SailPoint

WHITE PAPER

The 7 Tenets of Successful **Identity Governance**

Data breaches. The outlook is not promising. Headlines practically write themselves as new breaches are uncovered. From Home Depot to the US Government's Office of Personnel Management to Ashley Madison, targeted attacks are on the rise. They have increased 91% since 2013 which was known as the year of the Mega Breach.[1]

The total number of breaches themselves have increased 62% since that same time and the role of insiders in these breaches is significant. According to Verizon's Data Breach report, 88% of insider breaches are due to privilege abuse. In fact, according to SailPoint's own survey, 1 in 7 employees would be willing to sell their login credentials for as little as $150.

The insider risk remains. The external and internal risk are real.

The Disappearing Perimeter

The relationship between enterprises and their data is much more complex than ever before. In a regular workday, the average employee touches a massive number of systems – each with different levels of privilege demands. A head of HR needs high levels of privilege access to the HR system but low privilege to the IT infrastructure, product intellectual property or the sales database. Product managers need almost the opposite access. How do you know each only has access to the level they are authorized?

And while everyone thinks about employees and IT staff access, what about the contractors and suppliers? Many may not consider customers as needing access, but they leverage product support, partner portals and all sorts of semi-privileged data. Then, there are the former employees who still have their personal phones, computers and data sources they accessed while still on the inside. Were their access rights revoked timely?

[1] According to Symantec

With all these scenarios and complexity, the notion of network and perimeter is becoming irrelevant. Data is in the cloud and on mobile devices; it is accessed not just by employees but also external parties.

Enterprise security is in need of a new paradigm and evolving from network-centric to identity-centric. The increasingly complex relationships between people and data is redefining perimeter defenses and making us think about security in a very different way.

Enterprise Security Has Become Identity-Centric

Security starts with a subject (an employee or a program) gaining access to a resource (an application or data file) via access controls. Access controls are the system-level constraints that make sure that the **right** people have the **right** access and the bad guys are kept out. Application services now support a vast array of internal customers from employees to contractors to partners. In addition, it is common today to host applications on-premises and in the cloud in true hybrid environments. Between mobile platforms and data hosted in multiple clouds, system-to-system data flows are complex.

The role of identity governance is simple in principle: give the right people the right access to the right data. To do this, trusted and properly managed identity access has to become the primary control. It comes down to three basic questions to govern access:

1. **Who has access today?** This is a question of inventory and compliance. It starts with understanding the current state. It is about cataloging and understanding access in order to ensure it is correct.
2. **Who should have access?** Models and automation are the cornerstones to determining who should have access. For us to answer the question "should Joe have access to this file," we must first know who Joe is. We then have to understand and classify the data he is attempting to access. We have to establish a model that defines if Joe's access conforms to his pre-defined policy. While partitioning data this way may be more complex, it is critical to implementing any form of preventive controls.
3. **Who did have access?** This is a question of monitoring and audit. It is no longer enough to understand who does and who should have access. It is vital for IT security forensics and auditing to surface who was actually granted access, in addition to when and where it was last used.

Know the Points of Weakness

When looking at the post-incident forensic reports from any high-profile data breach, there are always basic identity errors at the root cause. Simple things like overly complex data access and unknown data classification are usually a factor. Some questions you may ask yourself include:

1. Can we tell what files have been stolen? What kind of data inventory do we have to help us find out?
2. How many separate login systems are we managing between Product, Sales, Ops, Finance and Support? Are they all on-premises or are some hosted in the cloud?
3. Are our data pools in large repositories; how finely have we partitioned access?
4. What is the difference in access level to our employees, contractors, partners and customers? Are they all accessing the same networks at different levels or do we host duplicate but separate networks for each?
5. Can we tell the difference between a valid account and a rogue account?

There are many more factors and the identity questions get complex quickly.

At SailPoint, we have had the privilege to be invited into a wide range of customer environments and witnessed an even wider range of identity challenges. We have assembled the knowledge we gained from these experiences into 7 basic tenets of best practices enterprises should use when designing and integrating a next-generation identity program.

Consider Everything

Identity governance is no longer a 'do it yourself' project. The sheer number of users, data applications, interfaces and platforms in the modern enterprise requires an integrated identity system. From password management across multiple data repository platforms to compliance to role management to audit, misalign one interface and at best, your system will fail. At worst, your identity system ends up with a vulnerability that does not surface immediately, but that a cybercriminal might exploit later. A single integrated identity platform can coordinate all rules, all compliance and all monitoring into one place ensuring that nothing is missed.

Patching together an enterprise-level identity governance solution by stitching the embedded identity control systems of multiple SaaS and enterprise software vendors leaves your network open to potential gaps in coverage and creates fragile links between systems. An integrated enterprise solution will control and monitor all your users, all your applications, all your data, and all access rights.

2

Remember Your Customer

The enterprise has to service a wide range of internal customers with different data access needs from different locations using different access devices. Your identity governance solution must be adaptable across all this. Whether a user is accessing a sales database from a hotel in Europe via their smartphone, an ERP system from a tablet on a production floor or a finance system from a desktop at the corporate headquarters, each access needs to be authenticated quickly, transparently and accurately.

This includes an internal contractor requesting simple access to a new application, a business user adjusting data ownership rights, a high-level compliance officer monitoring compliance or a road warrior asking for a password reset behind the corporate firewall. Any user, any platform, any time. In a friendly, easy way.

3

Be Context-Aware

Understanding users and, most importantly, the data and resources they should and typically access is critical. Identity context is about sharing and understanding these relationships and translating them into entitlements or rights. That context model needs to sit in the center of the security and operations infrastructure as the identity governance and administration engine. It is a model of known relationships between people, accounts, privileges and data.

For example, when a security event is generated out of a SIEM or DLP system, a context-aware identity governance system can use its knowledge of people, their accounts and the data they are allowed to access and take remediation actions. If an access request is outside the boundaries of their approved access levels, a good identity system may suspend their account or even lock their mobile container.

4

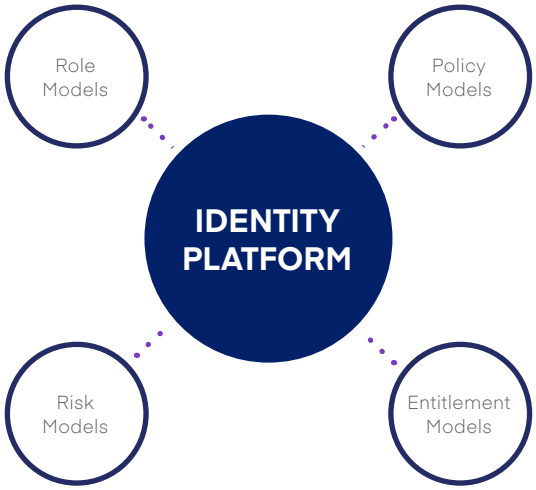
Govern by Model

Managing the access of thousands of users requires governance models. These models are what make the identity engine effective. They consist of a set of automation models, role models, change models, risk models and control models. They each drive individual compliance and groupings interactions which, as a group, drive common policy.

Models often start in HR and monitor new employees, employee changes and employee terminations. These are called joiner/mover/leaver events. From there, access models are created for the bulk of users who operate in self-service modes.

In addition, IT security requires models for automation and control to closely monitor access activity, and the IT audit department needs special compliance and audit actions that wrap around the core of the enterprise's data protection strategy.

Placing governance models at the center creates a stable, repeatable and scalable approach to enterprise identity control.



5

Managing Risk is a Verb

Managing risk is the mechanism for how you know when an action falls outside of normal usage. Identity risk scoring can be accomplished by model in an advanced identity governance system. Risk scoring allows for faster access authentication and tracking strategies. For instance, a low risk account may have only read privileges, no policy violations and no access to high risk data or applications. A high risk profile may have orphaned accounts, system administrative access to highly sensitive data with lots of privileges, or has been associated with active policy violations. These accounts may require event-based certification whenever something changes in their environments for logins rather than a simple quarterly review audit.

And in between are the accounts upgraded from low risk or downgraded from high risk. For these, a series of failed login attempts may prompt immediate event-based certification, restrict their access request environments or other actions. In any case, knowing a user's risk profile helps in assessing how closely their online activities need to be monitored.

6

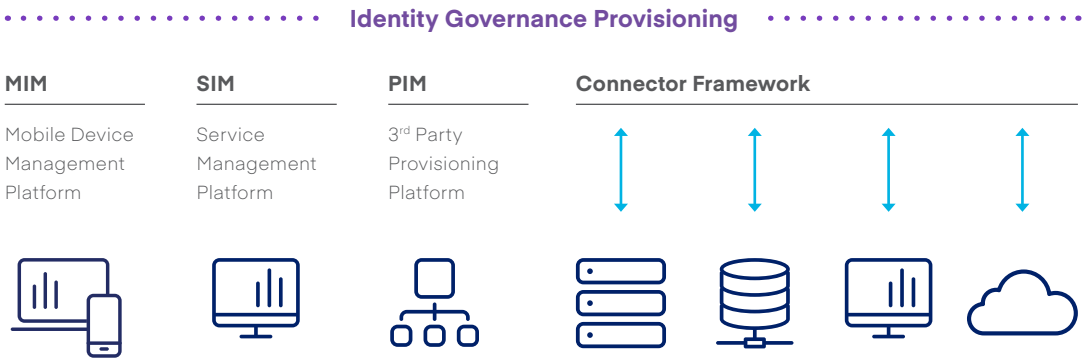
Connect to Everything

When considering an extensively-integrated IT system such as identity, the most difficult decision an enterprise needs to make is determining how much of an existing platform to keep and how much needs to be replaced. Some parts of their

internal IT architecture will stay the same and so the identity governance platform needs to be flexible enough to connect to everything and anything. Effective identity governance requires connectivity from any kind of platform to any kind of data repository.

This may mean working with older 3rd party provisioning platforms as well as more recent infrastructure like Mobile Device Management software managing mobile security or Service Management Platforms that may still be using manual fulfillment processes.

Accomplishing this requires a direct connector framework with the ability to manage databases, directories and servers. Also important is the ability to provide out-of-the-box connectors for enterprise applications like SAP and Oracle Fusion, mainframe security managers, cloud and SaaS apps. Agentless technology that makes each connector easier to deploy and maintain over time is key for a successful identity platform deployment.



7

Be Consistent

This may sound intuitive but consistency in all these actions and approaches is key. The business user wants access regardless of where the apps are served. The auditor only cares about compliance, not where data is stored. The identity governance solution needs to bridge gaps like these seamlessly and consistently to secure the business in a scalable way.

Regardless of where the data resides, one-off connections or patched provisioning should be excluded from the identity implementation design, otherwise scalability will be impacted whether data is structured or unstructured.

Summary

The modern enterprise is more complex than ever and identity is at its core. While it is possible for enterprises to piece together their own solutions, the number of rules, best practices, and intricacies involved with implementing a secure identity governance solution is huge. There is a lot at stake. It only takes one misconfiguration to open your enterprise to anyone wanting in.

Only SailPoint offers all these 7 tenets in one solution. Since our inception, SailPoint has been integrating complex identity solutions for a wide range of customers in a wide range of markets. SailPoint is the identity market leader and has been a Gartner Magic Quadrant market leader for several years with over 500 customers around the world. We are innovators in the area of identity governance and have helped a lot of customers navigate through exactly the obstacles we have shared in the 7 tenets.

We understand business users, business complexities and most of all, we understand what is at stake when it comes to accurate identity monitoring and compliance. You spent your life's work on your business. We have done the same in identity. We have refined the mechanisms for fast and effective identity governance strategy and are ready to share our vision, solutions and knowledge with your organization.

Visit SailPoint.com for more information and to schedule a demonstration.

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 in virtually every industry, including: 9 of the top banks, 7 of the top retail brands, 6 of the top healthcare providers, 6 of the top property and casualty insurance providers, and 6 of the top pharmaceutical companies.

WP1007-1709