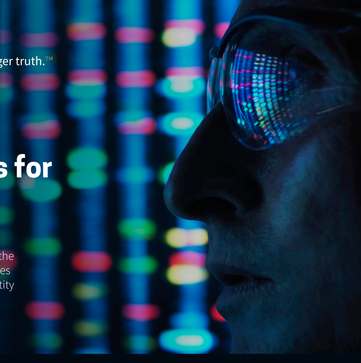
ESG a division of TechTarget

Enterprise Strategy Group | Getting to the bigger truth.™

Identity Governance and Zero Trust Initiatives for the Hybrid Workplace



Zero trust is now serving as a strategic framework for modernizing the access requirements of a hybrid workplace. Core zero trust principles such as least privilege access and role scoping are enabled by identity governance and administration (IGA) solutions. To put a zero trust approach in action, however, purposeful controls are required.

The Data Shows Zero Trust is a Top Priority

81%
view zero trust as an important aspect and thus strategic for their IGA program.

The Hybrid Workplace Requires a Focus on Identity Governance

In a hybrid workplace, employees require access to cloud-based and on-premises applications, independent of their location. This will require that organizations reexamine their policies toward identity governance and administration.

Percentage of your organization's total employees that are **remote users:**

Before COVID-19

Currently

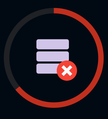

Future plans

41%
are expected to continue working remotely even once it is safe for employees to return to the office.

93% AGREE
The COVID-19 outbreak has made remote work scenarios the new normal, which requires us to reexamine our organization's policies toward identity governance and administration (IGA).

Compromised Identities Are Leading to Data and Financial Loss

Cyber-adversaries employ a range of identity-related attacks such as compromised credentials to achieve their objectives—cyber fraud, data exfiltration, and more. Many organizations lack the visibility and governance of their digital identities to determine whether they have lost data or experienced financial loss due to cyber fraud scheme.



64%
know or suspect their organization has lost data due to an identity-related cybersecurity incident in the last 12 months.

61%
know or suspect their organization has experienced financial loss due to compromised credentials employed in a cyber fraud scheme in the last 12 months.

You indicated that your organization experienced data loss or financial loss due to an identity-related cybersecurity incident. **Which of the following led to this incident?**

40%
Compromised service account

40%
Compromised a privileged account

38%
Exploit of a vulnerability to compromise a user or service account

37%
Compromised user credentials

IGA Investments Deliver Compelling Returns

Digital transformation initiatives modernize business models by retooling business operations to be more efficient. A modern, cloud-based IGA solution allows organizations to keep pace with the speed of today's digital enterprises with an adaptive approach that improves employee productivity while streamlining identity governance practices.

Thinking of your organization's IGA solution today, if you had to pick a limited number of improvements from the list below, **which would increase your organization's return on its IGA investment most?**

49%
Improved employee productivity

42%
Adaptibility to business requirements

39%
Streamlined review of segregation duties

36%
Efficient user account provisioning and de-provisioning

33%
Eliminates manual audit preparation

31%
Streamlined review of privileges

About Omada

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 achieve compliance, reduce risk, and maximize efficiency. Founded in 2000, Omada delivers innovative identity management to complex hybrid environments based on our proven best-practice process framework and deployment approach.

LEARN MORE

Omada

Source: ESG Research Insights Report, *The Role of Modern Identity Management and Governance in a Zero trust Strategy*, April 2021