PULSE 🛛 🗞 Bravura Security

Despite being vital to an organization's security strategy, only 16% of organizations have a fully realized and mature Identity and Access Management program.

Mature Identity and Privileged Access Management programs that promote Zero Trust principals are a good way to prevent hackers from gaining control of data and infrastructure.

Organizations are accelerating their digital transformation, and the rising sophistication, speed, and volume of cyber attacks is a major concern. As a result, IT security teams are tasked with access governance for user accounts across disparate technological environments while upholding their organizations' digital safety. As simple access governance can bring about a slew of cybersecurity challenges, the series of tasks or practices known as identity and access management and privileged access management offer a more secure way of handling user access to data, applications, and systems.

Pulse surveyed 100 IT security executives to understand the varying levels of identity and access management maturity based on their ability to safeguard against vulnerabilities.

THE OVERALL AVERAGE IDENTITY **PRIVILEGED ACCESS MANAGEMENT MATURITY OF THE COMPANIES** Level 4: security-first SURVEYED IS 2.12 OUT OF 4. enterprise that has already embraced zero trust principles and adopted most of the identity and access management Level 3: has reached best practices the latter stages of identity and access management systems' adoption and looking ahead to other security Level 2: has come to operations realize the need to advancements centralize security systems and adopt a consistent approach to audit and compliance Level 1: just waking up to complex security demands with a reactionary or sporadic approach to security

More sophisticated identity and access management and privileged access management processes and policies are more effective at safeguarding organizations. They employ automated tools to consistently validate users are who they say they are and provide the right level of access when they need it. However, only 9% of IT security executives surveyed have adopted a Zero Trust security strategy or evolved their program to ensure a consistent privileged access management system. Less advanced identity and access management and privileged access management programs often have more irregular user validation abilities, forgo regulatory compliance mandates, and sometimes miss or may be missing privileged access management entirely.

51% are looking ahead to centralizing their identity management principles while the more mature organizations are focused on separating identity storage from applications and systems (25%) or integrating identity-driven systems (10%).





More than half (55%) either have a single directory or simply a consolidated view of their internal and external identities. 29% separate applications from identity storage and use identity storage virtualization while only 16% have integrated all identity systems with their identity and access management system.

What is your organization's current provisioning and role management process?

32%

24%

52%

ad-hoc basis

Level 1: We handle provisioning

Level 2: We have a defined processes

deletion, and handle role management

for identity creation, change, and

during provisioning

and role management on an

Level 2: We have one consistent view of all identities (both internal and external)

23%

Level 1: We have a single, trusted directory

29% Level 3: We separate applications and identity storage and use identity storage virtualization

16%

7%

170/

Level 4: We use business role

information and system access

management for control of

and provide role-driven

information rights

Level 3: We have open provisioning workflows and

enabled advanced

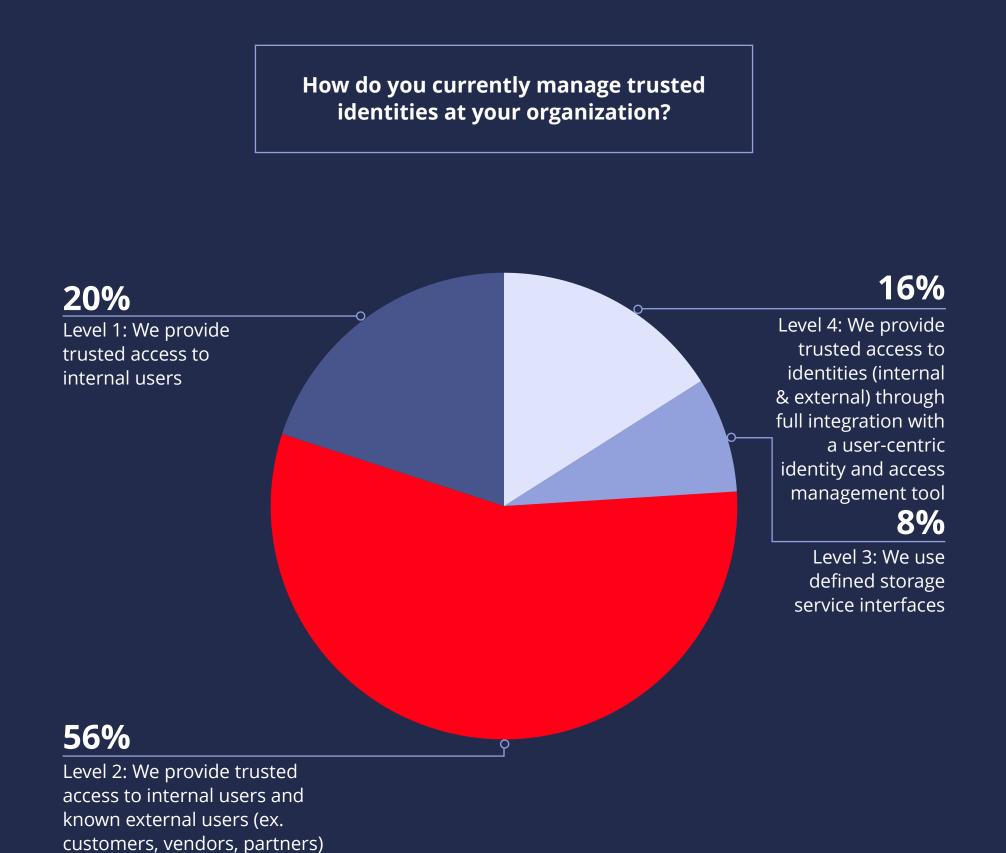
role concepts

Level 4: We integrate all identity systems with our identity and access management system

Most respondents (41%) are able to adequately manage access management on several levels: web, application, server, etc. However, only 9% of respondents have evolved their program into a consistent access management system or a <u>Zero Trust security strategy.</u>



72% of respondents provide trusted access to internal and known external users, but worryingly, only 16% use a fully integrated identity and access management tool to do so.



51% HOPE TO CENTRALIZE IDENTITY MANAGEMENT

23% of respondents have a consistent audit policy for their identity and access management processes that involves delving into log service interfaces, and 8% have a cross-system audit policy that looks at control of information and system accesses. Most organizations (50%) have ad-hoc audit procedures.

How does your organization audit and manage your identity management processes?

Level 4: We have crosssystem policies for audit and control of information and system access

Level 1: We audit at the system level, and are planning to implement a policy-based

<u>19%</u>



8%

Level 3: We use a consistent policy approach across systems and audit log service interfaces for access to different logs

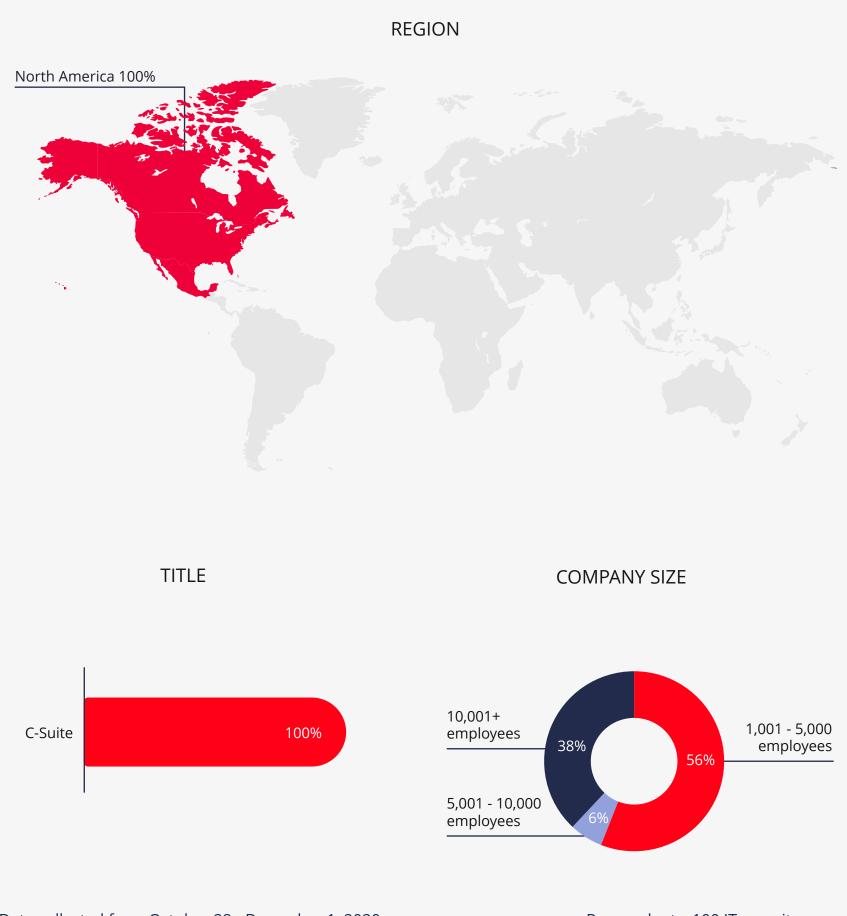
50%

Level 2: We use policy-driven control for singular systems and audit on an ad-hoc basis

15% of respondents are foregoing their identity access management compliance efforts. Meanwhile, more than half (51%) have loosely integrated their audit and compliance tools with their identity management process and 24% enjoy a greater level of automation.



RESPONDENT BREAKDOWN



Data collected from October 28 - December 1, 2020

Respondents: 100 IT security executives