EBOOK

Securing Privileged Access for the Modern Enterprise:

The Evolution of PAM

Saviynt

Table of contents

Saviynt

In the future, 2020 might well be remembered in IT circles as the year of the cloud data breach. After all, nearly 79% of CISOs responding to a midyear survey conducted by **IDC Research** reported that their organization had suffered a cloud data breach at some point in the last 18 months. Among these organizations, 89% had experienced three or more cloud breach events. And 43% had seen ten or more.

It's clear that the challenges security and identity professionals face are significant. The business case for making a move to the cloud has never been more compelling. Enterprises must deliver the rapid innovation that today's consumers expect or face falling far behind their more nimble competitors. At the same time, sophisticated and well-resourced advanced persistent threat actors are specifically targeting cloud resources. As long as attackers can adapt their strategies and techniques more quickly than businesses can evolve their defenses, we can only expect the same troubling trends to continue.

2020's events accelerated shifts to the cloud. Organizations fast-tracked their adoption of remote work, doubling down on cloud migration and digitization efforts. But rapid transformation can increase security risks, especially if done too hastily. As a result, the number of cloud misconfiguration-related data breaches has steeply increased since last year, now comprising more than 10% of all breaches examined in the **2020 Verizon Data Breach Investigations Report**. It's becoming increasingly apparent that yesterday's security tools and management models are ineffective in today's cloud-based world.

Nowhere is this more true than the realm of Privileged Access Management (PAM). According to research consultancy **Forrester**, 80% of breaches in recent years involved privileged credential misuse. Legacy PAM solutions built for on-premises infrastructure and resources are simply inadequate for managing access in environments comprised of various software-as-a-service (SaaS) applications, cloud databases, and modern development platforms spread across multiple cloud providers. Applying policies consistently and uniformly across these intricate and rapidly-changing computing ecosystems is just too complicated for tools that weren't designed for the task.

It's now crucial that security leaders build processes and solutions that will enable them to achieve secure risk-based access controls, holistic visibility, and uniform governance in a cloud-first world.

Since 2017, Misconfiguration errors have been increasing. Source: 2020 Data Breach Investigation Report, Verizon

Cloud Security is a Business-Critical Need Today

The benefits of moving to the cloud – streamlining business processes, accelerating growth, becoming better able to meet customers' needs – were once nice to have. Now they're essential for enterprises who want to retain market share and competitive advantage. Migrating workloads to the cloud reduces administrative and infrastructure costs, speeds development and time-to-market for new services, and enables anywhere, anytime access to enterprise computing resources. This is an indispensable enabler for modern, dynamic business.

But cloud environments are inherently different from legacy on-premises IT environments. These differences are responsible for many of the benefits of cloud migration, but also have the potential to create new security vulnerabilities.

- Cloud environments are scalable and elastic, which means that resources are ephemeral, making it challenging to secure them with solutions designed for static on-premises IT infrastructures.
- Cloud environments are borderless computing ecosystems in which distributed workforces can access resources from anywhere, rendering the traditional "castle and moat" model of perimeter-centric security irrelevant.
- Cloud environments are built for speed and agility, which can result in security gaps when cumbersome tools designed for on-premises architectures run periodic scans instead of continuous monitoring.
- Cloud environments enable applications to communicate with one another in real time, an integration pattern that's incompatible with legacy inter-application communications in which data gets pulled from other applications on an occasional, scheduled basis.

Real-world cloud computing ecosystems tend to be complex, requiring new tools and processes to monitor and manage them. As companies increasingly move towards hybrid and multi-cloud environments that combine on-premises systems and elements from multiple public cloud providers' offerings, complexity continues to grow. This further amplifies the challenges of maintaining visibility and control. Legacy tools not specifically designed to work in these environments are usually not up to the task. Even when they can be re-platformed for the cloud, often they'll only work in one provider's environment with limited functionality and a cumbersome architecture.

And because traditional network borders have largely dissolved in today's enterprise computing environments, the role that perimeter-based defenses once played has been supplanted by a new model for comprehensive security and risk management.

Once security leaders begin thinking of identity as the new perimeter, they'll soon discover that identities and privileges must be managed and monitored centrally to eliminate one-off configurations, simplify operational workflows and support compliance. They'll also realize that identity context is critical for making privileged access decisions – blanket permissions introduce too much risk, while blocking access without understanding when and where it's needed interrupts workflows and impedes productivity.

Limitations of Legacy PAM in the Cloud

Decision-makers who understand that identity is the new perimeter will view identity governance and PAM as among the most critical functions of their security solution stack. And the poor fit between legacy security processes and technologies and the needs of today's cloud-based computing environments is especially salient when considering PAM solutions.

Yesterday's PAM technologies typically handle privileged accounts by storing administrative accounts' credentials in a password vault. These tools then grant privileged accounts rights to access resources. Typically, these rights are neither time-nor task-limited. Instead they have what is known as standing privilege: anyone with such rights has privileged access to resources for an unlimited amount of time.

And while legacy PAM solutions scan environments at regular intervals, those intervals weren't designed to suit dynamic cloud environments where new services and workloads can be spun up and scaled down in minutes.

What's more, legacy PAM solutions were designed to handle traditional user accounts that get accessed with a username and password and attached to a human identity. Many lack the capabilities needed to handle new cloud-based identities and machine-to-machine communications. They weren't built to handle the Internet of Things (IoT), or Industrial Internet of Things (IIoT) device communications, or robotic process automation (RPA) bots. Nor were they designed to work with serverless functions, containers, or workloads-as-services, or to integrate into CI/CD pipelines.

As SaaS app adoption continues, it's important to consider how this trend effects privileged access management at the application and individual user level. SaaS solutions manage identity and access in ways that are very different from their on-premises predecessors, which is becoming increasingly problematic for companies that have made the full — or partial — transition to the cloud. Why? Most legacy PAM vendors offer application control solutions that get deployed directly to endpoint solutions via agents. This approach provides privileged access by elevating applications instead of individual users. However, in our SaaS-driven world, this approach is quickly becoming obsolete. Legacy vendors don't provide a modern means to manage these types of applications, and organizations should consider solutions that have addressed this gap in traditional PAM workflows.

Additionally, in legacy environments, users requiring privileged access to applications would often be provided with two accounts: standard access and privileged. This worked well with the perpetual licensing models widely used for on-premises applications, but adds unnecessary licensing costs for SaaS offerings that are priced according to their total number of users.

Legacy PAM also introduces additional complexity into the process of identity lifecycle management. It makes it relatively easy for orphaned accounts – belonging to terminated employees or other former users – to persist in the environment for long periods without monitoring or oversight. Furthermore, legacy PAM solutions cannot cope with the fine-grained nature of role assignments and permission sets in SaaS applications.

Due to their hefty server and infrastructure requirements, legacy PAM tools are cumbersome to manage, even in entirely on-premises environments. Add the increased operational overhead that the cloud's complexity brings, and security and identity teams will face an untenable burden.

Legacy PAM is also ill-suited to modern ways of doing business, and especially the extended enterprise. It's increasingly common for partners, vendors, contractors, and other third parties to require privileged access to an organization's data and systems – a situation that legacy vendors can't handle.

How Privileged Access is Different in the Cloud:

The primary interfaces through which privileged access to any organization's computing resources can be obtained are:

Management Consoles:

- Access assignments were traditionally static or persistent
- Privileges were typically assigned on a long-term basis
- Segregated admin accounts lead to privileged identity proliferation

What's needed is to eliminate admin accounts and define privileges in more granular and creative ways.

Instances and Workloads:

- Consist of Linux and Windows virtual machines (VMs) and containers
- Often use static operating system (OS) accounts

Persistent privileged accounts are a key attack vector in an elastic cloud environment when static OS accounts are employed.

Serverless Functions:

- Privileged roles are typically assigned within CI/CD pipelines
- Application-as-code makes finding privileges a challenge
- Code scans are time and resource-intensive

Traditional PAM tools fail to find and manage privileged-access vulnerabilities in code.

API Interfaces:

- It's not uncommon for developers to leave API keys behind in code uploaded to public repositories, creating major, lasting vulnerabilities
- Permissions assigned to APIs are rarely reviewed

It's extremely important to have an effective strategy for managing the permissions assigned to APIs in the cloud.

Cloud Databases:

- Because cloud databases lack APIs, access cannot be managed through privileged account lifecycle management solutions
- Making use of highly privileged default accounts is rampant

Because data resides here, it's especially important to protect cloud databases. Failing to do so creates enormous risk exposure that can lead to large-scale breaches.

Command-Line Interfaces:

- DevOps teams, developers and engineers use command-line interfaces frequently to interact with underlying infrastructure
- There are granular differences between the syntax and arguments used in different cloud providers' environments
- Often make use of long-term keys as authentication credentials

Should a privileged user's workstation be accessed – or their laptop stolen – the risk of exposing access keys is high.

Zero Trust and Zero Standing Privilege – New Paradigms for Modern Computing Ecosystems

Today's enterprises are embracing cloud technologies – and the dynamic business models that they enable – on an unprecedented scale. They're supporting remote and geographically distributed workforces. They're striving to provide new products and services at revolutionary speed. And they're seeking cost and efficiency advantages that only the cloud can offer. As a result, they need to apply new paradigms when thinking about how to secure these environments.

Zero Trust is a radically different way of thinking about security architectures. Instead of relying on perimeter-based defenses to police an internal "trusted" zone where network traffic and entities are deemed safe, Zero Trust practitioners consider everything and everyone to be untrustworthy. Thus, every single user, device or application must prove who they are and why they need privileged access to a resource.

As a paradigm, Zero Trust consists of three core tenets:

- Never Trust, Always Verify Explicitly
- Use Least Privilege Access
- Assume Breach

Four Aspects to Access Limitation

Least Privilege

Least privilege ensures that users only gain access to the specific tools they need to complete a task.

Temporary Access

Zero Trust grants access on a “time-limited” basis, so access is automatically removed after a given period of time.

Gatekeeping

The Zero Trust gatekeeper evaluates a user requesting access based on their identity profile and either grants access or not. Fine-grained entitlements allow the gatekeeper to grant access precisely.

Zero Standing Privilege

Zero standing privilege means that no user will ever be able to bypass the gatekeeper. No user ever has standing privilege based on location or device.

What is Zero Standing Privilege?

Zero Standing Privilege (ZSP) is a means of applying Zero Trust principles to problems in privileged access management. Originally coined by the analyst firm Gartner, ZSP means that instead of granting administrative privileges to accounts on a permanent basis, users, devices or services are granted access to privileged resources for a limited time only, on the basis of need. Each access request is decided according to predetermined policies or criteria based on behavioral analytics. ZSP is an example of a Just-in-Time access model.

Adhering to the Zero Trust paradigm means that whenever privileged access is granted, it's granted for a limited time only, and is intended to be just enough access for the task at hand. Zero Trust combines ZSP with intelligent context-based decision making that takes place every time a user or application submits an access request. It enables organizations to secure identity as the new perimeter and prepares them to defend modern infrastructures against today's threats.

Securing Privileged Cloud Access

Moving from theory to practice for the Zero Trust and ZSP paradigms requires more than a mindset shift on the part of security and identity leaders. It also demands new processes and technologies, ones that were created specifically for the task at hand. The inherent complexity and ephemerality of cloud environments renders many legacy administrative and development practices insecure. Even DevOps, which has become popular in part because it's naturally amenable to the fast-paced change that's synonymous with cloud computing, can introduce vulnerabilities into code if CI/CD pipelines aren't built with security in mind.

In particular, cloud environments require new ways of managing identity lifecycles while maintaining visibility across hybrid and multi-cloud ecosystems. And maintaining secure cloud development practices will necessitate new ways of managing secrets and privileged accounts within highly automated test and production environments. And privileged machine identities must be managed in a way that's dynamic as well as time-and function-limited. That's where PAM comes in.

PAM is designed for the cloud and built in the cloud to solve privilege management challenges specific to the cloud. It is specifically designed to work with SaaS applications as well as infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) computing models.

Purpose-built to make Just-in-Time access and ZSP paradigms enforceable, PAM automates simple decision-making about whether or not to grant particular access requests, and turns more complex requests over to a human for review. This eliminates errors while saving time and reducing management complexity. PAM is able to seamlessly incorporate risk-based business intelligence into approval workflows.

PAM natively integrates with DevOps tools as well as the communication platforms that are in widespread use in today's remote work-enabled business computing environments. It also works with security information and event management (SIEM) platforms and other security alerting infrastructures. And it integrates with identity governance solutions.

Because PAM is itself a SaaS solution, it comes with all the benefits that enterprises have come to expect from cloud-based platforms. There's no need to invest in infrastructure, management is done for you, and configuring and updating the software is easy. Deployment is simple, too. It's delivered via an agentless, zero-touch architecture and can be deployed in days even at a large organization.

CIEM vs. IGA vs. PAM

What is CIEM?

Cloud Infrastructure Entitlement Management (CIEM) is an emerging category of technologies that manage identity lifecycles and provide access governance controls across hybrid and multi-cloud IaaS architectures.

- CIEM streamlines the implementation of least privilege access controls in highly-dynamic cloud environments.
- CIEM integrates visibility and governance from Identity Governance Administration (IGA) solutions in the cloud to manage entitlements consistently.
- CIEM resolves management and oversight challenges in cloud environments.

What is IGA?

Identity Governance Administration (IGA) solutions manage digital identity lifecycles and account provisioning across SaaS solutions as well as enterprise applications that are hosted on-premises or in cloud infrastructures.

IGA centralizes and simplifies identity management and by automating account provisioning and de-provisioning and ensuring that roles and profiles are always up to date.

CIEM fills in the gaps between IGA and legacy PAM (which handles privilege management only).

What is PAM?

PAM is an integrated approach that incorporates all three sets of capabilities.

Securing Service Accounts

What are service accounts?

A service account is a privileged account that belongs to and is used by software and machines. Traditionally, credentials are static, and are rarely changed because of the administrative overhead involved. Service accounts often have access to multiple resources, and it's not uncommon for them to be overprivileged. Service account passwords are often shared among IT or development teams and re-used across multiple systems, and service account sprawl is common.

Service accounts are commonly configured with a "set it and forget it" mentality. If they are compromised, service accounts provide a means for attackers to quickly move laterally across the environment, accessing multiple systems with a single password. Their existence represents a significant potential vulnerability in any enterprise environment.

Securing cloud infrastructure requires dynamic service accounts with specific, time-and function-limited access. Development teams often leave service account keys behind in code, since doing so facilitates easier testing. And would-be-attackers are constantly scanning code repositories for these keys.

What's needed is a mechanism for delivering time-limited access. With time-limited keys, credential access can be checked out like a book from the local public library, used only for the time that it's needed, and checked back in, when it will expire.

It's also possible to deliver time-limited access automatically, relying on a credential-less approach in which access privileges are granted and revoked at predetermined times established by an administrator or security team member.

Moving from DevOps to DevSecOps in the Cloud

Relying on CI/CD pipelines is a core tenet in DevOps philosophy. But most CI/CD pipelines were built for speed and the ability to deliver dynamic updates without downtime; they weren't necessarily designed with security in mind.

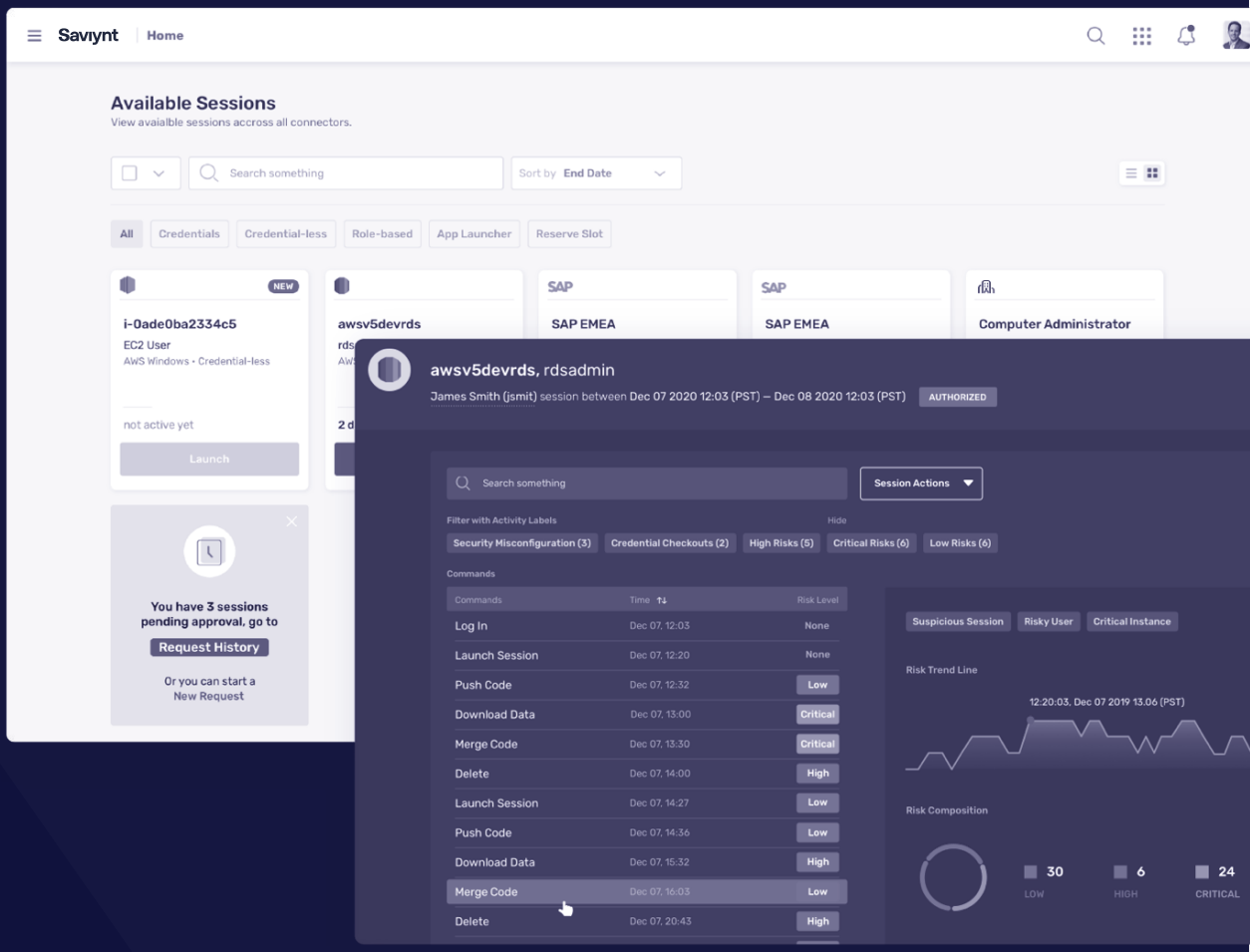
Automating whenever possible is also a core tenet in DevOps. DevOps practices strive to automate software testing as well as provisioning and deployment. Secrets management is crucial for security in DevOps environments.

PAM monitors secret distribution, limits privileged credentials' lifespans, and manages privileged accounts to minimize vulnerabilities and limit the potential for damage if compromise occurs. Because PAM integrates with the cloud-native toolsets that make up the CI/CD pipeline, it's able to limit access and provide visibility and accountability across the pipeline's entirety. Privileged accounts with rights to deploy code into the environment have been exploited in some of the most devastating recent large-scale breaches, and protecting the CI/CD process can dramatically reduce an enterprise's risks.

Securing Privileged Cloud Access

As new security challenges mount, the opportunity for new solutions to solve them is also growing. Industry analysts at **Gartner** predict that SaaS-delivered, converged platforms will become the preferred adoption method for IGA, AM and PAM capabilities by 2023, making up nearly half of all new deployments by then.

Saviynt PAM provides a frictionless user experience through its simple access request/approval process, user-friendly drag-and-drop workflows and readily configurable dashboards. It includes comprehensive auditing and reporting capabilities as well as traditional PAM functionalities, such as a password vault, session recording and keystroke logging, and command filtering. It also incorporates advanced behavioral analytics and risk-based scoring based on real-world data from an array of third-party security and risk solutions.



Are you interested in building a more proactive security posture?

Take steps today to secure your enterprise's future. Explore **our website**, schedule a **free demonstration** or **contact us** to learn more about our solutions.

REQUEST A DEMO

Saviynt

Headquarters, 1301 E
El Segundo Bl, Suite D, El Segundo, CA
90245, United States

310. 641. 1664 | info@saviynt.com
www.saviynt.com