SailPoint

SOLUTION BRIEF

Next-Generation Identity **Gets Smart for Healthcare**

The complexity of protecting health data in the current threat environment is ushering in a new era in cybersecurity – one that incorporates machine learning capabilities within identity management.

As the healthcare industry continues to digitally evolve, provider organizations are creating vast amounts of data, enabling numerous access points, and facilitating collaboration in the form of data sharing. Furthermore, because the healthcare industry is becoming increasingly integrated between provider organizations, vendor partners, contractors, etc., the user population and its diverse needs are ever expanding. Combining these factors with lean and limited IT resources make it increasingly difficult for provider organizations to gain visibility into who is accessing what, when and how.

Unfortunately, healthcare organizations cannot govern what they cannot see. To enforce security policies and reduce risky behavior, it is essential for IT administrators and data owners to monitor, analyze and quickly synthesize every identity interaction with every piece of data and application (clinical or non-clinical). While this may sound daunting, it can be achieved with the aid of artificial intelligence.

Not Just Sight, but Insight

Having visibility into your access environment is insufficient. It is contextual insight that enables organizations to manage their identities more intelligently, boost the impact of their identity governance efforts and manage potential risk by gaining a better understanding of high-risk or innocuous scenarios.

It delivers next-generation capabilities that significantly enhance its identity governance solution. It leverages artificial intelligence to ingest vast amounts of identity and event data to provide advanced insights. This capability is the equivalent of supercharging identity governance. Using machine learning techniques, SailPoint analyzes identity data such as account and entitlement assignments and combines

it with real-time activity information to discover suspicious or anomalous access and usage. Through this technology, SailPoint provides customers with deeper understanding into the risk associated with user access – and allows them to focus governance controls on higher risk components where they will matter most.

Benefits of a Smarter Identity Approach

Manage Risk
Rapidly escalating numbers of users, applications and data can flood healthcare provider organizations with an unmanageable pool of risk. Narrowing the scope of access management to high-risk resources or users lessens the likelihood that inappropriate access or malicious use of entitlements can sneak by even as the volume of alerts increases.

SailPoint enables provider organizations to detect anomalous access and potential risks with an analytics engine that uses time series analysis and deep learning to scan massive amounts of identity data to identify risks without having to rely on a team of security experts. Behavioral baselines are established over time as historical records translate into an established range of normal behavior. These patterns are refined as the solution learns what actions, if any, an administrator takes in response to unusual events. Over time, true high-risk events are preemptively identified from the steady stream of everyday activity.

Govern Smarter
Governance decisions made in isolation are prone to error because they only consider the immediate circumstance. For example, approving an entitlement without wider context might give unnecessary access to an employee and increase the threat of data exposure. A broader understanding of the environment aids in making rapid, accurate choices that decrease risk for the business.

The use of peer groups, in which identities are aligned by similar characteristics, can rapidly highlight any identities that have unusual attributes or entitlements. To illustrate, a peer group based on the users' clinical responsibilities and roles might indicate that most of the group has access to resources, such as the electronic health record (EHR) system, to assist them in their regular workflow. Any outlier, such as a single clinician that requested or obtained access to an HR database that was dissimilar to their peers, could then be easily identified. Furthermore, the individual's entitlements could then be revoked to eliminate potential risk to the provider organization.

Through IdentityAI, SailPoint also makes identity smarter by using artificial intelligence technology based on behavioral pattern recognition and statistical analysis to focus identity governance controls on high-risk scenarios in real time. An example of such a high-risk scenario would be the access of sensitive data or applications from new locations or at unusual hours. Because the technology utilizes a dynamic risk model rather than relying on pre-configured risk models, it continually adjusts its model as the environment evolves, identifying new and additional types of high-risk identities and activities.

Increase Efficiency

The pace of business is rapidly accelerating. As new opportunities present themselves in our global business environment, the volume of identities, data, and applications will continue to expand. This places a premium on efficiency gains for every business when a key differentiator is the ability to do more with less.

SailPoint improves operational efficiency of the IT organization and business productivity by giving the ability to automate low-risk access approvals, streamline access certifications and reduce false positive alerts of policy violations. This allows organizations to focus their limited IT and security resources on access to data and users that pose a higher risk.

The Power of Smart Identity

Healthcare providers require real insight into identities and how they behave in the operational ecosystem. Through SailPoint's advances and innovative application of machine learning technology, organizations can place contextual insight into the hands of business users, and reduce security and compliance risks.

Furthermore, SailPoint helps businesses govern their identities wisely, increase the effectiveness of their identity program and assist in the management of risks. Amidst an explosion in applications, data, identities and malicious actors seeking to exploit them, organizations must move from the mere knowledge of their environment to the wisdom to secure it. To do so, they must wield the power of smart identity.

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies.

SB1231-1806