Gartner Peer Insights “Lessons Learned”: Implementing Access Management Solutions

Gartner®

Gartner Peer Insights “Lessons Learned”: Implementing Access Management Solutions

PEERS Published 5 May 2021 - ID G00750486 - 9 min read

By Analysts Peer Contributors

Initiatives: Identity and Access Management and Fraud Detection

This content, which provides opinions and points of view expressed by users, does not represent the views of Gartner; Gartner neither endorses it nor makes any warranties about its accuracy or completeness.

Access management provides secure access to applications for multiple use cases through adaptive access control, centralized authentication and cloud applications/services. Security and risk management leaders can learn from the experiences shared by peers on Gartner Peer Insights.

Overview

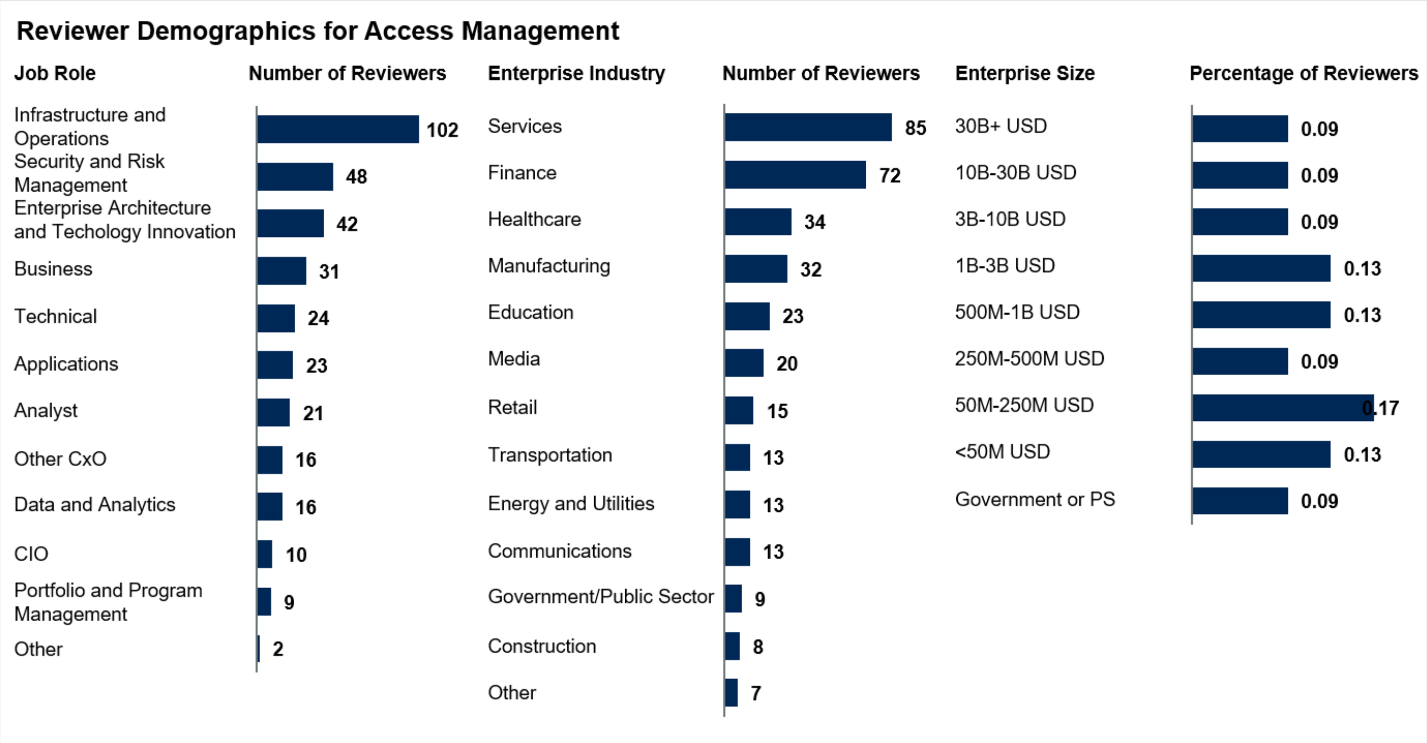
Gartner Peer Insights is a free peer review and ratings platform designed for enterprise software and services decision makers. Reviews go through a strict validation and moderation process to ensure they are authentic.

We analyzed 344 Peer Insights reviews to identify lessons learned implementing access management solutions. This report focuses on the responses to the questions: **“If you could start over, what would your organization do differently?”** and **“What one piece of advice would you give other prospective customers?”** To browse all reviews, see the full list of Access Management reviews on Peer Insights.

Peer Lessons Learned

This “Peer Lessons Learned” summarizes clients’ firsthand experiences with implementing access management solutions. The peer advice results both from successful implementation of projects and learnings based on what went wrong. This peer perspective, along with the individual detailed reviews, is complementary to expert research and provides a holistic view to the implementation process. Reviewers who submitted their lessons learned represent a cross-section of small- to midsize and large organizations. See Figure 1 for demographic details.

Figure 1: Reviewer Demographics



n = 344

Source: Reviews submitted to Gartner Peer Insights between April 2020 – April 2021,
ID: 750486

Below are some key lessons learned and most cited recommendations by Peer Insights reviewers to help security and risk management (SRM) leaders in the implementation process of their access management solution.

Lesson 1: Identify Your Business Goals, Requirements and Use Cases for an Access Management Solution

Peer reviewers recommend that SRM leaders should identify their business requirements, including architectural requirements, and use cases for smooth SaaS implementation. The peers stress on the importance of establishing a goal and clear set of requirements at the start to streamline the tool selection and implementation process.

A peer reviewer suggests:

> Understand how identity and access management takes place in your environment, and then find a solution that fits into all your existing solutions, to make an easy integration and transition to the end users without disruption.
>
> — *Technical Professional, Service Sector*

With a focus on leveraging access management solutions, a peer reviewer says:

> Have a good understanding of your use cases to start and look into how access management solutions can be leveraged throughout your strategic plan. Such solutions can grow and scale very nicely with your organization.
>
> — *Security and Risk Management Professional, Energy and Utility Sector*

Another peer reviewer suggests:

> Set a clear goal of what you want to accomplish and understand your business processes. This enables you to select product features accordingly and provide insight into the cost of implementation.
>
> — *Infrastructure and Operations Professional, Finance Sector*

Peer recommendations include:

- Begin with a business-centric approach rather than focusing on technology first to ensure better business involvement from the start of the process.
- List your requirements to ensure that the solution does not focus on just one aspect but fulfills multiple business needs.
- Establish an understanding of your business size, user base and existing applications.

Recommended reading:

Buyer's Guide for Access Management

Lesson 2: Compare Multiple Vendors Against Your Business Needs and Feature Requirements

Peer reviewers suggest that SRM leaders should conduct a thorough research on multiple vendors to make an informed decision. They suggest choosing a solution after comparing vendor capabilities against their requirements, including multifactor authentication (MFA), hybrid solutions and cloud integration. Peers also advise to take time for this process while ensuring that vendors have proper documentation and foresight to adapt to changes.

A peer reviewer recommends:

> **Talk with the vendor about all your initiatives. Also inquire from them if you missed any initiatives.Then create a matrix of what you need, and which part of the vendor's product will fulfill it. Take an informed decision based on the matrix.**
>
> — *Security and Risk Management Professional, Government or Public Sector*

A peer reviewer points out the importance of comparing features during vendor evaluation:

> **Our organization should have explored a breadth of other features that are available with similar products in the market. Would like to see the same or different product which simplifies the process of connecting to the workplace even better. For example — generation of quick response codes and ability to scan it through mobile phones would be a great feature.**
>
> — *Business Professional, Manufacturing Sector*

Another peer reviewer suggests:

> **Make a list of requirements that you need from MFA product and assess vendors based on those requirements. One that often catches people out is the requirement for a hardware-based one-time password (OTP) token. These come included with some of the packages, but many other vendors include it as an additional cost.**
>
> — *Enterprise Architecture and Technology Innovation Professional, Service Sector*

Peer recommendations include:

- Survey the available options and don't be afraid to adopt a hybrid solution of both cloud and on-premises. Search for a more fully stacked service offering that integrates easily with native, cybersecurity, analytics, reporting, governance and so forth.
- Discuss possible enhancements, including customizations, with the vendor if the use case requires it.
- Conduct a functionality review to select and evaluate a vendor. This will also ensure a pricing comparison among vendors.
- Allocate time for vendor selection. Spend time with vendors to assess their actions and understand if the sales pitch matches the execution consistently.
- Select a vendor with proper documentation, tools and foresight to see where the market is headed while continuing to provide valuable solutions.

Recommended reading:

Critical Capabilities for Access Management

Lesson 3: Map Points of Integration With Existing Architecture and Plan Migration Strategies

Peer reviewers recommend that SRM leaders should consider integration of the software with the existing organizational architecture. Peers advise determining the integration requirements for all applications and fully document them before starting out. They also suggest looking at cloud models while migrating.

A peer reviewer suggests:

> Moving access management to the cloud can be a tough sell for companies that require extreme customizability and are adverse towards or paranoid about cloud technology. If doing it again we may have looked at shifting directly to a cloud-only model. As with anything security related, integrating performance measurements into your strategy will go a long way in assuring return on investment.
>
> — *Infrastructure and Operations Professional, Service Sector*

Another peer reviewer says:

> Take the time to sit down and learn how to use the software to solve your company's problems. Take time to learn not only authentication but also some of the application integrations that may be possible by using such solutions. The time spent in this meeting and even understanding how to integrate with such a solution will pay dividends down the road.
>
> — *Infrastructure and Operations Professional, Healthcare Sector*

Peer recommendations include:

- Consider moving the existing access management architecture to a cloud platform. Ensure all devices are updated for smooth migration.
- Modify and target applications in use to simplify the migration process for your organization.
- Conduct a self-assessment and dependency mapping of your application integration points prior to starting your implementation.

Recommended reading:

IAM Leaders’ Guide to Access Management

Lesson 4: Invest Time in Training; Engage End Users for Faster Adoption

As access management solutions manage user access to applications, peer reviewers advise SRM leaders to conduct training sessions with users for smooth deployment. A cross section of peers recommends ensuring the user community understands the need of the product to reduce any backlash.

A peer reviewer recommends:

> **Our implementation was successful through constant communication to users, and I would recommend that you lay solid groundwork with your users to avoid growing pains during implementation.**
>
> — *Security and Risk Management Professional, Healthcare Sector*

Another peer reviewer recommends early training and testing the tool’s functionalities:

> **Try and get as much training before you start designing the system. Start by building a laboratory environment where users can test the interface, see the functionalities and discover features. This will allow you to better plan the deployment.**
>
> — *Enterprise Architecture and Technology Innovation Professional, Healthcare Sector*

Another peer reviewer says:

> **My advice to prospective customers is to discuss overall training as part of a new engagement. While access management products are relatively straightforward to implement if you have a good background in single sign-on, an in-depth training will open up new opportunities to leverage the products beyond their obvious use cases.**
>
> — *Security and Risk Management Professional, Communications Sector*

Peer recommendations include:

- Train a group of experts to ensure backup options. Offer certification training for the product to speed up deployment.
- Involve all the concerned parties form the beginning of the project to avoid any resistance at a later stage of the project.
- Ensure that you have buy-in from the wider business, allowing you to take advantage of the self-enrollment process. This helps sell the end users on the ease of use of the product, and saves time and cost.

Recommended reading:

Identity and Access Management for Technical Professionals Primer for 2021

Lesson 5: Create a Dedicated Team to Build and Deploy Your Implementation Plan in a Phased Manner

A cross section of peers advises that SRM leaders deploy a dedicated team who has a clear understanding of the organization's policies and include internal experts for an efficient implementation process. They suggest that implementation of the product and its solutions should be done in a phased manner for faster enrollment.

A peer reviewer recommends a phased implementation process:

> **If your user base is new to two-factor authentication, take a risk-prioritized phased approach to implementation. Start with your users that work with highest risk data assets and work outwards until your entire organization is using two-factor authentication. We started with those that work with sensitive data as our first phase, then came to all employees.**
>
> — *Infrastructure and Operations Professional, Education Sector*

Describing their implementation strategy, a peer reviewer recommends against using external experts:

> I would not use a vendor to implement the code. That gave me a disadvantage when trying to figure out how things were supposed to work after things were in production. It would have been better to work up front so that I could support the technology better after the service team was released from the contract.
>
> *— Business Professional, Media Sector*

Peer recommendations include:

- Assign a dedicated internal team for implementation. Ensure a development expert is also a part of the implementation team.
- Use the out-of-the-box features and refrain from using too many custom implementations. Additionally, make use of the cloud setup.
- Initiate implementation in smaller groups and allow self-enrollment for users. It will ensure faster buy-in at scale and give support services time to familiarize themselves with the product.
- Review the number of features being implemented for your customer base. Consider implementing features according to need-based clusters.

Recommended reading:

2021 Planning Guide for Identity and Access Management

Methodology

Of the Peer Insights survey data considered for this market, only those responses meeting the following criteria were included in this synthesis:

● Reviews less than 12 months old.

● Responses that pertain to the project experience and are not tied to the capabilities of a vendor.

● Reviews were clustered into the top-five most-referenced categories (lessons learned) and then listed in order of relevant phases in the project life cycle.

The results of this synthesis are representative of the respondent base and not necessarily the market as a whole.

“The data used in this report is drawn from reviews on Peer Insights, a crowdsourced enterprise review platform that relies on dynamic data. Key to maintaining the integrity of the site is our ongoing moderation and validation of those reviews. Reviews are examined before publishing to the site and periodically, post-publishing. Due to the dynamic nature of the data, the external Peer Insights site will always have the most updated view of the data in this report.”

Document Revision History

Gartner Peer Insights “Lessons Learned”: Implementing Access Management Solutions - 18 March 2020

Recommended by the Author

Critical Capabilities for Access Management

Magic Quadrant for Access Management

2021 Planning Guide for Identity and Access Management

Technology Insight for Customer Identity and Access Management

IT Score for Identity and Access Management

Identity and Access Management for Technical Professionals Primer for 2021

Follow these best practices to create a resilient, scalable and agile cybersecurity strategy.

The IT Roadmap for Cybersecurity

About Gartner

Gartner is the world's leading research and advisory company and a member of the S&P 500. We equip business leaders with indispensable insights, advice and tools to achieve their mission-critical priorities today and build the successful organizations of tomorrow.

Our unmatched combination of expert-led, practitioner-sourced and data-driven research steers clients toward the right decisions on the issues that matter most. We are a trusted advisor and an objective resource for more than 14,000 enterprises in more than 100 countries — across all major functions, in every industry and enterprise size.

To learn more about how we help decision makers fuel the future of business, visit gartner.com.

Become a Client

Get access to this level of insight all year long — plus contextualized support for your strategic priorities — by becoming a client.

gartner.com/en/become-a-client

U.S.: 1 800 213 4848

International: +44 (0) 3331 306 809

Gartner®