Veriato

Veriato® Recon

Veriato Recon is a User Behavior & Entity Analytics Software that detects threats to data security from within the perimeter by monitoring user behavior and alerting when actions contradict policies or vary from well-defined patterns. Rather than focusing on protecting assets, Veriato Recon monitors user behavior for indicators of compromise, recording and alerting when insider risk is elevated, enabling rapid interdiction, reducing false positives, and insuring actionable reporting. Veriato Recon is designed for companies who have sensitive intellectual property, which if stolen or exposed poses risk to the company, and want to protect critical information without locking systems down so tightly that productivity is hindered.

Veriato Recon

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.

DEFENSE CONTRACTORS	**8**	OF TOP 10
TECHNOLOGY PROVIDERS	**8**	OF TOP 10
FINANCIAL SERVICES	**7**	OF TOP 10
HEALTHCARE	**6**	OF TOP 10

⚙ Key Features

Recon is always on, monitoring the behavior patterns of users and scanning for signs of an insider threat. The software learns what normal looks like, and adapts to changes in routine seamlessly. The agent runs silently, in the background, and Veriato Recon does not interfere with business processes or productivity.

Veriato Recon applies machine learning and advanced statistical analysis to detect, prioritize, and alert on indicators of compromise by watching for anomalies in user behavior. Veriato Recon also includes alerting on keyword and phrase usage that are proven indicators of insider threat activity.

Employee activity logs are created and stored on the local machine where the activity is occurring for up to 30 days. To ensure the logs are safe and available, these employee activity logs are encrypted and obfuscated. The employee activity logs provide a comprehensive record of everything that an employee did before, during, and after an alert.

✨ Benefits

Veriato Recon's behavioral analytics capability provides critical insight into shifts in established patterns that are directly related to insider threat behavior. Early detection is key to mitigating risk, harm and the threats insiders pose. By focusing directly on the behavior of insiders, Veriato Recon can isolate anomalies and alert on them immediately.

No more piecing together information from disparate sources in an effort to reconstruct what happened. Save time and money with a system of record that doesn't require specialized expertise to decipher. Veriato Recon supports best practice of reviewing departing employee online activity during the 30-day period prior to resignation or termination.

Best practice dictates aggregating user activity data with other sources of intelligence to minimize the risk of an insider threat. Integrations with leading SIEM providers, along with the ability to export data via syslog, provide a powerful stream of user activity intelligence to the solutions you've already invested in – making them even more effective.

🔖 Capabilities

Analyze
Machine learning and statistical analysis applied to identity anomalies that indicate risk to data security stemming from trusted insiders or compromised credential attacks

Collect
Full fidelity user activity data collected at the endpoint where the activity occurs, and from the network to support detection of additional indicators of compromise
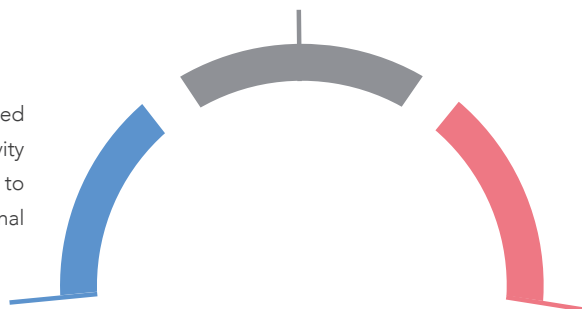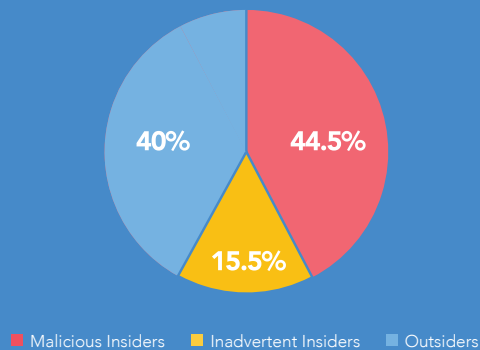
Alert
Meaningful anomaly alerts plus alerting on critical events, activities, and language (keyword and phrase) usage sent to your SIEM or anywhere else you need them
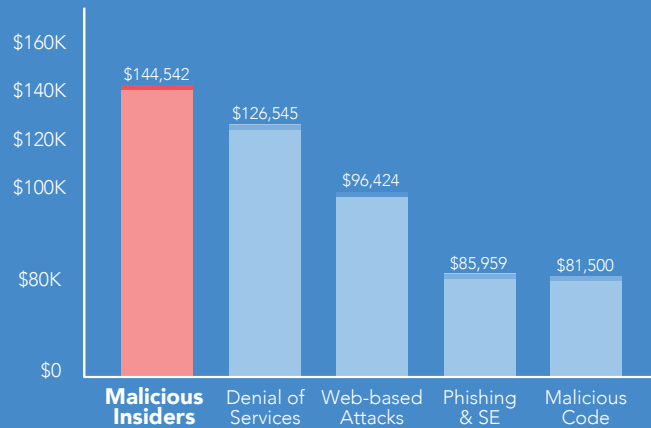
60% Of Cyber Attacks Were Carried out by Insiders

Breach Source

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

- Malicious Insiders — 44.5%
- Inadvertent Insiders — 15.5%
- Outsiders — 40%

In a recent 451 research survey, **insider threats ranked as the 2nd highest cybersecurity concern** and the fastest growing among organizations.

Cost per Incident

	Cost
Malicious Insiders	$144,542
Denial of Services	$126,545
Web-based Attacks	$96,424
Phishing & SE	$85,959
Malicious Code	$81,500

Businesses are more vulnerable to these attacks because **traditional security investments fail to detect insider threats**

Common Uses

Data Leak Prevention

Specifically designed to augment traditional DLP and other preventative security measures, Veriato Recon identifies insider risk and threat to data security by watching for changes in data access and movement. A robust data security strategy requires focus on device, data, and user.
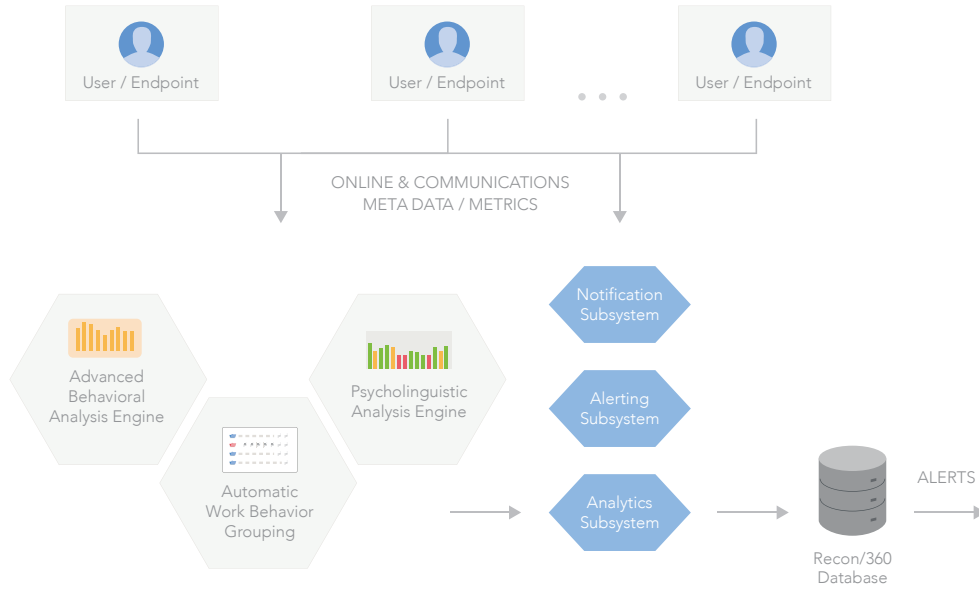
IP Theft

Malicious insiders and departing employees target valuable intellectual property. Veriato Recon not only alerts on the deviations in data movement that occur when IP is taken, it creates a system of record that supports best practices related to the threat that exists when employees leave.
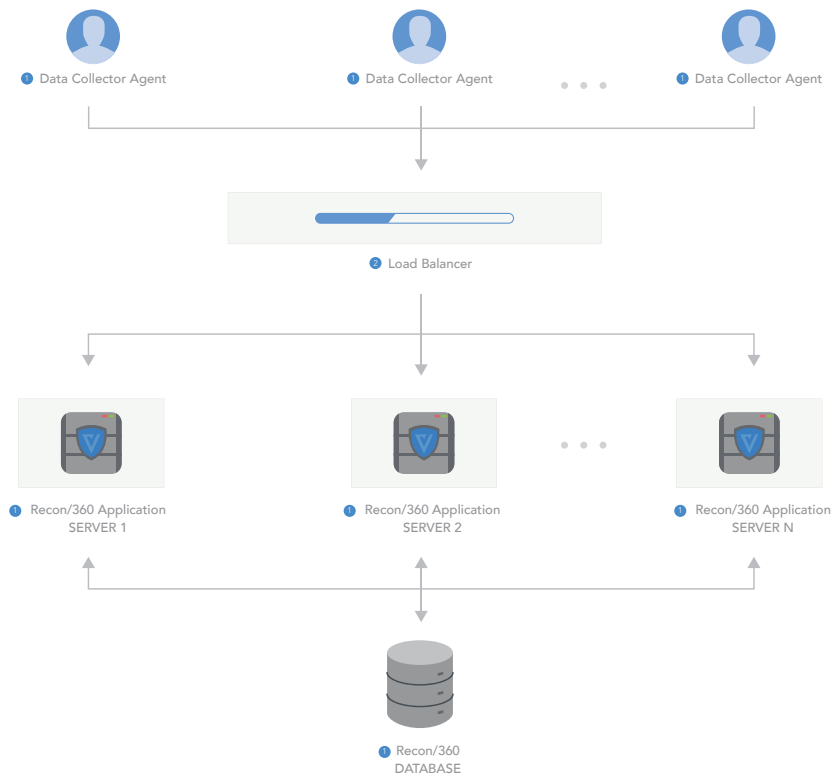
High Risk Insiders

The behaviors of highly privileged users, employees involved in negative workplace events, and contractors, need to be more closely inspected and monitored to protect against a damaging attack. Veriato Recon evaluates behavior shifts in near real-time, so security teams can focus resources where they can be most effective.

Components

User / Endpoint   User / Endpoint   · · ·   User / Endpoint

ONLINE & COMMUNICATIONS
META DATA / METRICS

Advanced
Behavioral
Analysis Engine

Automatic
Work Behavior
Grouping

Psycholinguistic
Analysis Engine

Notification
Subsystem

Alerting
Subsystem

Analytics
Subsystem

Recon/360
Database

ALERTS

Architecture

Data Collector Agent   Data Collector Agent   · · ·   Data Collector Agent

Load Balancer

Recon/360 Application
SERVER 1

Recon/360 Application
SERVER 2

· · ·

Recon/360 Application
SERVER N

Recon/360
DATABASE

ANALYZE
Analyze a wide range of activity as it occurs

DETECT
Identifies & alerts on anomalies in data access & movement

PRIORITIZE
Cuts through noise by isolating meaningful signals

RESPOND
Reduces time & staff needed to investigate

Analyze - Detect - Prioritize - Respond

Veriato Recon is purpose-built to lever the power of machine learning and advanced statistical analysis. The software analyzes the behaviors of the users on your network to detect indicators of compromise that would otherwise be missed, and cuts through the noise to provide meaningful alerts through an elegantly simple prioritization capability. When used in conjunction with Veriato 360, Veriato Recon is a key part of a robust insider threat solution, supporting the four pillars of User and Entity Behavioral Analytics.

Trusted by **thousands** of companies in more than 110 countries around the world

Get a Quote

Download 15-Day Trial

Veriato

Go to **www.veriato.com** for a Free Trial or email us at: sales@veriato.com