White Paper

The 7 Tenets of Successful Identity Security

The Disappearing Perimeter

The relationship between enterprises and their data has never been more complex.

Network is becoming irrelevant. Work is on-premises, remote, and hybrid. Data is in the cloud and on mobile devices; it is accessed not just by employees and contractors, but also authorized external partners.

For the modern enterprise, securely connecting the right people to the right technology at the right time is incredibly difficult, and has moved well beyond human capacity. Most enterprises house thousands to millions of identities, each with varying access requirements that change constantly in response to ever-evolving business needs.

In a regular workday, the typical employee touches a huge number of systems – each with different levels of privilege demands. 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. And then there are former employees who still have the personal phones, computers, and data sources they accessed when they were on the inside. Have their access rights been revoked in a timely manner?

Each access point represents a potential exposure point if not properly managed and secured… and cyber criminals know it.

Targeted Data Breach Attacks are on the rise:

91%

increase in targeted attacks since 2013.[1]

84%

of organizations experienced an identity-related breach in the last year.[2]

88%

of insider breaches are due to privilege abuse.[3]

1 in 7

employees would be willing to sell their login credentials for as little as **$150.**[4]

[1] NortonLifeLock, Internet Security Threat Report, 2014.
[2] Identity Defined Security Alliance (ISDA), 2022 Trends in Securing Digital Identities Report (**www.idsalliance.org/press-release/new-study-reveals-84-of-organizations-experienced-an-identity-related-breach-in-the-last-year/**).
[3] Verizon, 2014 Data Breaches Investigation Report.
[4] SailPoint, 7th Annual Market Pulse Survey, 2015.

Know the Points of Vulnerability

When looking at the post-incident forensic reports from any high-profile data breach, the root cause always includes basic identity errors. Some diagnostic questions to ask in the wake of a data breach 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, Operations, 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** for 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?

Enterprise Security Must Become Identity-Centric

The primary controls provided by network security are just not enough anymore.

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 bots 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 security is simple in principle: give the right people the right access to the right data at the right time.

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:

▶ Who has access today?

This is a question of **inventory** and **compliance**.

It starts with understanding the current state. It is about cataloging and analyzing existing access in order to ensure it is correct.

▶ 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 predefined policy. While partitioning data this way may be more complex, it is critical to implementing any form of preventive controls.

▶ 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.

There's Security at the Core

Enterprise security requires a new paradigm, evolving from network-centric to identity-centric.

Without a single view into all identities and their access rights, and the ability to manage them through Artificial Intelligence (AI) and Machine Learning (ML), organizations are needlessly exposed to business, brand, and financial risk.

Enterprises today require core Identity Security – a simple and autonomous way to both enable and secure your workforce.

At SailPoint, we have explored a wide range of customer environments and witnessed an extensive range of identity challenges. We have assembled the knowledge gained from these experiences into best practices tenets for enterprises integrating a next-generation core identity security program.

SailPoint's 7 Tenets of Successful Identity Security

1

Consider Everything

The sheer number and type of users, data applications, interfaces, and platforms in the modern enterprise demands an integrated identity system — one that will coordinate all rules, compliance, and monitoring of your users, applications, data, and access rights.

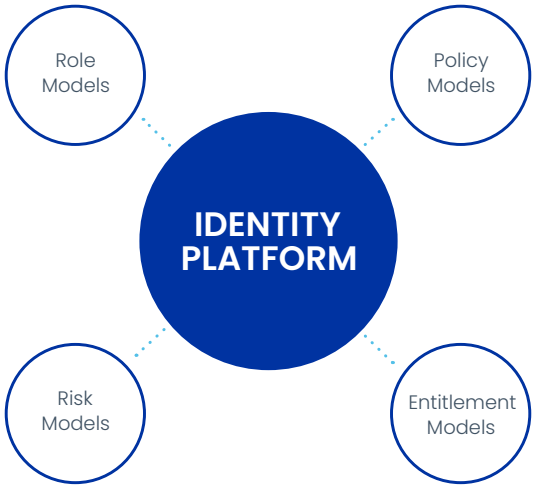
2

Remember Your Customer

Your identity security solution must be adaptable to different data access needs, from different locations, using different access devices. Any authorized user, any platform, any time. In a friendly, easy-to-use way.

3 Be Context-Aware

Identity context is about understanding the relationship among people, accounts, privilege, and data. That context model needs to sit in the center of the security and operations infrastructure as the identity security and administration engine.



4 Manage by Model

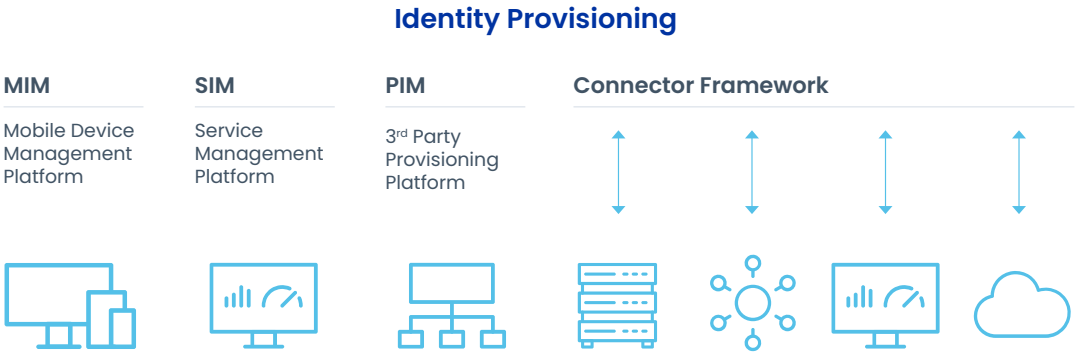
Security models — automation models, role models, change models, risk models, and control models — drive individual compliance and groupings interactions, which drive common policy. They are what make the identity engine effective, creating a stable, repeatable, and scalable approach to enterprise identity control.

5 Understand Risk

In an advanced identity security system, identity risk scoring can be accomplished by model, allowing for faster access authentication and tracking strategies. Knowing a user's risk profile — and what actions fall outside of normal usage — helps determine how closely their online activities need to be monitored.

6 Connect to Everything

Effective identity security requires the flexibility to connect from any kind of platform to any kind of data repository. 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 the successful deployment of an identity security platform.



7 Be Consistent

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. An identity security solution needs to bridge gaps like these seamlessly and consistently to secure the business in a scalable way.

Summary

The modern enterprise is more complex than ever, making identity security essential to the successful operation of your business, no matter where you conduct it — on-premises, remote, or hybrid.

There is a lot at stake. It only takes one misconfiguration to make your enterprise vulnerable to cyber attacks. The risk to your business, your brand, and your bottom line is significant.

Only SailPoint addresses all these 7 Tenets in a single solution. That's why SailPoint stands above the rest. Our identity security cloud platform is made for the sophisticated needs of today's modern enterprise, delivering an intelligent, autonomous identity foundation that secures your business and fuels its growth.

Since our inception, SailPoint has been integrating complex identity security solutions for a wide range of customers in a wide range of markets. 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.

Your life's work is your business. It is the same for all of us at SailPoint, and our business is identity security. We created this space, and we remain both the innovator and the standard-bearing market leader in identity security.

We have refined the mechanisms for fast and effective identity security, and we are ready to share our vision, knowledge, and solutions with your organization.

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

SailPoint

About SailPoint

SailPoint is the leading provider of identity security for the modern enterprise. Enterprise security starts and ends with identities and their access, yet the ability to manage and secure identities today has moved well beyond human capacity. Using a foundation of artificial intelligence and machine learning, the SailPoint Identity Security Platform delivers the right level of access to the right identities and resources at the right time—matching the scale, velocity, and environmental needs of today's cloud-oriented enterprise. Our intelligent, autonomous, and integrated solutions put identity security at the core of digital business operations, enabling even the most complex organizations across the globe to build a security foundation capable of defending against today's most pressing threats.