EXECUTIVE BRIEF

Four Ways Isolated Authorization Challenges Zero Trust Success

AXIOMATICS
a LEONARDO company

Overview

The move to modernize enterprise work environments, embracing hybrid and remote options, has driven information and security teams to revisit their existing cybersecurity strategy. An integral element of this strategy is its authorization policies, which determines the parameters for how users access information.

Historically, organizations defaulted to isolated authorization, a process by which authorization was hard-coded and customized for each application. Not only is it application-specific, but it is also use-case specific, and creates silos from the rest of the organization as the authorization strategy is driven by individual application teams instead of being led by the identity and/or security team. As a result, there is no standardized approach to authorization, leading to an unscalable strategy and increased cybersecurity risks.

While incorporating a Zero Trust framework is now an industry standard, those looking to implement Zero Trust while still leveraging isolated authorization as part of their access management strategy will face significant roadblocks. A successful Zero Trust strategy is built on a modern approach to access control that is adopted by the organization, while attributes and signals for policy context continuously evolve based on new requirements and potential threats to the business. If the identity and security teams do not have visibility into authorization policies borne of an isolated approach, then your Zero Trust implementation will not succeed.

For a successful Zero Trust outcome, organizations must move from an isolated approach to a more policy-based approach to authorization.

This executive brief will explain why isolated authorization is incompatible with a Zero Trust cybersecurity framework and outline why leveraging policy-driven-authoirization within a Zero Trust model best meets the needs of the modern enterprise.

Why is isolated authorization incompatible with a Zero Trust strategy?

1 Isolated authorization does not enable the continuous risk evaluation central to Zero Trust. Why?

A core part of a Zero Trust strategy is the continuous evaluation of a subject (human or machine)'s risk. The identity or security team owns the visibility into a subject's risk and strives to bring that context into every security policy deployed in the organization. Risk can be determined from many different sources, whether it is a formal risk score, user location or even how the subject authenticated into the application. If authorization policies are created and isolated from the identity or security team's control, the organization will never bring this critical attribute into their authorization policies and, more broadly, into their access management strategy.

2 Isolated authorization is not externalized from the resource - a non-starter for a Zero Trust architecture. Why?

Isolated authorization means custom policies are often hard-coded directly into the application itself. Security and identity teams have zero visibility into those policies and cannot implement a dynamic approach to policy execution, which is required to address an ever-expanding list of cybersecurity threats. To achieve dynamic authorization policies, policy decisions should be externalized from the application so that as attributes and signals evolve, they automatically adjust without human intervention.

3 Isolated authorization does not enable effective auditing. Why?

Today's compliance requires granular visibility into entitlements and permissions. During the auditing process, isolated authorization makes it difficult to determine who has access to what application, and under which specific circumstances. With the lack of centralized management, there is no single framework against which to cross-reference applications or other resources. This could leave gaps that are missed by the auditor, or delay audit completion.

4 Isolated authorization policies can lead to over-privileged access. Why?

When users permanently or temporarily leave an organization, they might still register as a user on certain applications with standing privilege access. While application developers have the best intentions, the reality is security has been an afterthought for applications that have isolated authorization policies, which can result in this security gap. This means that as organizations adopt Zero Trust and ultimately a least-privileged approach to access, isolated authorization can leave the company exposed to risk when user accounts become orphaned accounts, without validating who is behind the screen.

The Zero Trust Solution

Developing a Zero Trust model is dependent on a shift to dynamic authorization strategies such as Orchestrated Authorization, since Zero Trust requires a centralized network to facilitate the right level of security and adaptability.

A policy-driven authorization strategy is a key component of a successful Zero Trust deployment, as it is a unified, context-based approach to authorization that equips developers with the tools they need to draft effective policies. While this approach requires central oversight by a security or identity leader within the organization, policy authoring is decentralized as it continues to be owned by different developers. The key difference is that developers or application owners have a unified framework to follow when authoring their policies, rather than interpreting the business requirements on their own.

Policy-driven authorization promotes a single repository for user attributes and business requirements that can be applied to all data platforms in an ABAC environment, combining unified identity management with context-based access.

With a centralized network and a decentralized policy authoring strategy, Policy-driven authorization is an approach that addresses the core needs of a Zero Trust model. Each component must align with one another to create a one-to-many solution that is easily adaptable to every application or data platform, resulting in a standardized approach to authorization. Much like a video game, Zero Trust ensures users must pass certain stages to get to the last mile of access, enabling a more connected and secure workplace.

The Bottom Line

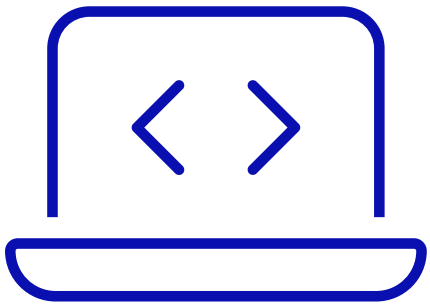
While there is no single approach to authorization, some approaches are more effective than others. The working environment continues to evolve faster than ever before, and organizations need a cybersecurity foundation that promotes business agility. Organizations must deliver on a modern and comprehensive cybersecurity strategy such as Zero Trust by developing a dynamic authorization approach that fits the needs of a dynamic workplace, and level up from isolated authorization.

If you want to learn more about how Zero Trust can fit into your authorization strategy, we're here to help.

Take the next steps

Learn how how a security vendor can help secure your access control while allowing you to focus on your core business initiatives.

Meet with our solution experts for a demo of our Axiomatics Authorization Management Platform and discuss how our approach can save your organization time and money.



Stay connected and informed

Get the latest insights, announcements, and assets from our thought leaders and customer success team:

- Blog articles
- Press releases and announcements
- Resources, solution briefs, and tools
- Join us on LinkedIn
- Subscribe to our Linkedin Newsletter
- Subscribe to our YouTube channel

Axiomatics - a Leonardo Company 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 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.

Follow us on LinkedIn: https://linkedin.com/company/axiomatics

Join us on YouTube: https://youtube.com/@axiomatics

Learn more or request a demo of our solution:

axiomatics.com

info@axiomatics.com

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