HERJAVEC GROUP

A Guide to Managed Identity & Access Management

Leveraging the New Digital Perimeter

HERJAVEC GROUP

A Guide to Managed Identity & Access Management

Table of contents

Enterprise Digital Transformation and its Greatest Vulnerability	3
Your Cybersecurity Defense is Only As Strong as Your Identity Program	4
Managed IAM Adoption Drivers	5
The Managed IAM Provider Market	7
Your IAM Provider's Service Offerings	8
Third-Party and Internal Risk Management	9
Taking an Aggregate Approach to IAM	11
Leveraging an Extension of Your In-House Team	11
3 Critical Questions to Ask Your Provider	12
Why Herjavec Group?	13

HERJAVEC GROUP

Addressing Rapid Enterprise Digital Transformation and its Greatest Vulnerability

Remote work and the hybrid work environment have increased the significance of and need for Identity and Access Management (IAM) now more than ever.

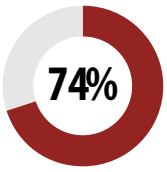
The complexity of digitally transformed enterprise environments, including the diverse set of endpoints/identities and internal and external/third party access, have resulted in increased vulnerabilities and opportunities for threat actors.

Human beings, devices and applications all have identities. It is imperative that your enterprise has a way of detecting anomalous behavior across all three categories. Remote and hybrid work "at scale" have certainly complicated this effort as behavior patterns have shifted significantly because of the pandemic. People are logging on at all hours of the day, their kids are using their corporate devices, personal emails are being accessed and the list goes on. The opportunities for hackers to take advantage of these new vulnerabilities are endless.

On top of internal identities and privileged access, organizations need to develop third-party risk mitigation as well. Identity Governance and Privileged Access Management are essential in third-party risk mitigation.

The fact is, compromised identities can be extremely valuable for cyber adversaries. It can be used to break into a network, move laterally within the network, and facilitate all kinds of damaging activity.

In a recent study, analysts found that 74% of surveyed IT professionals say they are only somewhat confident or not confident at all in their enterprise's ability to effectively manage and secure both human and non-human identities.



Your Cybersecurity Defense is Only As Strong as Your Identity Program

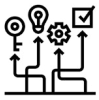
Identifying all identities and managing their individual access is necessary but no small feat!

You won't be able to spot truly anomalous behavior across users, devices and applications without robust programs in Identity Governance, Access Control (including authentication) and Privileged Access Management.

IAM is the new digital perimeter

The old perimeter was made up of legacy methods and technologies that relied on work environments that were largely on-premise and within a secured, more easily controllable network.

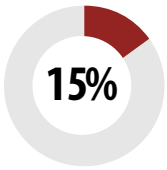
When teams were working in the corporate office, it was easy to identify users and their devices as they were all using one secured network and keeping predictable behavior patterns.



Today, the perimeter we once knew is gone – it is now formed by your enterprise IAM program as a result of remote and hybrid workforces. While the core basic approaches to IAM governance haven't changed, the importance of prioritizing it in enterprise cybersecurity has skyrocketed.

IAM provides key defensive measures against attempted attacks and risk mitigating tactics to lessen damage if an intruder is successful in breaching your network.

In a 2020 survey, when asked what workshops were prioritized to assess internal cybersecurity capabilities, Identity Strategy Development placed last with only 15% of individuals surveyed having assessed their IAM strategy in the past 12 months.



HERJAVEC GROUP

Managed IAM Adoption Drivers: Simplifying a Complex Security Challenge

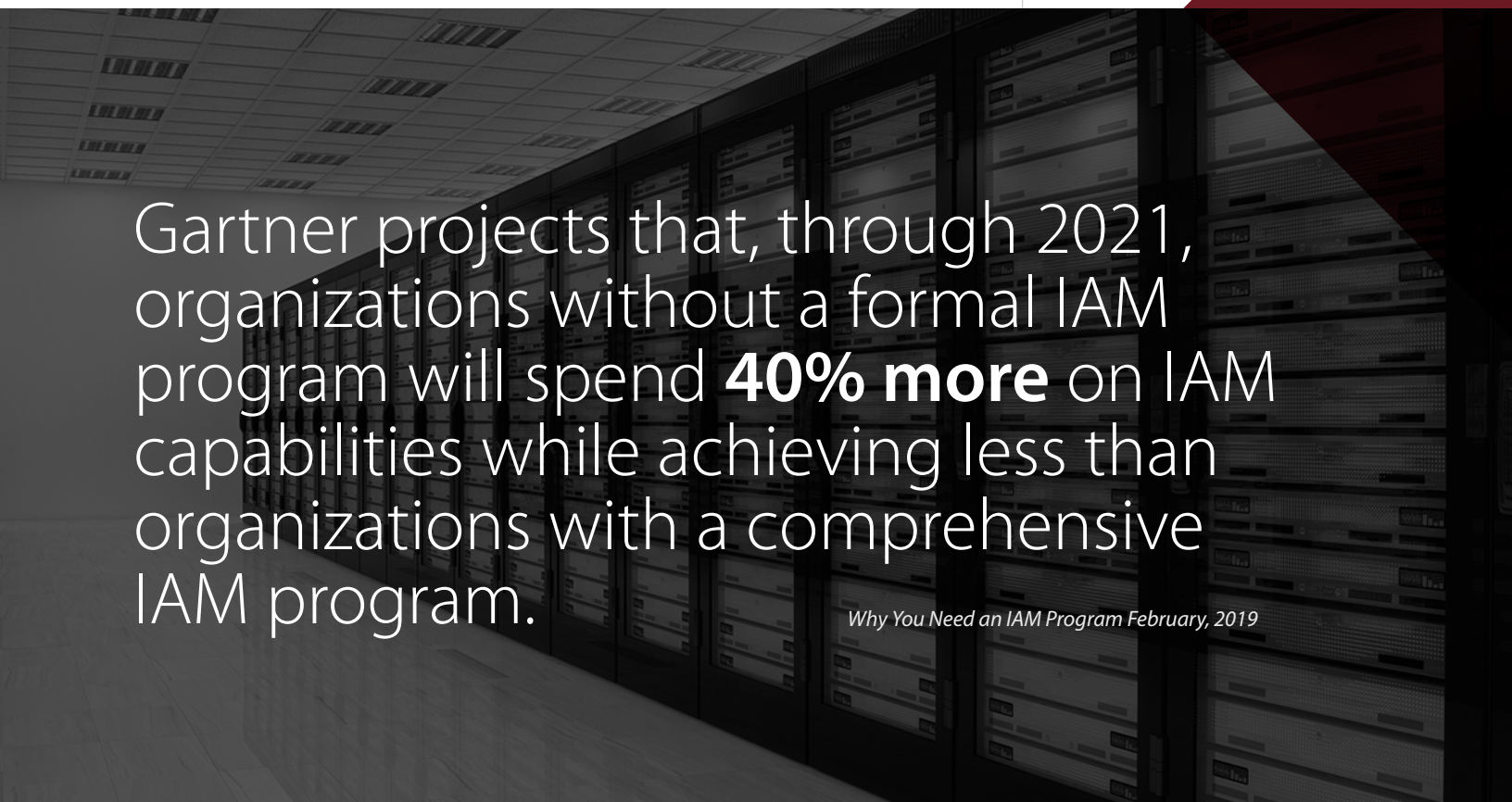
One of the most common questions infosec professionals have received since the pandemic began is: "how do we keep our data and employees secure now that we have deployed cloud operations?"

The answer is simple: Focus on identity – who is accessing your environment, at what time, from where, and for what reason? While the answer may be simple, the solution is not easy.

An effective IAM program is not a "one-and-done" product investment – it is an element of organizational change that will require ongoing activities and enhancements to continue to be successful. This perspective must be paramount when strategizing and implementing your IAM Program. Now think about your in-house security team. Do you have the capacity to build and deploy a comprehensive IAM program?

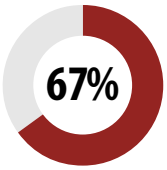
Recently, there has been a concerning pattern in IAM solution implementation. Analysts have found that many enterprises severely underestimate the scale and impact of change that results from implementing a comprehensive IAM program. This has led to unrealistic time frames, lack of proper strategy and planning, and often, a failure to plan and govern interdependent IAM initiatives under a coherent government structure.

> **Providing effective IAM services in the face of competing challenges demands multiple, often interdependent changes.**
>
> **Gartner, Kevin Kampman**



Drivers for Managed IAM include the need for:

- 24/7 Identity platform health monitoring without increasing in-house security staff
- Gaining visibility and control of user data and access permissions
- Quickly detecting risks and amending access entitlement issues associated with privileged users
- Automating the user provisioning process based on groups, policies, and approval workflows
- Accelerating compliance efforts with unified top-down governance processes for all users
- Receiving predictable OPEX and improved ROI on your IAM software
- Gaining access to on-demand expertise from certified IAM experts
- Enhanced third-party risk management



In a 2020 survey, 67% of surveyed individuals responded as not utilizing Managed IAM to continuously manage and assess identity governance and technical controls.

Consider your current approach to IAM. A strong IAM strategy should include:

- Prioritized identity proofing
- Strong, proactive third-party risk management skills and strategy
- Resources and education for employees to mitigate the risks of remote and hybrid workforces
- A robust IAM Operating Model with clearly defined stakeholders, accountable teams, departments, reporting structure, and approach to communications
- An IAM vision and strategy that is aligned with key organisational goals
- An architecture that has documented processes and sustainable technology that is easy to support in your specific industry

Sifting Through a Dynamic and Crowded Managed IAM Provider Market

As the IAM market is both mature and crowded, many providers overlap in core service offerings. When looking for the right Managed IAM Provider it's important to understand what to look for that will go above and beyond the basics.

The right Managed IAM Program will not only mitigate cyber risk, but also increase cybersecurity ROI and enable business operations.

The key pillars of Identity include:

Identity Governance & Administration (IGA)

IGA tools manage digital identity and access rights across multiple systems by aggregating and correlating disparate identity and access rights data that is distributed throughout the IT landscape to enhance control over user access.

Privileged Access Management (PAM)

PAM tools provide secure, privileged access to critical assets to only the intended users, and meet compliance requirements by securing, managing, and monitoring privileged accounts and the related access.

User Authentication

User authentication, including Single Sign On (SSO) and Multi Factor Authentication (MFA), is the real-time corroboration (with an implied or notional confidence level) of a person's claim to an identity previously established to enable access to an electronic or digital asset.

HERJAVEC GROUP

Your IAM Provider's Service Offerings Should Include:

Service Delivery Management

- Assigned trained personnel to maintain service delivery and service support.

Service Delivery and Performance Review and Reporting

- Facilitated service delivery and performance reviews

Facilitated service reporting of key metric measures including:

- Service Health
- Service Quality
- Service State
- Service Workplan and Financials
- Impact of Incidents

Architecture and Solution Review

- Facilitated architecture and solutions reviews to evaluate and make recommendations to the customer around potential service gaps.

Incident Management

- Investigation and verification of an incident's impact and severity.
- Initiation of change management procedures to implement product fixes or any other change required to restore to normal service.
- Detailed documentation of findings and steps taken to restore service to normal.

Problem Management

- Root cause analysis of incidents to reveal deficiencies within the solution.
- Review of support procedures for opportunities to improve event detection and speed service recovery.
- Initiation of change management to implement corrections to the solution or components based on the findings of the root cause analysis.

Change Management

- Provide subject matter expertise to evaluate proposed changes to the IAM program and identify potential risk of impact to mitigate risk service.

Achieving Resilient Third-Party and Internal Risk Management with Privileged Access Management

Privileged Access Management (PAM) utilizes tools and expertise to analyze the behavior of all identities accessing your organization's network and detect any unusual conduct. This includes granting access to, monitoring and securing current end-users as well as removing access and securing against former employees, vendors, or collaborators who should no longer have privileged access.

Key Indicators of Privileged Access Management Need

PAM is a tedious but essential task that is often overlooked. There are many benefits to implementing PAM under a well-rounded managed IAM program. This multi-faceted component addresses many of the challenges organizations face when dealing with privileged access.

PROBLEM	SOLUTION
Lack of policy and standard that define requirements for protecting and managing privileged accounts	Customized roadmap and strategy plans, standards, RACI chart, and prioritization/risk models.
Need for assistance with upgrading, installing, or implementing health checks of PAM software and platforms.	Expert guidance with design, architecture, review, and deployment of PAM tools.
Penetration Test and audit findings that indicate a compromised privileged account, 'pass the hash' vulnerability, or failure to meet PAM-related controls.	Set strategy and support deploying solutions to remediate findings.
Inability to manage prigileged credentials used in the DevOps pipeline.	Support securing privileged credentials for the DevOps pipeline using PAM tools to remove hard-coded credentials and authenticate applications using granular access controls.
Improper storage of credentials using high risk processes run by RPA bots using credentials managed by RPA platforms.	Expert support for enterprise IT and business administrators to define scope of privileged access and accounts that should be managed in a PAM tool platform.
Inability or lack of formal process to rotate service accounts or other application/system credentials.	Access to experts with experience in a variety of workflows to manage application credentials.
Difficulty securing and managing third-party access to internal systems	Managed PAM tools leveraged to manage remote vendors by providing just-in-time privileges using multi-factor authentication.

An effective PAM program will allow you to:

Identify unusual end-user behavior that could signify malicious activity

Give necessary privileged access to internal and external parties

Systematically de-provision those who don't require privileged access

Third-Party Risk Management

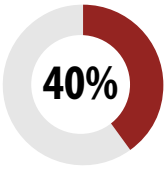
Negligent PAM has led to some of the worst cyber-breaches in the past decade. Think back to the 2019 Capital One breach. A former employee of a third-party vendor was able to hack in and gain access to 100 million credit card applications and accounts. To this day, it remains one of the biggest data breaches in history.

Develop a process starting with your Legal and Compliance teams to ensure the right privileged access is given and only for the necessary amount of time. The process should include a thorough assessment of all potential third-party vendor cybersecurity. When engaging a third party, ask questions and look for indicators of best cybersecurity practices that align with yours. Streamlining this due diligence frees your security team to focus on critical risks.

ASK YOURSELF

- **How is my enterprise enforcing its password policy for privileged accounts?**
- **Is my organization protecting RPA bot credentials for high-risk processes?**
- **Does my enterprise have visibility into how privileged access is being used?**
- **How manual is the request/approval process of accessing privileged credentials?**
- **Does my organization have the ability to detect and respond to threats against privileged credentials?**
- **Is my enterprise protecting credentials used in the DevOps pipeline?**
- **Does my enterprise have any password management or vaulting solutions in place today?**
- **How is my organization addressing endpoint threats like malware/ransomware and local admin credential theft?**
- **How is my organization managing service accounts today?**

Gartner predicts that by 2023, 40% of IAM application convergence will primarily be driven by MSSPs that focus on delivery of best-of-breed solutions in an integrated approach, shifting influence from product vendors to service partners.



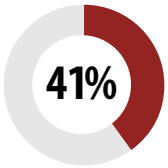
Taking an Aggregate Approach to IAM

With the paradigm shift resulting from the pandemic, IAM needs have evolved and increased – IAM providers have had to keep up. Today, taking an integrated approach to IAM and cybersecurity is key to gaining comprehensive visibility and protection. Engaging a comprehensive security services provider that offers Managed IAM along with all other managed cybersecurity services often results in a more streamlined, holistic, and user-friendly experience. Along with this - Identity and Access Management data is a rich source of critical information that can enhance other cybersecurity infrastructure including SIEM and SOAR solutions.

Benefits of integrating your IAM strategy with your overarching managed cybersecurity program:

- Goals and objectives align with business needs
- Required resources are fully understood and managed by all necessary parties
- Efficient use of budget - rework and duplication of effort is minimized
- More comprehensive and proactive cybersecurity coverage

According to a recent study, 41% of surveyed enterprises identified "lack of skilled staff" as a key challenge when managing their organization's access and identity.



Leveraging an Extension of Your In-House Team

One of the biggest challenges many enterprises face today is the cybersecurity skills shortage. Engaging an outsourced provider can be an ideal solution – but not all providers are the same. A good third-party cybersecurity provider shouldn't operate like an external team. For full security coverage and streamlined operations, your IAM provider should act as an extension of your in-house team by:

- **Gaining a thorough understanding of your cybersecurity and business objectives during the onboarding stages.**
- **Developing an IAM program that will provide comprehensive coverage while simultaneously enabling your business.**
- **Assessing all current IAM and cybersecurity programs and technologies already in place, providing any solutions for identified gaps, eliminating unnecessary components, and optimizing existing solutions.**
- **Including all necessary stakeholders in the strategizing, development, and implementation of the IAM program to ensure an integrated and streamlined approach.**
- **Assigning personal to maintain service delivery and support ensuring constant, open communication and accessibility.**
- **Regular reporting to ensure all necessary parties are aware of performance, required adjustments, and key metrics.**

HERJAVEC GROUP

Assess Potential Managed IAM Providers with These 3 Critical Questions:

What is your approach to managing an enterprise IAM Platform?

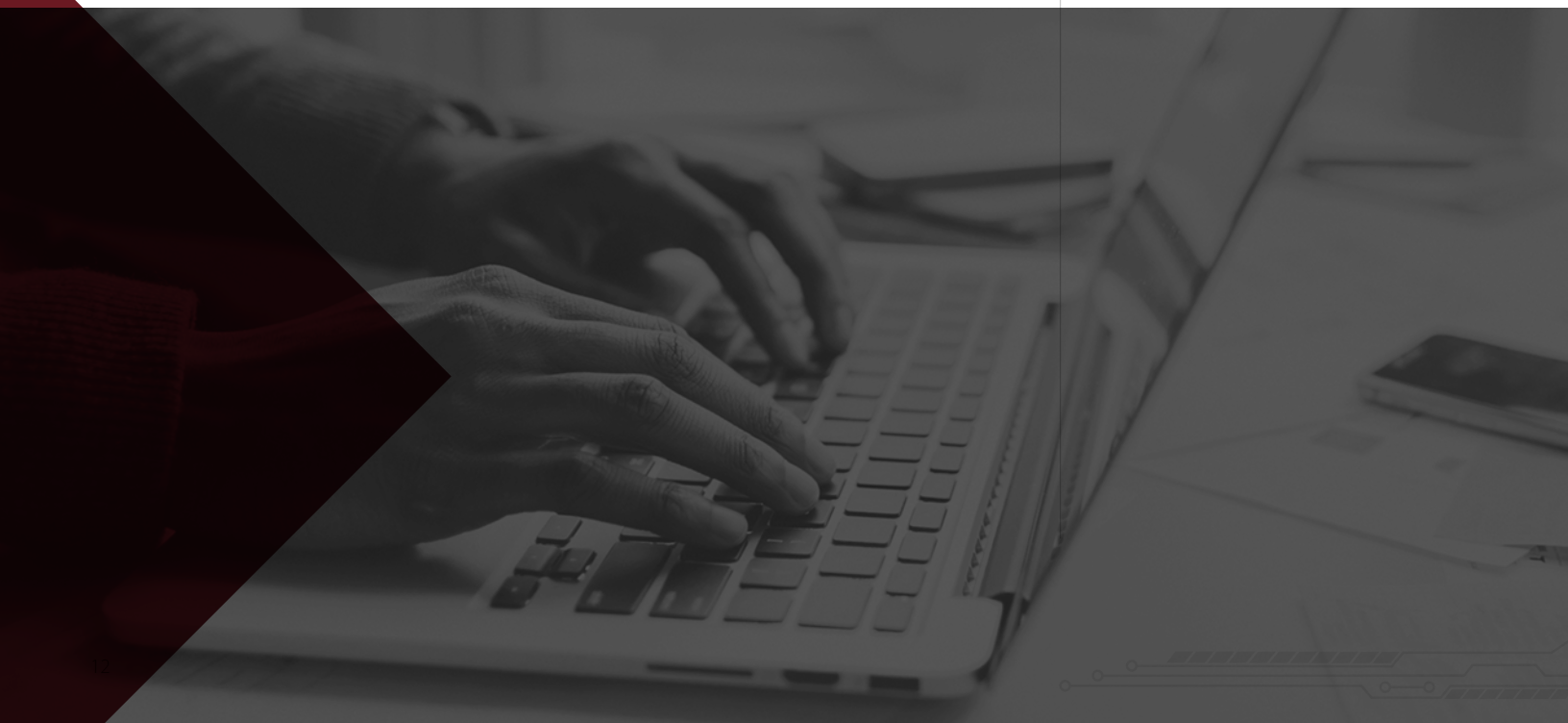
Your ideal provider should provide 24/7 proactive monitoring for business-as-usual and brake-fix operations, ongoing capacity planning, trend management, and scheduled reporting, and continuous improvement through regular health check and architecture reviews.

Do you provide comprehensive expert solution support?

Review the potential IAM provider's team certifications and expertise to ensure they can provide all technical solution support you require. Providers should have the capacity to manage vendor technical support, contract maintenance, product enhancement requests, and corrective actions. They should also perform regular quality assurance checks for enhancements and updates.

What is your process for ongoing maintenance?

Over and beyond the development and implementation of your Managed IAM Program, your provider should define and execute their patch management strategy, ensure the solution they develop is continuously secure and kept within vendor support limits, and analyze and plan for incoming solution upgrades.



Why Herjavec Group?

Herjavec Group's Managed Security Services Practice defends global, enterprise-level organizations from increasingly sophisticated, targeted cybercrime threats. Our industry-recognized HG SOC Operations take on the day-to-day defense of your infrastructure by monitoring your network, systems, and data, 24/7/365. With HG MDR and our supporting HG Managed Security Services, we deliver an integrated, measurable, threat-centric, holistic service.

"Once again Herjavec Group has exceeded our expectations and brought the best possible service. My phone is inundated with cybersecurity salespeople selling services. From my jaded experience very, very few people deliver. Herjavec Group does.

- CISO, Healthcare & HG Identity Services Customer

Herjavec Group's Identity & Access Management team leverages our award-winning service offerings to transform your organization's access requirements into an information advantage at any stage in IAM maturity. Whether your enterprise requires IAM Advisory and Professional Services or IAM Managed Services, our team is here to help you protect your corporate data and information assets and safeguard your business's reputation, legal responsibilities, and financial wellbeing.

We provide comprehensive Managed Services for Identity & Access Management (IAM). Our Managed Identity Services include IAM expert solution operations for both business and technical aspects of IAM infrastructure and policy management.

Recognized Industry-Wide

MARKET LEADER IN MSS

CDM CYBER DEFENSE MAGAZINE GLOBAL INFOSEC AWARDS

4 ON THE

MSSP Alert TOP 250 MSSPs

SECURITY SERVICES LEADER

IDC Analyze the Future

MARKET LEADER IN IAM

CDM CYBER DEFENSE MAGAZINE GLOBAL INFOSEC AWARDS

MOST INNOVATIVE SECURITY COMPANY OF THE YEAR

CDM CYBER DEFENSE MAGAZINE GLOBAL INFOSEC AWARDS

F1™

HERJAVEC GROUP

Official Cyber Security Services Provider of Formula 1®

HERJAVEC GROUP

Robert Herjavec founded Herjavec Group in 2003 to provide cybersecurity products and services to enterprise organizations. We have been recognized as one of the world's most innovative cybersecurity operations leaders, and excel in complex, multi-technology environments. We have expertise in comprehensive security services, including Advisory Services, Technology Architecture & Implementation, Identity & Access Management, Managed Security Services, Threat Hunting & Management, Digital Forensics and Incident Response. Herjavec Group has offices and Security Operations Centers across the United States, United Kingdom, Canada and India.
For more information, visit HerjavecGroup.com or contact us at info@herjavecgroup.com.