SPIRION

SOLUTION OVERVIEW

Spirion Sensitive Data Watcher: Privacy risk management for unauthorized or abnormal access to sensitive data

Spirion Sensitive Data Watcher

Spirion Sensitive Data Watcher (SD Watcher) on the Spirion Sensitive Data Platform collects and monitors user activity on files and folders. It enables quick identification of patterns in a wide range of behaviors that might indicate privacy violations, data breaches and exfiltration, or malware infections to reduce the likelihood of malicious activities. It allows organizations to focus not just on where sensitive data exists, but also on what is being done to that data and by whom.

Sensitive data challenges

All organizations struggle with concerns over misuse and exfiltration of sensitive data by internal and external bad actors plus inadvertent privacy lapses due to sensitive data being accessed by authorized employees. To increase visibility and accountability for data privacy and security, you need more information than just where your sensitive data
is located.

Monitoring access to centralized databases and cloud repositories is often the easiest point of control over sensitive data. However, in the normal course of business, large amounts of sensitive data can end up on laptops, workstations, and file servers regardless of centralized controls. This data proliferation has accelerated with the move to broader remote and work from home infrastructure, making the security perimeter of centralized data unavoidably much more porous and riskier. Privacy regulations require that you locate and secure all sensitive data you hold on consumers, not just the data in your centralized databases.

The solution

Spirion SD Watcher, powered by the Spirion Sensitive Data Platform, collects file and folder activity on endpoints to help identify unauthorized or abnormal behavior on sensitive data, thus allowing companies to prioritize privacy risk management by determining if sensitive data may have been accessed or exfiltrated. It watches over usage and movements of sensitive files and folders as well as detecting some common malware and breach indicators, such as deletion of log files and accesses to system folders. By providing these alerts, it provides another means to proactively detect, monitor, and stop potential privacy violations and loss of data privacy.

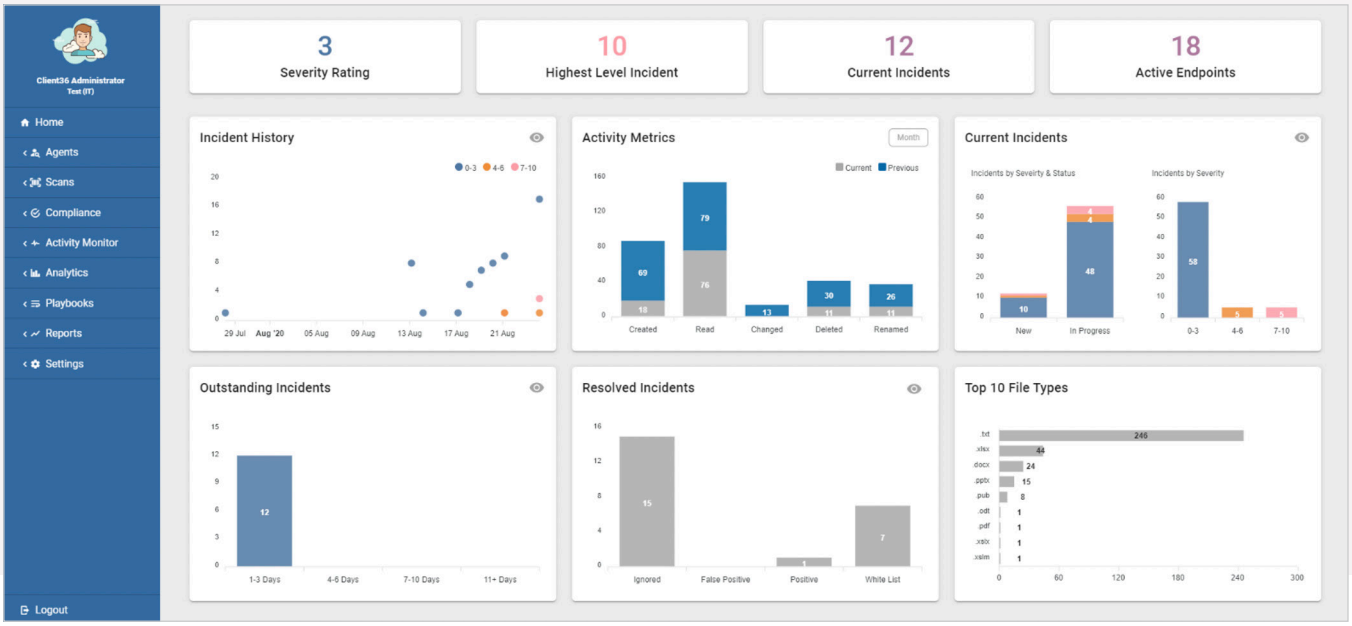
With a growing body of regional privacy laws and regulations, Spirion SD Watcher also helps implement tighter control over sensitive personal data to help remain in compliance. It helps organizations track and identify potential factors and exposures to enable real-time privacy risk management for sensitive data—no matter where it lives or goes in your IT infrastructure.

Key features

1. Monitor activity Collect user behavior analytics (UEBA) activity on files and folders in customer-designated areas on endpoints and servers. The activity captured includes all create, read, update and delete (CRUD) activity on any data where the agent is installed.

2. Pre-built queries an incident definitions Leverage right out of the box, or configure queries and incident definitions specific for your organization. Configurable items include severity rating, description, and associating queries to the incident definition. When thresholds are met, incidents are created and users are able to review and investigate.

3. Expose potential threats Leveraging queries that are based on the MITRE ATT&CK framework, users can identify potentially malicious activity. For example, one of the queries will raise an alert when .log or .txt files are deleted from an endpoint to address the MITRE ATT&CK defense evasion technique “indicator removal on host.”



Example dashboard shows several key metrics at a glance.

Summary

Spirion SD Watcher augments the accuracy and breadth of data discovery delivered by the Spirion Sensitive Data Platform by allowing data stewards to better to manage compliance and privacy risk via intelligent and targeted activity monitoring. By prioritizing privacy risk management based not just on the presence of sensitive data but also on ongoing user activity on folders and files, organizations can determine if, when and, how sensitive data may have been accessed or exfiltrated and build a stronger security posture.

Talk to a Spirion data security and compliance expert today: expert@spirion.com

Spirion has relentlessly solved real data protection problems since 2006 with accurate, contextual discovery of structured and unstructured data; purposeful classification; automated real-time risk remediation; and powerful analytics and dashboards to give organizations greater visibility into their most at-risk data and assets. Visit us at spirion.com