Guide

5 Reasons to Prioritize Identity Governance and Administration Today

Omada

Do more with identity

Table of Contents

Introduction.. 1

1. See Unique, Tangible Return on Investment 3

2. Enable the Workforce 5

3. Reduce the Risk of Breaches with Least Privilege 6

4. Meet Evolving Compliance Mandates and Audit Requirements 7

5. Confidently Undergo Digital Transformations 8

Meet the Demands of Modern Business 9

Introduction

The attention paid to digital identities has increasingly become a top priority for organizations, as the workforce proliferates, emerging threats emerge, compliance grows more complex, and business needs change. In Gartner's 7 Top Trends in Cybersecurity for 2022, the first three trends were noted as "attack surface expansion," "identity system defense" and "digital supply chain risk" Gartner notes that "Currently, 60% of knowledge workers are remote, and at least 18% will not return to the office," in discussing the continued trend of working remotely, and also that "identity systems are coming under sustained attacks." This combination creates difficult situations for security and risk management teams as their workforce continues to require access to a variety of systems, data, and infrastructure from anywhere, and attackers continue to find new ways of breaching the network by leveraging digital identities and attacking software supply chains. Worth noting, is that the latest OWASP Top 10, which ranks the most critical security risk to web applications, has 'broken access control' as the most serious web application security risk.

91%	53%
IAM budgets will significantly increase	IT experts do not know how well their cybersecurity tools are working

As a result, the amount of time, money, and energy spent on cybersecurity and identity-related solutions has ballooned, with recent research reporting that 91% of organizations' Identity and Access Management (IAM) budgets will receive a significant increase relative to the rest of their cybersecurity budgets. However, allocating budget, team resources, and time on this growing sector has led to some confusion, with recent Ponemon research noting that 53% of IT experts admit they do not know how well the cybersecurity tools they've deployed are working. Picking the right solutions takes top-down alignment on what the business objectives are, and how they relate to the bottom line, improving security, optimizing efficiencies, and putting the organization in the best possible spot to meet compliance mandates.

Identity Governance & Administration (IGA) is the linchpin of IAM that allows enterprises to continuously monitor, manage, and administer access rights to a constantly evolving set of resources that live across cloud, on-premise and hybrid environments. Making it a critical tool for any organization looking to reduce their risk, meet compliance, or enable their workforce. IGA solutions provide visibility across all applications and IT systems by managing entitlements and access across the increasingly complex landscape, with clear ways of tracking return on investment for business leaders.

Five reasons every organization should prioritize IGA today:

1. See unique, tangible return on investment
2. Enable the workforce
3. Reduce the risk of breaches with least privilege
4. Meet evolving compliance mandates and audit requirements
5. Confidently undergo digital transformations

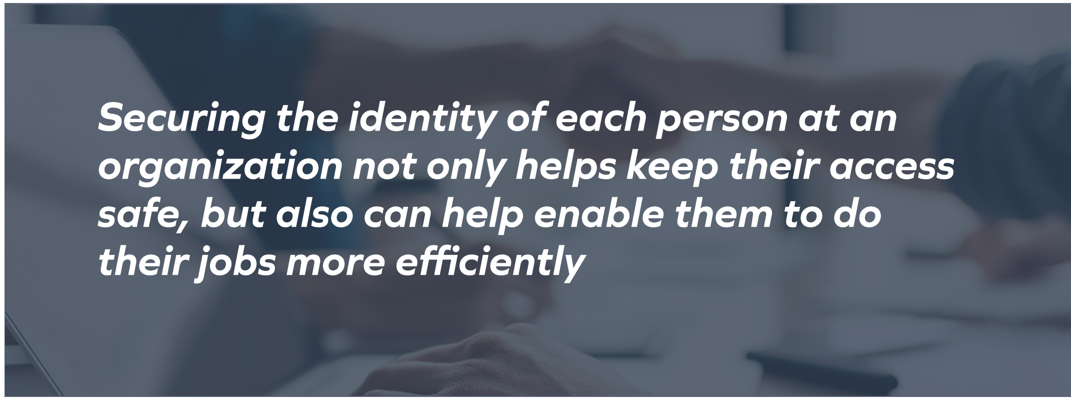
1. See Unique, Tangible Return on Investment

The shift to cloud and remote working has driven an increase in the number of security tools that organizations are on average using, from 64 to 76, just over the past two years. The number of security tools to manage has increased, and a lot of these tools solve emerging edge use cases that are flashy and promise to solve the next frontier of organizational requirements. As a way of illustrating this, it has been recorded that in just the first half of 2022 a staggering $12.5 billion in venture capital money was poured into cybersecurity ventures. However, the sheer number of tools makes it very challenging to identify what to start with, and even more challenging to determine which tools are delivering on their promises.

64 - 76 **Increase in the # of security tools that average organization uses**

$12.5 billion **in venture capital money was poured into cybersecurity ventures, in the first half of 2022**

Much has been written about how identity is the new perimeter. Gone are the days where a firewall, an intrusion prevention / detection system and a VPN can keep the organization safe. Today's organizations have growing mixes of employees working remotely and at home, third-party vendors as part of the supply chain, contractors, auditors, interns, and seasonal workers who need access to a variety of systems hosted in the cloud and on-premises in the datacenter.



> ***Securing the identity of each person at an organization not only helps keep their access safe, but also can help enable them to do their jobs more efficiently***

Securing the identity of each person at an organization not only helps keep their access safe, but also can help enable them to do their jobs more efficiently, without feeling like they are being hindered by clunky legacy solutions.
When building out a cybersecurity program from scratch, or even when evaluating core goals of the security team in today's climate requires a laser focus on tools that can deliver the most amount of impact and help reach organizational business goals. IGA is uniquely positioned to help organizations ensure they are secure, efficient, and compliant, with many ways to deliver value back to the business.

- **Optimize Efficiency.** IGA helps organizations automate processes like access requests, provisioning and deprovisioning access, certifying access, and tracking access across the hybrid landscape, which helps minimize calls to the help desk, minimize time spent manually tracking access and pulling reports, and maximizes the time people spend working, and allows security professionals to focus on their most critical tasks.

- **Meet Compliance.** IGA helps organizations track access rights and entitlements across the enterprise, provide dashboards for IAM teams to easily prove compliance, and maintain records of access rights as they evolve over time, helping organizations avoid hefty fines and reputational damage that comes from missed audits.

- **Increase Security**. IGA helps organizations centralize management of all identities and access rights, minimize the number of orphaned accounts, reconcile accounts to check anomalies, and classify systems and assets based on risk to help avoid massive data breaches that impact the bottom line, and stay out of the headlines.

IGA focuses on quickly maximizing ROI by helping organizations get rid of slow, costly, and error-prone manual processes and moves to enable the workforce, meet compliance, and enhance security. This helps by reducing time spent on edge cases and maximizes output to secure your organization's most valuable resources: people and data.

2. Enable the Workforce

In November of 2021, 4.5 million Americans quit or changed their jobs, which is the highest in recorded history, and was the 4th time in 2021 that a new record was reached. Even in Europe, where, historically, culturally job hopping is less common, 20% of millennials in western Europe reported that they quit their jobs since 2020. Every organization must deal with people joining, moving roles or projects, or leaving the organization, and this includes not just full-time employees, but also third-party contractors, outsourced IT, auditors, interns, and other seasonal workers.

IGA solutions help organizations onboard new members of the workforce to enable them to be productive on day 1 by ensuring that they are assigned 'birthrights' and are assigned role- or policy-based access based on who they are, what their job function is, where they are located, and other contextual factors. Without IGA in place, this process can take days, if not weeks for IT and HR to empower new members of the organization with proper access that can stunt productivity, cost the organization money, and incentivize people to create unsafe workarounds for the access they require to do their jobs. In fact, 52% of organizations say it takes multiple weeks to even months to provision access to business-critical applications.

For people that are moving within the company, assigning new access that may be required, like for instance, someone in Product Management moving to Sales will need access to the CRM, prospecting tools, and more. For productivity to be maintained that process needs to be seamless, but if they maintain access to systems they no longer need, like project management applications, product launch tools, and more, this can be a blind spot for security and be sitting ducks for attackers. IGA solutions help IT teams seamlessly move identities into their new roles with new access, but while decommissioning entitlements that are no longer needed. This concept is also essential in removing access for people that are leaving the organization, more on that on the next page.

Finally, throughout the normal course of business operations, people will undoubtedly need to request access to additional systems or applications, which if handled manually can also stifle productivity. 50% of organizations have noted that they either manually review all or most access requests, meaning that people are waiting around for access requests to be fulfilled to provide them with access they need. IGA solutions help organizations with providing end users and administrators with autonomy to request and review access automatically.

Identity governance and administration helps organizations enable their entire workforce to be productive the moment they walk in the door and remove excess access risk when they change roles or leave the organization.

3. Reduce the Risk of Breaches with Least Privilege

With each year that passes, a new record is reached for the average cost of a data breach, and in 2022, the cost of an average data breach was $4.35 million, up 2.6% from the prior high in 2021. Organizations also regularly face new and evolving threats, but must deal with them with fewer resources, with unfilled cybersecurity jobs growing 350% between 2013 and 2021, with 3.5 million unfilled cybersecurity jobs across the globe. IGA has been proven to help organizations keep their most critical assets, their people and their data safe by implementing the following:

- **Automatically obtain an inventory of applications.** You cannot secure what you do not know exists. As such, organizations need to identify identities, resources, and data and make sure they know who has access to what. IGA provides centralized views to who has access to what, for how long, for what reasons, and who approved it. By tracing access rights for both cloud and on-premises resources, organizations gain visibility into who has access to what and can get to work on ensuring their desired state of access is met.
- **Continuously assign access based on policies and roles.** Assigning access can be a tedious job. With IGA, organizations can set policy- and role-based access to automate entitlements based on who the person is, what their job function is, and more. IGA solutions can then detect risks like unowned accounts (more on that below), unwanted or unneeded access, or people who collected excessive permissions along the way and reduce access to strictly what is needed. In addition, IGA solutions help reduce risk by classifying which systems, assets, and data are most risky and tagging them accordingly.
- **Remove unneeded access.** Attackers and malicious insiders regularly gain entry to organizations through trusted but over-permissioned access and use it to exfiltrate data. IGA solutions can help reduce unnecessary access and ensure least privilege by implementing regular certification campaigns to certify that access is still needed by asking questions about when the last time access was used and for what reasons.
- **Assign ownership of unowned accounts.** Accounts without designated owners, or with misassigned owners similarly present risks and can greatly expand the blast radius in a ransomware attack. IGA solutions help limit the attack vector and potential damage from ransomware attacks by automatically detecting when accounts are not assigned properly. 90% of organizations recently agreed that implementing an IGA program is an important aspect of their approach to combatting ransomware.
- **Initiate identity lockout.** Unfortunately, many organizations will face an identity-related security incident, with recent research pointing to 84% of organizations having faced an identity-related breach in the past year. When preventative measures fail, it is critical to leverage IGA to suspend access to all systems for identities that are suspected of being breached, and resume access once the threat has been dealt with.

4. Meet Evolving Compliance Mandates and Audit Requirements

As compliance and audit requirements grow more comprehensive and widespread for organizations of all shapes and sizes, there becomes more of a need for comprehensive proof that security measures are taken. Unfortunately, the amount of time that the average security decision-maker spends on generating manual reports has surged from 40% to 54% in the past two years. Further, the cost associated with inefficient manual processes to certify access, pull reports, or remediation processes is very high. Too many organizations rely on manual processes to prove compliance, and too few organizations even have controls to put themselves in a position to meet modern requirements. IGA helps organizations meet compliance mandates and audit requirements by:

Implementing Secure Controls

While compliance and audit measures will have a variety of different controls that need to be implemented based on what type of business you operate, where the business is located, who the customers are, size of the company, etc., IGA at its core helps organizations pass audits and meet compliance with the following controls, all of which are also recorded for future audit requests:

- Manage identities and access privileges throughout their tenure
- Continually verify access is required, relevant, and current
- Control access to resources based on policy
- Separate duties, or privileges to prevent toxic combinations of access
- Risk detection and alerting, including peer group recommendations for access requests

40-54%

Increase in the amount of time spent generating reports

Automating Compliance and Audit Reporting

Throughout the course of an audit, organizations likely will need to provide evidence of well-defined user roles, responsibilities, policies, and other activities that people perform in the course of their day-to-day jobs. Being able to track all of this without a centralized solution requires Herculean effort, particularly in a time crunch when an audit comes up, or a new compliance mandate is implemented. IGA is specifically designed to help organizations efficiently manage digital identities, access rights, and entitlements across hybrid, cloud, and multi-cloud environments by:

- Automatically track access requests, reviews, with full audit logs and proof
- Document access justifications and monitoring of who has access to what and why
- Seamlessly pull reports based on systems, identity types, roles, and more
- Easily produce proof of compliance to auditors

5. Confidently Undergo Digital Transformations

Digital transformation is a far-reaching term that describes processes and technologies being optimized to meet the current and future demands of organizations. Often this marks moving infrastructure, applications, and data storage to the cloud, and taking advantage of cloud economies of scale. It also likely means adopting technologies and processes to help people work from anywhere and enhancing communication in a world where the workforce continues to proliferate. However, organizations are optimizing processes and technologies, IGA can help ensure that as these new initiatives are introduced that they are properly secured and managed.

Rise in SaaS Applications, Infrastructure as a Service, and Shadow IT

Recent research points to most new applications being deployed as a Service. The reasons are straightforward; SaaS applications and infrastructure help organizations deploy quicker, lower their costs, upgrade with ease, and easily wrangle these systems to do exactly what the organization wants. In recent findings, 69% of net-new business-critical applications that were deployed in the past 24 months, were cloud-based.

As new applications and cloud-based infrastructure are introduced, it is critical to have an IGA solution in place, and itself deployed as a Service, that can connect to them to ensure that:

- Access is provisioned (and deprovisioned)
- People can easily request access to additional resources if not assigned
- Access requests are reviewed by the proper manager or administrator
- Risk scores are assigned based on the type of system
- Security teams can cope with dynamic handling of cloud applications

69%

Net-new business-critical applications deployed in past 2 years were SaaS [1]

Proliferation of the Workforce

In addition to the cloud surge, the workforce continues to spread out as digital transformations take place. This not only means remote work, but also in the amount of contracted work that takes place by people who are not full-time employees at the organization, with recent surveys showing that approximately 36% of the workforce is considered a contract worker.

As people require access from anywhere, and the number of people that require access are not considered full-time employees, an IGA solution can help by:

- Gathering identity data from a variety of authoritative sources
- Implementing role- and policy-based access control
- Automatically assigning time-based access for contract workers

[1] Advancements and Trends in Modern Identity Governance and Administration

Meet the Demands of Modern Business

Identity governance and administration solutions are a critical component for any organization that is looking to ensure that their workforce, including employees, contractors, auditors, interns, and more, is secure, efficient, and in compliance. In today's climate where there are thousands of security vendors positioning their tools as being 'the next big thing,' finding value in solutions that target big problems, but that can be deployed quickly and scaled with confidence is a critical endeavor for IT, security, the executive team, procurement, and will influence the entire business.

IGA solutions help organizations:

1. See unique, tangible return on investment as they make organizational shifts with how they enable their workforces, meet compliance, and enhance security. IGA helps by reducing time spent on edge cases and maximizes output to secure your organization's most valuable resources: people and data.

2. Enable the workforce by enabling them to be productive the moment they walk in the door and secure, by removing excess access when they change roles or leave the organization.

3. Reduce the risk of data breaches with least privilege by providing visibility into the entire organization's access rights, removing access that is excessive or no longer needed, and providing processes to stop attackers in their tracks.

4. Meet evolving compliance mandates and audit requirements by implementing secure controls to meet a laundry list of requirements, while simplifying reporting to enable teams to quickly find the information needed to pass.

5. Confidently undergo digital transformations by ensuring that SaaS applications are managed, and people can be productive regardless of who or where they are.

Omada, a global market leader in Identity Governance and Administration (IGA), offers a full-featured, enterprise-grade, cloud-native IGA solution that enables organizations to maximize efficiency, reduce risk, and meet compliance requirements. Founded in 2000, Omada delivers innovative identity management to complex hybrid environments based on our leading technology, proven best practice process framework, and best-in-breed deployment approach.

Omada

www.omadaidentity.com | info@omadaidentity.com