can increase the cost of defending against wrongful termination claims and expose the organization to legal risks. Veriato solutions are used everyday to create definitive records of events that have been tested and proven reliable over and over again. In addition, studies have shown more than 90% of insider threat cases were preceded by negative workplace events[3], making workplace investigations a security issue as well.

MONITORING HIGH RISK POSITIONS

All employees have some level of access to corporate data and systems. Some, by the nature of their positions, have elevated privileges. Frequently these are employees involved in the creation of the products and services that make up the organization's value proposition, or have access to sensitive data types like customer records, financials, and employee PII. Trust is a foundational element of an organization's relationship with its people, but trust without verification places the organization at risk. Veriato's ability to provide insight into both the behavioral patterns, and online activity, of privileged users sits at the core of a robust data protection strategy.

INCIDENT RESPONSE

When external forces attack, company cyber security experts handle the response. Insider attacks require an extended incident response team, typically including Legal, HR, business line management, and at times, the courts. Swift decision-making and sure response requires clear communication of exactly what is happening and who is involved. Presenting evidence in clear, concise, non-technical format can make the difference between effective response and damaging attack. CSIRT teams worldwide use Veriato to gain swift understanding of the size, scope, and severity of insider driven incidents, and to share that understanding quickly and effectively with the extended team to get results.

PRODUCTIVITY & PLANNING

Having insight into employee and departmental workflows is invaluable when making staffing decisions. Assessing the effectiveness of tools in use and training programs can lead to marked upticks in efficiency. Studying the way top performers structure their day, and the resources they use to achieve results, can inform new hire onboarding, cutting down on ramp up times and improving overall productivity. Veriato collects and aggregates a wide-range of information related to the day-to-day activity taking place in the online and communications fabric of an organization, and delivers high value reports and insight that are used to both increase the top line and improve the bottom line.

[1] *Source: BM 2016 Cyber Security Intelligence Index* [2,3] *Source: Deloitte Debrief, March 2016*

Veriato

What's at Stake

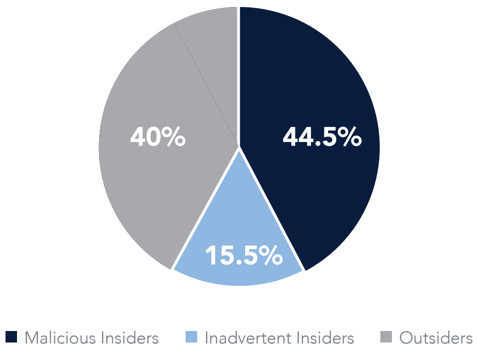
Insiders Represent the Biggest Security Threat

60% of Cyber Attacks in 2015 Were Carried out by Insiders

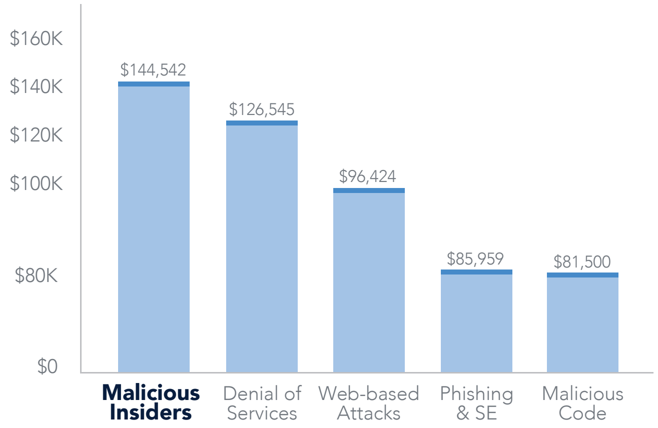
- Insider-related breaches drove about 80% of total losses in 2015
- In a recent 451 Research survey, insider threats ranked as the 2nd highest cybersecurity concern and the fastest growing among organizations
- Businesses are more vulnerable to these attacks because traditional security investments fail to detect insider threats

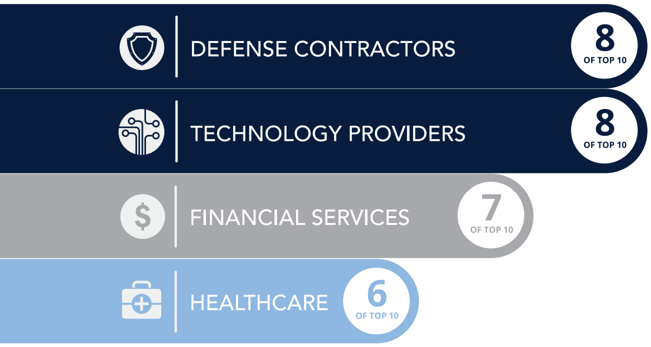
Breach Source

Insiders are the cause for **over half (55.5%)** of all Breaches



2015 Cost per Incident





Why Veriato

Veriato is an innovator in actionable User & Entity Behavior Analytics and the global leader in User Activity Monitoring. Based in Palm Beach Gardens, Florida; founded in 1998 and backed by private equity firms Harbourvest Partners and Westview Capital Partners.

Veriato provides a unique, fully integrated solution that focuses on detection and response to insider threats through a combination of advanced behavioral analysis and context-rich logging of insider activity.

Built to detect the unknowns within your perimeter, our solution conducts constant reconnaissance within the online and communications fabric of your company, detecting risks and threats that would otherwise go unnoticed until they became actual attacks.