AXIOMATICS

REPORT

The State of Authorization 2022

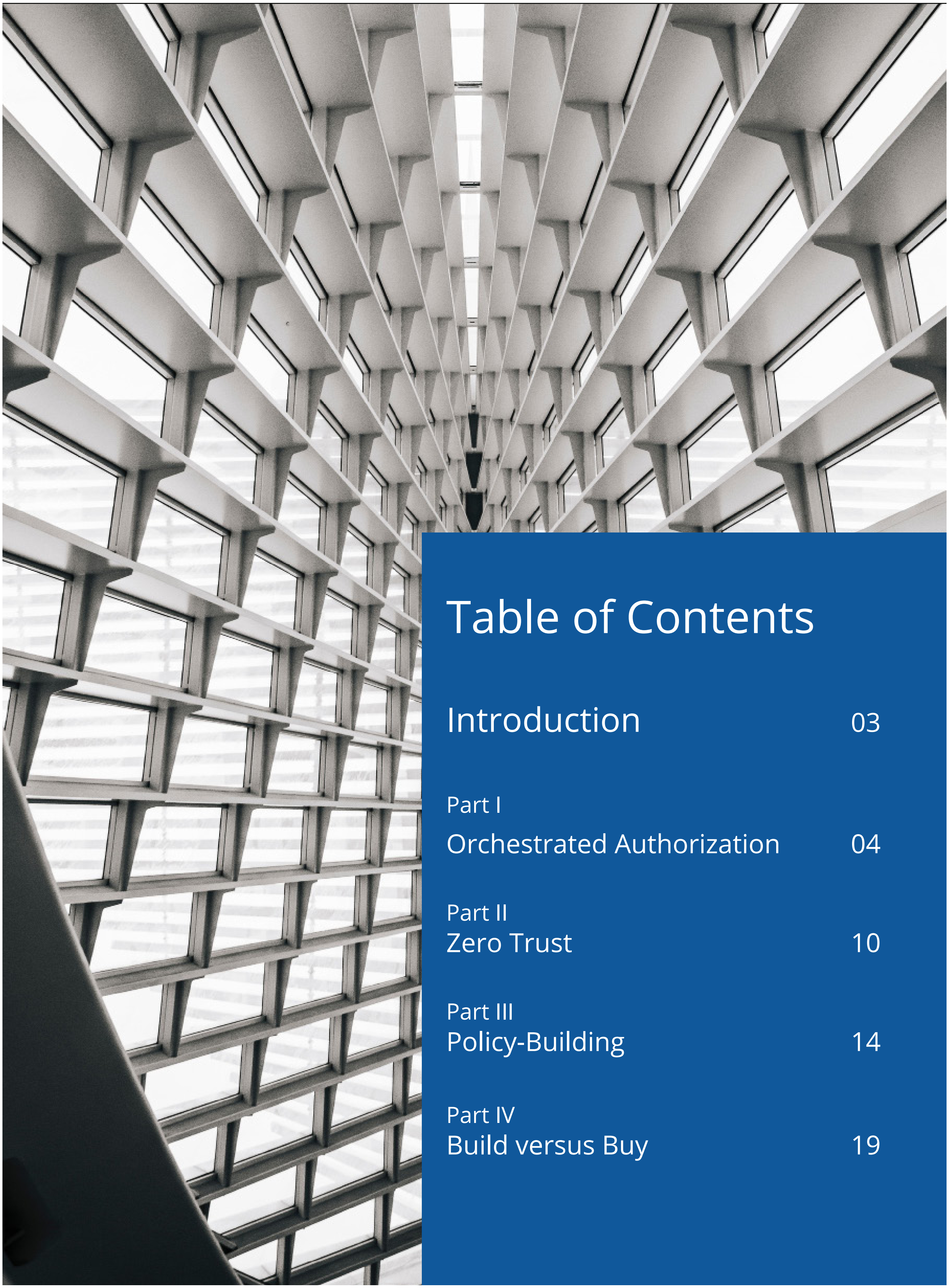


Table of Contents

Authorization is not a new concept. Organizations have been implementing authorization and policy controls across applications and data sources since the dawn of application development. So what has changed that brings authorization to the forefront of a CISOs toolset in solving the ongoing challenge of access control and data protection? And where does the authorization market stand in 2022?

There are three fundamental shifts that have emerged in the last two or three years: the pace of innovation to move to new development architectures, the maturity of Zero Trust and the evolution of accountability and ownership for authorization in an organization. While these three are separate conditions, when combined they shape the new era driving the adoption of authorization.

The pace of innovation has dramatically accelerated, and we see organizations adopting new development architectures to speed the rate of creating and deploying applications faster than ever before. While a few years ago it would have taken months or even years to deploy an application, most organizations demand applications come to market within weeks. The creates a growing dependence on cloud-based solutions, which can mean more risk as well as access control challenges in the process.

At the same time, there is a natural evolution of Zero Trust as it matures from a theoretical reference architecture to a board-level mandate which has active projects and budget dollars attached. This higher visibility brings with it a shift in accountability throughout the organization in terms of who is responsible for the authorization program and policies.

Accountability has shifted from the developer or a business unit who created an application with implementing authorization as a 'side of desk' job, to the CISO or identity leader who is solving for the challenge of authorization standards, access control and, more broadly governance across the enterprise.

This report will take a look at Orchestrated Authorization as a new way for organizations to deploy and see value from their authorization initiatives as well as how this methodology will influence Zero Trust, policy authoring, and its impact on the age-old debate of building versus buying an authorization solution.

The overall identity and access management market has come a long way in the last decade. With this maturity, 2022 is set up to be a watershed moment for authorization initiatives, making it crucial for organizations to get this right.

Part I
Orchestrated Authorization

Part I

Introducing Orchestrated Authorization

When we look at the last 15 years of identity and access management technology, we see a shift in the access control arena. Where authentication took center stage ten years ago, authorization is now moving into the spotlight.
We still very much need authentication solutions (particularly as many organizations still have yet to adopt meaningful authentication strategies such as multi-factor authentication), however the unique needs of authorization are increasingly recognized as a critical next step in delivering a successful identity-first security strategy.

In our view, the maturation of the authentication market was a necessity, as it paved the way for authorization. Even with the maturity of the authorization market, we see two important shifts indicating an elevated understanding and energy behind increased awareness and adoption of authorization:

1. Awareness and accountability for authorization has shifted
2. Collaboration across stakeholders is key

Awareness and accountability for authorization has shifted

Whether widely known or not, all organizations employ some form of authorization.

Traditionally, this ability to permit or deny access to critical data or processes was manually developed or coded into individual applications. When changes were required, it fell to the development team to amend or adjust as needed, which pulled them away from their day-to-day responsibilities. In effect, authorization became a 'side of desk' job for these developers. In addition to costing valuable developer time, larger organizations (particularly those in highly-regulated industries or globally-matrixed enterprises) discovered homegrown authorization strategies were incredibly difficult to scale or deploy across the organization.

Fueled in part by the pandemic, accelerated dependence on leveraging the cloud (be it public or private) as well as a permanent move to remote or hybrid workforces catapulted access control and authorization from a solution for IT or security teams to a board-level mandate to ensure critical corporate assets are accessed appropriately. That means CISOs and/or corporate identity leaders are tasked with creating a security-centric strategy with strong, practical access control at the core. This is no easy task, as it requires looking across a variety of data, applications and processes (legacy, cloud-based, and so on), with disparate and siloed instances of authorization into one unified, cohesive strategy that can be easily governed and managed.

Collaboration across stakeholders is key

For years, we've heard various vendors tout their offerings as key to helping security enable the business, bridging the gap between security and compliance requirements and business demands.

Few have delivered while the gap between two seemingly divergent interests persists and is amplified due to the complexity driven by initiatives including digital transformation, or security-specific initiatives including Zero Trust and identity-first security. The challenge for CISOs and identity leaders is how to orchestrate successful and secure access control across the enterprise.
For more than a decade, Axiomatics has worked with some of the world's largest, most complex and/or highly-regulated organizations to deliver dynamic authorization based on an attribute-based access control (ABAC) approach. We continue to evolve our technology to address the needs of stakeholders across the enterprise, including CISOs, solution architects and developers, as we believe all of these play a critical role in delivering a successful access control strategy.

In looking at the increasing number of challenges our customers face (and the increasing complexity of these challenges), we believe it is time for authorization to evolve once more. This next generation of authorization leverages the strong technology required by development teams with the elements that enable CISOs and identity leaders to deliver a flexible strategy addressing multiple stakeholders across the organization.

Orchestrated Authorization is a modern approach to ABAC, leveraging the considerable advances in identity and access management to solve for even the most complex access challenges.

Orchestrated Authorization is the future of authorization.

Orchestrated Authorization: the **Next Generation** of Authorization

Deploying an ABAC strategy in and of itself can be fraught. As discussed in the last section, many organizations struggle with legacy applications or databases, which can feature homegrown authorization code and/or solutions, or grapple with a variety of solutions, each deployed in a siloed manner, offering little to no visibility beyond what they specifically solve for. These challenges, faced by organizations worldwide, need a better, broader solution.

We believe Orchestrated Authorization is the framework best able to solve the real-time challenges organizations face and speaks to the value Axiomatics brings in runtime authorization.

Connecting People

Historically, one of the biggest challenges with implementing authorization within an organization has been understanding who owns it. This is an issue that persists today and has resulted in a variety of solutions from a variety of vendors, each offering a different focus.

While some focus their appeal to business or non-technical users, others prioritize the development crowd. Though these approaches can be successful, where they fall down is in trying to scale a focused or siloed authorization rollout across the organization. This is particularly true when considering large, globally-matrixed enterprises.

Orchestrated Authorization (OA) considers authorization delivered through an attribute-based access control (ABAC) solution a critical piece of an overall access management strategy.

As detailed in earlier sections, though authorization was at one time an oft-ignored or discounted piece of a broader security initiative, it is now more highly prioritized, with compliance as well as best practice security architectures (e.g. NIST, Zero Trust) mandating it as part of a security strategy. The CISO and/or identity leader is tasked with demonstrating the value derived from their ABAC deployment, which is almost impossible if authorization efforts are scattered in silos across the organization. To be successful and demonstrate value, the CISO needs to know they're implementing the right access policies and that these policies line up to meet the organization's overall security strategy.

For business users, an OA approach ensures they remain critical to an authorization deployment as they inform requirements for any and all policies, be it to a specific application or database, or looking at a broader purview. Business users are focused on results and do not want to spend time creating policies that might not align with the organization's overall security strategy and/or conflict with existing policies enacted for other applications or databases. Their insight into requirements (for instance – who should have access to citizenship information within an HR database) is critical. An OA strategy enables them to provide this valuable insight, without bogging them down in writing complicated, technical policies that create conflict or chaos when delivered at scale.

Development teams have traditionally controlled authorization within enterprises, where authorization policies were manually built and hard-coded into individual applications. Make no mistake about it – developers want to write code that reflects policies, however, their time is incredibly valuable and in high demand. Whereas in the past enterprises wanted quality applications delivered in a few months, that timeline has accelerated with the demand for applications now measured in weeks or even days. Added to this is the fact that though authorization can be manually added to applications, this often results in a variety of uniquely-coded authorization solutions, making this approach incredibly difficult to replicate and scale across an organization. For developers, an OA strategy offers the ability to provide expertise in creating consistent, scalable and sustainable policies, without having to take time away from application development to focus efforts into ongoing authorization implementation.

Connecting Access Through Policy

Organizations need to build demanding policies that address the real-life challenges organizations face daily, and ensure hundreds of applications and databases are only accessed as instructed by these policies. This is an ongoing need to orchestrate that growth and demand. As organizations adopt security strategies like Zero Trust, NIST or and identity first model they are all trying to connect multiple components of security solutions into one holistic decision about policy and enforcing that policy at the right time whether it be at the application level, at the unstructured data level (documents and files) or at the database level.

Orchestrated Authorization is focused on creating a consistent, holistic strategy across an organization, powered by the access control solutions already in place. After all, authorization does not exist in a vacuum, rather, it is the "tip of the spear" of an access management strategy. For that reason, Axiomatics approaches OA in a manner similar to the security orchestration, automation and response (SOAR) market. Like SOAR, the goal of an OA strategy is to take in a variety of signals or attributes and use those to make a decision from a policy perspective as to not only grant or deny access, but also to determine how much access should be granted. Moreover, leveraging Axiomatics, that decision is extended beyond the application layer to include application components all the way down to different databases.

OA takes signals or attributes from other security solutions to provide real-time or just-in-time access decisions, ensuring users (humans or machines) have the right access at the right time to the right resources…and nothing more.

For global enterprises, enterprises in highly-regulated industries, or those with a mature identity and access management (IAM) posture, OA represents the next-generation of both authorization and access management, enabling them to address complex, real-world challenges they face daily.

When it comes to Orchestrated Authorization, what are the top three things to be aware of?

1. There are many different stakeholders involved in defining policy (people, policies, attributes). Orchestrated Authorization connects all of these parties in an organized way to achieve a consistent, organization-wide approach to authorization.

2. Like a great orchestra, there is a conductor in the organization accountable for authorization. Typically, this is the identity leader or CISO who will have visibility across the entire security strategy. It is important this leader has the capabilities necessary to present how authorization as part of a broader access management strategy adheres to the organizational policies and the broader security strategy.

3. This is a journey. It's not about serving more functionality, it's about applying the capabilities across the different stages of authorization maturity throughout the organization. Consider what craw vs. walk vs. run for your organization might look like.

Part II
Zero Trust

Part II

Zero Trust **starts** with authorization

Years ago, while working as an analyst at Forrester, John Kindervag introduced a new philosophy as to how organizations could implement effective and successful security, calling it Zero Trust. Since that time, the term has evolved somewhat and matured, with organizations worldwide clamoring to understand how they can deploy a strategy with a mantra of "never trust, always verify."

Though Zero Trust has matured, its core remains the same – ensuring organizations protect their most critical or sensitive data and processes so that they are accessible in the right way, at the right time, and by the right people. No exceptions. In fact, Kindervag once likened Zero Trust protection to the way in which the Secret Service protects the President of the United States – no one is given unfettered or unretractable access to the President, who is the most valuable asset within the American government. Each touch point with this world leader is carefully vetted. That anecdote is powerful because it does a good job of illustrating the way in which Zero Trust can be used.

In the last couple of years, fueled by many issues (including a pandemic), Zero Trust has moved from a philosophy to methodology organizations know they must enact. It's the path to deploying Zero Trust that continues to challenge most organizations, as although everyone is aware Zero Trust can be successful, the steps to a successful deployment can be confusing.

In its examination of Zero Trust, the National Institute of Standards and Technology (NIST) detailed the solutions enterprises should consider as they looked to deploy a Zero Trust architecture, as "a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise-owned boundary." To that end, NIST stated that to lessen uncertainties (as they cannot be eliminated), the focus is on authentication, authorization, and shrinking implicit trust zones while maintaining availability and minimizing temporal delays in authentication mechanisms."

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Using Orchestrated Authorization to kick start Zero Trust

As organizations the world over understand, embarking on a Zero Trust deployment can feel overwhelming. Though the initial view of Zero Trust was through a network-centric lens, it's now commonly known Zero Trust can and should consider not only the network, but also applications, processes and data.

Authorization based on an attribute-based access control (ABAC) model considers all of these elements and, as rightly noted by NIST, should be a central part of any Zero Trust architecture. Because it is dynamic in nature, authorization ensures organizations can continually apply Zero Trust to access decisions in real time. But that validation does little to cut through confusion around how to leverage authorization as part of a Zero Trust methodology, both in implementation and in practice.

Adopting an Orchestrated Authorization (OA) approach as part of a Zero Trust strategy alleviates some of the confusion around adapting access control strategies to be in line with Zero Trust. Because OA advocates a centralized approach, organizations can be assured of full visibility around access decisions, allowing for a quick response, prediction monitoring and standardization. This also means improved audibility, as policies are uniformly defined for both business and IT.

Additionally, OA is a transparent methodology that enables organizations to assess risk in real-time (via decisions on access requests) to inform policies. This ensures organizational policies are Zero Trust policies, as they are both dynamic and risk-based, alleviating one of the most fraught elements of a Zero Trust deployment.

Those policies, in fact, are what define a successful OA approach to Zero Trust.
OA looks to connect multiple components of access solutions to inform a holistic decision about policy, and enforces that decision in real time, either at the application level or the database level.

In addition, using the Axiomatics platform at the heart of an OA Zero Trust approach enables organizations to pull attributes served by other security or Zero Trust solutions into the Axiomatics Decision Service (ADS) to create real-time grant/deny access decisions. Alternatively, Axiomatics ensures applications served by the company's platform receive log and information signals to be better informed and maintain updated access control.
Every security solution deployed by an organization sends out signals of the data they consume, which includes a variety of attributes (user identity, role, geography, time, etc.). OA is about pulling in as many

signals as possible, using this information to round out a successful, enterprise-wide Zero Trust strategy.

Will this approach ensure success?
Well, there's no such thing as an absolute in security (or anywhere else, really). Any organization measuring success in terms of 'full' or 'absolute' security will always miss the mark. Zero Trust is about quantifying and measuring risk, determining the level of risk that's acceptable to an organization.
Leveraging Orchestrated Authorization at the heart of a Zero Trust methodology ensures a consistent, pragmatic approach to risk that's continually assessed in real-time.

Part III
Policy Building

Part III

Evolving policy building through Orchestrated Authorization

Policies. They're the backbone of any organization's cybersecurity posture, yet few people want to talk about what is required to build a strong policy, how that can (and should) inform technology investments, and how to ensure these policies reflect the changing nature of the security landscape and organizational appetite for risk.

Though understood as something every organization has (or...should have), there's little robust debate around how to build policies the right way, something particularly true when it comes to access policies. Traditionally, access policies merely had to identify who could access a particular asset or process based on where they logged in. Once they were authenticated as requesting access from a corporate office, access could be successfully granted. With a hybrid or remote workforce now a permanent fixture at most organizations, creating access policies that are both efficient and effective is more challenging. To unpack these challenges, it is important to consider two elements – the stakeholders and the attributes.

The stakeholders

Though discussing stakeholders for any project can be straightforward, it's actually a more involved conversation when it comes to access policies. Development teams have a critical role to play here, as they will ensure the apps they develop adhere to these access policies. That is why in the past, authorization has been manually coded into each application (something the next section goes into in further detail). Developers want to ensure policies don't disrupt the work they've done to bring quality applications to market. They understand how to write policies that are not only effective, but also efficient. More on that later.

Business stakeholders have a significant role to play, as they know quite a bit about who should have access to an organization's data and policies. For example – the finance department oversees a number of functions including payroll, budgets and revenue forecasts, but not all members of the finance department need unfettered access to all of that information. A payroll specialist may not need insight into revenue forecasts presented to a Board of Directors, and so on.
Executive stakeholders like an identity leader or CISO must also have input into access policies, as they are ultimately responsible for demonstrating how these policies contribute to a variety of corporate cyber initiatives, including adhering to global privacy and compliance regulations. Moreover, they have a broad view of the organization's overall security stance and how these access policies reflect those larger initiatives.

Though authorization initiatives have evolved and now, in many cases, roll up to the CISO or identity leader, these leaders also must reconcile legacy policies that emerged from business or development stakeholders, many of which conflict or are simply outdated/inefficient.

In working with organizations of all sizes around the world, the Axiomatics team understands it is not one person or one role in the organization that should define or own policy creation outright. Leveraging an Orchestrated Authorization strategy ensures stakeholders are able to contribute in appropriate, meaningful ways with regard to building access policies, as well as ensuring the policies themselves are accurate, efficient, and without conflict.

The attributes

Creating access policies can be quite sensitive and requires expertise as well as transparency across all stakeholders. For small organizations, policies might be quite simple, reflecting something such as, "if a user is in role X, they can do this/ access this data." But as the organization grows and becomes more complex, policies start to interact (organizational policies versus application-specific policies versus departmental policies), and the relationships between all of these must be examined.

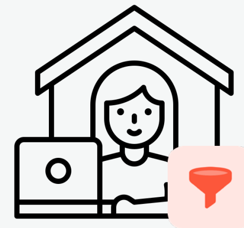
When most users were in an office accessing data, access policies were static. Today, modern organizations require policies to be dynamic, reflecting that users (both human and machine) will require access on multiple occasions, from varying locations and in many cases, from different types of devices. So…how do you make a policy dynamic? Well, you don't need to actually continue to update the policy itself. Instead, in an attribute-based access control (ABAC) environment, policies remain few and static and what changes are attribute values, which in turn impact the policy decision as well as outcomes.

Here's an example – a policy might say only employees can access all information within an organization's HR system, while contractors can access only some information in the same database. Or, employees with higher security clearance can access healthcare information within the database while employees with lower security clearance do not have that access. These policies are fairly straightforward and look at 'employment' or 'role' as their primary attributes.

Now, if Kelly moves and becomes a remote worker alongside Harry, the amount and type of access she has could change. This does not mean the policy has changed in any way, rather the attributes for the users changed, granting a different access decision.

If Kelly is an employee working from corporate headquarters with high security clearance, she has access to healthcare information in the database.

If Harry is a remote employee working on an unsecured home network, he may not have that same level of access.



Now, if Kelly moves and becomes a remote worker alongside Harry, the amount and type of access she has could change. This does not mean the policy has changed in any way, rather the attributes for the users changed, granting a different access decision.

Orchestrating Policies

An Orchestrated Authorization strategy enables this type of dynamism when it comes to access policies. It ensures the right stakeholders inform policies in the right way, without conflict, based on dynamic attributes. In this strategy, the CISO or identity leader (the 'conductor,' if you will) is ultimately accountable for ensuring policies are accurate, consistent and efficient.

Business users application owners play a role in informing policy creation by providing an understanding to policy modelers on specific access requirements. Considering the earlier example, a business leader would be the one to determine that only employees with high security clearance have full access to a particular asset or database. In our experience, business users play a critical role articulating policies in a natural language and collaborate with policy modelers who express those policies in a formal authorization language. However, business users want to stay focused on their core competencies and do not have any desire to manage/develop policies themselves.

Policy writing is done by defined policy modelers, stakeholders who most often reside on a technical or development team. These stakeholders understand how to implement access requirements as part of a well-crafted and efficient policy, ensuring that the way in which the policies are modeled does not bog down the authorization engine issuing a permit/deny decision.

Not all voices agree on this particular delineation of duty, with some in the authorization and access markets advocating that anyone can create an access policy. But not all policies are created equal, and the type of policy may require a different modelling approach. If the organization requires complex or demanding policies, enabling any stakeholder to create policy could be problematic, as those who do not have policy modeling experience may inadvertently write policies that slow down the authorization and authentication engines making the access decision or, worse yet, create policies that conflict with other policies, creating access chaos and subjecting the organization to risk. Policy modeling is a specialized skill, much like coding is a specialized skill. In some instances, a novice coder might be able to create code that satisfies development requirements. In other circumstances, a veteran coder would be the best solution, as that person could write code that is both fast and effective, satisfying more complex projects or specific outcomes.

An Orchestrated Authorization approach ensures all stakeholders have the right seat at the table, creating effective and efficient access policies that reflect the dynamic nature of modern organizations.

Part IV
Build vs Buy

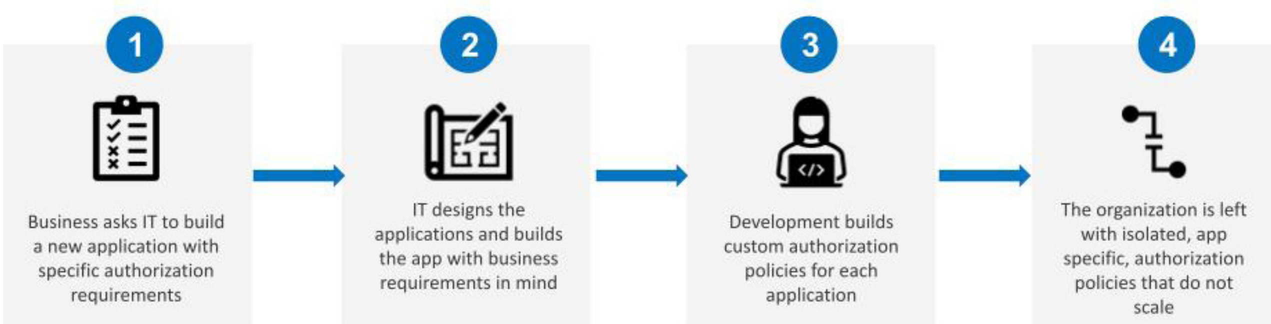
Part IV

It's time to settle the "build versus buy" authorization debate

Though the approach to identity and access management (IAM) has seen rapid maturation over the last decade, there's one area where an outdated approach within enterprises can still persist - authorization. Traditionally, authorization was firmly an IT or development team initiative, manually hard coded into individual applications leading to an isolated authorization strategy.

Deploying isolated homegrown authorization policies to one or two applications was manageable. The reality is that as the pressures to innovate, pivot and change have driven application development forward, most organizations have been left with an isolated authorization strategy that spans their entire application as well as enterprise data environment.

No organization sets out to create isolated authorization, which is authorization manually developed for each application. Application owners and IT or development teams had the right intentions when developing authorization policies for their respective projects. Generally speaking, the process would be as outlined in the graphic below:



The end result: authorization requirements would get defined and developers would build the policies into the application. Then...everything changed.

We have made it this far with a homegrown solution - why stop now?

In the last two years, the market has evolved quickly, in turn demanding organizations to adapt as vigorously, or else become vulnerable to risk. At a high level, the evolution has occurred in three core areas:

1. Zero Trust | Compliance

Once an aspirational goal, Zero Trust is quickly becoming an industry standard, requiring organizations to deploy continuous verification of access for every application based on context, such as risk. Furthermore, Zero Trust is being deployed not only because it leads to the right cyber strategy, but supports the increased pressures from regulators to prove that the organization is protecting sensitive data. Demonstrating to regulators (with proof/audit trails) that applications are being developed through a centralized authorization strategy with security/governance oversight is critical to maintaining compliance.

2. Accelerated Pace of Innovation

More than ever, organizations are embracing the adoption of cloud and microservices, which often results in the creation of hundreds of applications to keep pace with innovation requirements. Development teams do not have the time/ resources to keep building and supporting their own authorization solutions to scale to this demand.

3. Hyperscale Application Performance Expectations

To keep pace with innovation (and with competitors), application owners and users demand millisecond response times for authorization decisions. Domain specific solutions delivered by vendors are built to scale to these expectations. Attempting to build homegrown authorization policies in silos will struggle to meet the performance expectations of the modern enterprise.

In parallel to these market drivers, authorization is now considered in a new light. While in the past, authorization was viewed as an application-specific requirement, it is now an organizational imperative as part of a broader access management approach. This is particularly true as broader security initiatives including Zero Trust require a strong, “always validate” approach to access that is inherent with attribute-based access control (ABAC) solutions like the Axiomatics platform. Accompanied by the market evolution factors outlined above, it is this shift in how authorization is viewed that is slowly changing the narrative from “should I build or should I buy” to “how can I move from what I’ve built to a best-in-class solution I can buy.”

The case for an externalized, centralized and dynamic approach

It is becoming clear that more and more high-performing IT organizations have shifted their efforts to focus on core competencies, which can then be augmented by leveraging best-in-class solutions for pretty much everything else. For example, on multiple occasions, the Axiomatics team has encountered organizations that have built their own authorization systems through internal software development teams, serving hundreds of applications. While that approach might have addressed the organization's 'now term' goals, it also created a significant resource-intensive environment, fraught with risk, and one requiring manually-delivered updates with any new requirement.

Every new regulation, new policy or even code introduced could mean weeks spent manually updating code consistently across all applications. While this might be a significant inconvenience for some small organizations, it is untenable for a large enterprise or organization in a highly-regulated industry.

Those organizations who move to purchase an authorization solution do so for a few reasons:

1. Dynamic policies fuelled by dynamic attributes

As mentioned in the policy building section, externalized authorization offers the ability to create policies that are dynamic in nature (always up-to-date) fuelled by a dynamic approach to considering attributes before rendering a permit or deny decision to an access request. For example – an organization looking to implement Zero Trust is looking to "always verify" access requests, something that is incredibly difficult, if not impossible, with homegrown authorization solutions. Organizations leveraging Zero Trust increasingly understand that policies rooted in ABAC-based authorization are key to implementing an effective Zero Trust strategy.

2. Scalability

As organizations grow, so do the number of applications or databases within these companies. At a point, it simply becomes unsustainable to continue to lean on internal development teams to add authorization as a 'side of desk' job in addition to where their talents are needed most – developing effective and efficient applications.

3. Looking ahead

Mentioned above, this bears repeating – though building an authorization solution in-house may appear to check all the boxes for an organization's development strategy, it does not and cannot adequately ensure that organization is ready to address a cyber as well as technology landscape that becomes more complicated and offers more risk with each day.

Organizations shifting from a homegrown or isolated authorization strategy see that the issues of scalability and future-proofing are well addressed through an Orchestrated Authorization strategy. Indeed, this broader, connected approach to authorization ensures a more modern approach to security challenges, the ability to successfully implement Zero Trust or identity-first strategies, and a way to lessen challenges associated with shifting policies or central security initiatives across the organization.

Isolated authorization as a result of homegrown efforts remains status quo for many enterprises. But as the last two years have shown, organizations must be ready to rapidly evolve their access strategy as market conditions shift, something only attainable through purchasing a best-in-class authorization platform.

About Axiomatics

Axiomatics is the originator and leading provider of runtime, fine-grained authorization delivered with attribute-based access control (ABAC) for applications, data, APIs and microservices. The company's Orchestrated Authorization strategy enables enterprises to effectively and efficiently connect Axiomatics' award-winning authorization platform to critical security implementations, such as Zero Trust or identity-first security. The world's largest enterprises and government agencies continually depend on Axiomatics' award-winning authorization platform to share sensitive, valuable and regulated digital assets – but only to authorized users and in the right context.

Learn more or request a demo of our solution:

axiomatics.com

webinfo@axiomatics.com

US Office: +1 (312) 374-3443 | Europe Office: +46 8 51 510 240

AXIOMATICS