WHITE PAPER | MAY 2017

A Privileged Access Management Maturity Model for Digital Transformation and Automation at Scale

ca technologies

Table of Contents

Executive Summary

Challenge

Organizations undergoing digital transformations are dealing with amplified concerns around risk and security, which isn't surprising. Digital transformation initiatives inevitably result in more points of access to enterprise infrastructure that are outside of existing controls, accessible by a greater number and more diverse set of identities, and proliferated across a distributed and dynamic infrastructure.

Opportunity

Knowing your privileged users is knowing your risk. Privileged access management tools themselves must be able to support automation in the authorization process and enable scalability through support for both dynamic operations and ephemeral infrastructure—such as Amazon Web Services (AWS) administrative accounts for human identities.

Benefits

Better pinpointing attacks exploiting credential theft isn't simply a question of accumulating more data but involves incorporating better data about privileged user behavior, which can identify significant changes that represent real risk. This approach is further reinforced via integration with privileged access governance systems to enable behavioral analytics across users with comparable roles.

Section 1

Introduction

Software is now at the core of how enterprises compete and operate effectively in the 21st century. Technology has long played a pivotal role in business strategy. Digital transformation, however, has elevated initiatives to transform and accelerate the software delivery cycle and application development processes to an imperative that reaches across the business and increasingly intersects with that other pressing boardroom concern: cybersecurity.

By necessity, transformation involves change, and by extension, risk. As enterprises advance in their digital transformation journeys, their risk becomes more pronounced—unless they have a plan in place for access security and governance to move in lockstep with their initiatives and mirror the priorities of many digital transformation plans:

- Enabling automation with accountability and visibility
- Fostering speed in delivery in tandem with protection of enterprise assets
- Ensuring scale with integrated access governance and threat detection

> Ensuring visibility and accountability for compliance, security and governance while enabling flexibility for digital transformation requires a fresh and more tightly aligned approach to who—and now what in the form of applications, services, machines and things—are given the keys to the kingdom: privileged access.

In the same way that many enterprises are now engaged in defining a practical map for their digital transformation journeys, security teams need the right tools and integration capabilities to progressively automate, accelerate and scale access management and risk mitigation in line with business needs—without the need for significant new investments.

Section 2

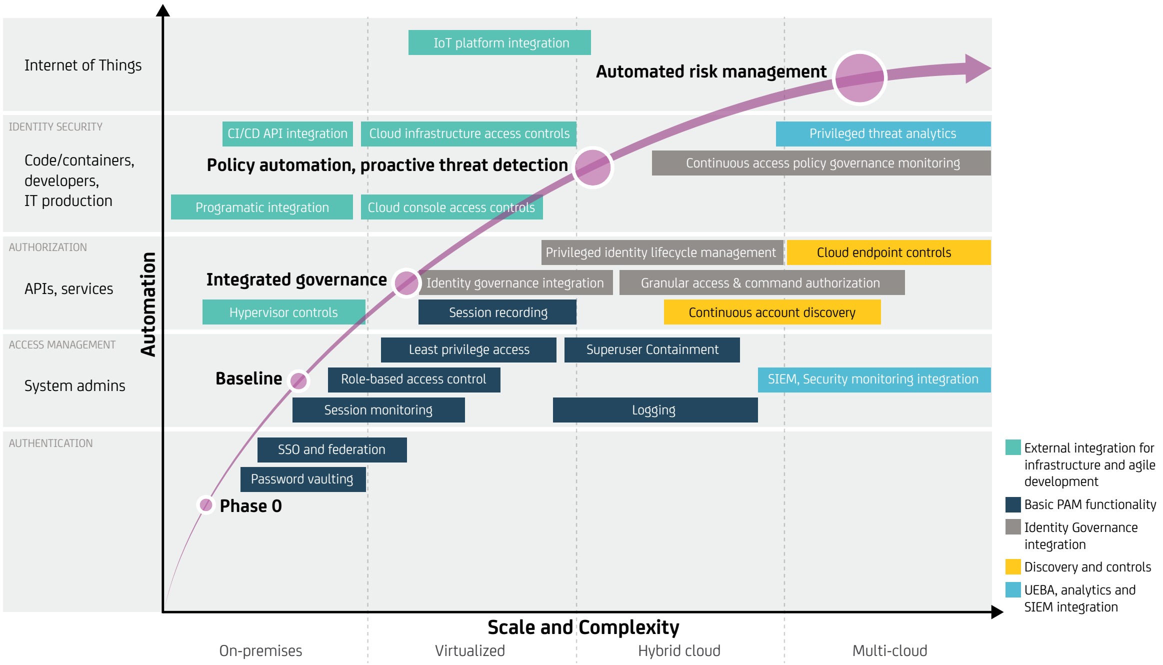
Digital Transformation Raises the Stakes for Privileged Access Risk

By necessity, digital transformation changes, accelerates and automates how code, machines and human identities interact. Risk and security concerns become more amplified because digital transformation initiatives inevitably result in more points of access to enterprise infrastructure outside of existing controls that are accessible by a greater number and more diverse set of identities than before, and proliferated across a distributed and dynamic infrastructure (on-premises, virtual and cloud).

Determining which identities should have access to specific services and resources, managing their credentials to the resources and ensuring that the access is appropriate with minimal manual intervention and based on policy is a central challenge to enabling automation, scale and speed.

Also, to come to terms with the mobility revolution, enterprises must now prepare themselves for the Internet of Things (IoT), which increases, by orders of magnitude, the volume of transactions across their infrastructure. As a result of the adoption of digital transformation tools, the who element of the access management equation undergoes a dramatic shift—even before IoT devices are brought into the mix.

For privileged access management to serve as a key enabler for digital transformation and not be a choke point, the technology and tools need to deliver a consolidated and extensible solution to the risks created by the transformation journey.


Internet of Things
IoT platform integration
Automated risk management
IDENTITY SECURITY
Code/containers, developers, IT production
CI/CD API integration
Cloud infrastructure access controls
Privileged threat analytics
Policy automation, proactive threat detection
Continuous access policy governance monitoring
Programatic integration
Cloud console access controls
AUTHORIZATION
APIs, services
Privileged identity lifecycle management
Cloud endpoint controls
Integrated governance
Identity governance integration
Granular access & command authorization
Hypervisor controls
Session recording
Continuous account discovery
ACCESS MANAGEMENT
System admins
Least privilege access
Superuser Containment
Baseline
Role-based access control
SIEM, Security monitoring integration
Session monitoring
Logging
AUTHENTICATION
SSO and federation
Password vaulting
Phase 0
Automation
Scale and Complexity
On-premises
Virtualized
Hybrid cloud
Multi-cloud
External integration for infrastructure and agile development
Basic PAM functionality
Identity Governance integration
Discovery and controls
UEBA, analytics and SIEM integration

Integrated governance

Manual approaches that rely on a human certification process cannot scale when digital transformation both expands the number of users that need privileged access outside of traditional system administrator roles, and entities that can act as privileged identities. To balance agility and security for new access scenarios—whether developers with access to privileged credentials in production, virtualized containers and hosts with authorization to data sources or administrators with super-user access to cloud services—authorization and role requests must be managed through an integrated governance process.

Policy automation

Hybrid cloud development and deployment architectures that span on-premises resources, virtualized data centers and public cloud environment can result in a fragmented, siloed approach to privileged identities. To ensure consistency (and avoid vendor lock-in), centralized governance and access control policies should be applied dynamically to environment-specific privileged accounts (such as AWS superadmin accounts).

Proactive threat detection

In contrast to managing access to a shared password for static infrastructure, such as a physical data center server, enterprises now must manage how to authorize, monitor and log access to privileged credentials for an hour, a day or even minutes, as well as assess whether the changes made or actions taken with those credentials is legitimate and doesn't elevate risk. Taking a context-driven approach that leverages machine learning and behavioral analytics can drive real-time detection and trigger risk mitigation steps, even in dynamic, ephemeral environments.

Automated risk management

The adoption of IoT not only introduces a new type of machine privileged identity in the form of IoT device controllers but the use of the technology contributes to a potentially exponentially larger number of transactions that must be explicitly authorized and monitored for potential attacks. To deal with the scale of identities and the volume of transactions by privileged identities requires an automated model that is effective at threat detection and supports mechanisms to evaluate risk and implement mitigation, without significantly disrupting business processes.

Section 3:

Achieve Integrated Governance and Policy Automation: One Step at a Time

Managing and securing privileged access in the context of digital transformation is a pressing challenge, but not an insurmountable one.

But with attackers increasingly (and successfully) leveraging privileged user credentials to gain unauthorized access, a maturity model is needed to limit policy and monitor blind posts, and to enable a proactive detection model through machine-learning-driven analytics that can reinforce the value of existing investments and improve accuracy.

To facilitate, rather than impede digital transformation, privileged access to infrastructure, sensitive systems and data should be based on a set of realistic, coordinated phases in the context of a maturity model. The most obvious action is to reduce the number of manual steps required to provision access to privileged credentials, and tie the authorization decisions to clearly defined policies.

In turn, the more tightly integrated privileged access management and identity lifecycle management processes are, the more scope security teams have to enable automation at scale. Applying automated checks to the roles and access authorizations assigned to privileged identities can help proactively flag violations, such as a developer being provided access to credentials to production code.

The important point here is that the privileged access management tools themselves must be able to support automation in the authorization process, and enable scalability through support for both dynamic operations and ephemeral infrastructure, such as AWS administrative accounts for human identities.

Many existing approaches to privileged access management are predicated on coverage of a subset of privileged identities, and were not designed with modern IT infrastructure in mind. To advance through the phases of a maturity model, enterprises need to consider how privileged access management approaches address privileged identity proliferation, distribution and transformation, based on the ability to:

- Extend governance of and visibility for privileged identities from on-premises to virtualized data centers and cloud services.
- Automate authorization of privileged access on the basis of operational requirements through integration with identity management role-based policies, rather than manual approval processes.
- Scale and integrate controls and monitoring into dynamic and ephemeral infrastructure.
- Facilitate centralized continuous monitoring and governance to identify when excessive privileges are initially granted, and trigger a remediation workflow.
- Incorporate the ability to detect and remediate as new threats evolve through machine learning and data-driven models.

Section 4:

Put Risk into the Right Context

Because digital transformation programs result in distributed networks, high rates of change, transactional volume and more privileged identities, they present a challenge to traditional, rules-based approaches to detecting misuse or theft of privileged credentials—which have already proven to be inadequate, even for existing threats.

Taking a generalized approach to privileged analytics and pushing more data into security information and event management (SIEM) systems misses important context that enables security analysts and IT operations to make the critical distinction between an inconsistency, a serious anomaly and high-risk activity that requires remediation.

Instead, what's needed is a domain-specific approach that leverages context and knowledge about privileged user roles and behavior to narrow down and respond to the needle in the haystack—the actions that represent tangible evidence of an attack or compromise.

A domain-specific approach will operate on the same principles of defining behavioral baselines. What actions privileged users are taking, what they've done in the past and the level or risk associated with actions, including the sensitivity of the target resource and how they're accessing systems. But the approach must also incorporate a graph entity relationship that puts the behavior into context.

Section 5

Know Your Privileged Users, Know Your Risk

Better pinpointing attacks exploiting credential theft isn't simply a question of accumulating more data but involves incorporating better data about privileged user behavior, which can identify significant changes that represent real risk.

This approach is further reinforced via integration with privileged access governance systems to enable behavioral analytics across users with comparable roles. When a privileged user or machine is accessing a system that is not consistent with their role and their peers, or accessing a system from a different IP address than normal and performing actions that are inconsistent with past patterns, the system can more accurately detect behavior consistent with an attack, and enable appropriate remediation.

Section 6:

Conclusion

Digital transformation isn’t an overnight process but will inevitably rely on the ability to automate both security policy enforcement for the riskiest of identities and the detection of potential threats from misuse of those privileged identities. Implementing a risk-based approach means ensuring that security controls and analytics can operate in lockstep with the digital transformation journey, and cost-effectively enable automation, scale and speed without compromise. This journey requires one to think through a clear roadmap that spans multiple years, anticipating near- and long-term requirements from a privileged access management solution and ensuring scope and scale needs at a reasonable cost of ownership through the entire lifecycle.

Security is an imperative, but its scope, scale and cost cannot become an impediment to digital transformation.

To learn more about how CA PAM can benefit your business,
visit **ca.com/pam**

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

Copyright © 2017 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. This document is for your informational purposes only. To the extent permitted by applicable law, CA provides this document “as is” without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill or lost data, even if CA is expressly advised in advance of the possibility of such damages.