Intelligent Infrastructure Security:

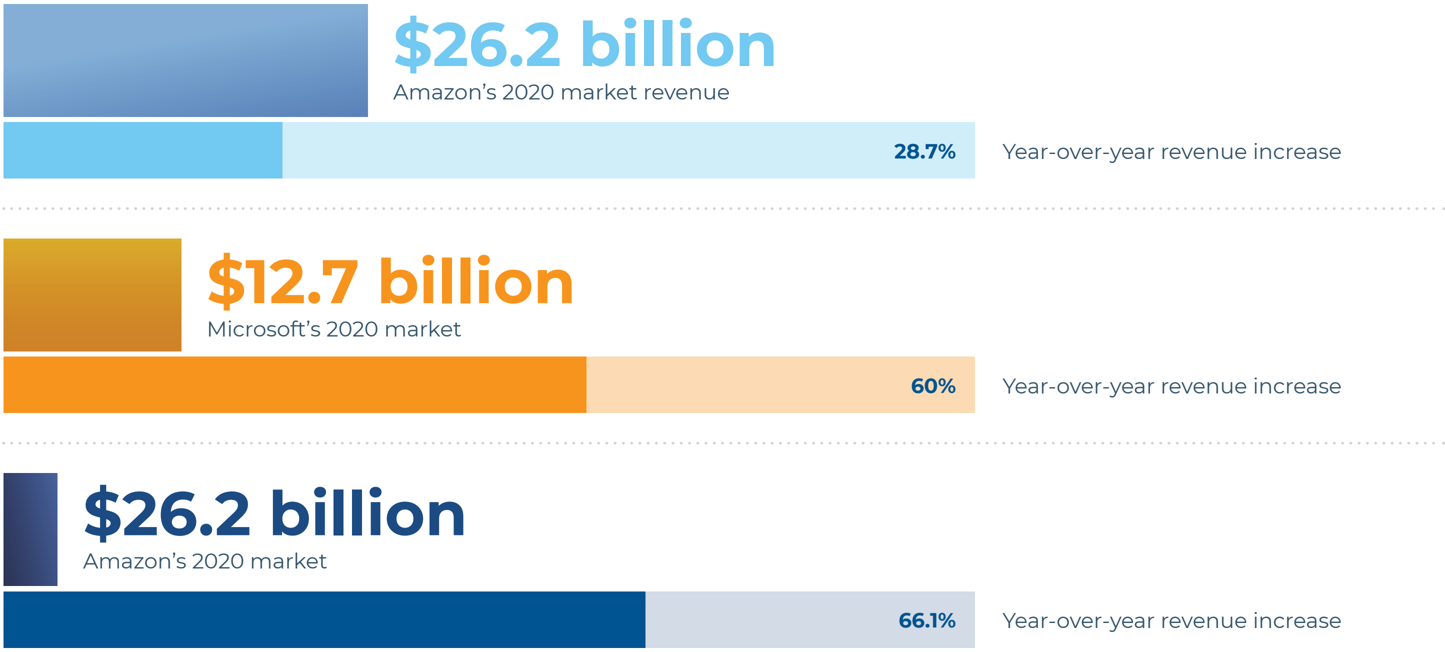
The reason for Cloud PAM in an IaaS Era.

State of IaaS Adoption

According to Gartner, the IaaS public cloud services **market grew** by more than 40% in 2020, reaching a high of $64.3 billion. Amazon outpaced the market with $26.2 billion of revenue – and an impressive 41% market share.

Microsoft was the second-largest IaaS provider, posting revenue of $12.7B last year, an increase of nearly 60% year-over-year. Data suggest that the pandemic-induced **disruption in workplace environments** increased demand to migrate mission-critical workloads.

TABLE OF CONTENTS



64%

IaaS revenue increase

Google saw a 66% IaaS revenue increase to almost $4 billion, boosted by uptake in retail, government, and healthcare. Renewed focus on “the development and deployment of cloud applications in both a hybrid and multi-cloud model,” accounted for the jump, **shares** Computer Weekly.

Going forward, IDC sees no signs of slowing: The combined public cloud market is **expected** to have revenues of $400 billion in 2025 with a compound annual growth rate (CAGR) of 28.8% during the 2021-2025 forecast period.

> "Enterprise spending on public cloud infrastructure continues to grow faster than traditional IT infrastructure segments."
>
> Andrew Smith
> IDC - Cloud Infrastructure Services

Rapid Growth Exposes IaaS Security Challenges

EXPLORING GENERAL SECURITY ISSUES

As cloud use expands, access and permissions increase. Managing these expands enterprises’ security challenges. A recent study **found that** nearly 80% of enterprises have experienced a cloud data breach – and 43% suffered ten or more!

These findings underscore security concerns from mass cloud migration in the last two years. Concerningly, traditional security controls and management practices can’t keep pace with dynamic cloud infrastructure; cloud environments simply don’t reflect the on-premises IT environments that legacy tools were designed to support.

Here are some security concerns enterprises need to consider as IaaS deployments grow.

Nearly

80%

of enterprises have experienced a cloud data breach

ISSUE #1 - CLOUD DYNAMISM

Cloud environments are scalable and elastic, which means that resources are ephemeral. Security solutions designed for static, on-premises IT infrastructure underperform in a dynamic setting.

ISSUE #2 - CLOUD BORDERLESSNESS

Cloud environments are borderless computing ecosystems. Distributed workforces can access resources from anywhere, making the traditional “castle and moat” model of perimeter-centric security useless.

ISSUE #3 - CLOUD SPEED & AGILITY

Cloud environments prioritize speed and agility. This creates security gaps when cumbersome tools designed for on-premises architectures run periodic scans instead of continuously monitoring for new instances and anomalous activities.

ISSUE #4 - CLOUD PERMISSION VISIBILITY

Complex multi-cloud environments make it difficult to discover changes within elastic workloads, accounts, and access. The result: a fragmented security posture, misconfigured objects, and over-permissioning instead of continuous entitlement and session monitoring.

ISSUE #5 - CLOUD DEVELOPER/DEVOPS ACCESS

Developers interacting with cloud infrastructure may use long-term keys as authentication credentials. Breach and exposure risks increase if malicious actors access these users’ workstations. Often, these interactions are outside of IT’s purview and thus hard to manage. Companies must maintain management agility (and a single security posture) across key tools in the DevOps pipeline, including open-source applications, with continuous discovery, monitoring, and remediation of infrastructure as code objects.

> "Multi-cloud organizations reported more security incidents in the last twelve months than those using a single platform.”
>
> Sophos
> Report: The State of Cloud Security 2020

Exploring Identity & Privilege Management Issues

When discussing cloud security, HelpNetSecurity shares how IAM deficiencies and excessive permissions **prove** most damaging. Notably, existing IAM tools don’t deliver necessary identity governance and privileged access management agility. Piecemeal solutions limit digital transformation efforts and slow the gains afforded by elastic cloud ecosystems.

However, converging IGA and PAM in a cloud PAM for workloads solution unlocks these capabilities – and helps enterprises gain visibility and reduce risk across their chosen architectures.

Increasingly, enterprises need a single solution to secure their cloud infrastructure. The solution must provide a consolidated view of user, application, and data access – as well as real-time discovery of workloads at scale.

Let’s explore additional security concerns introduced when enterprises deploy IaaS alongside outdated PAM tools.

SURFACING VISIBILITY AND PRIVILEGED ACCESS CONTROL RISKS

First, multi-cloud use compounds ongoing access governance issues. Often, this relates to poor visibility and discovery of cloud infrastructure. Enterprises must grow awareness of identities, resources, and entitlements at a more granular level. Continuous discovery and remediation of risks and/or misconfigured objects are a critical starting point.

By 2023, about

75%

of security failures will result from inadequate management of identities, access and privileges, up from 50% during 2020.

Source: Gartner

Next, enterprises must contend with over-privileging. Bad actors want to compromise accounts that allow them deeper network access (e.g., privileged accounts). These accounts provide cyberattackers means to change permissions, install backdoors, or access otherwise off-limits data.

Organizations often establish standing over-privilege to simplify account management. To resolve the results of this, companies must be able to *identify* erring accounts before they can disable them. Only then can they apply Just-In-Time and/or zero-standing privileges for cloud assets.

Additional issues stem from scheduled scans, jump-hosts, security keys, and thick clients.

Scheduled Scans: Challenges arise from infrequent, scheduled scans. In dynamic cloud ecosystems, new resources may be spun up in minutes, requiring more rapid enterprise response.

Jump-Hosts: Passing traffic through a jump-host undercuts the usefulness of identity as the new security perimeter. Enterprises should "untrust" users by default as they reduce administrative session friction – instead of trying to manage, license, and configure jump-hosts on-prem.

Security Keys: Bad actors continually scan accessible code looking for privileged access credentials. On-prem, companies must figure out how to manage, rotate, and protect these keys. A cloud PAM approach generates and decommissions these based on your policies.

Thick Clients: When run on end-user laptops or desktops, users need privileged credentials to run some of their desired applications – this raises obvious security concerns. Companies may also lack visibility into user activity and app sessions.

As each of these issues suggests, solutions that are not "built for the cloud" simply fail in highly dynamic, elastic environments. Solving these – and creating frictionless administrative sessions and limiting cloud management console access must be prioritized.

Finally, as DevOps evolves, companies need to address privileged access in the context of continuous integration and continuous delivery. Bad actors now routinely look at this vector as ripe to attack. As enterprises adopt more agile processes and speed up deployment, they need to ensure that privileged accounts with rights to deploy code don't persist indefinitely. The recent SolarWinds supply chain **attack** highlights the urgency of this – and why enterprises must solve for instances of standing privilege.

> “To maximize security and solution return, look for a consolidated platform which converges IGA, PAM, cloud security, and DevSecOps technologies.”
>
> Vibhuti Sinha
> Chief Cloud Officer, Saviynt

Solving IaaS Security Concerns

Cloud Dynamism:

- Automated real-time discovery of workloads
- Cloud security posture mgmt

Cloud Borderlessness:

- Policies
- Remove ZSP and enable JIT access
- User status (ZTAA)

Cloud Speed and Agility:

- Automated real-time discovery of workloads

Cloud Compatibility:

- Visibility, single pane of glass across all providers (whether infra, app, or data)

Cloud Permission Visibility:

- CSPM
- CIEM
- Continuous Controls Monitoring

Cloud Developer/ DevOps Access:

- Vaulting of creds/keys
- Role-elevation with only rights they need at the time they need
- AAPM for dev tools (via API calls)

Fortifying IaaS Security with Cloud PAM

Cloud PAM unifies traditionally disparate privileged access management, cloud infrastructure entitlement management (CIEM), cloud security posture management (CSPM), and identity governance and administration (IGA) solutions.

By avoiding inefficient point solutions, enterprises build in-depth understanding of entitlements – and unify governance, compliance, and security efforts across their cloud. This enterprise-wide consistency is vital to **maintain security** and compliance in the cloud.

BENEFITS OF PAM IN THE CLOUD

Security leaders are often only familiar with traditional PAM functionality. Below, we introduce Cloud PAM's access control features, and highlight additional benefits derived from an integrated Cloud PAM platform.

As expected, Cloud PAM provides critical access management capabilities including risk-aware intelligent access requests, credential and key management and vaulting, session management, session monitoring, session recording, keystroke invocation policy, and keystroke logging of privileged users.

With **Microsoft users**, for instance, these features are applied across the Azure console, Virtual Machines, Databases, Storage, and Serverless Functions (as well as providing tenant administration over Microsoft 365 applications and Azure AD.)

Transformation Tip!
While legacy PAM offers degrees of session monitoring and indirect access to credentials (channeled through a controlled interface), Cloud PAM extends this visibility across all cloud platforms, illuminating otherwise missed privileged usage.

Cloud PAM supports zero-standing privilege (ZSP) by granting access to privileged resources for a "limited time only." By validating access requests in real-time (according to predetermined policies based on behavioral analytics), enterprises embrace smart management of cloud security architectures. And removing persistent admin rights via ZSP is an essential part of a Zero Trust framework.

Four aspects of access limitation with Saviynt's Cloud PAM platform:

Least privilege:

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

Temporary access:

Access is granted on a "time-limited" basis and automatically removed after a given period.

Gatekeeping:

Admins evaluate a user requesting access based on their identity profile and grant or deny access. Fine-grained entitlements allow them to grant precise access.

Zero standing privilege:

Users cannot bypass admin controls or experience standing privilege based on location or device.

As risk awareness grows, enterprises require flexibility and sophistication in risk modeling to make better access decisions. Cloud PAM **enables dynamic risk** scoring derived from usage, behavioral analytics, peer group analysis, and risk information gathered from external applications.

Additionally, enterprises trying to solve PAM for the cloud may run into issues managing privileged access for management consoles/CLIs. Because native IAM constructs manage access to these entities via static roles, permissions, or policies, intelligent changes (for instance, when a user's job profile changes) are hard to incorporate. Cloud PAM adds intelligence to elevate/drop/change access assignments, reducing manual effort and management costs.

Transformation Tip!
Privileged access isn't just for on-premise servers and admin users. It applies to the 'risky' access identities have in cloud infrastructure and applications including DevOps tools, continuous integration (CI) and continuous delivery (CD) solutions, cloud workloads, and data stores.

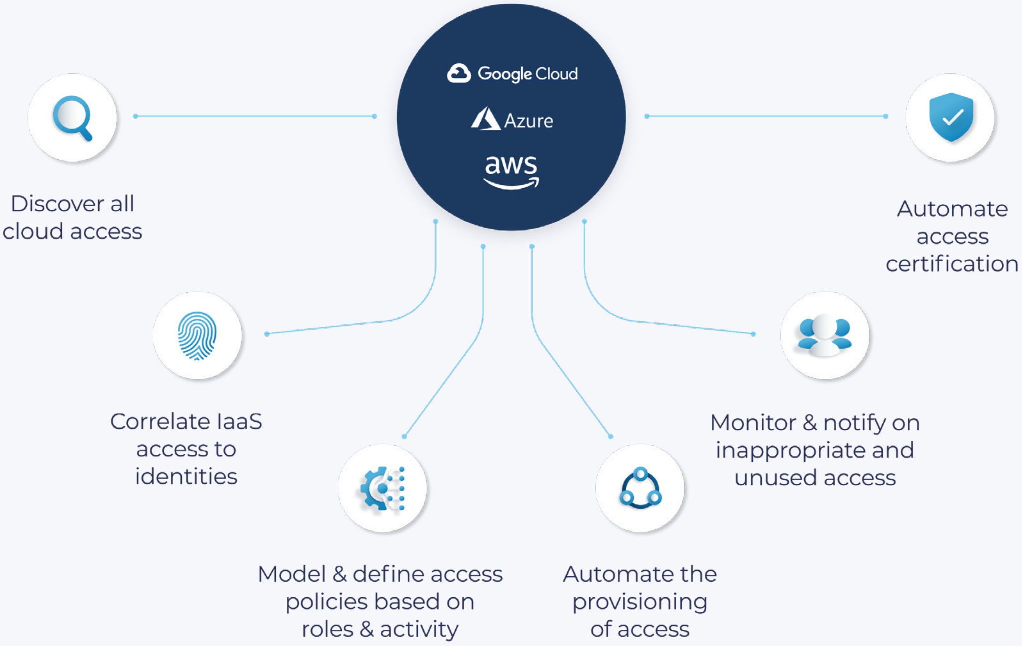
Handling cloud velocity requires enterprises to provide approved, time-bound, least privilege access to critical assets that can be monitored and audited. The missing piece? Real-time discovery of assets continually spun up in the cloud!

With Cloud PAM, companies reduce their vulnerable surfaces, unlock a consolidated view of risk, and gain visibility on misconfigurations and violations. Too often, misconfigured cloud (and on-prem) resources become entry points for data breaches and attacks.

To enhance usability, Cloud PAM provides comprehensive control libraries, mapped to industry standards. Further, Saviynt's platform **reduces** persistent access and identity sprawl using password-less access to workloads.

> "Saviynt's instance registration provides near-real-time detection of and response to potential security risks from workloads, databases, serverless processes, and other cloud artifacts."
>
> Vibhuti Sinha
> Chief Product Officer - Saviynt

Cloud PAM: Fortifying Iaas Security


Google Cloud
Azure
aws
Discover all cloud access
Automate access certification
Correlate IaaS access to identities
Monitor & notify on inappropriate and unused access
Model & define access policies based on roles & activity
Automate the provisioning of access

Cloud PAM opens the door to many powerful capabilities not available with traditional PAM.

Saviynt CPAM – Key Solution Benefits

Total Visibility & Privileged Permissions Management

- Identity lifecycle & automation management
- Auto-discovery of dynamic workloads at scale
- Credential vaulting, session monitoring & recording
- Rapid termination and access revocation
- 360° visibility in cloud deployments with single dashboard
- Proactive, continuous scanning of cloud objects
- Risk-based access certification for roles & groups
- Continuous entitlements monitoring
- Disable backdoor privileged accounts
- On-demand bootstrapping of discovered workloads

Continuous Compliance

- Enforcement and management of security policies and compliance controls
- Controls for report mapping including CIS & NIST Controls, SOC 2, SOX, FISMA, PCI, and HIPAA/ HITRUST
- Actionable controls with real-time prevention and remediation
- Support for multi-cloud providers and applications

Frictionless Experience

- Built in IGA functionality & federated group management
- Streamlined access requests & reviews
- Low TCO cloud deployment
- Drill-down dashboard view of security controls
- Business-ready interface
- Automated SoD management controls
- Meet users wherever they are: console, APIs, command line, DevOps tools

Saviynt CPAM

A COMPREHENSIVE PAM SOLUTION

Comprehensive PAM Capabilities

Password & Secrets Vault
Policy Based
Session Recording
Keystroke Logging
Full Attribution
In-Session Monitoring

Just-in-Time PAM for Risk Reduction

Time-Bound Access
Application of Least Privilege
Dynamic Risk Assessment
Standing Privilege Reduction
Migration to Zero Standing Access
Credential-Less Access

Real Time Detection & Onboarding for Identities, Assets and Workloads

Closure of Timing Gaps
Workload Governance
Application of Privilege Policy
Retirement of Embedded Passwords
Data Sprawl Reduction

Conclusion

For companies transitioning workloads to the cloud, traditional PAM underperforms. But inflexible architecture, weak visibility and context for user access, and persistent over-privileging don't have to limit your security posture.

We believe enterprises shouldn't compromise digital transformation strategies with weak identity and governance administration. Deploy a modern platform and retain the access, agility, high availability, and scalability that your cloud infrastructure offers. After all, aren't these the benefits that prompted cloud adoption in the first place?

SAVIYNT

Saviynt is the leading identity governance platform built for the cloud. It helps enterprise customers accelerate modern cloud initiatives and solve the toughest security and compliance challenges in record time. The Saviynt Enterprise Identity Cloud converges IGA, granular application access, cloud security, and privileged access into the industry's only enterprise-grade SaaS solution. Learn more at saviynt.com.

Want to talk to an identity and security expert?

Schedule a Call Today