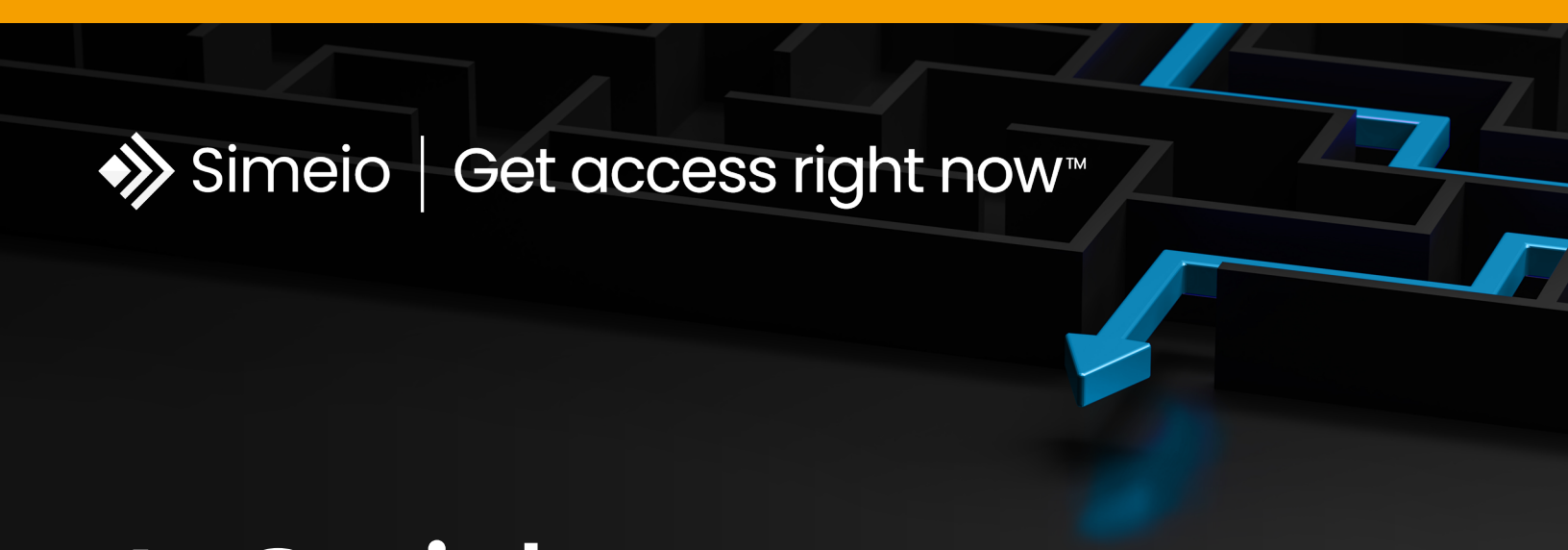
Simeio | Get access right now™



A Guide to Choosing the Right Managed Identity Security Provider

A guide to help CIOs, CISOs, COOs, and CFOs evaluate when to outsource their identity and access management (IAM) programs and how to choose the right managed identity service partner.

Contents

Introduction: A Guide to Deciding When You Should Engage Managed Identity Providers..... 3

The Top 7 Use Cases for Engaging Managed Identity Providers..... 4

Part I. A Five-Step Guide to Choosing the Right Managed Identity Provider 7

1. Is IAM a core focus?..... 7

2. Does the provider offer a complete, affordable solution?..... 8

3. Does the provider have a clear vision for the future of your program? 9

4. Does the Managed Identity Provider deliver clear value?..... 10

5. Will your team like working with this provider? 10

Part II: Measuring Value: Calculating ROI on Managed Identity 11

Real-World Use Cases and ROI Calculations 12

Conclusion: Simeio Brings the Focus, Flex, and Full-service Solution to Get IAM Right the First Time..... 14

Let's Talk About You 15

Introduction:

A Guide to Deciding When You Should Engage Managed Identity Security Providers

Access Takes Orchestration

If identity is the new perimeter of security, we can think of Identity and Access Management (IAM) as the company's control tower. If you don't build strong IAM, your company finds itself vulnerable to attacks, breaches, failed audits, and burnout within the ranks.

This guide explores when it makes sense to bring in reinforcements and offers a step-by-step process for finding the right partner to manage and secure your identity practice. We'll start with the challenges.

"It's complicated"

As the foundation of Zero Trust, today's IAM is a strategic discipline that goes beyond authentication and password management to include specialized practices like privileged access management (PAM) and consumer identity and access management (CIAM). The cost and complexity of IAM only stands to get worse with the rise of machine identities and new, AI-led attacks on identity.

It doesn't help that the identity landscape is filled with hundreds of vendors promising anything and everything, and platforms that offer partial solutions. Each point solution comes with separate contracts, licenses, training, and support, and even "managed" offerings that claim to take care of everything can bury your team with irrelevant tickets.

Modern IAM includes:

- Identity Governance and Administration (IGA)
- Access Management (AM)
- Privileged Access Management (PAM)
- Customer IAM (CIAM)
- Managing non-human identities

Bad identity hygiene drives bad outcomes

Trying to manage everything in-house without a roadmap spirals out of control quickly, turning up hidden risks, costs, and user frustration:

- **Monthly software costs run over** due to over-licensing and poor entitlement management
- **Tools and features go unused** leading to wasted spend and investments in training
- **Siloed systems and overlapping contracts** compound over time
- **IT and user productivity suffer** as teams juggle too many solutions, tickets, manual processes, and fragmented systems
- **Gaps in visibility and IAM coverage leave businesses vulnerable** to attack, breaches, reputation loss, and higher cyber insurance premiums

What matters depends on who you ask . . .

Role	Challenges	What's Required
CFO	IAM investments scattered across too many siloed tools, no clear ROI, failed audits	Tool integration and consolidation, clear reporting
CIO	Can't onboard apps fast enough, ops team stretched too thin, digital transformation stalls	Proven onboarding process, frictionless workflows, consolidated identity infrastructure
CISO	Poor visibility into entitlements, inconsistent controls, gaps in coverage lead to breaches	End-to-end identity security strategy and coverage, phishing resistance, continuous visibility and monitoring
COO	Access inefficiencies, M&A integration issues, lost productivity	Seamless user experience, collaboration between IAM and security teams

Some of these situations may be tolerated short-term but will ultimately lead to security debt. So, when is it time to do something about it?

The Top 7 Use Cases for Engaging Managed Identity Security Services Providers

Enterprises all need to give the right people the right access. For some, it makes sense to engage a managed identity and access management provider to build, scale, consolidate, or fix their identity programs when:

1. **They're engaged in mergers and acquisitions (M&A) and/or restructuring.** Teams may lack knowledge of some identity systems and public awareness of M&As signals opportunity for threat actors. Inconsistent or incomplete identity governance my also put compliance at risk.
2. **Their IAM program is fragmented across disparate tools.** Disconnected systems create visibility gaps, risk, and operational inefficiencies.
3. **The company fails an audit or certifications take too long.** Non-compliance puts your business at risk and delays key initiatives.
4. **IT or security teams get overextended.** Many internal teams lack the bandwidth to manage identity programs at scale. Even routine tasks (like handling tickets and maintaining change documentation) may stretch resources too thin.
5. **Identity programs stall after initial deployment.** Programs tend to lose momentum post-implementation resulting in underutilized platforms and delayed ROI.
6. **Budget constraints demand greater efficiency.** IAM teams struggle to demonstrate value or total cost of ownership (TCO) is too high making it harder to secure the resources needed to finish the job.
7. **They suffer a breach.** Security incidents reveal the blind spots lurking in identity coverage and early indicators your team may have missed or failed to respond to in time.

Is it Time?

If you are asking yourself these questions, it may be time to change your approach to outsource.

Strategic Alignment

- Is identity core to our business's digital transformation—or just a compliance checkbox?
- Are we treating IAM as infrastructure or as a strategic control layer?
- Can our current team realistically support modern IAM at scale, 24/7?

Financial Impact

- Are we overpaying for licenses or features we're not using?
- Do we have full visibility into the total cost of ownership (TCO) for our current identity ecosystem?
- Could outsourcing reduce software overruns, duplicate vendor costs, or audit penalties?

Team Capacity & Skills

- Are our internal teams stretched too thin managing identity-related tickets?
- Do we have the specialized expertise needed for onboarding, governance, PAM, CIAM, and audits?
- What happens when our one IAM expert takes PTO—or leaves?

Security & Risk

- Can we show consistent enforcement of access policies across all systems?
- How quickly could we respond if a breach happened today?
- Are we missing audit windows or struggling to maintain cyber insurance compliance?

Flexibility & Scalability

- Are we confident we can onboard new apps or divest business units quickly during M&A?
- Can we adapt to new compliance requirements, platform shifts, or user demands without major rework?
- Are we relying on fragile, tribal knowledge or repeatable, documented processes?

Reporting & Leadership Insight

- Can we show year-over-year IAM improvements to our board or CFO?
- Are we using identity data to proactively improve posture—or just react to issues?
- Do we have a consistent view of entitlements, user behavior, and risk?

Once you recognize that outsourcing all or part of IAM is the strategic choice, the critical next question becomes:

What Kind of Partner Should You Engage?

Identity consistently ranks at the top of the CISO's agenda so more managed service providers (MSPs) and managed security service providers (MSSPs) offer the basics—like single sign-on (SSO), multifactor authentication (MFA), and directory services—as part of their bundled offerings. Putting these popular items on the menu lets clients (and the providers themselves) check some boxes for compliance and Zero Trust best practices. That's useful for audits and cyber insurance but doesn't necessarily make your company safe from attacks that can shut down business operations.

IAM requires a depth of expertise, modern automation, and a proven strategic framework and methodology to meet your real goals for identity security — stopping breaches, lowering cost, and improving user experience. As new threats and defensive technologies emerge, partnering with a managed identity security services provider that offers a clear roadmap and foresight into the future of identity can meet those goals—better and faster than companies can on their own.

Choose the right partner carefully
A specialized strategic provider should:

- Use a mix of proven and cutting-edge technologies
- Offer services on a subscription basis
- Provide end-to-end IAM solutions featuring top-tier products, advisory services, and ongoing support from specialized identity experts — everything you need to build and scale IAM across your cloud and on-premises environments

The next section offers a step-by-step guide to identifying and engaging your ideal partner.

Part I.

A Five-Step Guide to Choosing a Managed Identity Service Provider

Most MSPs, MSSPs, and managed identity security services providers claim to offer world-class products, platforms, and professional services that make your job effortless. Reading between the lines of polished marketing means asking the right questions to find the company that understands your situation—the one who can design, implement, operate, scale, and measure the value of your IAM program—at a price you can afford.

Delve into these five areas to rate prospective providers:

1 IAM a core focus?

Real managed identity providers specialize—vs. dabble—in building and managing IAM programs. They field teams of experts who know what works and how to deliver it effectively.

The right provider . . .
Brings the vision, tools, technologies, skills, certifications, track record, references, and metrics for demonstrating success.

Questions to ask prospective partners
To ensure you're partnering with a true specialist, ask:

- **What IAM platforms do you provide and manage?** Leaders should be proficient and maintain certifications on leading platforms such as SailPoint, Saviynt, Ping, Okta, CyberArk, BeyondTrust, Microsoft, and IBM. Ideally, they would also offer preferred pricing.
- **How deep is your bench?** Look for bench strength to support large or complex initiatives and sudden spikes in requirements, like during M&As or following breaches.
- **Where are resources based and when are they delivered?** Time zones matter. If your company operates in California and key resources are based in places like Poland, you may face delays in communication, issue resolution, or project velocity. Ensure alignment in working hours for critical functions.
- **How well do you know our industry?** The provider's experience should include knowledge of compliance frameworks like SOX (finance), HIPAA (healthcare), or NERC-CIP (energy) to make sure your program won't fall short under scrutiny.
- **Can you provide references?** Look for companies whose identity-focused projects have goals and parameters similar to yours. Never be the test case!

Insider Tip:

Get to know the company's senior Senior Implementation Specialist. If they're true IAM visionaries, their leadership will shape the mindset, quality, and consistency of their team — and yours.

2 Does the provider offer a complete, affordable solution?

Look for a holistic, single-source solution versus fragmented tools and programs that burn through your resources.

The right provider . . .
Solves and simplifies your identity challenges end-to-end with a unified IAM offering:

- Products and technology
- Planning and managing installation
- Proven processes and IP that automate and accelerate implementations
- Ongoing support and management
- Advisory and roadmap capabilities
- Visibility and actionable reporting on the entire program

Insider Tip:

Look for providers that offer proprietary tools or accelerators that streamline application onboarding—these are strong indicators of operational maturity and long-term scalability.

Questions to ask prospective partners

- **What components do you offer?** Are the offerings and bundles flexible to fill gaps, work with and extend your existing investments?
- **How do you balance automation and analyst expertise?** How many people will support your implementation? What level of skills do they bring? How quickly can they provider add support if needed?
- **Are there areas you can't help improve?** Make sure the provider offers implementation, management, training and advisory services—or whatever mix of capabilities you need.
- **What exactly do your SLAs cover?** Are issue resolution times defined? Is 24/7 support available? Is support reactive or proactive? Does the 'single point of contact' extend to solutions you already have in place?
- **How much will everything cost?** Pricing should be predictable, scoped to your needs, and aligned to usage, not shelfware. Bundled offerings should be flexible and include software licensing, managing implementations, day-to-day operations, and professional advisory services. Make sure the partner offers a package that aligns to your company's size, budget, and future goals for growth.

Insider Tip:

The right partner won't hesitate to commit to response times, root cause analysis, and regular optimization reviews.

3 Does the provider have a clear vision for the future of your program?

A strategic partner constantly looks for ways to innovate, streamline, and reduce your long-term costs. Their value lies not only in managing operations, but evolving your identity program to be more efficient, resilient, and future-ready.

The right provider . . .
Doesn't just sell tools and execute tasks. They have and can articulate a 1-, 3-, and possibly even a 5-year plan for evolving your IAM program. If the vision involves ongoing investment, they should be able to articulate and help quantify the need for that investment to the board, the risk of not investing, and its value to your company.

Look for a partner who can outline a detailed, proactive strategy—not just maintain the status quo. Make sure they bring ideas for the next phase of your IAM journey.

Questions to ask prospective partners

- **What is your vision for my IAM program over the next 1–3 years?** Understand whether the roadmap addresses technology, governance, automation, risk, and cost optimization.
- **How will your plan add or reduce cost and complexity?** Ask the provider to get specific as they explain recommendations for adding tools, support, and analyst coverage.
- **Do you have formal structures for regular program evaluation, such as annual reviews or maturity assessments?** Ongoing evaluation proves essential to keeping business goals and evolving threat landscapes aligned.
- **How do you balance automation with human expertise?** Automation increases efficiency, but it needs to be guided by expert oversight to avoid risk and ensure effectiveness.
- **Can you help maximize the investments we've already made?**

A good partner should help you get more value from your existing tools before recommending new ones. Ask about integrations, partnerships with vendors, and bundled implementation and support offerings.

4 Does the provider deliver clear value?

You shouldn't have to guess whether your IAM investment is working or generating value. A strong managed identity provider can clearly demonstrate the program's effectiveness through transparent reporting, actionable metrics, and measurable outcomes.

The right provider . . .
Establishes clear criteria and metrics for measuring success at the outset of the program. Examples include:

- Improvements in risk scores year over year
- Tool utilization
- Efficiency gains for processes like access reviews
- Demonstrating readiness during compliance audits
- Reduced training or specialized skills requirements

Questions to ask prospective partners

- **How do you track, measure, and communicate the value of the IAM program over time?**
- **Do your reports and analytics clearly quantify return on investment (ROI)?** Make sure regular reporting translates easily in board-level reports required to secure ongoing funding for IAM and other security initiatives.

Ask the provider to walk you through their reporting tools or dashboards to see how they track and communicate program effectiveness in real time—a strong indicator of their maturity and transparency.

5 Will your team like working with this provider?

All successful partnerships depend on how well companies work together. Meet the team to evaluate the chemistry between your teams and whether your relationship would be founded on mutual respect, transparency, and collaboration.

The right provider . . .
Communicates clearly, sets clear expectations and works closely with your internal team and IAM vendors.

Questions to ask prospective partners

- **What does a day-to-day engagement look like?** Understand how communication flows, how issues are tracked, and what cadence to expect for updates, health-checks, and regular reports.
- **Will I have a single point of contact? What does the support and delivery structure look like?** Clear accountability and defined roles help avoid confusion and ensure smooth collaboration.

"We picked our partner. Now what happens?"

Once you choose the right partner, you can get down to business: identify gaps, designing solutions to fill them, and creating a schedule, budget, and project plan for moving forward with assessments, installations, and ongoing services.

To help level-set, ask the partner to help you run targeted ROI calculations and define reporting that shows when, where, and how far your new IAM program moves the needle.

Part II.

Measuring Value: Calculating ROI on Managed Identity

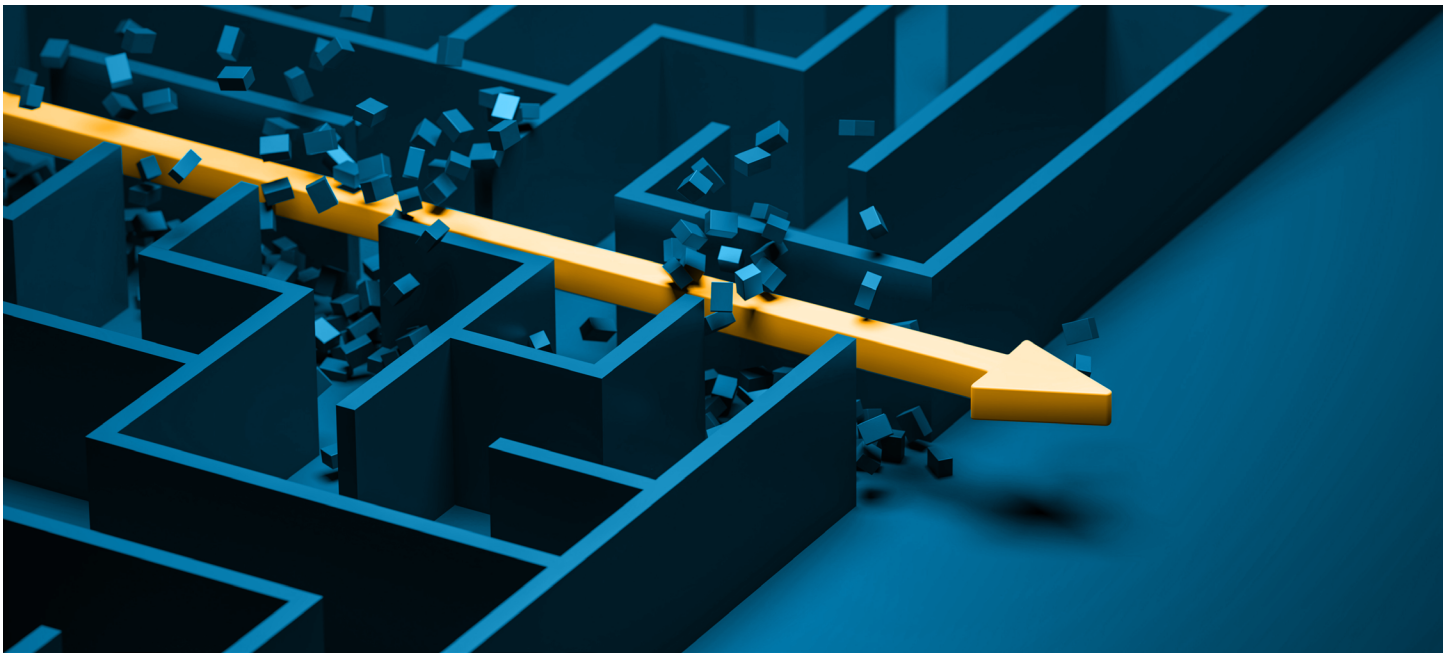
Every business and identity program is different, so every ROI calculation is different, but analyzing the value of managed identity services should always cover some basic criteria:

Procurement – the cost of licenses purchased through a Managed Identity Provider versus standard list prices. Does the provider offer favorable pricing based on established vendor relationships?

Implementation – Outsourcing may result in faster deployment with fewer delays and surprises. How much will you save by keeping your own team free to focus on the core business?

Management – Ongoing IAM programs require expertise for roadmap planning and staffing for implementation, 24/7 monitoring, and reporting. Will strategic advisory resources be available—as part of ongoing services—after rolling out products?

Expertise – Having to hire and train more staff adds delays, risk, and cost. How much more quickly can you scale with your partner and how much is that time worth?



Real-World Use Cases and ROI Calculations

Luxury Hotel Company Saves 77% on IAM

A $5B luxury hotel company engaged a Managed Identity Provider to establish its IAM strategy, beginning with PAM to secure privileged users at headquarters and across multiple cities and brands. Outsourcing its program avoided the need to hire a large in-house team while ensuring long-term security and scalability.

With 36K employees worldwide, engaging a managed identity provider saved the company:

88%
on procuring licenses

26%
on implementation

54%
on management

77%
overall

Global Manufacturer Streamlines Access Management, Cuts Costs by 60%

A $10B global manufacturer with 50,000 employees faced mounting challenges managing user access across hundreds of applications and production sites. By partnering with a Managed Identity Provider to deploy a unified access management platform (that includes SSO and MFA), the company eliminated legacy point solutions and manual processes.

A centralized access management solution helped the manufacturer save:

75% %
on licensing fees

32%
on IT support and access-related helpdesk tickets

60%
on access management overall

Software Company Strengthens Identity and Access Management After a Ransomware Attack

A $1B software company with no PAM strategy in place suffered a major ransomware attack. Following the incident, which involved a compromised privileged attack, the company outsourced IAM to stabilize and mature its identity security quickly.

Despite undergoing three leadership changes during the engagement, the organization maintained consistent progress and was able to meet mandates by the US Attorney General to strengthen its IAM program. Working closely with its Managed Identity partner, the company developed a rapid-response action plan while saving:

52.1%
on procuring licenses

24.2%
on implementation

74.5%
on management

49.1%
overall

$3B US Bank Reduces Costs Nearly 50%

implementation had critical misconfigurations. With multiple underutilized tools and no dedicated team to manage daily operations, engaging a managed identity partner helped the company consolidate its technology stack to save:

38.5%
on procuring licenses

28.5%
on implementation

73.7%
on management

48.6%
overall

National Retailer Modernizes IGA, Reduces Audit Costs by 70%

A leading national retailer with 80,000 employees and thousands of seasonal workers needed to modernize its IGA practice to meet new regulatory requirements and streamline onboarding. By outsourcing to a Managed Identity Provider, the retailer automated user provisioning, access reviews, and compliance reporting.

The managed IGA solution saved the company:

82%
on compliance and audit preparation

40%
on onboarding time for new hires

55%
on ongoing management costs

70%
overall on IGA

State Government Launches CIAM Portal, Boosts Engagement While Lowering Cost

A US state government leveraged a Managed Identity Provider to build and launch a secure, scalable Customer Identity and Access Management (CIAM) portal to serve 2 million citizens and businesses. Frictionless digital service led to improved adoption rates and citizen satisfaction along with formidable savings:

68%
on development and integration costs

50%
in access-related support calls

45%
on ongoing management

62%
overall

Conclusion:

Simeio Brings the Focus, Flex, and Full-Service Solution to Get IAM Right the First Time

Simeio is how enterprises give the right people the right digital access. We live and breathe identity access and security—it's all we do. We bring the depth needed to solve today's problems and scale to meet tomorrow's challenges. And we bring complete solutions that simplify the IAM journey from managing onboarding to managing credentials, compliance, and user experience.

We become your IAM team
Simeio brings unmatched expertise, ecosystem depth, and a singular mission to make managing identity seamless, secure, and scalable. Whether you're rolling out your first access policy or untangling the aftermath of an acquisition, Simeio brings the technology, people, and process maturity to accelerate success.

We lower cost and increase scale
Offerings include real-time credentialing, policy enforcement, and access management—without juggling multiple vendors or invoices. Flexible bundles bring together licenses, managed services, and 24/7 support at predictable pricing—so you only pay for what you use and always know what to expect. Pricing stays predictable, scoped to your needs, and designed to scale with you.

Simeio IO adds the 'secret sauce'
Our platform is the engine we use to unify your identity fabric, onboard applications faster, drive continuous compliance, and deliver real-time analytics. Whether you're leveraging IO directly or benefiting from orchestration and automation behind the scenes, you'll gain full observability, lower cost, and improve outcomes.

We even grade ourselves
Simeio's annual Report Cards don't just track our progress—they help you demonstrate investment value. We audit your IAM posture, explain the scores and changes, and identify the next highest-value steps you can take.

With Simeio, identity finally becomes a source of clarity and confidence—not complexity.

Global Certifications:

- SOC 2 Type-II Compliant
- ISO 27001 Certified
- ISO 27018 Certified
- CSA Star Certified
- AWS Advance Security Partner Certified

Simplify, Automate, Secure

- Unify Your IAM Infrastructure
- Identity Security Posture Management (ISPM)
- Effortless Audit and Compliance Management
- Automated Remediation of Control Gaps
- Continuous Identity Control Lifecycle Management
- Seamless Migration from Legacy Systems

> Simeio's IAM solutions have been a **game-changer** for our organization. We've seen a **35% increase** in staff productivity and a **50% reduction** in security incidents."
>
> —IT Director, Forture 500 Company

Let's Talk About You

Share your IAM goals and challenges with a Simeio identity expert and we'll help you run a personalized ROI calculation or condentity Maturity Benchmark Session to help fast-track progress on your identity journey.

Request a Demo

Simeio | Get access right now™

info@simeio.com | www.simeio.com