Saviynt | GUIDEPOINT® SECURITY

Building a Strong Foundation for Emerging Identity Threats

Your First Step Toward a Modern Identity Security Program

Contents

Identity-Based Risks on the Rise	3
Identities Under Threat	4
Step 1: Creating Internal Alignment	4
Assessment: The Foundation of Your Strategic Identity Security Roadmap	6
Choosing Identity Security Technologies	10
Ongoing Program Maintenance for the Long Term	10
Conclusion	12
About Saviynt	13

Identity-Based Risks on the Rise

Organizations have made major recent investments in securing their attack surfaces, but threat actors just keep moving faster and getting stealthier. Increasingly, this means they're targeting identities. Identity-based attacks often look just like legitimate end user behavior while giving bad actors far-ranging access to everything from cloud resources and data stores to critical business systems. According to the **Identity Defined Security Alliance,** the number of organizations experiencing identity-related incidents severe enough to require them to invoke formal incident response procedures has nearly doubled since 2023.

These incidents demonstrate that a new breed of attacker is emerging: one who no longer needs to hack into systems. Instead, this attacker simply logs in.

The massive global adoption of cloud infrastructures and SaaS apps is adding to this identity security challenge. These apps tend to be onboarded rapidly, creating complex ecosystems of services and inhibiting visibility.

Increasing SaaS adoption has also led to an explosion of non-human identities (NHI) — including workloads, bots, and credentials. They exist in the environment, but many organizations fail to build robust oversight and governance processes for these identities. This makes them an easy target for attackers. Plus, modern cloud environments are dynamic. As ephemeral workloads, containers and services come and go, it's hard to know which resources need to be protected at any given moment.

To combat rising and evolving identity threats, organizations must create and mature their identity and access management (IAM) strategies to prevent legitimate means of access from becoming avenues that attackers can exploit. This is the foundation for a modern identity security strategy and will reduce these risks now and in the future.

But going from idea to action can be challenging.

To achieve meaningful identity-related risk reduction, the organization will need to:

- **Align internal stakeholders**
- **Implement the needed tools and integrations**
- **Build a comprehensive identity strategy and roadmap**
- **Develop a long-term continuous improvement plan**

In the remainder of this white paper, we'll take a closer look at what's needed for success in each of these areas.

Identities Under Threat

In 2024, **69% of organizations fell victim to phishing attacks,** while 37% were compromised through the use of stolen credentials.

FANCY BEAR, a Russian threat actor group, reportedly connected to Microsoft Exchange servers and changed high-level account mailbox permissions in its victims' environments **using credentials collected during phishing campaigns.**

A rival group, COZY BEAR, used Microsoft Teams messaging to **bypass multi-factor authentication (MFA) protections** for a large number of Microsoft 365 accounts.

LockBit, the ransomware operator responsible for the largest volume of attacks, **continues to leverage stolen credentials** (especially for virtual private networks (VPNs)) to gain initial access to victim environments. Using these identity-based methods, the group has successfully breached more than 2,000 environments and collected more than $120 million in payments from victims worldwide.

First Step: Creating Internal Alignment

Change isn't always easy. Introducing new processes and technologies can either boost productivity or threaten it, depending on how the changes are received. Some of the most important aspects of change management are shifting organizational cultures and gaining stakeholder buy-in. This sets a foundation for identity security transformation.

Start by engaging key stakeholders

It's crucial for project and program leaders to effectively communicate the value of advancing identity security. This way, everyone with a role to play can have accurate expectations.

Understanding the "why" behind the changes helps everyone get on board with process transformation. A successful implementation involves much more than simply deploying a tool—it requires a strategic roadmap that begins with appropriate expectations and cross-organizational alignment. This includes executive sponsorship, aligning efforts with organizational objectives, and maintaining clear communication throughout the process.

Who	What they need to do
Senior leadership and executives	These stakeholders need to be aware that there will likely be pushback to implementing identity security controls. Getting HR and IT operations teams to coordinate across modern and legacy technologies to keep business-critical applications running is a complex task.
Application owners	Application owners need to be involved in moving access lifecycle processes, governance controls, and auto remediation steps to new identity security solutions.
Risk and compliance teams	These key project contributors need to define the organization's risk appetite while advancing governance controls. Their partnership is necessary for managing expectations throughout the project lifecycle.
Identity security project team	This team needs to understand that progress is more important than perfection, and that all hurdles can be overcome. Visibility into and reporting on multi-year program management are crucial for tracking progress.
SIEM, SOAR, and SOC teams	These contributors have been working in silos for too long. It's time to bridge the gaps. Integrating security information and event management (SIEM) and security orchestration, automation, and response (SOAR) tools into the identity strategy and defining incident response plans are critical for mitigating identity-driven threats.

Highlight the bigger-picture objectives

Help all stakeholders understand the value that identity security can bring to the business. A successful enterprise identity security strategy will enable agility while elevating security. It will help the organization eliminate manual processes, streamline compliance, simplify reporting, and leverage automation, AI, and behavioral analytics.

The goals are to:

- Reduce costs
- Minimize risks
- Enable innovation

While balancing:

- User experience
- Process efficiency
- Compliance
- Auditability
- An actionable remediation roadmap

Assessment: The Foundation of Your Strategic Identity Security Roadmap

Today, identity isn't just about humans—it also involves machine identities, service accounts, APIs and much more. For this reason, effective identity security roadmapping begins with an assessment of the behavior and access paths of all entities that access resources within your organization. These include employees and contractors, but workloads, containers, and bots are just as important.

This assessment should yield a clear picture of your current identity security maturity. It should also help you identify vulnerabilities so that you can understand where your organization is most at risk.

Look closely at legacy applications. All too often, they're poorly managed, lack integration options or were deprioritized in identity modernization planning. But these weak spots are exactly where attackers are most likely to strike.

Areas to assess	Questions to ask
Identities: • **Human:** employees, contractors, consumers, customers, guests, supply chain members • **Non-human:** service accounts, APIs, bots, containers, workloads	• Do we have a streamlined, consistent process for onboarding and offboarding human identities? • What is the trigger point for the creation of non-human identities? • Is there an authoritative source for all non-human identities across the entire organization? • Have we established a standardized lifecycle for non-human identities?
Access paths: • **Traditional:** accounts, groups • **Indirect:** policy inheritance, role assumption	• What static and dynamic access controls have we put in place? • To what extent have we streamlined static access control by defining roles and enforcing policies? • Are elevated privileges granted permanently or ephemerally?
Vulnerabilities: • **Stale accounts** • **Hidden paths to privileges** • **Behavioral anomalies**	• What mechanisms have we established to provide visibility into dormant accounts or those whose access has been suspended? • How do we define "normal" or baseline behavior for every aspect of access? • What constitutes an anomaly or outlier? • What mechanisms do we have to detect such anomalous access behavior?

Understand your risk tolerance:

It's no longer a question of if an attack will occur, but when it will happen and which vulnerabilities are most likely to be exploited. If you can answer these questions and understand which types of attacks you can actually mitigate, you can set smart priorities. This empowers you to build high-impact defenses.

Understanding your business's risk tolerance is critical. Ask yourself the following questions:

- If an attack happened, what would the damage look like?
- Among the vulnerabilities in our identity security ecosystem, which are most likely to be exploited?
- Which risks pose the greatest threat to operations?

The answers will help you determine which concerns can take a back seat, and which demand immediate attention.

Build out baseline controls for access hygiene:

Start by safeguarding how users authenticate. Implement industry standard best practices such as multi-factor authentication (MFA) or a passwordless authentication solution. Choose technologies that align with your users' needs and that can be deployed rapidly.

Then, work on improving visibility across your identity and access ecosystem. Develop a clear understanding of who is accessing what within your systems.

Gain visibility:

Develop a clear understanding of who is accessing what within your environment. This provides a robust foundation for establishing governance frameworks and enforcing controls. Such visibility is also invaluable for identifying risks so that you can proactively address vulnerabilities before they lead to breaches.

Establish a comprehensive identity store:

Centralizing identities on an organization-wide scale makes it possible to build out lifecycle processes for all identity types. This also sets the foundation for creating efficiencies through automation and by implementing more granular controls.

The centralized identity store will simplify governance-related processes including access reviews, audit preparation, and reporting. It gives your team an authoritative data source covering all connected endpoints.

Accurate, high-quality identity data will enable your identity security solutions to work as well as possible. This is particularly true for AI. This data will also make it easier to implement more advanced controls, such as Just-in-Time (JIT) access, role-based access controls (RBAC), and attribute-based access controls (ABAC), should your organization need these.

Introduce AI and automation:

As your identity security maturity grows, you'll likely discover a number of opportunities to streamline processes. AI-powered technologies can help you enhance identity security across the organization, reducing manual effort while increasing effectiveness. Automation can be used to define roles, delimit permissions, enforce segregation of duties (SoD), and create reports.

Automation can also help detect the anomalous end-user behavior that signals an in-progress attack. Machine learning (ML), for instance, can automatically define "normal" or baseline behavior across all identities and access types. It can then identify the most common outlier behaviors, and can continuously re-evaluate access permissions during ongoing sessions.

Managing Non-Human Identities (NHI)

Increasingly prevalent in today's SaaS-forward technology environments, NHIs demand a well-defined, strategic process for management and oversight.

This is often lacking in organizations that have experienced rapid SaaS adoption, where a rush to "just get it done" took precedence over establishing strong governance. Without well-defined processes for decommissioning orphan accounts and maintaining visibility into how NHIs communicate, SaaS adoption creates new vulnerabilities.

We recommend you take the following four steps to manage and secure NHIs.

1. Define formal NHI management processes: Establish clear, start-to-end workflows for how NHIs are created, used, and decommissioned. This is the foundation for everything else.

2. Leverage AI tools strategically: AI has tremendous potential to improve NHI governance. It can help you discover NHIs and their access, provide a real-time inventory of your NHI landscape, and illustrate your NHI security posture.

3. Limit long-term access: Identify opportunities to reduce risks by applying temporary or dynamic access restrictions wherever possible. This minimizes risk exposure and reduces the potential blast radius from a breach.

4. Adopt dynamic access processes: While it may not be feasible to do so everywhere, dynamic access controls should be applied in as many places as possible to increase security while enabling flexibility.

Broaden the scope of your identity and access management (IAM) security program:

Identity security isn't just about the workforce. The program's measures can and should be extended to encompass all identities in your organization, including customers, partners, vendors, and non-human identities (NHI).

You can also implement proactive detection strategies (including threat hunting in the identity domain) and expand technical capabilities into areas such as privileged access management (PAM), customer identity and access management (CIAM), and cloud infrastructure entitlement management (CIEM).

Adding automation and orchestration

Integrating automation into your identity security stack is one of the fastest ways to add efficiencies so that you can achieve more without adding staff.

Success in this area does require a relatively high level of maturity to start with, but organizations can de-risk their automation journey by taking a phase adoption approach.

Begin with a focus on the areas that will deliver the most immediate value while thinking ahead to enable scalability for future needs.

1. Start with foundational infrastructure: Begin by addressing your infrastructure. This is typically the organization's most heavily-utilized set of resources, and may include cloud or on-premises systems, or both, depending on your individual setup. Streamlining infrastructure-related processes on Day 1 can significantly reduce overhead. It can also improve operational efficiency for immediate productivity gains.

2. Identify automation-ready technologies and stakeholders: Engage with the app owners and business stakeholders who are most amenable to automation. This group usually includes cloud technologists, since they often work with APIs and structured data—ideal candidates for early automation. Focus on access orchestration (especially access provisioning) as a starting point. Adding automation here typically offers a quick win with measurable results.

3. Expand to systems with more complex integration needs: Once you have gained confidence in your tools and processes for implementing automation, you can start to tackle areas where integration may be more challenging. Examples include legacy systems requiring flat-file integration and older tools lacking straightforward API access. While more effort is required in these areas, it is worthwhile: even partial visibility and automation can deliver significant value.

4. Leverage existing tools and integrations: If your organization already has tools in place like a ticketing system or workflow solution, you can take advantage of these existing integrations. This will simplify the process of automating your identity technology stack. These tools can often streamline processes and enhance visibility and control over your automated workflows.

Choosing Identity Security Technologies

When evaluating vendors' identity security offerings, it's crucial to involve the hands-on practitioners who will be the tools' primary users early in the process. These stakeholders have a vital role to play in the adoption and integration of the tools. If their expectations are aligned, many potential issues that could otherwise derail the project can be prevented.

No vendor assessment should ever take place in a vacuum. Instead, vendor offerings need to be evaluated in the context of your risk assessment findings.

Here are three main factors to consider during the technology assessment process:

- **Application priority matrix:** Identify which of your applications are used the most frequently and where automation will have the biggest impact. Pay particular attention to applications that can enhance efficiency and those that handle sensitive data, especially if regulatory compliance is an issue. These should be your top-priority targets for integration.

- **Technical integration readiness:** Assess where quick integration is most feasible. In addition, look for solutions with robust APIs or other tools that make them integration-ready for a smoother and faster implementation process.

- **The vendor's converged platform capabilities:** The lines between Privileged Access Management (PAM), Identity Governance and Administration (IGA) and Identity Security Posture Management (ISPM) are increasingly blurry. Many vendors are evolving their offerings from single solutions to broader platform-based approaches. As they do, it's becoming more important to evaluate vendors' current ability to address multiple aspects of identity security and cybersecurity. Leveraging a single, integrated identity security platform can significantly streamline your operations.

By focusing on these areas, you can position your organization to select a tool that not only meets your immediate needs but also aligns with your long-term cybersecurity strategy.

You'll also want to consider the vendor's future plans for expanding their capabilities.
How will they respond to the emergence of new identity-based attack vectors? What kinds of detections do they support, and how do they plan to extend these as the threat landscape shifts? What types of automated remediation do they currently offer, and is this a growth area for them? What about identity-based deception technologies?

Ongoing Program Maintenance for the Long Term

Once you've created and matured an IAM security program, you'll need to keep it operating smoothly and continuing to improve.

We recommend focusing your ongoing efforts in three key areas: maintenance, improvements, and reporting.

Maintenance

This includes keeping the lights on and finding and fixing bugs whenever needed.

- Set up daily, monthly, and quarterly tasks to ensure that the solution will be maintained optimally.
- Set aside time to investigate what's causing break-fix issues, as well as other unintended system behavior.

Improvements

Development efforts should be channeled towards improving things that cause issues during everyday operations. Dedicating time in this area ensures that the solution's maturity will continue to evolve over time. Often, opportunities for improvement will be discovered during routine maintenance, so these processes should inform one another.

Maturity reporting:

These reports assess maturity and allow leadership to see growth trends. They should give a sense of the current state of the IAM technology implementation and indicate paths towards improving maturity. Quarterly updates can show maturity over time.

Identity and Access Management Maturity: Metrics to Monitor

- **Time to Value:** How quickly can the program achieve the proposed business outcomes? If it will take longer than six to nine months to roll out a solution, that timeline may be too extended. Consider breaking the implementation into smaller, manageable chunks for faster value realization.
- **Maturity Scoring:** You can use maturity scoring systems to evaluate your progress. Metrics measuring financial considerations, risk tolerance, and operational improvements can be combined into a customized maturity assessment. This should include a means of tracking and documenting progress. It can also provide a clear path to incremental growth.
- **Impact on Daily Operations:** IAM maturity should simplify day-to-day operations. Are there fewer support tickets than there were in the past? Do automation and streamlined processes free up team members to innovate, since they are no longer overwhelmed by repetitive tasks? These are key indicators that your program is effective.
- **Gains in Efficiency and Risk Mitigation:** What improvements are you seeing in efficiency, visibility, and risk mitigation? Start by identifying these gains. Then, evaluate how they contribute to overall system maturity and security posture.

Conclusion

Developing and maturing IAM at your organization isn't something that happens overnight. It takes time, effort, the right strategy, and stakeholder buy-in to build a robust program that meaningfully reduces your risks. Every viable IAM security program encompasses people and processes as well as technologies. Adjustments need to be made in all three areas, and success involves culture change as well as tool deployment. End user acceptance of the new tools is just as important.

For organizations in the early stages of this journey, it's important to start with achievable milestones — such as gaining visibility into identities and entitlements, implementing strong authentication, and establishing governance processes. Early wins build momentum and credibility, helping to sustain long-term commitment.

But once this foundation is in place, you now have the building blocks and are on your way to developing a modern, comprehensive Identity Security strategy.

On a mission to safeguard enterprises through intelligent, cloud-first identity governance and access management solutions, Saviynt provides the world's #1 converged identity platform. The Saviynt Identity Cloud converges IGA, granular application access, cloud security, privileged access and posture management into the industry's only enterprise-grade SaaS solution.

Creating and executing an identity and access management security roadmap can be complicated, but having the right partner by your side will simplify the process. GuidePoint Security has multiple decades of experience helping clients navigate the complex maze of risk-based cybersecurity decision-making while becoming better informed and moving at the speed of business. With a deep understanding of the language and key concepts that resonate with different stakeholders across the organization, GuidePoint is well prepared to serve as a trusted advisor to organizations confronting complex issues and nuanced risks.

Visit **saviynt.com** or **GuidePoint Security** to learn more.

ABOUT SAVIYNT

Saviynt's AI-powered identity platform manages and governs human and non-human access to all of an organization's applications, data, and business processes. Customers trust Saviynt to safeguard their digital assets, drive operational efficiency, and reduce compliance costs. Built for the AI age, Saviynt is today helping organizations safely accelerate their deployment and usage of AI. Saviynt is recognized as the leader in identity security, with solutions that protect and empower the world's leading brands, Fortune 500 companies and government institutions. For more information, please visit **www.saviynt.com.**

Saviynt

Headquarters, 1301 E
El Segundo Bl, Suite D, El Segundo, CA
90245, United States

310. 641. 1664 | info@saviynt.com
www.saviynt.com