IDMWORKS

The Future of Identity:

Managed Identity Security Services

www.idmworks.com

EXECUTIVE OVERVIEW

Once a niche subset of Infosec, Identity and Access Management (IAM) now sits squarely in the center of enabling digital transformation. IAM programs (and those who run them) must evolve to deliver an agile, adaptive, centralized service that enables business innovation with minimal friction while ensuring security and safeguarding privacy.

This poses a significant challenge to small and medium businesses and enterprise alike on multiple fronts:

- IAM has always been complex. The addition of consumer identities, maturing business identity needs and rapidly advancing IoT requirements creates an environment that requires a long-term roadmap.
- IAM services and solutions are evolving at a break-neck pace as they struggle to keep pace with an explosion of digital-first engagement models and remote work.
- Many organizations continue to grapple with identity sprawl and technical debt with monolithic on-premises legacy vendor solutions that stifle innovation.
- There is a critical shortage of cybersecurity skilled talent, particularly those with identity and access management experience.

As a result, organizations are increasingly turning to managed security services partners to help them attack IAM. In this paper we will

- Business benefits a managed identity security services partner can bring
- Key criteria for finding the right managed sescurity services partner
- IAM program management models

EVOLVING IAM LANDSCAPE

Identity and access management (IAM) has evolved rapidly over the past five years, maturing from a straightforward point-to-point secure connection (largely on-premises,) to a complex model of connections between people, things, devices, and applications that live both on-premises and in the cloud.

The ability to easily identify people, applications and devices and securely connect with them is the foundation of how we work, communicate, collaborate, and consume services. As the digital world advances, the volume and complexity of those connections will continue to explode, creating business demands most IAM teams aren't equipped to address on their own.

While the technology trends straining the capabilities of IAM aren't new, the scope of these trends taken together creates a significant challenge, and opportunity, for IAM teams.

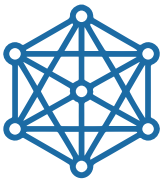
TECHNOLOGY TRENDS IMPACTING IAM

CLOUD

Cloud computing is not a new challenge for IAM solutions; over the past decade, it has fundamentally changed the way we think about securing access and spawned a whole new era of IAM vendors and solutions. As we evolve from securing access to applications in the cloud to how we leverage cloud benefits from an IAM perspective (identity storage, Identity as a Service offerings), our view of the "right" IAM architecture also changes and creates the possibility of approaching IAM as a centralized set of microservices.

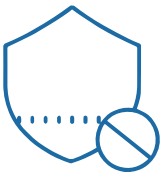
MOBILE

Like cloud-first, mobile access changed how we think about access security. When devices are no longer housed within a secure physical perimeter, our notion of perimeter must change. Today mobile wireless access is more common than not. As mobile devices increase in capability and wireless access increases in coverage and usability, the scope of what we will do on our mobile devices (and even the definition of a mobile device) will continue to evolve the IAM landscape.



BIG DATA

Cloud As IoT, mobile, and social grow, so too does the volume of associated data and the need to manage that data. Big data, coupled with advances in machine learning, supports the business desire to monetize insights across broad data sets. While this trend can help IAM organizations better secure end-points, it also increases challenges on the privacy front, driving sweeping regulatory demands that identity and access management teams aren't always equipped to comply with.



PII PRIVACY

The volume of potentially personallyidentifiable information gathered as a result of mobile access and smart, connected devices has changed how we must view privacy and is driving regulatory responses across the globe. Landmark changes, like those required of the GDPR and the California Data Protection Act, are pushing IAM solutions beyond their current limits; driving innovation for better privacy control at both a device and data level.

TECHNOLOGY TRENDS IMPACTING IAM

INTERNET OF THINGS

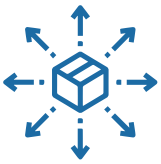
The Internet of Things is here, with the volume of connected smart devices exploding. Soon nearly every object we interact with will have the potential to be a smart, connected device. How these devices connect over the internet, both to each other and to individuals and businesses, as well as the sheer volume of sensitive data they generate has created a security challenge in scope and complexity that most IAM organizations are not equipped to address.

BOARD VISIBILITY

Security continues to be a number one priority for executive teams, which is no surprise given the board-level visibility surrounding risk and the potential brand exposure even a minor breach can bring. We're seeing this play out in the increasing trend of CISOs reporting directly to the CEO or board of directors and bypassing the IT organization completely. As the profile of the CISO increases, so does the visibility and expectation of the IAM organization.

DEVOPS & DEVSECOPS

The removal of silos/walls between operations and development brings many business advantages, but at the smae time many of the security processes (e.g. segregation of duties, the principle of least privilege) were put in place to protect organizations. As businesses adopt a DevOps model, the need to provide appropriate access across the entire SDLC and incorporation of DevSecOps is a must. IAM services are key to support effective operations of DevOps and is a key component of DevSecOps.



MICROSERVICES

The rapid adoption of cloud technologies, services and design principles, coupled with enterprise service focused dev methodologies, is increasing the enterprise's ability to leverage microservices. When microservices involve integration with APIs, applications and other microservices, it introducescomplexity from an authentication and authorization (IAM) perspective. Because microservices are heavily development focused, they must be able to leverage easily consumable IAM services.

INCREASING IAM COMPLEXITY

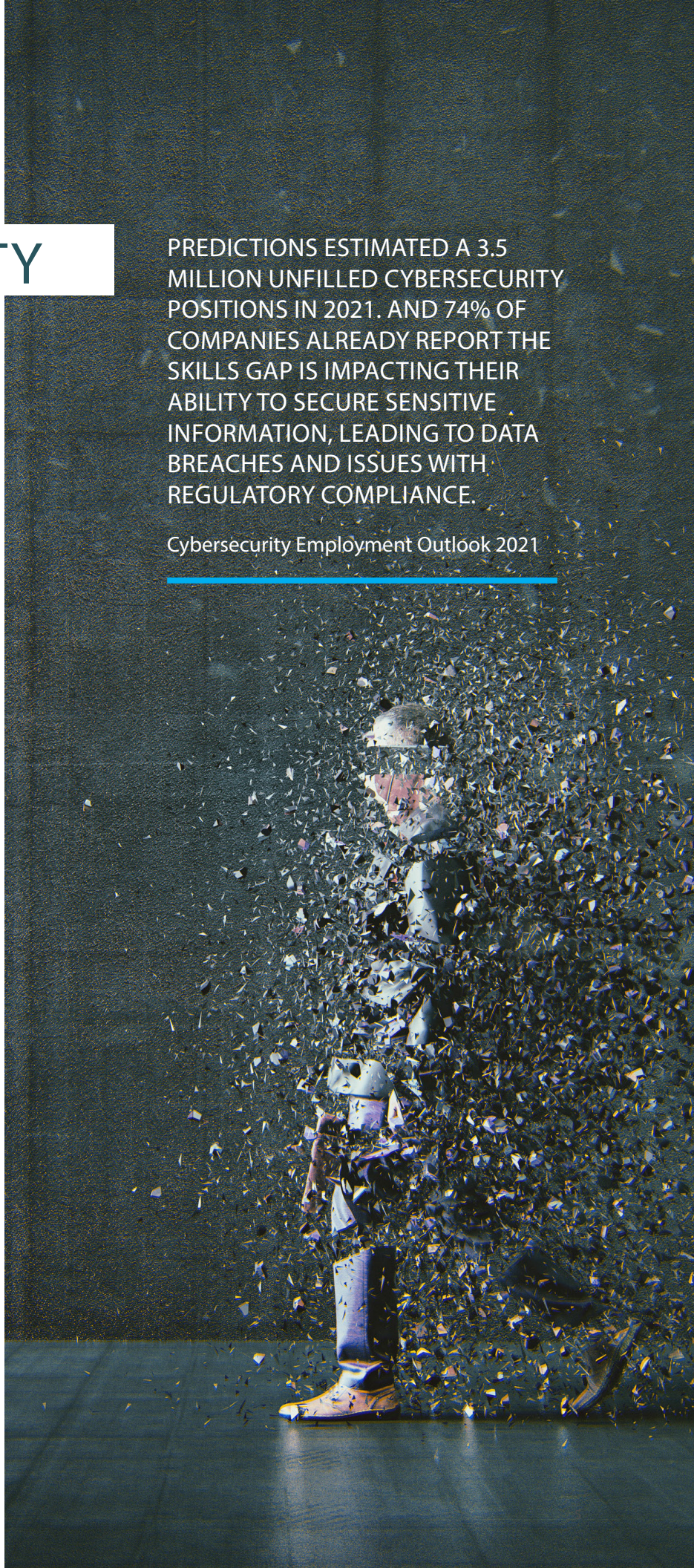
The technology trends enterprises are embracing continue to drive an explosion of new IAM solution categories and vendors, as well as changes to how traditional IAM vendors deliver their services. This evolution is accelerating the demise of the old IAM monolithic platform approach in favor of IAM microservices-oriented solutions. We've already seen significant market movement in the past 18 months leading to a very different IAM environment than years past. Forrester predicted that 2021 would see:

- IAM suites become loosely coupled preintegrated offerings.
- IDaaS becomes a viable alternative for all IAM services and adds identity analytics.
- B2C IAM (CIAM) spawns a new class of customer management services.

This prediction seems largely on-point. Despite market movement, there appears to be little appetite for a single-stack solution is waning in favor of a compilation of best-of-breed technologies purpose-built to tackle specific subsets of IAM functionality or to solve specific use cases.

PREDICTIONS ESTIMATED A 3.5 MILLION UNFILLED CYBERSECURITY POSITIONS IN 2021. AND 74% OF COMPANIES ALREADY REPORT THE SKILLS GAP IS IMPACTING THEIR ABILITY TO SECURE SENSITIVE INFORMATION, LEADING TO DATA BREACHES AND ISSUES WITH REGULATORY COMPLIANCE.

Cybersecurity Employment Outlook 2021



> ORGANIZATIONS LACK THE QUALIFIED RESOURCES AND SKILLS TO PLAN, DEVELOP, ACQUIRE AND IMPLEMENT COMPREHENSIVE IAM SOLUTIONS. AS A RESULT, THEY'RE CONTRACTING PROFESSIONAL SERVICES FIRMS TO PROVIDE THE NECESSARY SUPPORT, PARTICULARLY WHERE MULTIPLE FUNCTIONS NEED TO BE ADDRESSED SIMULTANEOUSLY.
>
> MORE AND MORE, ORGANIZATIONS WILL RELY ON MSSP FIRMS FOR ADVICE, GUIDANCE AND INTEGRATION RECOMMENDATIONS.
>
> 5 Key Predictions for Identity and Access Management and Fraud Detection
> Smarter With Gartner, March 2021

CHOOSE YOUR OWN ADVENTURE

The a la carte IAM vendor concept is appealing for a lot of reasons; however, it carries its own challenges:

- There are hundreds of offerings on the market (with dozens more added each year) to sort through and "short list."
- Even when you've whittled down to a short list, it can be painfully difficult to ascertain how well the vendors will play together -- not just the seamlessness of the integration, but also the complementary and sometimes overlapping nature of the feature sets they bring to the table.
- Every environment is unique. It's difficult to find other enterprises applying the same mix of IAM vendors to an environment similar to yours to decipher how the solution will perform.

It's critical to ensure that vendors will meet not just current functionality requirements, but future extensibility & interoperability needs as well continues to mature.

IAM SOLUTION SPRAWL

Identity sprawl is a reality at nearly every sizeable enterprise. Why?

Many organizations – even smaller businesses grow through mergers & acquisitions. What does this mean to enterprise identity management? It means having to work with multiple heterogeneous user stores — authentication protocols — legacy systems and much more.

IAM spans the entire business and can empower it, but the business needs won't wait for IT. Without a solid IAM base and a centralized service, organizations end up with disconnected decision makers, parallel initiatives and siloed projects.

Bottom line — too many IAM infrastructures are only designed to address short term goals or projects. They cannot extend and soon start to look like a Rube Goldberg machine; creating a maintenance nightmare and limiting the ability to add new features and functionality as the industry continues to mature.

DIY SOLUTIONS LEAVE A LEGACY OF COMPLEXITY

A large financial institution in the USA needed to build a unified access control platform across the company. They had more than 70 teams internally, and each team had developed their own way of controlling access. Some had used a database to store access control rules in their own schemas, while others had just hardcoded them into the application code.

These applications had evolved over many years — and in some teams, no one even knew how things worked — and were hesitant to make even a minor change. There were also teams of people who were very much comfortable with what they had and were reluctant to move out of their comfort zone.

BUSINESS VALUE OF MANAGED SERVICES

Managed service solutions provide a wide range of functional IAM capabilities such as identity lifecycle management, access management, and privileged identity management through dedicated service offerings that can manage support and integration on a 24x7x365 basis.

01

VENDOR SIMPLIFICATION

A high-quality MSP will work with a broad spectrum of vendors and maintain strict vendor-neutrality.

Read more on page 9

02

IT/BUSINESS ALIGNMENT

Identity should ultimately be an "utility." Imagine a world where it is easy to consume a service that allows you to simply identify individuals,..

Read more on page 10

03

MATURE IAM PROGRAM

Less than 20% of enterprise organizations have automated, standardized IAM processes.

Read more on page 11

04

OPTIMIZE INVESTMENT

Despite MSSPs firms' reputations for high hourly rates, engaging with them is often the most economical way to augment an IAM program's capabilities to create.

Read more on page 12

05

STREAMLINE OPERATIONS

With an MSSP, your IT and security organizations are freed up to focus on business initiatives.

Read more on page 13

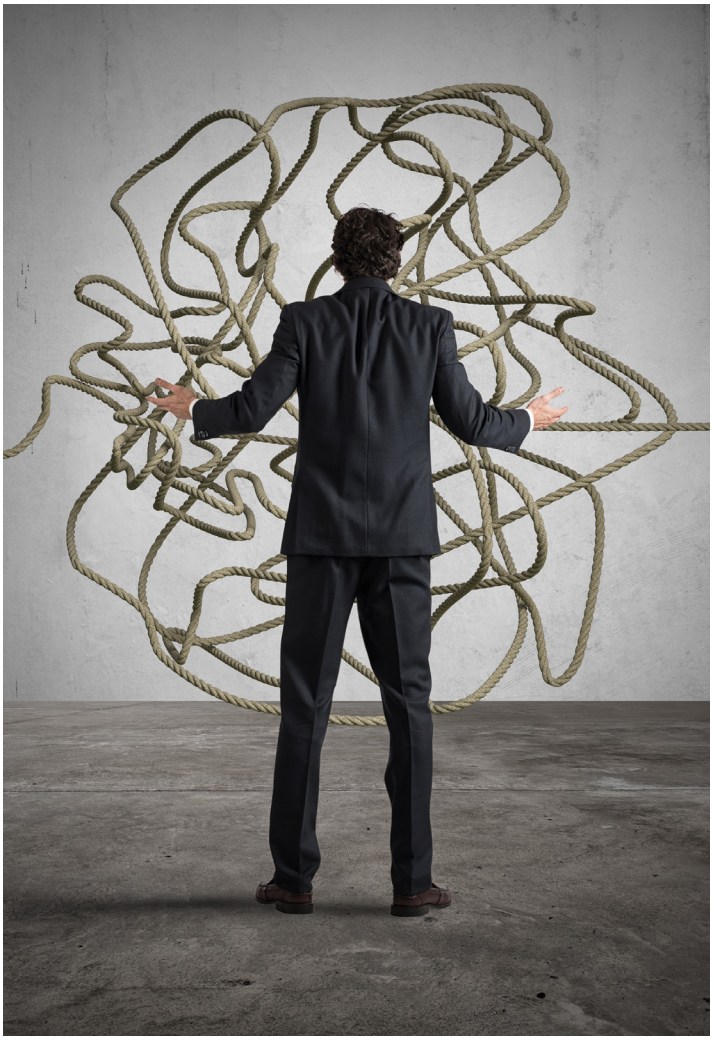
06

EXTEND IAM TEAM

An MSSP brings highly trained, skilled, experienced IAM experts to your corner so you can achieve dynamic, flexible scale.

Read more on page 13

01 VENDOR SIMPLIFICATION



> A high-quality MSSP will work with a broad spectrum of vendors and maintain strict vendor-neutrality.

Partnering with an MSSP can cut through the IAM vendor complexity when you utilize them as a trusted advisor for their broad industry expertise, deep insights into what each vendor brings to the table, and their understanding of emerging trends and technologies.

This can help ensure that you stay abreast of any new functionality that will improve your overall security posture. This becomes increasingly more important as vendors shift to a microservices approach -- how can you stay on top of all the new IAM vendor offerings to ensure that you've got the best possible combination of solutions?

MSSPs will become Increasingly important as IAM vendors shift to a microservices approach. In addition to navigating the complexity of the vendor landscape, MSSPs have deep industry knowledge of:

- What your peers and best-in-class leaders are doing to deliver identity services to their organizations
- What emerging business trends are relevant to your industry and your IAM environment
- New technologies & vendors and how they can or should fit into your IAM arsenal

02 BRIDGE THE IT/BUSINESS DISCONNECT

Identity should ultimately be an "utility." Imagine a world where it is easy to consume a service that allows you to simply identify individuals, applications and things and use them as needed under proper security controls that are privacycentric.

WITH THE RIGHT MSP, IAM BECOMES A BUSINESS ENABLER THAT YOUR ORGANIZATION CAN PLUG INTO AS A FRAMEWORK.

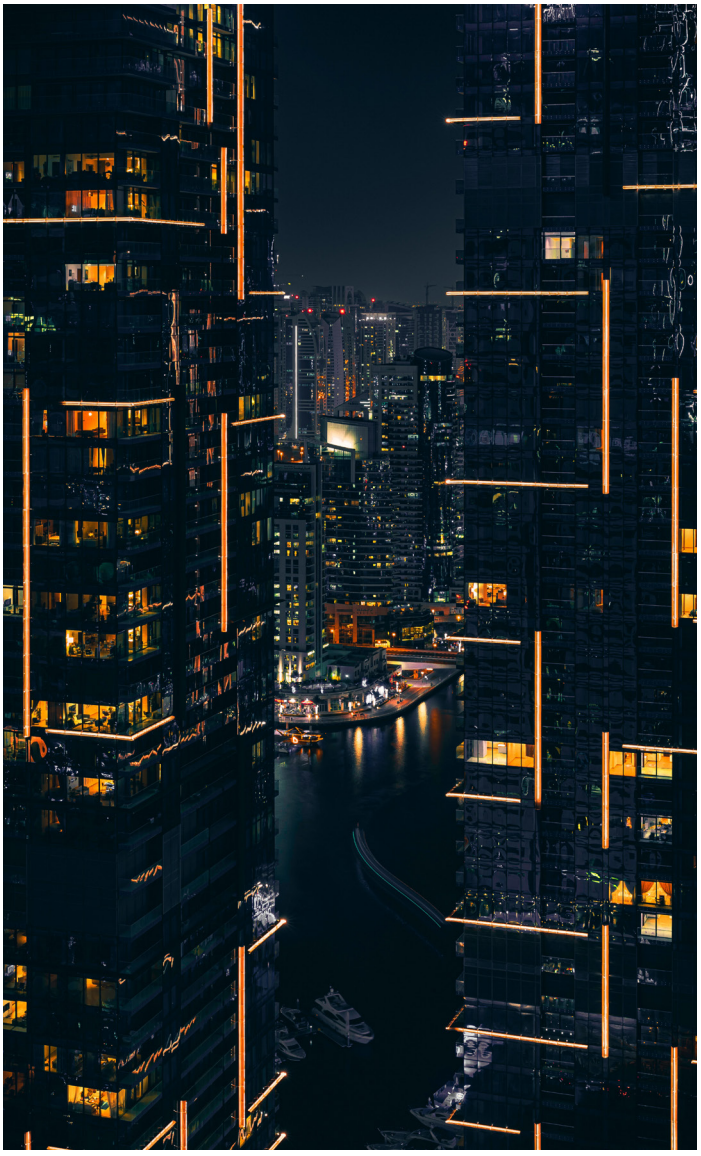
The Future of Identity Management (2018-2023), TechVision, 2018

There are a few critical areas where an MSSP will help bridge the IT and business agendas:

- By delivering advanced IAM services, MSSPs can put IT teams in a position to globally manage identities and access privileges across the business' entire application estate, regardless of the number, complexity or types of applications running in the cloud and on-premises.
- An MSSP is already set up to help the business quickly evaluate the security of existing and planned applications. Should the business move forward with planned applications, with an MSSP, your team is ready to support the business with all the necessary IAM capabilities (SSO, access cert, security modeling, etc.)
- MSSPs are quickly able to translate audit requirements into technical requirements (as any IAM pro will tell you, this is easier said than done.)

03 BENCHMARK & IMPROVE PROGRAM MATURITY

> Less than 20% of enterprise organizations have automated, standardized IAM processes, and just over 5 percent have reached the point at which they have optimized their IAM operations.*



In the thousands of IAM assessments we've performed, a good percentage of enterprises have had no ability to benchmark their performance against their peers and weren't really sure where they should be from a maturity perspective.

Having an MSSP who has a broad range of customers across many industries, and ideally a deep portfolio of your peers, gives you insight into what best-in-class looks like, what's realistic for your organization, and how you can measure your IAM maturation over time.

IMMATURE IAM PROGRAMS ARE LIKELY TO BE INEFFICIENT, INEFFECTIVE AND UNABLE TO DELIVER THEIR FULL BUSINESS VALUE.

Gartner IAM Maturity Scale 2018

04 OPTIMIZE INVESTMENT (MINIMIZE MAINTENANCE SPEND)

Despite MSSPs firms' reputations for high hourly rates, engaging with them is often the most economical way to augment an IAM program's capabilities to create, extend or enhance its services. In fact, there are many industry studies citing operational savings of 50% or more with the right MSSP partner.

With an MSSP, the enterprise is paying for the services being performed only when those services are performed, thus reducing the burden of carrying staff for those purposes. Specific areas of long-term benefit that impact operating expenses include:

- Reduced cost of IT infrastructure
- Staff optimization
- Increased application availability

05 STREAMILINE OPERATIONS & 06 EXTEND YOUR TEAM

With an MSSP, your IT and security organizations are freed up to focus on business initiatives. Staffing IAM is a challenge and the nature of IAM initiatives drives surges in resource requirements that don't always require a large full-time staff.

MSSPs provide critical surge capacity, allowing you to staff for dayto-day operations and leverage outside resources when needed to adjust how the program operates, especially when adding or upgrading capabilities.

Additionally MSSPs can fill geographic gaps by offering services in remote locations where there is no IAM program staff.

An MSSP brings highly trained, skilled, experienced IAM experts to your corner so you can achieve dynamic, flexible scale with the ability to expand and contract as needed without impacting existing full-time employees.

CONCLUSION

A managed services environment for IAM is no longer an outlier. The IAM market continues to evolve at a rapid pace with an increase in cloud-first strategies combined with broad security acceptance of a managed service environment and their ability to secure sensitive information.

These changes are driving a fundamental shift in how organizations view managed services for Identity and Access Management.

As organizations increasingly look to engage a managed services partner for their identity and access management program, understanding what benefits exist within an MSSP/Client relationship, how to achieve those benefits, and how to measure performance are top of mind.

The right managed services partner will be with you for the long haul -- they will help you from initial assessment to developing a strategy, to selecting the right mix of vendor solutions, to implementation & day-to-day management, to benchmarking performance, and back to taking in new business requirements and evolving your program over time.

ASK THE IAM EXPERTS

Company Address
IDMWORKS
2200 Segovia Circle
Coral Gables, FL 33134

Phone & Fax
Sales: (888) 687-0436 ext. 1
Support: (888) 687-0436 ext. 6

Online Info
Email 1: sales@idmworks.com
Website: idmworks.com

IDMWORKS