SailPoint

SOLUTION BRIEF

Address Cyber Threats with Alerting and Forensics

In today's data-centric landscape, organizations are dealing with a growing number of applications and data used by their employees, partners, vendors and many other types of users. Without the right identity governance approach to manage and monitor access to these applications and data throughout each user's lifecycle with the organization, enterprises expose themselves to a wide range of insider and external threats.

As the number of users and individual points of access continues to grow, so too does the risk, especially when many enterprises maintain millions of files, folders and other data repositories that house sensitive company and personally identifiable information. Maintaining a clear line of sight to the sheer volume of user access, and determining whether day-to-day user access activities are appropriate and compliant with company policies, becomes an overwhelming task.

Cyber Threats to Your Organization

Data breaches continue to be an ongoing problem impacting organizations across every industry. Companies that maintain large volumes of sensitive information will often be targeted by external actors, but breaches also arise from the malicious or unintentional actions of insiders. Often, breaches are the consequence of poor security practices, including the inability to properly govern user access with a least privilege model across applications and file storage systems. This results in the ability for a hacker to take over the credentials of an employee, or for an insider to gain unauthorized access to sensitive data. Breaches have become so prevalent that in a recent survey, 3 in 5 organizations responded they expect to be breached within the next year, and one-third of them will be unaware that one occurred.

[1]SailPoint, *2017 Market Pulse Survey*

Ransomware is another concern plaguing organizations around the globe. This malware can exploit vulnerabilities in a network or through phishing to gain access to sensitive company data. Once the ransomware infiltrates an organization, it begins to systematically encrypt data across servers and files shares. With open access enabled by users on the network, thousands or millions of files can quickly undergo a suffix change as they are encrypted. Organizations such as hospitals, utilities, government agencies and financial institutions may be particularly susceptible, due to highly sensitive data that may require immediate access.

Lack of Visibility

Organizations that have dealt with a security incident can often trace it back to security gaps related to limited insight and control of their data stored in files. It becomes difficult to know where data is located, what sensitive information is within it, and how users (or cybercriminals) are accessing the data. According to Gartner, upwards of 80% of enterprise data is comprised of unstructured data, yet organizations are not taking the necessary steps to protect this data. This growing volume of ungoverned, unstructured data provides hackers with an easy target that is rich with valuable information.

Adding to this shortcoming is an inconsistent or non-existent set of access controls that should span across both applications and files. There may be controls in place to govern access to applications, but as users extract data from these applications and store them in file shares or in the cloud, sensitive data may become unprotected. Without visibility and an understanding of who has access to files across the enterprise, organizations expose themselves to both inside and external threats.

Failure to secure access to these files also opens up significant compliance risk. Privacy regulations, including GDPR and HIPAA, require companies to protect access to personal data, with harsh penalties resulting for companies that are unable to comply.

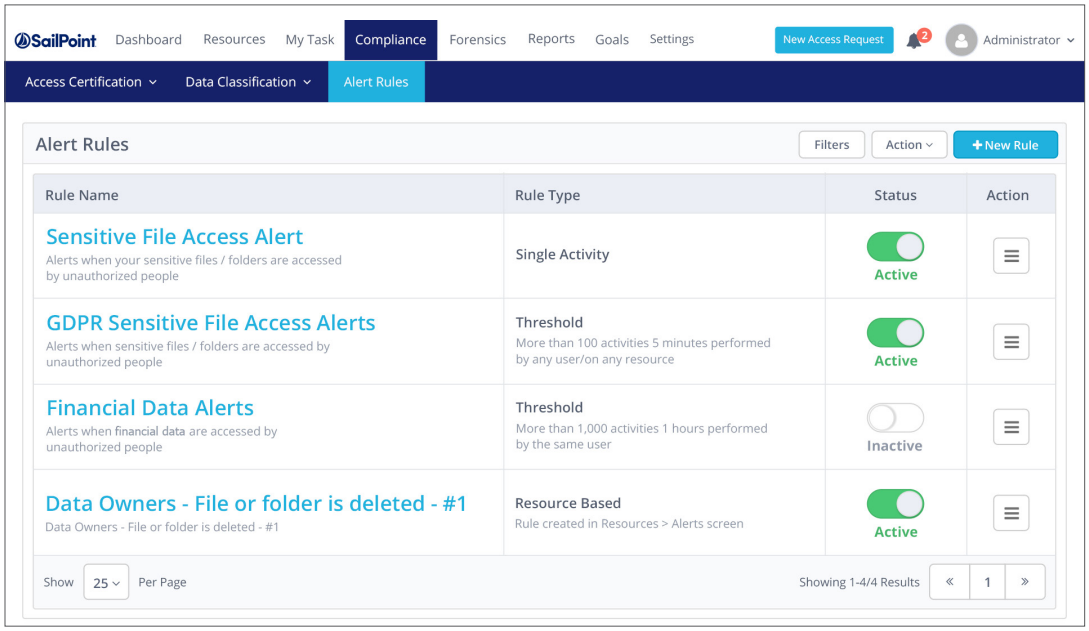
Build Upon a Foundation of Identity Governance

Reducing exposure to cyber risk should start by taking a comprehensive identity governance approach across all applications and files. By leveraging a consistent set of access controls and monitoring capabilities, which includes access to files, organizations can gain the visibility and control needed to identify suspicious activities before it's too late. Maintaining clear visibility into the activities of thousands of users across terabytes or even petabytes of unstructured data is a task that simply cannot be done without the right technology and processes.

Stay Ahead of Cyber Threats with Risk-based Alerting

SailPoint File Access Manager arms organizations with risk-based alerting capabilities to help detect suspicious activities, and stay informed of violations in real-time. File Access Manager monitors activities on files, and when a violation of access policies is detected, it alerts data owners and admins who can respond with the appropriate action. If something is identified as a threat, additional steps can be taken such as a full revocation of the user's access as part of a closed-loop risk mitigation action in the identity goverance platform.

With an automated alert management framework, rules can be easily configured in an intuitive interface based on a single activity, a threshold of multiple activities, or access to specific resources. The threshold alert is valuable in identifying patterns that are associated with complex threats, such as ransomware. This type of alert rule sends out a notification when a number of activities in a given timeframe exceeds a defined limit, e.g. a user is accessing more than 500 files in an hour. Automated alert rules are a key line of defense to help detect and respond to a variety of threats in real-time.



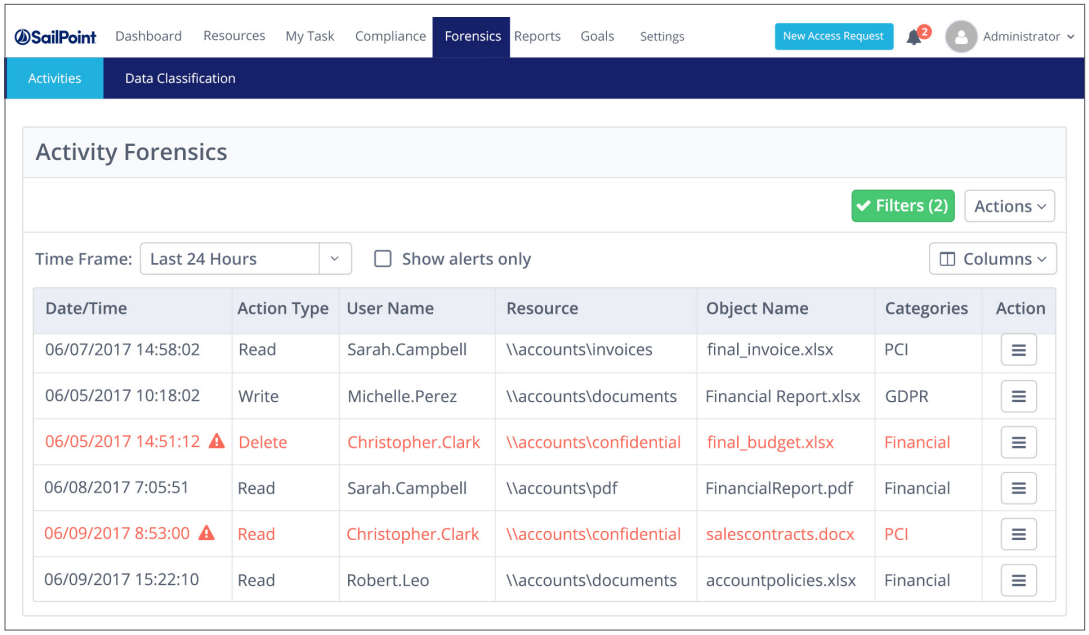
Configure and manage a variety of alert rules in a consolidated interface.

Gain Insight with Activity Forensics

Leveraging forensics to gain deeper insight into the activities affiliated with a potential threat is paramount to protecting sensitive data across the organization. With thousands of users involved in a myriad of daily activities, it becomes challenging to distinguish suspicious from regular activity.

File Access Manager offers an activity forensics interface with dashboard-level insight into user activity. Rather than providing an overwhelming collection of activity information, the interface surfaces high risk activities to quickly enable the organization to evaluate and take the appropriate action. In support of forensic investigations, admins can drill into specific events and get a complete view of all related activities. File Access Manager can also leverage identity context from the SailPoint identity governance platform, which provides a complete picture of a user's role, status and entitlements amongst other valuable background information for making access-related decisions.

By becoming more aware of potentially malicious activity or tracing back to the root cause of an issue, organizations can better protect their data assets.



Surface suspicious activity with the highest risk to take appropriate action.

Address Cyber Threats with a New Frontier of Identity Governance

Dealing with today's onslaught of cyber threats requires an approach that goes beyond applications and also extends to governing data stored in files. Taking a comprehensive approach to identity governance is the key to harnessing the power of data, securely and compliantly. SailPoint Predictive Identity enables organizations to leverage insight and awareness across their applications and files to proactively reduce security and compliance risks.

SAILPOINT: RETHINK IDENTITY

sailpoint.com

SailPoint, the leader in identity management, delivers an innovative approach to securing access across the enterprise with the SailPoint Predictive Identity™ platform. With SailPoint, enterprises can ensure that everyone and everything has the exact access they need, exactly when they need it, intuitively and automatically. Powered by patented Artificial Intelligence (AI) and Machine Learning (ML) technologies, the SailPoint Predictive Identity™ platform is designed to securely accelerate the business while delivering adaptive security, continuous compliance and improved business efficiency. As an identity pioneer and market leader serving some of the world's most prominent global companies, SailPoint consistently pushes the industry to rethink identity to the benefit of their customers' dynamic business needs.

Stay up-to-date on SailPoint by following us on **Twitter** and **LinkedIn** and by subscribing to the **SailPoint blog**.

SB1236-2005