White Paper

Now is the time to modernize your identity security

Putting identity at the core of your strategy

The drive to modernize identity security

A host of reasons can drive the enterprise to modernize its identity security. Older identity security systems may already be constraining your business and represent operational risks, requiring too many processes that are still manual and lacking visibility into usage. These systems may not provide critical integrations to different applications within your infrastructure, have limited workflow automation capabilities, and are increasingly difficult and costly to support – let alone upgrade. In some cases, there is the looming specter of the end of primary support and you may be limiting your on-going investment.

Identity security modernization is frequently driven by top-down strategic business initiatives. These might be structural changes such as mergers or divestitures, or expansion into new markets or regions. Or these transformations may be technological, like going "cloud-first" and consolidating datacenters, streamlining operations by adopting more SaaS business applications, or replacing a business-critical technology platform. Strategic initiatives tend to elevate and "draw in" the need to modernize securing identities and access even as they, ironically, proliferate new identities.

A productive workforce requires an up-to-date identity security solution. Outdated systems cannot efficiently accommodate increasingly dynamic identity and access requirements – think Work from Anywhere (WFA) and third-party users – making for frustrating user experience and IT teams. Outdated systems typically do not offer intelligent self-service options designed to facilitate secure access and reduce support. They cannot easily be connected to other enterprise applications and systems.

Compounding these challenges are increasingly complex multi-cloud and hybrid infrastructures with distinct identity and access paradigms. There is also the need to comply with more stringent identity security and privacy regulations.

Risk mitigation has never been more critical: Virtually every cyber breach now involves compromised identity and illegitimate access.

Modern identity security provides a comprehensive and integrated solution that can manage and protect the identities of users, devices, and applications across multiple platforms and domains. Leveraging technologies such as artificial intelligence and machine learning (AI/ML), data analysis and advanced process automation, *modern identity security offers business benefits beyond security: enhanced scalability, better user experiences supporting productivity, as well as reduced costs and risks to the enterprise.*

Older systems were simply never designed for today's diverse user base, pace of change, and complex working environments. Sub-standard identity security means more than risk of cyber breach; it means you cannot get to where you want to be as a business. Inaction also carries risk; these challenges will only increase in scale, complexity, and costs. Now is the time to modernize.

Identity is core to successful enterprise security

Securing identity is crucial to controlling operational risk and protecting against cyber threats. By appropriately authenticating and authorizing user, device, and application access, identity security systems provide the foundation of digital trust and accountability throughout the modern enterprise.

This is no easy task given today's expanding digital workforce (employees and non-employees), non-human identities, and the complexity and speed of the enterprise environment.

- More employees are WFA, working on different devices, including their personal devices, across multi-cloud and hybrid infrastructures.
- The contemporary enterprise includes third-party workers such as temporary staff from an agency, consultants, contractors, cloud or software vendor personnel, on-premises software support, supply-chain workers, and other professional services.
- Other non-employee types of users include contractors, partners, customers, students or interns, and volunteers. And for organizations built on the franchise model, franchisees might be considered non-employee users.
- Increasing non-human identities also require access, especially if you consider extended supply chains: service accounts, bots or robotic process automation (RPA), IoT devices, and operational technology (OT) controls.

These trends have created a greatly expanded attack surface. The risk to the enterprise is compounded by the flexibility and speed required to accommodate today's user. It is no surprise that compromised identity and access is at the root of most cyber breaches, whether that results from misconfigured cloud permissions, insufficient third-party identity management, or mismanaged privilege within the organization.

84%

of respondents indicated they experienced an identity-related breach in the past year [2]

[1]2022 Trends in securing digital identities- IDSA

Yet the paradigms, the very foundation upon which older identity systems are built, have serious limits supporting precisely the more powerful, advanced technologies that organizations must employ to remain competitive. Consider access certification. Certification on older systems, across SaaS and multi-cloud environments (let alone for a changing, WFA workforce) are inefficient, slow, and cumbersome at best. Quarterly or even annual certifications can lead to fatigue and managerial "rubber stamping" permissions. Even these certifications are not sufficient to protect today's users.

To be effective certifications need to be current. What is needed is a forward-looking approach that encompasses visibility on identity data across your environment – including user attributes, roles, access history, and entitlements. Leveraging AI/ML on this data, a modern system can offer actionable, data-driven insights to make certifications more "accurate" and current. *Only in this way can organizations proactively identify access anomalies, spot potential risks faster, and remediate them in a timely manner.*

Initially, older identity management systems may have focused on IT efficiency, with "good enough" identity and access security. But in today's digital business and threat environment "good enough" identity security is increasingly risky. Moreover, these older identity security systems may now be hobbling your business. The modern identity security solution can contribute more than risk mitigation to the success of today's business.

How modern identity security enables the business

Putting identity at the core of your enterprise security demonstrates you are taking the steps necessary to effectively protect your assets, customer information, and control risk. Modern identity security provides superior protection by delivering the right access at the right time, throughout the broader infrastructure of today's complex enterprise. The modern solution allows you

to govern access throughout the digital identity's lifecycle; it is designed to handle the speed and scale at which access is required by today's expanded, dynamic user base.

Yet implementing an AI powered, modern identity security solution shows more: it proves you are thinking strategically about how your business can continue to improve, be productive, and more successful. Such a system is distinguished by providing business benefits beyond protecting the enterprise.

These benefits go hand in hand, and in some ways reflect the natural evolution of modern identity and access management. You not only control risk and improve your security posture, but you also reduce operational costs, accelerate your business, and enhance the user experience leading to increased productivity.

Let's revisit the certification example above. By leveraging stored identity data with AI/ML we can make certifications more current with timely, data-driven recommendations. This enables the organization to proactively identify access anomalies, spot potential risks, and remediate faster. But additional business benefits include reduced managerial overhead (less fatigue and rubber stamping of certifications), faster access for users when they need it, and likely fewer calls to IT or the help desk. Compliance auditing processes are made simpler and accelerated. And there is a continuous improvement feedback loop in the sense that the changes and their impact are recorded and can further enhance the AI/ML recommendations. Data-driven decision-making has become a critical component of business success. It allows for:

- Improved accuracy and efficiency
- Better forecasting and planning
- Increased transparency and accountability

55%

of companies rely on manual processes to adjust access when IT environments rapidly change.[2]

[2] "Identity is the Zero Trust Keystone," Dimensional Research and SailPoint Report, 2021

Why would this be any different for identity and access management? Indeed, comprehensive identity and access data should be a fundamental component to many decisions relevant to your business success.

More data driven insights and recommendations, based on the actual day to day access within your environment and analyzed by AI/ML technology, can reduce "noise", and relieve staff, from security teams to the help desk.

Proactively spot and prevent overprovisioning faster

Automated workflows allow users to start access certifications and respond to potential risks in real-time. If risk is high, access can automatically be disabled. A feedback loop into the machine learning model allows the machine to continuously improve automated recommendations and contextual insights giving managers the ability to make smarter access decisions in less time.

Applied data science and AI/ML

By applying advanced analytics and machine learning techniques to identity and access data, organizations gain near-real-time insights into user behavior, detect anomalies and risks faster, and inject data-driven criteria into automated security procedures such as on-boarding, granting access, auditing, certification and more.

Additional business benefits of applied data science and AI in enterprise identity security are:

- **Enhanced user experience:** Data-driven assists can improve efficiency and productivity by enabling users (and appropriate non-employee resources) to access the resources they need quickly and securely. Applied data science can enable more 'frictionless' authentication methods, such as biometrics, behavioral analysis, and adaptive multi-factor authentication. These methods enhance security (applied automatically, appropriately, and consistently across an organization) but also, by reducing the burden of passwords and tokens, can improve user satisfaction and productivity.
- **Reduced fraud and identity theft:** Data science and AI can help identify and prevent fraudulent activities, such as account takeover, phishing, and credential stuffing. AI/ML technology can assist security teams by analyzing user behavior within a context and flag suspicious or anomalous actions, e.g., Separation of Duties (SoD), and trigger appropriate responses, such as alerts, verification, or access revocation.
- **Improved compliance and governance:** Data-driven decisions can help organizations comply with regulatory and industry standards, such as SOX, GDPR, HIPAA, PCI-DSS, and NIST. Comprehensive visibility into user access and activity, coupled with more automated security policies and auditing processes, ensures that identity data is protected, managed, and reported in accordance with the relevant frameworks and best practices.

More and more effective self-service options are another outcome of the modern, AI-powered identity security solution. More than simple automation, it is the context and intelligence afforded by AI analysis that makes self-service on-boarding, authorization, and more a secure reality. Self-service processes can further reduce help desk calls and improve the user experience.

Automating more workflows increases productivity

Managing many common identity security processes in older systems can be time-consuming, error-prone, and inefficient. Automation of workflows is a recognized approach to reducing human error, improving compliance, enhancing the user experience, and lowering operational costs.
Yet the scope, accuracy and efficiency afforded by automation is only as good as the data upon which it is based. It is certainly possible to automate 'bad' processes. AI/ML powered automation, based on a comprehensive, up to date database of actual identity related activity, can extend the scope, accuracy and benefits of your automation initiatives.
Another good example: onboarding. The visibility across your identity universe allows AI-enabled processes to automatically review and approve low- risk access. Further, the solution can suggest and create high quality roles based on similar access between users. It can quickly provide the insights you need to model and adapt access roles based on the ever-changing patterns within your organization. This is a faster, data-driven way to create and maintain role-based access control (RBAC). In turn, this creates fewer access requests and certifications of common and non-risky access – everyone is more productive.

More inclusive, improved automation enables the enterprise to scale faster, handle large volumes of users and devices across multiple platforms and environments (think mergers and acquisitions). AI/ML-driven automation also adapts to changing business needs and requirements as it goes, without requiring manual intervention or configuration. Centralized identity security also enables other automatic processes, including machine to machine communication, used in many business processes besides security, speeding business results and increasing productivity, e.g., facilitating ticketing mean time to resolution (MTTR), or automatic compliance auditing, filing and record-keeping.

AI/ML-driven automation can reduce friction in many business processes. Enterprises can increase their productivity and focus resources on core business objectives. It will take time to get to 100% autonomous identity security. But applying data science and AI to automating processes is a good first step.

Easy, scalable connectivity and integration

Today's enterprise is driven by hundreds if not thousands of applications, including a rapidly growing set of cloud and SaaS applications. This workflow ecosystem of diverse applications and data stores is used by employees and third parties with different access rights. Secure, smooth access to and connectivity between these applications is crucial to greater productivity and business success.

The modern identity security system provides multiple secure paths to integrate with enterprise applications. The most straight-forward are out-of-the-box connectors to common business applications, e.g., Microsoft Active Directory, Azure Active Directory, LDAP, Unix, SAP HR, etc.

Another path to integration is protocol-based (instantiated as an API). The most common communication protocols include System for Cross-domain Identity Management (SCIM), REST or SOAP, and JDBC (for database types). Instead of tying up resources building integrations, using an extensibility framework with a toolkit of webhooks and APIs is not only more efficient, but provides deeper insights and control of user access lifecycles on integrated applications.

Here, too, the modern identity security solution can improve the user experience. By easily integrating with specialist enterprise security functionality like single sign-on (SSO), or multi-factor authentication (MFA) systems, the modern solution enforces strong authentication methods across the larger body of enterprise applications. Users can access various applications and services with a single login credential, reducing the need to remember multiple passwords or enter them repeatedly. Self-service options can also simplify and reduce the resetting or changing passwords, as well as managing user accounts and permissions.

Beyond more granular control over user access rights and privileges, integration provides audit trails and reports for compliance purposes, as well as reduces the risk of human errors, inconsistencies, and duplications that can compromise security, compliance, and data quality. Integrations with modern identity security solutions, backed by AI-driven intelligence, infuse identity context and decisions into the everyday workflow of the broader business environment, creating a more productive, user-centric experience that improves time to value.

REST APIs allow organizations to build their own applications, web sites, and tools that take advantage of data, features, and flows from the modern identity security solution. The APIs use familiar RESTful query and path parameters, request/response headers, and JSON request/response bodies.

This enables the creation of automated low to no code workflows to connect to a virtually limitless number of external applications and platforms. HTTP webhooks emitted from the platform can be received by a multitude of downstream applications. For example, request to see a Slack notification every time a Jira ticket changes. Or auto-invite new employees to your #welcome Slack channel every time a new user is added to your directory.

Now's the time

Older identity security systems represent growing operational risks to the enterprise, as well as inadequate protection against increasing cyber threats targeting identity. They are already constraining your business, with increasing support costs, limited workflow automation capabilities, and a lack of coverage across all points of access. Indeed, you may already be restricting your investment in your current identity security system.

You may be starting, or already in a technological transformation – "cloud-first" initiatives, more business-critical SaaS applications, or consolidating datacenters. The success of all these transformations will be limited by the lack of a modern identity security solution. The enterprise attack surface has changed, with the proliferation and wider distribution of identity and access points. The risk is compounded by the flexibility and speed required to accommodate today's diverse and more demanding user. These challenges and risks will not be going away.

Now is the time to consider moving to a modern identity security solution built on AI and machine learning. Moving to a modern identity security solution demonstrates you are thinking strategically about how your business can continue to improve, be productive, and more successful. A modern solution delivers more than stronger security, but also compounds business benefits as well: reduced operational costs, accelerated business processes, and enhanced user experience leading to increased productivity.

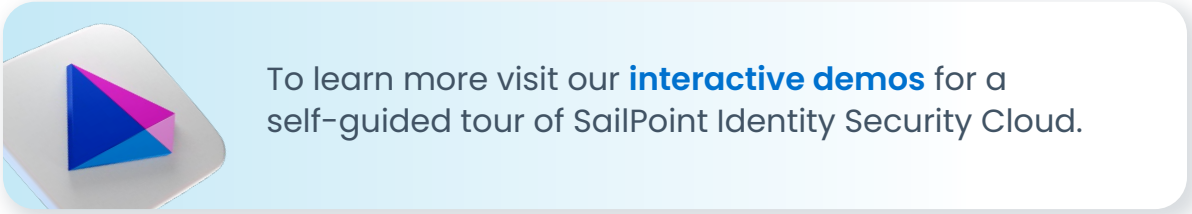
Choosing the right partner to guide you on your identity security journey

No other vendor has the breadth of experience delivering successful identity security solutions than SailPoint. We are the leader in Identity Security with a long track record of success with complex, global enterprise clients across many verticals.

By harnessing the power of AI and machine learning, SailPoint Identity Security Cloud helps companies seamlessly and autonomously deliver the right access to the right identities and technology resources at exactly the right time.

Designed with IT and security teams in mind, built-in Identity Security best practices allow for simplified administration without the need for specialized identity expertise. All new and updated features and maintenance updates are automatically delivered, requiring zero downtime and IT effort. This frees up IT resources and allows organizations to focus on delivering Identity Security program results.

Trust SailPoint Identity Security Cloud to help you discover, manage, and secure all identities across your hybrid environment.



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.