SailPoint

eBook

The guide to securing digital identities and minimizing risk in the enterprise

According to the experts at Control Risks, Cyber Risk is a top 5 risk for 2023[1], and deservedly so. The ongoing operations anywhere and digital transformation shifts have exposed security weaknesses inherent in a dramatically increased attack surface and fully "castle wall-less" work environment in today's modern enterprise. Identity has truly become the new perimeter, which is confirmed in survey after survey: in the past year, 84% of organizations have experienced an identity-related breach, with a whopping 96% believing that these breaches could have been prevented or minimized by implementing identity-focused security outcomes.[2]

Despite the security risks, organizations will continue to pursue digital and cloud transformation efforts due to the benefits of dramatically increased corporate agility and increased worker productivity. This shift, however, will lead to a continued explosion in both human and machine identities, along with exponentially more access requests, increasing an organization's security risk even further. And yet, according to our recent **Horizons of identity security report**, a staggering 74% of companies still have immature identity programs, having not moved beyond fragmented technologies and manual processes for even the simplest of identity-related tasks.

From ransomware to phishing to credential stuffing to supply chain attacks, almost all attacks involve gaining a foothold in a network, often through a compromised identity, then moving laterally and looking to gain privilege through another compromised identity. It takes just one to enable a potentially massive breach; and there's a lot of room for error when managing identities including during initial onboarding, when making access changes for workers shifting roles, and while offboarding employees. When manual processes are used, the risks include over-provisioning and over-privilege of that single, ripe-for-compromise credential – especially when you consider each employee has an average of 30 separate identities -- and machines with 45X that number.[3]

$387M

Mega breach cost in 2022 with 50-60 million records

$4.35M

Average breach cost in 2022

Cost of a Data Breach Report 2022, IBM

[1] https://www.controlrisks.com/riskmap/top-risks

[2] 2022 Trends in Securing Digital Identities, IDSA

[3] Massive Growth of Digital Identities Is Driving Rise in Cybersecurity Debt, CyberArk

> **“...the research shows a clear correlation between a focus on identity-centric security outcomes and lower breach levels.**
>
> **Julie Smith**
> Executive Director of the IDSA

Cyber risk becomes business risk

Identity security risk is about far more than security risk. As companies accelerate their digital and organizational transformation and look for new ways to innovate, those without strong identity programs have turned to SailPoint expressing the following challenges:

- “Our legacy identity platform cannot cope with the rapid change and complexity of new technology being deployed.”
- “We can’t empower line-of-business personnel or end users to do anything identity-related without IT intervention.”
- “Governance is entirely out of reach.”

They’ve recognized that without foundational modern identity security capabilities in place, they may experience increased risk of data breaches which leads to:

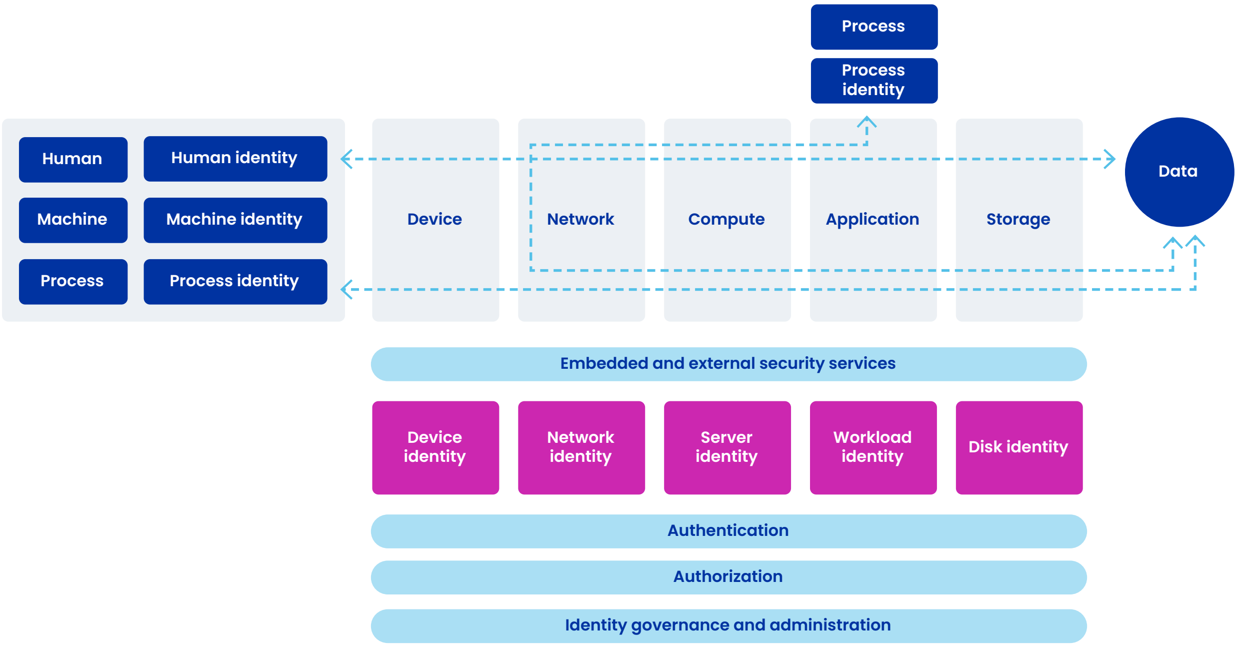
- Loss of revenue
- Crippling regulatory fines
- Delays during any sort of innovation or digital transformation as well as mergers and divestitures, severely limiting overall corporate agility

Simply put, the lack of a modern, advanced identity security program and platform has become a risk to core enterprise operations. Using an advanced identity security program as a foundation to mitigate both cyber and corporate risk should be top-of-mind for all cybersecurity and IT risk management practitioners – and it’s not as expensive or time consuming as you might think.

Where to begin?

First and foremost, truly shoring up identity security risk – and thus the vast majority of cyber risk in enterprise organizations today – requires a fundamentally different way of thinking about cyber security. Instead of outside-in, as in preventing attackers from entering your network, modern cyber security shops are thinking in terms of inside-out: assume your entire network is open and you need to truly protect that which is most valuable. So, you need to make sure that at all times, those accessing your data, applications and systems across your hybrid environment are who they say they are, and that they’re authorized to access that information. Simple, right?

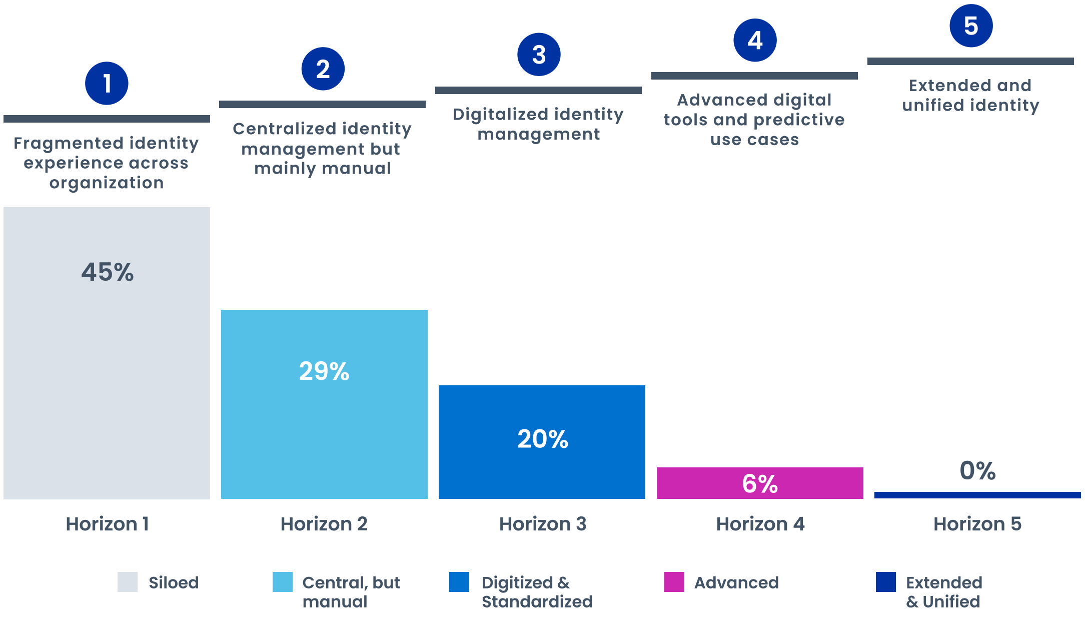
Conceptually, yes. Practically, no. Executing on this simple concept becomes extremely complex when factoring in thousands to potentially millions of employees, contractors, customers, and partners; an order of magnitude more of machine types and related identities; and exponentially more access requests. If all of this sounds suspiciously like Zero Trust, that's because it is. At the outset, primarily a network-based concept, it's becoming widely recognized that identity should form the basis, the foundation, of a Zero Trust cyber security strategy. In an IDSA paper called, "The Path to Zero Trust Starts with Identity," they published a conceptual model on how to think about every point-to-point access request which they called, "Identity Defined Security Scenarios," as seen below. With that concept in mind, this paper will focus on the more practical aspects of the needed capabilities and deployment strategies of an advanced identity security program and platform with automation and AI at its core to handle such an architecture.



Source: Identity Defined Security Scenarios, IDSA

The journey to advanced identity security

All companies are on a journey to advanced identity security – most just don't know it yet. Mentioned in the introduction, SailPoint's horizons of identity security report defines the core capabilities of five distinct horizons of identity security, from beginning to advanced, depending not only on technical capabilities, but also on the company's strategy, operating model, and talent.



% are total number of organizations in the study

Where would you like to go?

Per the Horizons report, best-in-class companies leverage identity as a key control point to reduce cybersecurity risk and deliver business value. Specifically, organizations dramatically improve their security posture and resilience, and thus, of course minimize their cyber risk, as they grow in maturity. For example, the study found that an organization moving from Horizon 3 to Horizon 4, where the program is fully scaled and steeped in the use of AI/ML, will detect and respond to attacks ~40% faster thanks to the AI and better visibility across the environment – decreasing average response time to a security breach from three hours to as fast as three minutes. And as you well know, response times are critical to containing damage and reducing risk.

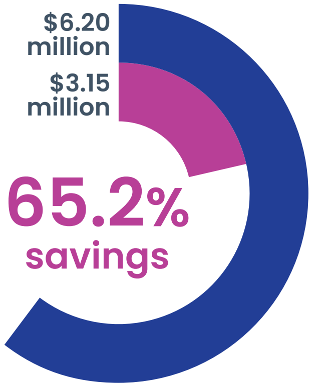
3 hours to as low as 3 minutes: Breach response times when moving from Horizon 3 to Horizon 4

Breaking down the underlying platform of a mature identity security program

While strategy, operating model and talent are all critical components of an advanced identity security program, the technology platform underpinning such efforts is key, simply because securely connecting the right people to the right technology via an inside-out conceptual strategy has moved well beyond human capacity. Truly reducing cyber risk with an identity security program that can scale to meet the demands boils down to three core areas of needed capabilities: **visibility and intelligence** across your entire environment, **automation** of manual processes, and an efficient ability to **integrate** identity functionality across your infrastructure.

Visibility and intelligence

At the core of any advanced identity security platform is artificial intelligence and machine learning that provides 360° visibility and insight so you can adapt and ensure the security of every identity. With AI and machine learning, you can collect the right data on each identity (humans and machines) to better assess what they currently have access to, how access is being used, and what they should have access to – driving smarter, more context-aware identity decisions. AI and machine learning can also spot risky user behaviors, detecting and preventing toxic access combinations that could lead to potential fraud or data theft. It also provides real-time access risk analysis that identifies potential risks **before** access is granted to users – another key to helping reduce data breaches. When considering the costs of data breaches alone, using AI and automation can help dramatically minimize the impact, as shown in the figure below.



Breaches at organizations with fully deployed security AI and automation cost USD 3.05 million less than breaches at organizations without security AI and automation, a 65.2% decrease in cost.

Cost of a Data Breach Report 2022, IBM.

Automation

Another critical component of an identity security solution involves protecting organizations against cyber threats by automating the discovery, management, and control of all user access. Automation ensures that each identity, human or non-human, has the access needed to do their job – no more, no less – and that access is automatically adjusted as their role changes or if they leave the organization. Automation streamlines identity processes and decisions such as access requests, role modeling, and access certifications, minimizing the risk of orphaned accounts and compromised identities while driving greater efficiencies across your organization. Automation also facilitates defining user roles and creating policies to govern access throughout the lifecycle of every digital identity that makes up today's workforce. It puts an emphasis on enablement, security, and compliance, which means not only providing access but also properly controlling that access. This frees workers to focus on innovation, collaboration, and productivity while reducing risk.

Comprehensive integration

Integration is another key component to help organizations mitigate cyber risk. Comprehensive and seamless integration extends your ability to centrally manage and control access to ALL data, applications, systems and cloud infrastructure across your hybrid infrastructure—for all identity types. Integrating an identity security solution with business and security systems provides the ability to infuse identity context and decisions into the everyday workflow of the business, creating a frictionless, user centric experience. It builds a strong security fabric by embedding identity data across your enterprise for holistic visibility into technology access and usage. It also enables deep identity context and access control across the entirety of an enterprise IT ecosystem, making the organization more connected – and thus more protected.

Not an arduous undertaking

Getting to a mature identity program, and thus helping your organization become more resilient to cyber risk, doesn't have to be an arduous undertaking. A great first step is to take our **quick six question maturity assessment** that will reveal areas most urgent to address in your identity security program and where the most value can be created from your investment. From there, we suggest choosing a transformation path based on driving incremental change if you're further along, or leapfrogging to an advanced solution if you're starting fresh – often easier than incremental efforts because legacy systems and processes are not in play.

Next, building a business case with executives and the organization as a whole will help establish overall buy-in. SailPoint has an entire Business Value Assessment, or BVA, team – dedicated to helping you develop your business case. All you need to do is reach out. In 2022 our team found an average potential ROI with SailPoint over 5 years is 345%, with a 1 – 2-year payback period.

345% over 5 years

The average ROI of a SailPoint deployment.

Deployment

It is essential to design the correct identity transformation deployment. Successful programs that can help mitigate cyber risk include the foundational capabilities needed to scale the program across the company. Two approaches can work, depending on the company's circumstances: a horizontal approach—piloting a program across the company and scaling up capabilities—or a vertical approach, such as deploying all identity needs to one business unit and scaling to other business units from there.

Less complex organizations often succeed with a horizontal approach if the program has an owner and is clearly defined, planned, and communicated using a few capabilities. In more complex companies, the identity team can use the first business unit to refine use cases, establish clear communication, prove the business value of the program, and build foundational capabilities. Once the program meets success metrics, the team can roll it out to one business unit at a time.

SailPoint Identity Security Cloud

Even with a well thought-through deployment strategy, getting started with an advanced – Horizon 4 – identity security solution can seem daunting. SailPoint's experience working with leading global brands has provided insight into exactly what is needed to solve this challenge: targeted, organized SaaS-based products that work together as a single solution. Our solution is called the SailPoint Identity Security Cloud. It...

- Is built with AI and machine learning at the foundation
- Enables organizations with the tools needed to automatically manage access from start to finish, understand how access is being used, and spot access risks before they create security problems
- Provides access to over 100+ out-of-the box connectors, a full set of APIs & event triggers, and key capabilities to extend identity security across an entire hybrid environment.

SailPoint's Identity Security Cloud offerings can be deployed rapidly, then modified over time to suit any enterprise's needs. Overall, this is a rapid path to get to Horizon 4, even for the most nascent identity security programs.

Bringing it all together

Companies deploying a modern, AI-based identity security program can significantly minimize their overall cyber and corporate risk posture while concurrently seeing a very large return on investment. How many corporate programs can say that? The key to maximizing the value of an identity investment, for most companies, is to leapfrog to an advanced identity program built with a focused strategy and proven technology platform, supported by a forward-looking operating model. With the right set of identity technology and supporting enablers, building a future proof, more resilient, scalable identity program is certainly achievable. To help fine-tune your business goals and create a transformation roadmap, reach out to us at **sailpoint.com/solutions/mitigate-cyber-risk.**

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.