



Why IGA Can't Wait: 5 Reasons to Prioritize Identity Governance Now





Contents

Executive Summary	03	4. Fueling Business Efficiency	10
1. Surging Cybersecurity Threats	04	5. Zero Trust Requires IGA	12
2. Complexity from Cloud and Hybrid IT	06	Conclusion	14
3. Rising Regulatory Pressure	08		

Executive Summary

Why IGA Can't Wait

Identity has become the control plane for modern business. It's also the first line of defense in today's cybersecurity landscape. As organizations accelerate digital transformation, the number of identities, access points, and applications has exploded. With this growth comes risk: mismanaged identities, excessive privileges, and orphaned accounts are now among the leading causes of data breaches and compliance failures.

At the same time, regulatory mandates are tightening, Zero Trust strategies are reshaping architectures, and organizations are under pressure to move faster while maintaining control. Traditional identity management can't keep up.

Identity Governance and Administration (IGA) provides the visibility, control, and automation required to manage access risk at scale across cloud, hybrid, and on-premises environments. More than just a security solution, IGA is a strategic enabler that helps organizations move faster, stay compliant, and respond to threats before they become business disruptions.

In this eBook, we explore 5 urgent reasons to prioritize IGA now, from rising cyber threats to regulatory pressure and the need to support agile, hybrid work. For security leaders, the message is clear: identity governance can't wait.



1. Surging Cybersecurity Threats

Identities Are the New Perimeter

Identity is now the #1 attack vector. Poorly governed identities especially privileged and orphaned accounts create serious vulnerabilities. IGA minimizes risk by ensuring the right people have the right access at the right time.

With cloud and remote work dissolving the traditional network edge, identity has become a primary and increasingly critical layer of defense. IGA ensures secure, policy-driven access in a borderless world.

IGA reduces risk by:

- **Policy-Driven Access Assignment:** Automating entitlements based on roles, context, and risk classification ensures people and systems get only the access they need, when they need it, with increased efficiency.
- **Access Visibility and Certification:** Centralizing comprehensive visibility into who has access to what, across cloud and on-prem systems, and enforces periodic reviews to certify or remove entitlements, contributing to security efficiency.
- **Orphaned and Overprivileged Account Detection:** Continuously identifying stale, misconfigured, or unowned accounts that could be exploited by attackers or abused internally.
- **Rapid Breach Response:** Enabling immediate access lockdown in the event of a suspected compromise, containing threats before they spread, boosting response efficiency.

Threat actors increasingly exploit privilege creep, and identity blind spots. IGA serves as the backbone of identity risk management, enforcing least privilege, operationalizing Zero Trust, and preventing lateral movement in identity-based attacks. By continuously governing entitlements and automating corrective actions, IGA helps reduce the risk of both external breaches and insider threats.



2. Complexity from Cloud and Hybrid IT

Sprawl Demands Centralized Governance

The shift to hybrid and multi-cloud environments has exploded the number of systems, apps, and identities to manage, driving new access needs across external vendors, internal stakeholders, and connected services. Meanwhile, machine identities are growing at twice the rate of human identities, due to API integrations, IoT systems, and AI workflows.



Without centralized scalable identity governance, this explosion in digital access points increases the risk of overprovisioning, shadow IT, and unmonitored entitlements. IGA empowers organizations to:

- **Secure SaaS Proliferation:** Automate provisioning and deprovisioning across hundreds of SaaS platforms ensuring access is assigned, reviewed, and revoked appropriately, all with high efficiency.
- **Adapt to AI and Machine Identity Growth:** Apply governance policies to service accounts, bots, and autonomous agents to ensure they follow the same least privilege and approval workflows as humans, maintaining governance efficiency.
- **Manage Multi-Cloud and Hybrid Environments:** Provide consistent visibility and policy enforcement across infrastructure, whether it's AWS, Azure, GCP, or on-prem, enhancing hybrid cloud management efficiency.
- **Support Time-Bound and Contextual Access:** Grant dynamic access for external collaborators or internal project-based roles with automatic expiry and audit logging, contributing to streamlined efficiency.

Modern IGA enables organizations to move fast without losing control. It scales with your digital ecosystem, secures access for all identity types, and supports innovation without introducing undue risk.



3. Rising Regulatory Pressure

Compliance Isn't Optional

The regulatory landscape is more demanding than ever. Governments and industry bodies are enforcing stricter data protection and compliance mandates. IGA helps demonstrate compliance with identity-related controls through clear audit trails, access reviews, and policy enforcement.

IGA plays a pivotal role in helping organizations meet these mandates by delivering continuous visibility, policy enforcement, and audit readiness across the access lifecycle.



IGA enables compliance through:



Centralized Access Control: Managing human and machine identities across hybrid environments to enforce least privilege and align with Zero Trust for streamlined access control efficiency.



Continuous Certification: Automating policy attestation and recertification processes to prove compliance with accountability requirements, such as those mandated by DORA and NIS2 saving significant time and improving compliance efficiency.



Audit-Ready Reporting: Providing real-time logs, access justifications, and activity reports needed to demonstrate compliance in regulated industries, enabling greater audit efficiency.

With evolving regulations redefining security and compliance baselines, IGA is now a non-negotiable capability. It ensures identity-based controls are consistently applied, monitored, and verified. Providing both resilience against threats and assurance under scrutiny.

4. Fueling Business Efficiency

Enabling Speed Without Sacrificing Control


Speed is now a competitive necessity. Businesses must adapt quickly, yet securely, to meet customer expectations and market demands. Traditional access management processes slow down progress and frustrate users due to manual approvals, delayed onboarding, and siloed governance.

Identity Governance and Administration (IGA) removes these barriers, fueling business agility by automating and intelligently managing access in real time. With IGA, organizations enable teams to move quickly while maintaining tight security controls.



IGA drives agility and efficiency through automation and AI-powered intelligence:

- **Smart Access Recommendations:** AI analyzes historical access patterns, user roles, and peer group behavior to suggest the most appropriate entitlements, reducing errors and speeding up approvals.
- **Automated Access Requests and Approvals:** Self-service access portals with automated routing and policy enforcement remove manual delays while maintaining governance.
- **Faster Onboarding and Offboarding:** AI-driven identity lifecycle management provisions and deprovisions access based on organizational role, business unit, or location, cutting onboarding time from days to minutes.
- **Adaptive Access Reviews:** Machine learning helps prioritize high-risk access during certifications, allowing reviewers to focus where it matters most, saving time while strengthening security.
- **Reduced IT and Help Desk Load:** AI-powered virtual assistants can guide users through access requests, while automated workflows eliminate routine ticket handling for IT.



By embedding intelligence into identity governance, IGA transforms access management from a governance bottleneck into a proactive, strategic enabler of business growth.

Modern IGA ensures people get the right access automatically, intelligently, and securely supporting workforce agility, accelerating transformation initiatives, and reducing operational drag. It's how forward-thinking organizations scale securely without slowing down.

5. Zero Trust Requires It

No Trust Without Identity Governance

At its core a Zero Trust strategy has a simple but radical principle: never trust, always verify. In this model, identity becomes the control point, and IGA becomes the operational engine that makes Zero Trust work in practice.

Legacy perimeter defenses can't protect today's hybrid workforce, dynamic access needs, and SaaS-first environments. Every access decision must be continuously verified based on who is requesting access, to what resource, under what conditions, and whether that access is appropriate.

Identity Governance and Administration (IGA) provides the policy enforcement, context awareness, and lifecycle management required to operationalize Zero Trust.

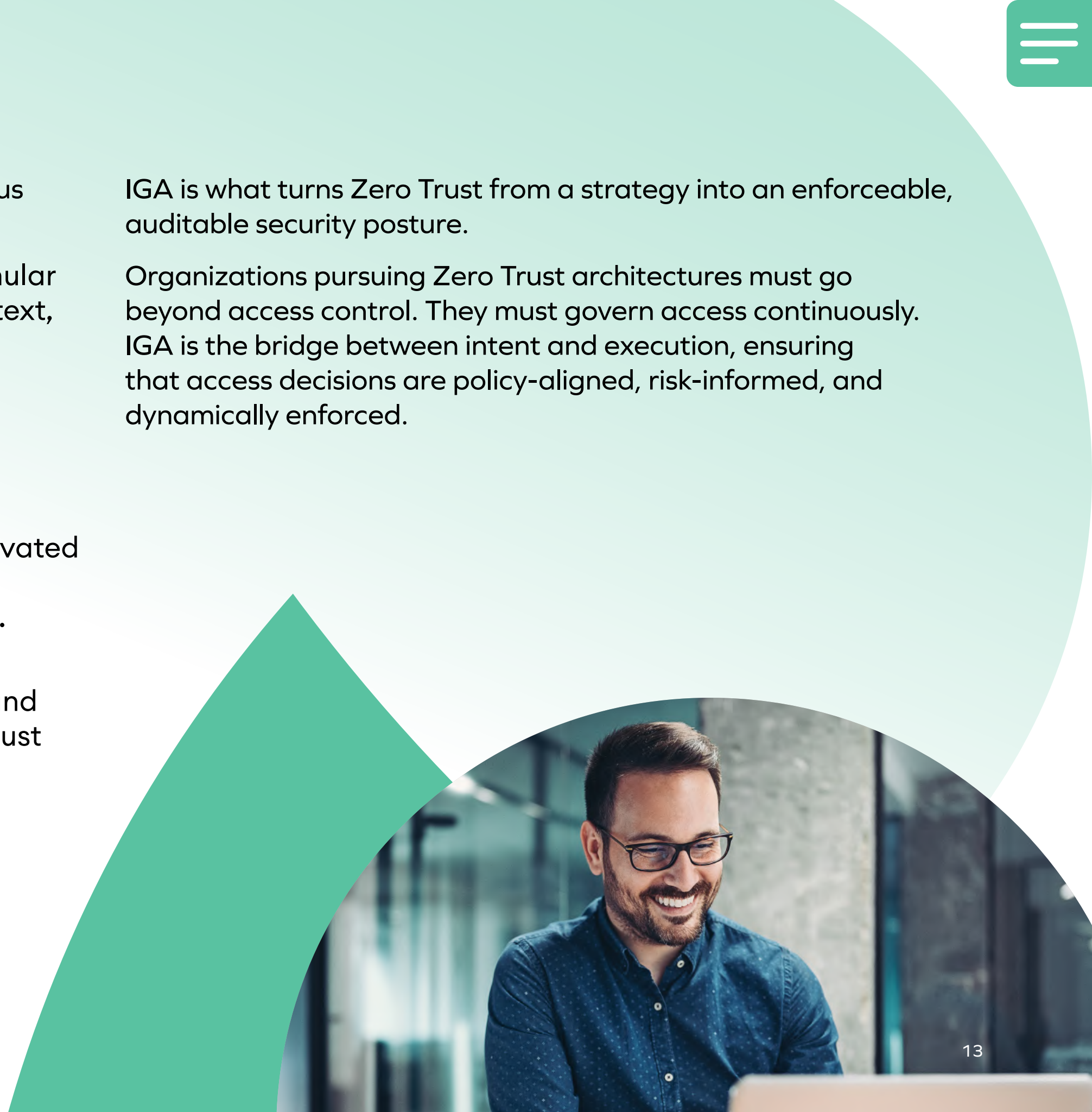


To make Zero Trust actionable, organizations need continuous identity governance. IGA enables Zero Trust through:

- **Policy-Based Access Controls:** Define access at a granular level using roles, attributes, risk scores, or business context, ensuring access is justified, approved, and auditable.
- **Dynamic Access Reviews:** Enforce continuous access certifications, automatically triggered by role changes, inactivity, or risk events, so access reflects real-time trustworthiness.
- **Just-In-Time Access Provisioning:** Grant temporary elevated access only when needed and revoke it automatically, reducing standing privileges and lateral movement risk.
- **AI-Powered Risk Insights:** Identify anomalous access behavior, recommend risk-adjusted access decisions, and highlight overexposed identities, all feeding into Zero Trust policy refinement.

IGA is what turns Zero Trust from a strategy into an enforceable, auditable security posture.

Organizations pursuing Zero Trust architectures must go beyond access control. They must govern access continuously. IGA is the bridge between intent and execution, ensuring that access decisions are policy-aligned, risk-informed, and dynamically enforced.





Conclusion

The Cost of Waiting Is Too High

The identity landscape is evolving too quickly and the stakes are too high for organizations to treat IGA as a “nice to have.” Every unmanaged account, every overprivileged user, every unreviewed entitlement adds to your risk surface.

Cyberattacks don’t wait. Auditors don’t wait. Your business can’t afford to wait either.

IGA provides a centralized, authoritative source of truth for identity and access entitlements across the organization.

IGA gives you the tools to:

- Reduce the risk of breaches and insider threats
- Prove compliance with evolving regulations
- Enable fast, secure access for a dynamic workforce
- Operationalize Zero Trust with confidence
- Strengthen business agility while maintaining control

Organizations that invest in IGA today are building not just a stronger security posture but a smarter, faster, and more resilient business.

The longer organizations delay modernizing IGA, the greater the exposure to threats, compliance failures, and operational drag.



Ready to Take the Next Step?

Omada simplifies Identity Governance by providing a full-featured, cloud-native IGA solution that streamlines the complex processes of managing user identities, access, and entitlements. With a focus on automation and user-centric design, Omada reduces manual tasks and enhances operational efficiency, ensuring that organizations can easily enforce security policies, comply with regulations, and manage user access at scale. By leveraging advanced technologies such as AI-driven decision making and role-based access control (RBAC), Omada enables businesses to achieve stronger security, better compliance, and improved user experiences—without the complexities traditionally associated with identity governance.

Visit [Omada](#) or [Contact us](#) to start the conversation.



Omada simplifies Identity Governance by providing a full-featured, cloud-native IGA solution that streamlines the complex processes of managing user identities, access, and entitlements. With a focus on automation and user-centric design, Omada reduces manual tasks and enhances operational efficiency, ensuring that organizations can easily enforce security policies, comply with regulations, and manage user access at scale. By leveraging advanced technologies such as AI-driven decision-making and role-based access control (RBAC), Omada enables businesses to achieve stronger security, better compliance, and improved user experiences—without the complexities traditionally associated with identity governance.