PULSE | Bravura Security

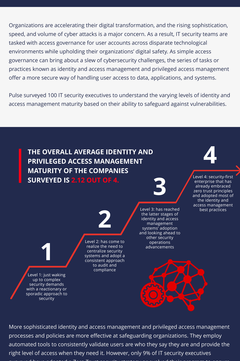
Despite being vital to an organization's security strategy, only 16% of organizations have a fully realized and mature Identity and Access Management program.

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 AND PRIVILEGED ACCESS MANAGEMENT MATURITY OF THE COMPANIES SURVEYED IS 2.12 OUT OF 4.



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%).

Which of the following is a key next step on your organization's identity management roadmap?

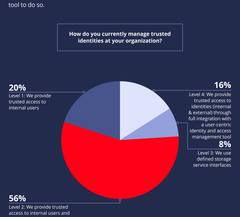
16% OF SECURITY EXECUTIVES USE A FULLY-INTEGRATED IDENTITY AND ACCESS MANAGEMENT TOOL

Although 52% have defined processes for role management and provisioning, 24% have an ad-hoc system.

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

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.

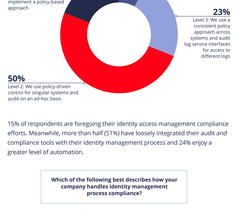
What is your organization's current provisioning and role management process?



ONLY 9% EMPLOY ZERO TRUST SECURITY PRINCIPLES

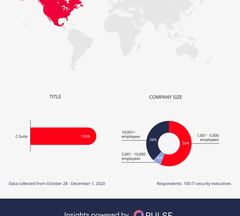
Most respondents (41%) are able to adequately manage access management on several levels: web, application, server, etc. However, only 9% of respondents have evolved their program into a consistent access management system or a Zero Trust security strategy.

How does your organization integrate system access across various applications and interfaces?



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.

How do you currently manage trusted identities at your organization?



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 processes.

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

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.

Which of the following best describes how your company handles identity management process compliance?

RESPONDENT BREAKDOWN

Data collected from October 28 - December 1, 2020

Respondents: 100 IT security executives