simeio

TOP 5 REASONS TO INVEST IN MANAGED IAM SERVICES

Safeguarding Trust & Wealth

www.simeio.com

Whether you're a bank, an insurance firm, or an investment advisory service, your customers rely upon you to keep their wealth safe. Both the ultra-rich CEO responsible for the employment of ten thousand people and the immigrant small-business owner responsible for his four kids rely upon institutions like yours. And both are the target of malicious thieves seeking to pilfer what you have been trusted with. When every unprotected attack surface is a countdown to breach and every identity is a target, that makes for a very large attack surface.

Against such dangers, you can't count on internal workers to get the job done. Institutional investors hire professionals to manage their investments. Likewise, your company needs security professionals to manage security against professional cyber criminals. It's not just about having the right technology. You need the right expertise, outsourcing to seasoned experts who know the difference between an IAM solution and a transformative identity service. Here's just five reasons why you should invest in a managed IAM service.

1 MORE EFFECTIVE PLANNING

Guided Assessment

A guided assessment presents an easily digestible view of your current identity fabric. This provides information on all aspects of your identity including ways you can become more efficient. However, your main takeaway will be the gaps in your security and how you can best rectify them. This managed service offering lets you "test the waters" with smaller investments, allowing you to gauge the effectiveness of both external IAM services in general and the specific provider in case you want to use them for implementation.

Maturity Rating as a Tool

A maturity rating tool helps provide a bird's eye view of your overall risk posture and helps keep you on track for continual improvement. At present, it is the best shorthand available for understanding and communicating your identity needs as well as charting out your improvements and priorities. A maturity model breaks down the fundamental aspects of your identity fabric, its weaknesses, and how those weaknesses can be addressed.

Maturity Rating	Maturity level	Descriptions
0	Non-Existent	Not understood, not formalized; need is not recognized
1	Ad-hoc or Initial	Occasional, not consistent, not planned, disorganized
2	Repeatable or Developing	Intuitive, not documented, occurs only when necessary
3	Defined	Documented, predictable, evaluated occasionally, understood
4	Measured or Managed	Well managed, formal, often automated, evaluated frequently
5	Optimized	Continuous and effective integrated, proactive, usually automated

Expert Insights

By engaging with a team of experts who have worked across multiple different businesses, you benefit from insight and planning skills only available from veteran service providers. They advise on the best programs and applications to bring in, as well as which to cut loose. They know how to cut your costs while boosting returns. Most importantly, they know how long your job is likely to take and what resources will be required to accomplish your objectives.

2 GREATER SECURITY OF PRIVILEGED DATA

Stopping Human Error

According to a 2023 Verizon report study, 44% of all data breaches come from credential insecurity (Verizon, 2023 Data Breach Investigations Report). If you don't have a strong fence around your authentication, then you're going to get burned. The first step is educating your employees about proper identity hygiene. But even that will leave you open to clever fakery and tricks. If you want to properly protect yourself from credential theft and abuse, you must adopt zero trust measures.

Better Monitoring

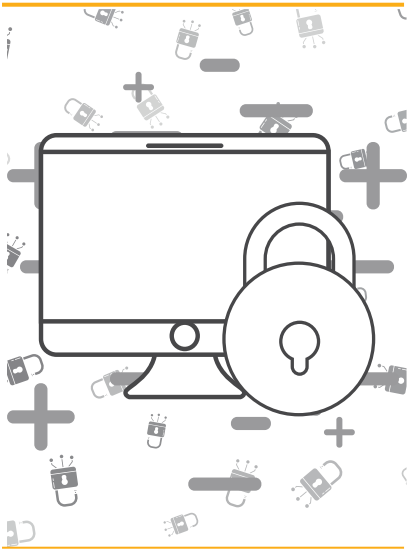
At any given moment of operations, you need to be able to answer the 6 big questions around how your systems are being used.
These are:

- Who has access to what?
- When did they get access?
- How did they get access?
- Who authorized their access?
- Is the access privileged?
- How is it being used?

If your monitoring solution answers all six satisfactorily you've covered your bases well, both for dissuasion and for remediation.

Remediation Strategy

Having a backup plan for if a breach does occur is not just vital for your safety, it is a key part of some compliances (namely PCI). You need to be able to point to what caused a breach as quickly as possible. Above all, you must have a plan you can enact at a moment's notice. Doing so can greatly reduce the damage done by an otherwise bad breach.
When paired with layers of role-based access, you can potentially keep your privileged and sensitive data safe even if less crucial information is compromised.



3 EASIER COMPLIANCE

Cost of Failure

As a financial institution, your biggest compliances are GDPR, PCI DSS, GLBA, SOX, and AML, and each has steep consequences for failure. Anti-money laundering (AML) directive violations alone cost banking and brokerage firms more than $8 BN in 2022 (Comply Advantage, Top AML Fines in 2022). GDPR infringements can cost 4% of annual worldwide turnover (European Commission, What if my company/organization fails to comply with the data protection rules?). PCI DSS violations can cost over $1 MN annually, yet according to the 2018 Verizon payment security report only 52.5% of all organizations are 100% PCI compliant (Verizon, 2018 Payment Security Report). Gramm-Leach-Bliley Act (GLBA) violations can inflict losses of $100k per incident and up to 5 years of jail time (Digital Guardian, What is GLBA Compliance?). Failing to comply with SOX can result in the company being delisted from the public stock exchange (Diligent, SOX penalties: What they are, how to avoid them & who is protected).

How IAM Helps Each Compliance

Preparing for these compliance requirements necessitates several capabilities and ongoing practices. Managed identity services help you not only meet your immediate compliance needs but help prepare you for years to come. Are your identities able to be swiftly de-provisioned and their associated data scrubbed? Do you know if your third-party vendors are creating security risks? How often do you curate your identities for orphaned accounts and delete them before they become a vulnerability? Managed IAM ensures you can answer these questions with minimal hassle, allowing you to focus on your enterprise instead of onerous compliance.

Benefits Beyond Compliance

Beyond just not getting fined, meeting regulatory standards with the aid of managed IAM makes your systems more efficient at countering cyber risks. Federated identity management can help ensure your security policies are automatically enforced. Managed identity governance helps counter identity sprawl, reining in extraneous accounts and reducing unnecessary attack surfaces. Privileged Access Management (PAM) grants real-time monitoring of sensitive accounts and automatically cuts off access the moment suspicious activity is detected.

ONLY 52.5% OF ALL ORGANIZATIONS ARE 100% PCI COMPLIANT

4 SAFER USERS: CUSTOMERS, PARTNERS & EMPLOYEES

Customers

Your enterprise lives or dies on the backs of customers, and IAM services enhance their security and experience in a single stroke. Implementing MFA and SSO keeps their assets under vigilant eyes without creating friction, their data is protected not just by your internal systems but by the service as well. Modern cybersecurity needs can only be properly satisfied if you have proper monitoring capabilities, and that can only happen if you have a service looking after your data at all hours. That means having automatic detection backed by a team ready to swoop in.

Partners

By unifying all your identity functions under a single umbrella, the same care you give to your customers can be applied to your partners. With managed IAM at their backs, your partners don't need to worry about their billing and other information being exposed. They'll be operating within a single secure framework aided by strong software and expertise from across the industry. You also don't need to worry about your partners exposing weaknesses in your own security fabric, since a unified security platform puts everything under a single pane of glass and enforces your policies upon anyone who uses your systems.

Employees

Don't forget that such a system extends its benefits to your employees as well. Ongoing monitoring of company machines ensures that everyone is held accountable. According to Verizon report, almost one out of every five data breaches comes from inside the company (Version, 2023 Data Breach Investigations Report). Furthermore, zero-trust takes a good bit of burden off them by making staying safe easier. A well-executed security solution for employees also reduces friction, since the authentication process is expedited by automation and SSO. Even recovery methods like MFA and self-service options contribute to bolstering both your security and efficiency.

ALMOST 1 OUT OF EVERY 5 DATA BREACHES COMES FROM INSIDE THE COMPANY.

5 BETTER ROI ON IDENTITY INVESTMENTS MEANS LESS WASTE

App Curation

Do you even know how many applications or services you are paying for, but not using? From the monthly fees to the very electricity needed to power the monitor using it, your costs pile up like garbage blocking a door. Clean up your costs with identity experts and pass on those savings to your customers and stockholders. A few fewer seconds of loading time is all it takes for customers to take notice, have a higher opinion of your company, and stay happy and paying.

App Onboarding and Integration

How well are your applications integrated? Tacking on new applications for every problem bloats budgets and hampers smooth operations. Stop sinking money into siloed inefficiencies and get federated platforms which do everything at a fraction of the cost. Having a tighter fabric means that you cut back on potential attack surfaces as well, so you will be gaining both better performance and better chances of staying secure.

Slashed overall IAM costs

All these savings add up to paying less to get out more. Not only does this yield results in the short term, but it makes future additions faster, easier, and better. You also can put less necessity on internal staff. External IAM service providers take up the slack and alleviate the burden of costly technical skills while being more accountable. After all, their reputation is staked upon your satisfaction.

Conclusion

Financial institutions are becoming more vulnerable to cyber attacks every year. The MOVEit breaches of 2023 proved that even Big Four companies are not immune to embarrassing and costly attacks. An IAM service can start you off on the right track, fortify your most valuable identities, prime you to pass all your key compliance tasks, build customer confidence, and optimize your organization for safety and efficiency. Too many companies ignored the advice of experts in not investing in IAM services; now far too many are reaping the whirlwind as cyber risks spread faster than they can handle.