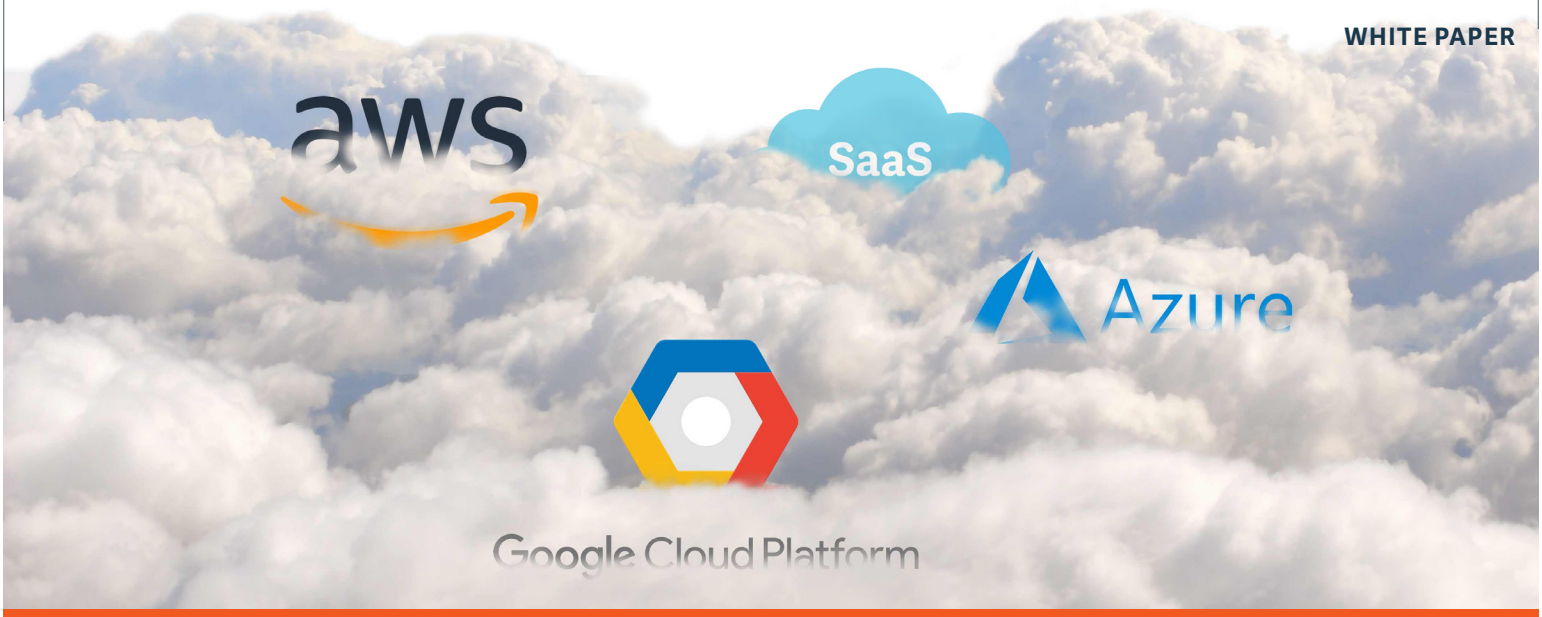
WHITE PAPER



THE GUIDE TO MULTICLOUD PRIVILEGE MANAGEMENT

Secure, Manage, & Audit All Privileged Access in a Hybrid & Multicloud World

BeyondTrust

TABLE OF CONTENTS

1 Introduction

Companies no longer heatedly debate whether or not to go to the cloud, it's now a question of how much technology and assets to deploy in the cloud and how fast. Whether or not a company leverages SaaS, IaaS, or PaaS models and hosts its own applications in a public or private cloud, their employees are almost certainly consuming some form of cloud applications and services.

The transition to the various cloud models confers many benefits and has been pivotal for companies to flexibly shift to remote access and work from home. Yet, the security that companies enjoy on-premises is often not portable to cloud environments. Or, the security enjoyed in one cloud environment may not be adequate or compatible for another cloud environment.

Today, organizations aren't locking themselves into just one IaaS or PaaS cloud environment. According to the RightScale State of the Cloud Report, almost every company (84%) that uses infrastructure-as-a-service (IaaS) or platform-as-a-service (PaaS) clouds uses more than one provider. And, most organizations employ three or more public clouds from leading providers, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

> *Multicloud, by definition, is the implementation of multiple cloud providers to support public, private, or hybrid environments for an application or service, to meet a business objective.*

Theoretically, multicloud provides some additional benefits beyond deploying to one IaaS/PaaS provider, such as:

- Redundancy and disaster recovery
- Leveraging workload portability to move workloads to the cloud environment(s) that offer the best use case and runtime costs
- Reduced latency and data privacy compliance by hosting with regional providers, which may be important for supporting multinational companies and local governments
- Cloud freedom (i.e. lack of vendor lock-in) to change hosting based on business, technology, or geopolitical concerns

Yet, there are drawbacks to multicloud environments too. For instance, each public cloud platform uses its own proprietary identity system (i.e. Azure Active Directory). Additionally, most companies are not 100% cloud – they operate with a hybrid model that includes an on-premises infrastructure, often based on legacy technology.

The benefits of cloud, multicloud, and hybrid environments can easily be scuttled by environmental complexity, siloed identity stores, and the sprawl of platform-dependent tools that must be learned and administered. This translates into heightened risks for security gaps, oversights, and vulnerabilities that can (and do) lead to breaches and outages, or other operational disruptions. And, the security interoperating between multicloud environments among multi-regions requires a new paradigm for security and data privacy, for which many organizations are ill-prepared.

As environments have become increasingly decentralized, identity has become the strongest foundation for security.

As environments have become increasingly decentralized, identity has become the strongest foundation for security. The identity challenge is the most important security problem for organizations to solve for across cloud and on-premises environments. Different cloud provider environments each require their own unique identities and have their own unique permission structures and terminologies.

Standardizing the management and security controls across the entire IT ecosystem is critical to the success of implementing your security strategy. In particular, privileged identities and privileged access pose the highest risk and represent the utmost urgency and security priority to discover, onboard, and securely manage. A compromised identity and its associated shared accounts are the single most effective attack vector for a threat actor to compromise an entire multicloud environment. This is especially true for any privileged accounts that are shared across a multicloud environment to facilitate management or the operation of the solutions or services.

Major cloud IaaS and PaaS vendors put a high focus on securing their own cloud infrastructure, yet they each acknowledge that cloud security is a shared responsibility with the customer.

THE SHARED RESPONSIBILITY MODELS & WHAT IT MEANS FOR PAM

Major cloud IaaS and PaaS vendors put a high focus on securing their own cloud infrastructure, yet they each acknowledge that cloud security is a shared responsibility – with the customer responsible for addressing the gaps where the vendor's responsibilities leave off. Of course, no two cloud platforms are equal, and each Cloud Service Provider (CSP) differs in their shared responsibility model. Likewise, each CSP differs in the native security and other toolsets they provide to their customers. Forrester Research has dubbed this shared security model as "the uneven handshake." Gartner projects that, "Through 2022, at least 95% of cloud security failures will be the customer's fault."

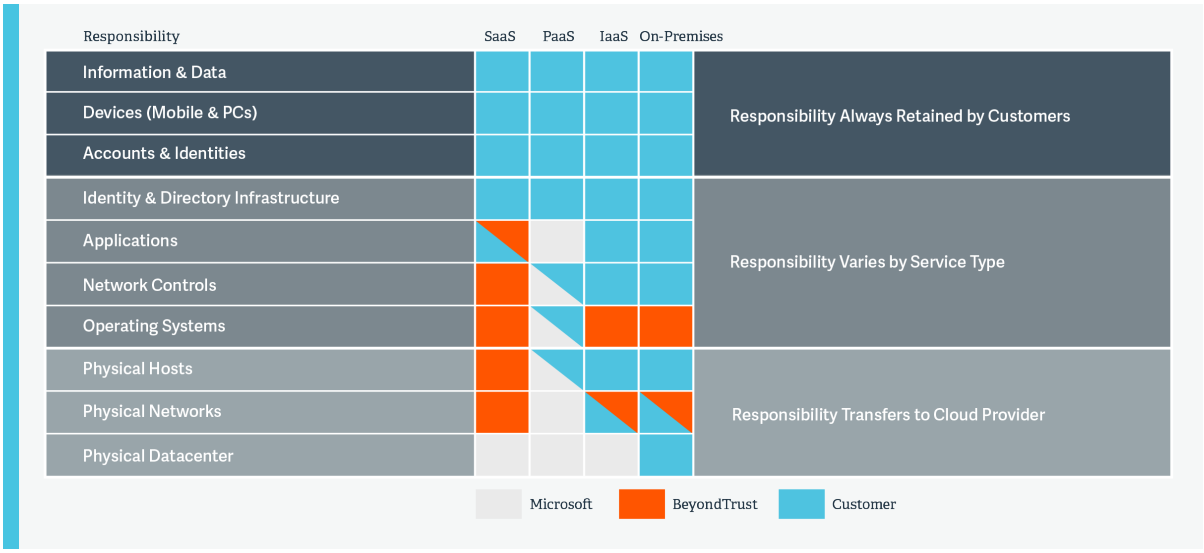


Figure 1: The Azure Shared Responsibility Model and Where BeyondTrust Can Help

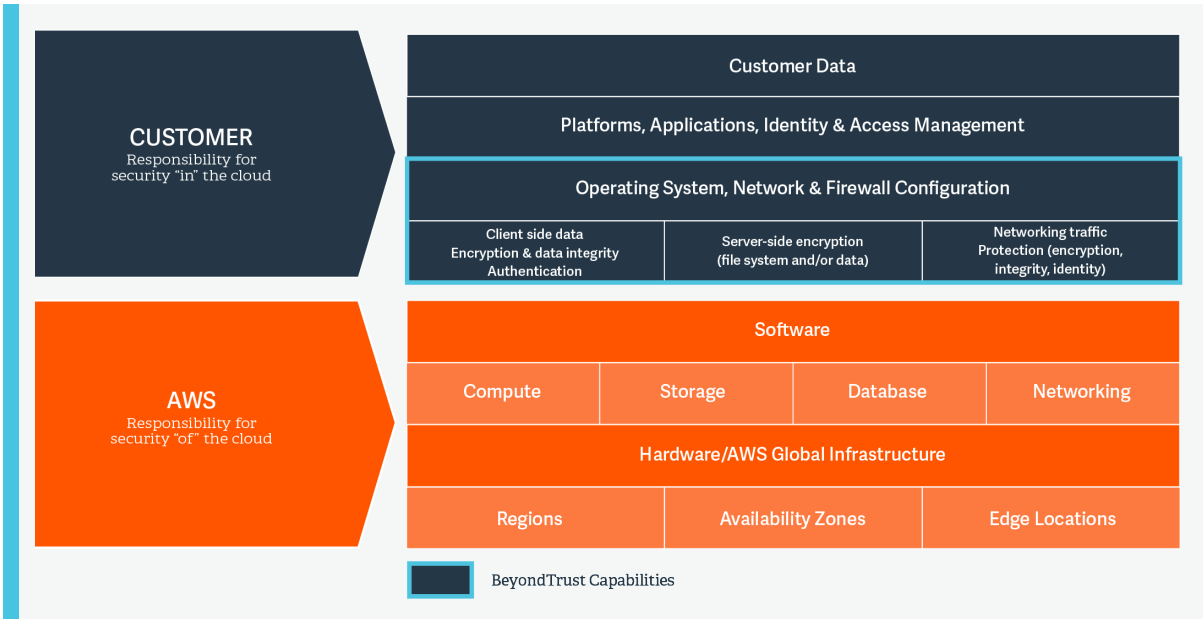


Figure 2: The AWS Shared Responsibility Model and Where BeyondTrust Can Help

Most cloud platforms (AWS, Azure, Google, etc.) provide only basic Identity and Access Management (IAM) controls, while addressing the gap in privileged access security controls is primarily left to the cloud platform's customers. Some of the most commonly used cloud and virtualization platforms only support their own native Multi-Factor Authentication (MFA) and that of a few industry leaders. Furthermore, built-in session monitoring capabilities are entirely absent from most platforms, while providing only rudimentary functions in others. Session management and monitoring is essential to ensure security, auditability, and accountability of cloud environments.

And, of course, these native tools are not applicable for the other cloud or on-premises environments where organizations may have security solutions hosted. These inconsistencies and cloud security deficiencies across cloud-based platforms create fertile opportunities for the misuse of accounts and access, which can result in the leaking of sensitive data, or potentially hijacked resources. In practice, cloud breaches are overwhelming the result of inadequate privilege management—often involving credentials, excessive privileged access, or misconfigurations.

Cloud breaches are overwhelming the result of inadequate privilege management—often involving credentials, excessive privileged access, or misconfigurations.

The scale of managing the exploding universe of privileges requires an integrated, universal approach, rather than relying on a stack of niche tools, each only helping to manage a slice of the privilege problem.

THE ELASTICITY OF THE CLOUD

The elasticity of the cloud means that cloud resources and their operating instances can be easily spun up and spun down based on task workload, testing, or demand. In doing so, new accounts—often with administrative privileges—are created at massive scale. The web-based cloud and virtualization control planes come with highly privileged accounts that rein over the entire cloud environment. SaaS applications, consumed by employees often provide access to sensitive resources and typically operate below the radar of managed resources. The elasticity of the cloud allows them to operate in an ephemeral state compared to their on-premises counterparts. This makes managing privileged access even harder since, at any given time, the instance may be present, or it may have been disposed.

The scale of managing the exploding universe of privileges requires an integrated, universal approach, rather than relying on a stack of niche tools, each only helping to manage a slice of the privilege problem. This is especially true when the elasticity of the cloud allows for rapid changes that even traditional tools for management and governance may miss.

Read this paper to understand:

- Access management gaps and privilege risk in cloud environments
- Best practices for securing privileged accounts and access for IaaS, PaaS, and SaaS
- How BeyondTrust solutions protect a variety of deployment environments—cloud, hybrid, and multicloud

Ultimately, your privileged access management strategy should ensure every privileged account, session, and asset is secured, managed, and monitored across your entire cloud infrastructure.

2 Cloud Challenges & Security Threats

Many organizations already run at high risk from over-privileged IT administrators and power users. As they migrate more workloads to the cloud, the on-premises complexity doesn't vanish. Instead, they tend to end up with the hybrid, multicloud management challenge shown in the figure below:

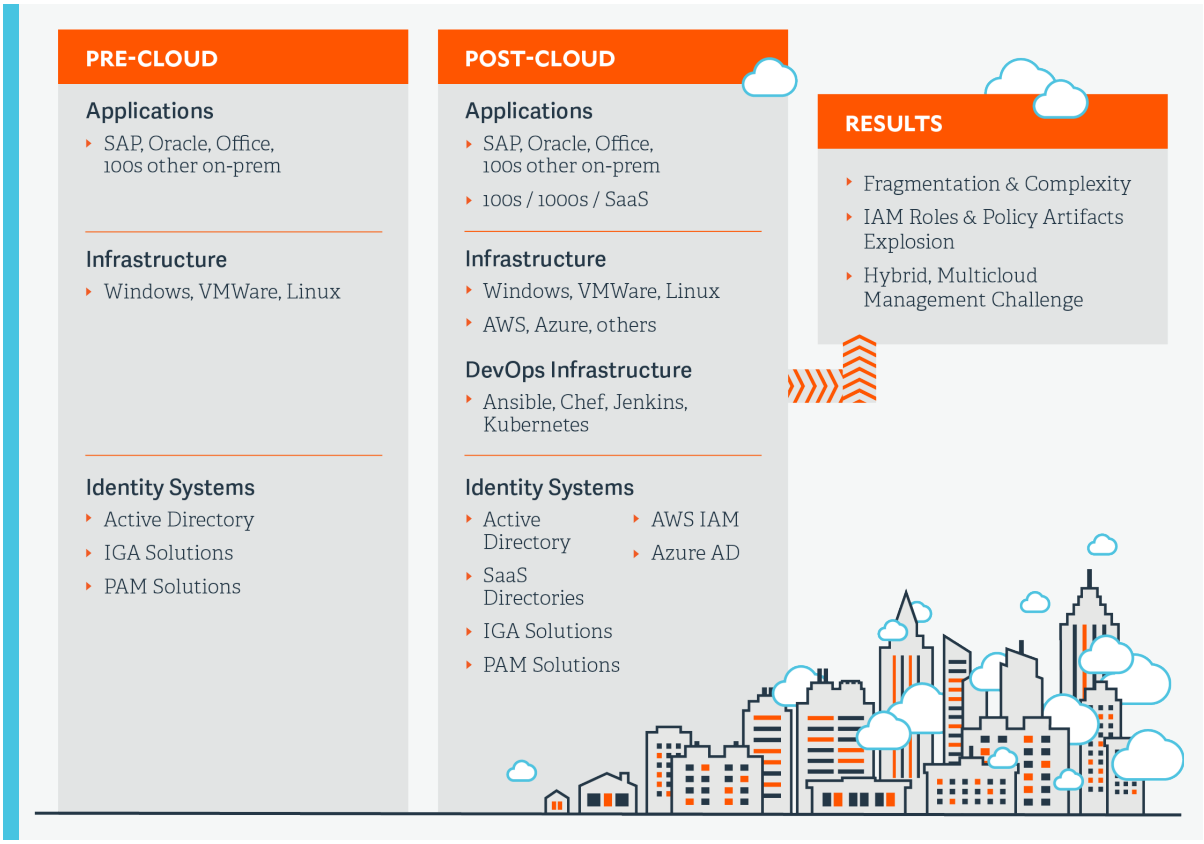


Figure 3: The Effect of Cloud Migration

In the Cloud Security Alliance's Top Threats to Cloud Computing research report, they dub their list of the top cloud environment threats as the "The Egregious 11". The chart on the following page shows how BeyondTrust PAM solutions address 10 of the 11 threats:

	CSA's Top Threats to Cloud Computing	How BeyondTrust Protects the Cloud
1	**Data Breaches**	Protects against the leading attack vectors for cloud security incidents, including credential theft, privilege abuse, compromised remote access, and lateral movement.
2	**Misconfiguration & Inadequate Change Control**	Enforces appropriate access and established workflows for change control. Also enables the security team to discover misconfigurations in privileged accounts.
3	**Lack of Cloud Security Architecture & Strategy**	Provides complete asset discovery to ensure all deployed active resources adhere to your cloud security architecture, strategy, and governance.
4	**Insufficient Identity, Credential, Access & Key Management**	Discovers, onboards, and securely manages all types of human and non-human passwords, keys, secrets, and other credentials across the cloud. Securely injects credentials into sessions without revealing the passwords, and monitors every session involved in privileged activity. Automatically rotates secrets to manage credential threats.
5	**Account Hijacking**	Robustly protects credentials and enforces password security best practices, such as complex passwords and password rotation. Prevents and mitigates attacks such as pass-the-hash, password reuse, and many others. Also, applies session monitoring and management, with the ability to pause or terminate suspicious sessions.
6	**Insider Threat**	Enforces least privilege across all users and implements advanced application control to limit lateral movement and privilege escalation. These controls restrict the activities a user can perform or execute to the minimum necessary, protecting against both malicious and inadvertent actions (errors). Command and script filtering and session monitoring/management capabilities provide additional protection against inappropriate activity.
7	**Insecure Interfaces & APIs**	Eliminates credentials embedded in code, centrally vaults all secrets using a secure API, and rotates them to ensure they don't become stale or vulnerable to re-use attacks.
8	**Weak Control Plane**	BeyondTrust significantly enhances security of the control plane in several ways: ‣ Proxies access to the control plane ‣ Eliminates unnecessary privileges and only enables the minimum privilege needed for administration ‣ Manages, monitors, and audits control plane sessions ‣ Enforces credential security best practices for all accounts accessing the control plane
9	**Metastructure & Applistructure Failures**	BeyondTrust does not provide a solution for this use case.
10	**Limited Cloud Usage Visibility**	Discovers and onboards all cloud assets. Also, monitors, manages, and audits all privileged sessions in the cloud, including for CI/CD DevOps automation.
11	**Abuse & Nefarious Use of Cloud Services**	Protects against misuse and abuse in at least these significant ways: ‣ Enforces least privilege to limit activities to only what is authorized ‣ Prevents privileged credential theft ‣ Enforces advanced application control to ensure only approved applications are running, and only with the minimum necessary privileges. Also, puts visibility and security around shadow IT resources ‣ Command and script filtering ensure only the right commands can be executed, and only within the proper context

Many of the top threats (breaches, hijacked accounts, etc.) cited in the CSA report have other root causes that are important to understand. Let's take a closer look at the significant underlying contributors to security incidents, breaches, and outages in the cloud before diving into cloud security best practices:

Lack of Control & Multitenancy

Leasing a public cloud service means organizations do not have ownership of the hardware, applications, or software on which the cloud services run. Ensure that you understand the cloud vendor's approach to these assets and their support for proprietary technology.

Lack of Visibility & Shadow IT

Organizations use, on average, about 1,935 cloud services.

CLOUD ADOPTION AND RISK REPORT 2019, MCAFEE

Cloud computing makes it easy to spin up new instances and environments, to subscribe to a SaaS application, and to create new accounts and entitlements. Unknown, or undermanaged, cloud environments present significant security risks, including breaches, data loss, intellectual property theft, and regulatory compliance issues. According to a McAfee report, organizations use, on average, about 1,935 cloud services. Users should adhere to strong acceptable use policies for obtaining authorization for, and for subscribing to, new cloud services or creating new instances.

Uncontrolled Privilege Proliferation

The sprawling number of human and machine privileges, and the dynamic nature of privileges in the cloud, presents an existential risk to cloud environments.

Privilege exploitation is a component of almost all cyberattacks today. Intentional, accidental, or indirect misuse of privileges jeopardizes the integrity of the cloud environment. Potential catastrophe awaits when the misuse involves a superuser account, such as root, or a cloud administrative console. The sprawling number of human and machine privileges, and the dynamic nature of privileges in the cloud, presents an existential risk to cloud environments.

Organizations tend to over-provision privileges to users—either to avoid privilege elevation requests for the service desk, or due to neglect in managing default privileges. Additionally, the default model for most organizations is persistent or standing privileges—meaning an account is always able to execute the privileges inherent to it.

In the cloud, there are many planes of privileges to account for across users, servers, applications, and workloads. Virtual machines can be instantiated at the scale of thousands via a few simple clicks, but the many privileged accounts generated with these instances tend to be overlooked.

Another concern is that cloud control planes (cloud management consoles), provide vast superuser access, but native tools are unable to granularly manage and audit this access. If the integrity of the control plane is undermined, it can compromise the entire cloud environment. All of this can be further compounded in DevOps environments, which, by their nature, are fast-charging, lean heavily on automation, and encompass massive scale.

Without enterprise-grade access controls, the privileged landscape presents a massive attack surface, leaving organizations vulnerable to everything from hijacking attacks, to privilege escalation, to lateral movement, ransomware, malware, insider access abuse, and more.

Poor Credential Management

Credential misuse continues to rank as the #1 one cause of breaches, according to the Verizon Data Breach Investigations Report 2020, and other prominent research. Verizon reported that compromised credentials were in involved in 77% of cloud breaches in 2019. Forrester Research has specifically cited privileged credentials as implicated in over 80% of breaches.

Password exploits are overwhelming due to insufficient credential management practices. Re-using passwords across multiple assets and accounts, sharing passwords with others, lack of password expiration, and cloud applications and DevOps code with default or embedded credentials, are just a few careless practices that leave organizations open to credential theft and account hijacking.

Due to the scale of human and machine identities and accounts in the cloud, any manual password management is simply untenable. Third-party credential and secrets management solutions that automate password security best practices are an absolute must-have.

Errors

Unintentional configuration changes, mistyped commands, and other errors are a leading cause of cloud data breaches. News in recent years has been full of breach stories around misconfigured AWS S3 buckets and other databases inadvertently exposed due to lack of password protection or other basic access controls. Far too often, these configuration errors involve simply neglecting to update default security settings.

A cloud security study by McAfee reported that, on average, organizations have 14 misconfigured IaaS instances running, resulting in an average of 2,269 misconfiguration incidents per month. Of all AWS S3 buckets, 5.5% were said to be misconfigured. Many of these misconfigured buckets include open write permissions that make them easy prey for attackers.

Malformed commands can also cause widescale disruption in the cloud. For instance, a mistyped command (now known as the "$150 million typo") by Amazon's S3 team during "routine debugging" resulted in a 5-hour long outage across multiple servers and services within AWS.

Putting guardrails around employees and assets, such as least privilege and privileged access controls (i.e. command filtering), can help prevent or curb many cloud errors and mitigate their impact.

Exposed & Unprotected APIs

Cloud applications often integrate and interface with other services, databases, and applications. This is typically achieved through an application programming interface (API). CSPs expose APIs so customers may leverage and manage cloud services. Due to the routinely exposed nature of APIs, they may be under constant attack.

API risk for an organization may increase roughly in proportion to the number of systems and resources that connect APIs together. API keys often endure unchanged for months or years. When an API is broken, exposed, or hacked, any data protected by the application may be easily accessible to unauthorized individuals by using programmatic techniques that go unmonitored by traditional user-based session recording technologies.

It's vital to understand the applications and people who have access to API data and to encrypt any sensitive information. Exploit of an API can compromise the underlying services and associated data.

Incompatibilities

IT tools architected for on-premises environments or one type of cloud are frequently incompatible with other cloud environments. Incompatibilities can translate into visibility and control gaps that expose organizations to risk from administrative complexity, misconfigurations, vulnerabilities, data leaks, excessive privileged access, and compliance issues.

Remote Employees & BYOD (Bring Your Own Device)

In recent years, telework has become the new normal based on a wide variety of environmental factors and cost-savings. Increasingly, employees and vendors are connecting remotely via unpatched routers, insecure Wi-Fi, and using personal devices that have not been hardened. Some of these devices may even be shared amongst household members.

VPN, RDP, SSH, and other protocols do not sufficiently secure remote access pathways for many of the most common cloud use cases. PAM solutions that include proxies, cloud bastion hosts, and/or jump hosts are a starting point for securing the most sensitive types of cloud access. These PAM solutions can also help secure access that occurs between endpoints or assets that may not be properly hardened or are of unknown status.

Vendor Access

Organizations may require vendors to administer on cloud servers or contribute on SaaS applications. Again, VPNs, RDP, SSH, and other frequently used remote access technologies may not be able to enforce least privilege on vendor access or monitor sessions. The BeyondTrust Privileged Access Threat Report found that the average organization has 182 vendors that connect to its systems each week, and 58% of organizations believe they have incurred a vendor-related breach.

It's important to ensure vendor endpoints are hardened and secured to the enterprise's standards and to restrict and monitor access to sensitive assets.

Unplanned Cloud Downtime

Cloud outages happen—whether due to a distributed denial of service (DDoS) attack, a misconfiguration, or other issue. Depending on how you leverage the cloud, an operational issue could take large parts of your business offline, or it might only impact one or a few services.

While any downtime hurts, it will be much more severe if it impacts your security and allows attackers to gain control of passwords or sensitive systems. That's why it's critical to implement break-glass processes so that special administration access can be granted to allow troubleshooting and to implement protective measures, such as password resets for a potentially compromised system.

3

Enforcing 7 Cloud Security Best Practices with BeyondTrust PAM

BeyondTrust's Privileged Access Management platform provides robust visibility and security across the entire universe of cloud (IaaS, PaaS, SaaS) and on-premises privileges. Our holistic, centralized, and elegantly automated approach to PAM ensures every privileged account (human and machine), session, and asset is accounted for and appropriately managed. With BeyondTrust, you can consistently discover, secure, and audit cloud instances, services, applications, assets, and identities.

BeyondTrust customers leverage our solutions to achieve consistent PAM best practices for their assets, users, and workloads across heterogeneous infrastructure. Our customers tell us this translates into these benefits:

- Improved end-user productivity and agility
- Reduced human errors/misconfigurations
- Condensed attack surface and lower rate of malware infections, breaches, and other security incidents
- Improved operational performance
- Simplified path to compliance

Outlined below are the 7 cloud security best practices enabled by BeyondTrust PAM.

1. DISCOVER & INVENTORY CLOUD INSTANCES & ASSETS

The first step in getting control over cloud assets is discovery. BeyondTrust's centralized administration and analytics platform, BeyondInsight, performs continuous discovery and inventory of assets across cloud, physical, and virtual environments.

Discovery in the cloud includes all online and offline instances, devices, servers, virtual machines, workloads, objects, users, accounts, and more.

BeyondInsight includes numerous, dedicated cloud connectors.

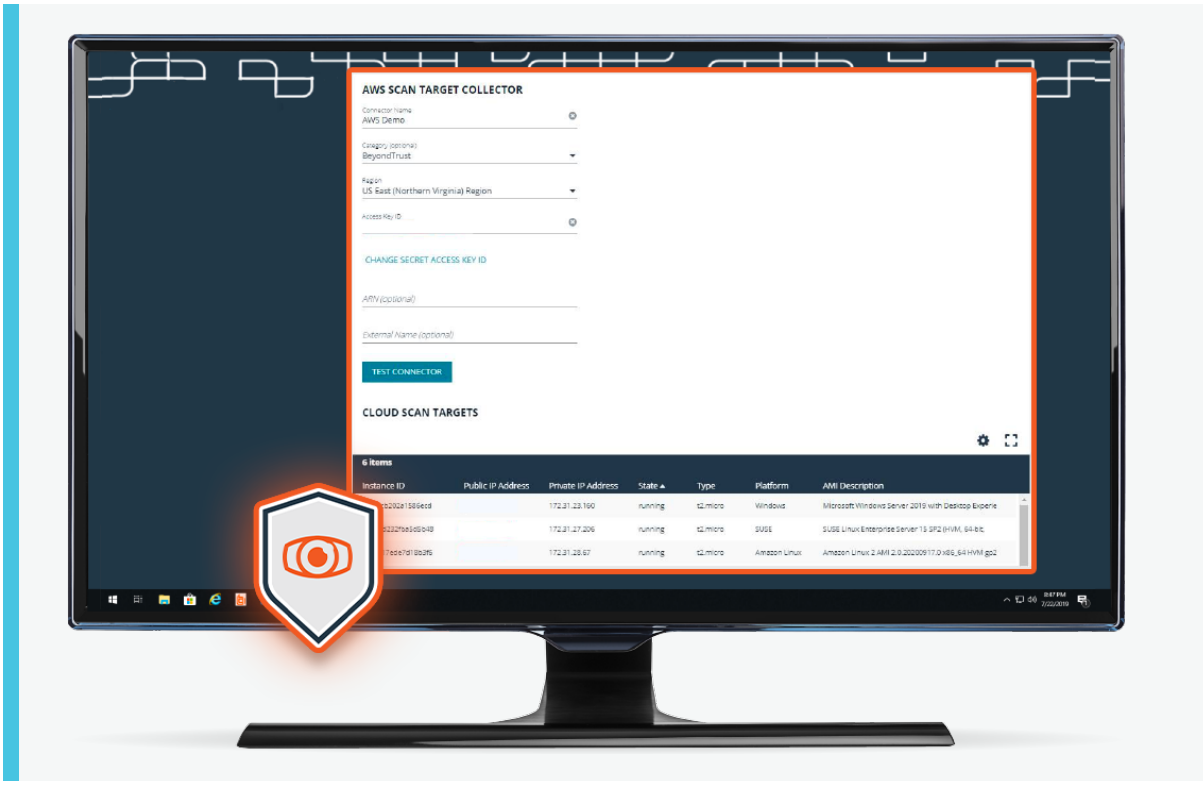


Figure 4: BeyondTrust finds and groups cloud instances so they can be properly managed.

These connectors can perform an accurate inventory of all cloud instances, regardless of runtime state. Once those instances are found, they must be managed to limit exposure.

Organizations can quickly group cloud instances and other assets into Smart Groups for consistent privilege management. Smart Groups and role-based access allow teams to assess and manage cloud instances according to an organization's unique business needs.

BeyondInsight also scans for privilege-related risks, such as default passwords.

2. ONBOARD & MANAGE PRIVILEGED ACCOUNTS & CREDENTIALS

The Cloud Control Plane (Virtual and Cloud Management Consoles and Instances)

All major public cloud and virtualization providers offer an internet-facing control plane, also known as a management console, that is used to administer over the various cloud services that these vendors provide. Cloud and virtualization control planes are governed by powerful privileged accounts, such as root. These portals may be accessible by humans, machines, APIs, and more.

Management consoles are typically used for:

- Setup, deployment, troubleshooting, and administration
- Adding, modifying, and deleting servers
- Configuration of services
- Basic security controls, such as authentication and access management
- Monitoring and reporting on usage
- Integrations/APIs
- Billing & purchasing

An exploit on the control plane can easily undermine the integrity of the entire cloud environment. Therefore, it is absolutely critical that the control plane's privileged administrative accounts are managed to security best practices by a third-party PAM solution.

These web-based cloud management consoles offer tremendous scale, which has considerable security implications. For instance, each of these new instances, no matter how ephemeral, has privileges that need to be managed and monitored. The AWS Console, for example, is also a de facto procurement system, enabling administrators to instantly order additional systems, storage, and network resources.

Just as with their IaaS and PaaS counterparts, SaaS solutions provide a web-based management console that is accessed by users and admins. This applies everywhere from SalesForce, ServiceNow, and GitHub to social media accounts, like Twitter, Facebook, and LinkedIn. Often, these admin accounts are shared between users, which multiplies the attack surface and also muddies the audit trail of who did what.

To adequately address cloud security and compliance, the native IaaS, PaaS, and SaaS access controls need to be augmented or replaced by a PAM solution.

Privileged Accounts

IT admins, developers, software engineers, and other technical workers routinely require privileged access, while non-IT users may occasionally need elevated access to cloud or on-premises applications, or to change settings on their desktop.

In IaaS environments, the non-human accounts—such as machines, applications, and scripts—that need privileges to properly function may actually outnumber human accounts.

The passwords, secrets, keys (SSH Keys, Azure Application Keys, etc.), and other credentials for all these human and non-human accounts need be secured, managed, and audited. API Access Keys rank as one of the most sensitive credentials to protect. These keys are often embedded in cloud applications or other code, where they are vulnerable to exploit by attackers.

BeyondTrust Password Safe unifies privileged password and privileged session management, providing comprehensive discovery, management, auditing, and monitoring for any privileged account/credential—human, application, machine, etc.

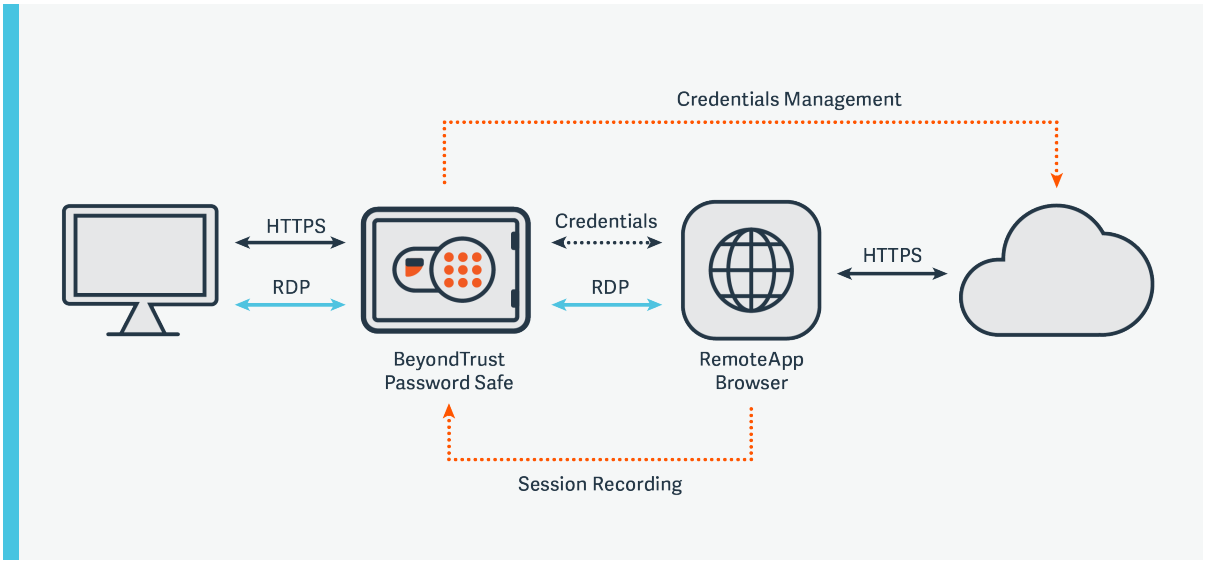


Figure 5: Password Safe discovers, onboards, monitors, and manages access to cloud credentials.

BeyondTrust Password Safe:

- Auto-onboards and vaults privileged user (Azure AD, AWS IAM, etc.), application, service account, machine, and other human and non-human credentials (passwords, secrets, SSH keys, etc.) across cloud and on-premises
- Enforces appropriate credential usage according to your policy, such as password complexity, uniqueness (different passwords per asset, account, etc.) expiration, rotation, check in and check out, and other rules
- Identifies and eliminates default and hard-coded passwords in cloud management consoles, applications, build scripts, and code and replaces with API calls or dynamic secrets
- Enables a simple workflow process for password check-out and injects passwords into sessions, never revealing them to the end user.
- Provides a complete workflow for cloud management platform and device access, including an approval process for when administrative access is required; also allows you to leverage your native clients (PuTTY, Microsoft MSTSC, etc.) to maintain your existing workflows
- Manages and monitors all privileged sessions and ensures all privileged activity is associated with a unique identity
- Provides secure, audited management of break-glass Administrator accounts
- Integrates with existing identity providers, cloud and on-premises identity stores, and MFA platforms

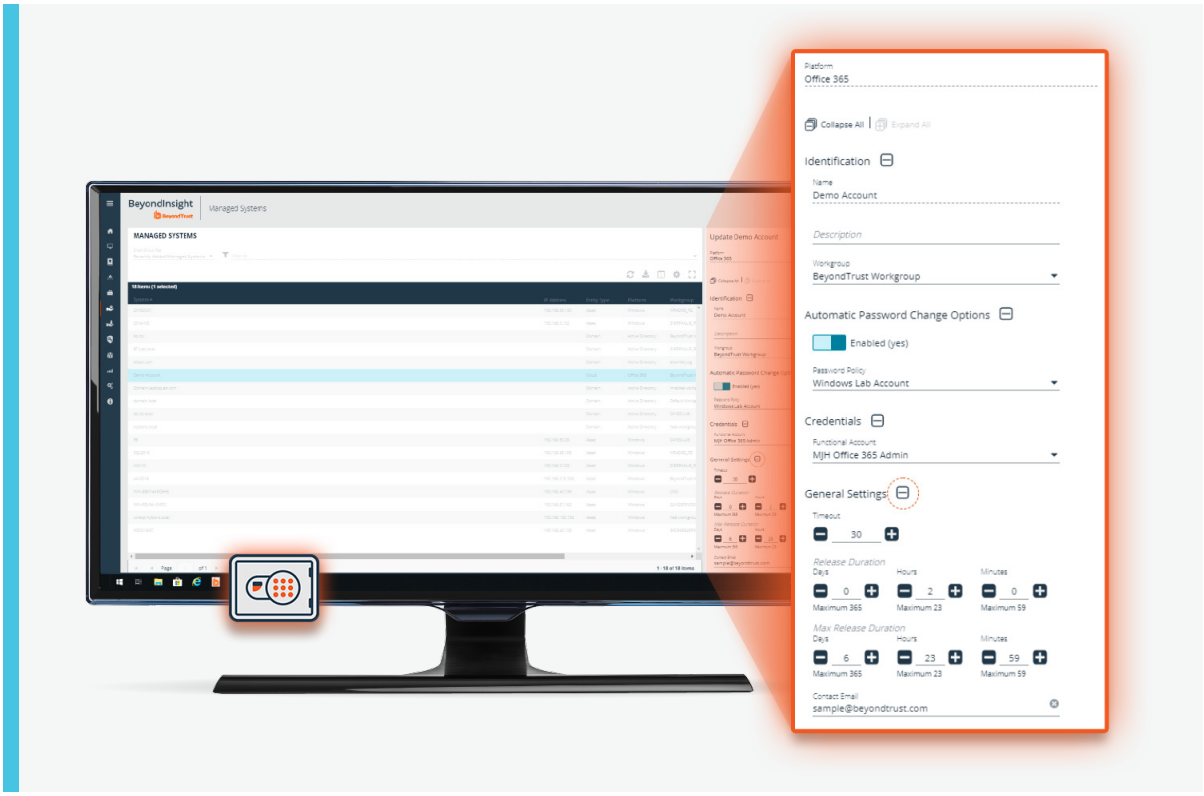


Figure 6: Password Safe enables the secure storage and management of cloud credentials.

3. SECURE, BROKER, & AUDIT ALL REMOTE ACCESS

Administrators and other users need a secure way to effectively control and audit resources in the cloud. Because the cloud control plane is used to manage the entire cloud environment, securing, controlling, and monitoring all access is absolutely critical.

VPNs, RDP, and SSH simply don't allow for the granular access controls, visibility, and auditing that is imperative for the most sensitive types of cloud and remote access. Home-based users, potentially using personal devices, and vendor access further complicate the security picture and present untenable risks for these types of remote access protocols.

In recent years, BlueKeep and DejaBlue attacks shined a spotlight on this issue because cloud-based virtual machines are the most convenient targets for these exploits. BlueKeep and DejaBlue permit attackers to break into systems via RDP and gain root-level access, without any credentials. And two-factor authentication is no protection. With "blue" attacks, the game is over before RDP even thinks about checking your password, let alone 2FA.

While you can now patch vulnerabilities exploited by BlueKeep and DejaBlue, those attacks delivered sobering confirmation that many widely used remote administration protocols are inappropriate for direct exposure to the Internet. Remote access to server instances hosted on Azure, AWS, and other clouds absolutely must be made available without exposing an RDP or SSH listening port to the Internet. The same goes for remote access to the cloud control plane.

The ideal solution is to create a secure gateway to cloud server instances and control planes by restricting traffic through a hardened proxy server, jump host, or bastion host. This essentially segments and isolates remote access traffic for your cloud, to protect your overall infrastructure. Segmentation is itself a core principle of least privilege and zero trust implementations.

Leveraging a zone approach to isolate instances, containers, applications, and full systems from each other protects resources and helps prevent lateral movement attacks, as well as bleed of one environment into adjacent ones.

By placing a proxy between the end user and the target system, you can prevent the privileged password, or its hash, from ever touching the user's endpoint. Managed privileged credentials must be programmatically injected and audited. The privileged credentials are used to open a session between the hardened appliance and the system being administered. Proxy technology also allows full-fidelity recording of privileged sessions for the capture of metadata and to make them searchable.

While most cloud providers require inbound ports to be opened to enable remote access, you can further improve security by leveraging a solution that only requires outbound ports for remote access.

How BeyondTrust Securely Brokers & Audits Access to Cloud/Virtualization Control Planes & Compute Resources

Many organizations utilize cloud access service brokers (CASBs) as a proxy for all cloud traffic. Usually implemented using reverse proxy (or a VPN connection), all internet-bound network traffic is funneled through these proxies to centralize access control and auditing. Most CASBs, however, deliver only generalized policies.

BeyondTrust provides two options that improve on CASB functionality, which we will now explore.

Leveraging BeyondTrust Secure Remote Access Solutions as a Bastion Host

The BeyondTrust Secure Remote Access solution enables organizations to secure, manage, and audit vendor, internal privileged user, and helpdesk remote access activity, both on-premises and in the cloud—without the need for a VPN or other tunneling technology. The solution enables secure session management, with the ability to proxy access to RDP, SSH, and Windows/Unix/Linux hosts.

Our Secure Remote Access solution can also be leveraged as a bastion host for cloud-based access. The solution's Web Jump helps address privileged access security gaps in the cloud by inserting a secure layer for authenticating to these systems with full session monitoring capabilities. The solution provides a Chromium-based browser embedded in a bastion host (proxy) that can access a web-based resource remotely. The BeyondTrust solution can automatically inject secure credentials—completely invisible to the end-user and without ever revealing the password—to access those resources in a controlled manner.

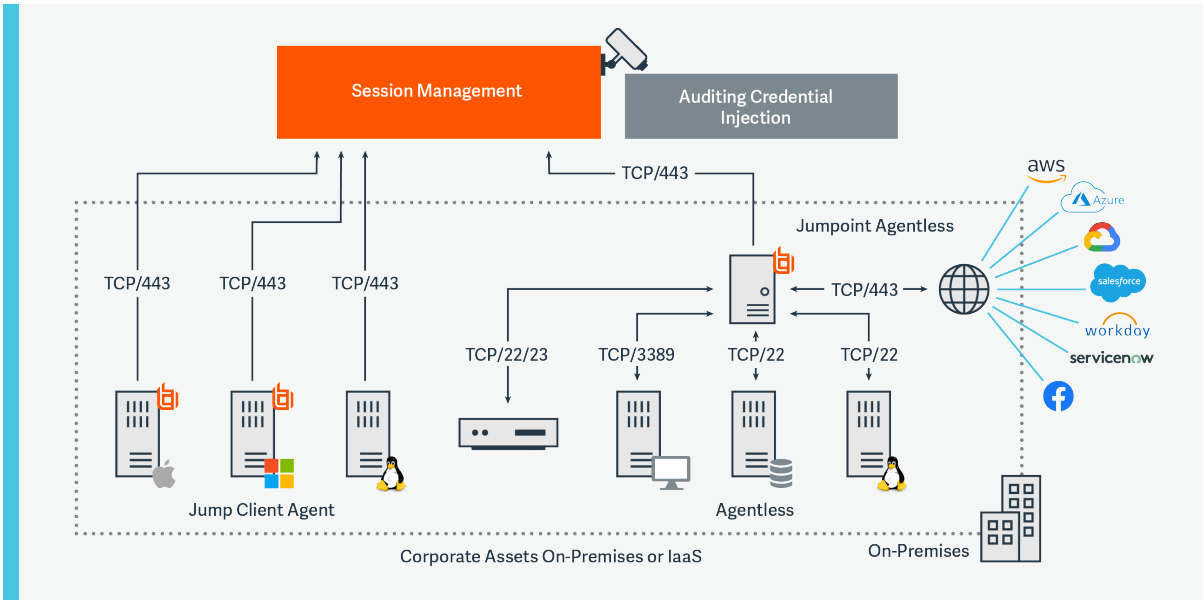


Figure 7: BeyondTrust Privileged Remote Access (part of Secure Remote Access) Architecture

BeyondTrust Privileged Remote Access (part of Secure Remote Access) offers several options for remote access into cloud environments:

1. A native agent which allows legacy access protocols to be disabled entirely (eg. RDP/SSH)
2. An agentless approach that leverages a bastion host and keeps all legacy traffic locally
3. The option of an embedded Chromium browser for virtual browser isolation — allowing for a safe/lockdown browser with credential injection and video recording

By applying access control lists (ACLs) and other security best practices, organizations can ensure that the Web Jump interface is the only authorized source into cloud resources. This prevents remote access sessions from being initiated from inappropriate sources and users. This setup blocks any rogue or suspicious activity, while forcing all user activity through a trusted browser.

The bastion host setup also obviates the need for a virtual desktop environment to act as terminal server or gateway just to host a browser to make this connection. BeyondTrust Secure Remote Access can also be leveraged for on-premises, web-based administration solutions to enforce proper network zoning and segmentation in the cloud. In addition, organizations can extend access to important assets in the cloud, or deep within an organization, using Jump Points and adhere to security best practices by limiting network traffic and ports to only authorized sources and applications.

BeyondTrust Secure Remote Access provides the following capabilities:

- Secures network architecture where all traffic is encrypted via HTTPS. No port-forwarding or firewall reconfigurations are necessary
- Provides access to untrusted third parties, giving them only the right level of access into your environment, mitigating the threat of a potentially infected system laterally spreading
- Integrates with BeyondTrust Password Safe to securely inject managed credentials into remote access sessions, applications, and web pages to add additional abstraction layers between the user and privileged secrets
- Provides access to web pages, such as the Azure or Office 365 portal, through a locked-down Chromium browser that supports automatic web credential injection and logs session recordings
- Provides detailed audit records and alerting, as well as integration into identity providers (such as Azure) with built-in MFA

Leveraging Privileged Password Management as a Cloud Access Service Proxy

Alternatively, BeyondTrust Password Safe can act as a cloud access service proxy for privileged accounts, enforcing access controls and auditing at a deeper level than is available via native controls and common remote access protocols.

Password Safe utilizes a secure jump server with multi-factor authentication, adaptive access authorization, and session monitoring for access that needs to traverse trust zones. This enables IT teams to segment access based on the context of the user, role, application, and data being requested. This setup reduces risk by minimizing the "line of sight" access that attackers have into internal systems. With Password Safe, for instance, you can lock down management of Azure/O365 Global Administrator roles by restricting network traffic to only the solution itself.

The diagram below depicts this capability:

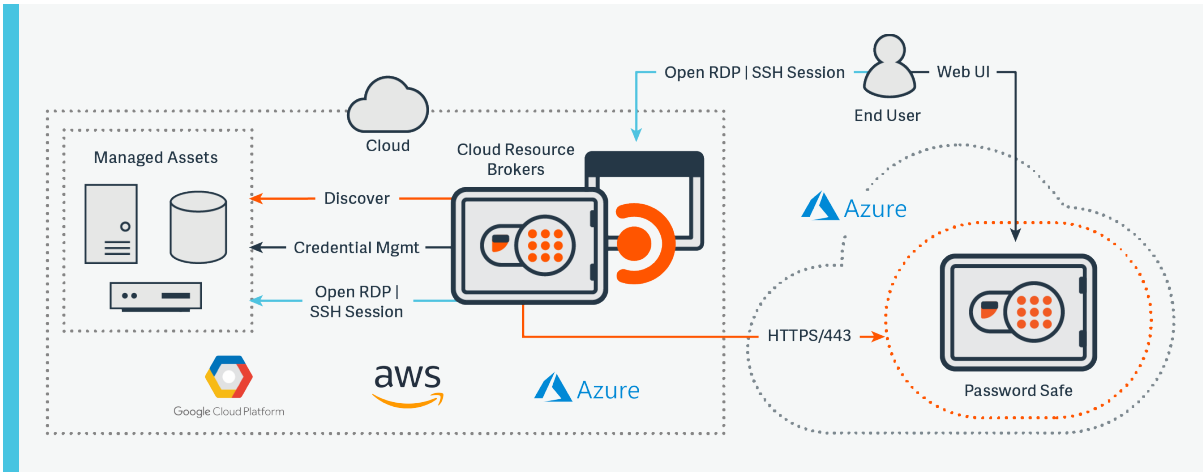


Figure 8: BeyondTrust Password Safe Architecture

Utilizing Password Safe as a single tunnel to cloud sessions enables tight control and audit of all activity. The image above depicts how the on-premises and IaaS implementations of the BeyondTrust solution works. However, Password Safe Cloud would utilize a "Resource Broker" between Password Safe and the targets and allow the implementation to be delivered as a self-contained service.

Password Safe capabilities extend beyond typical CASBs by:

- Enforcing privileged password management best practices – password discovery, vaulting, rotation, etc.
- Monitoring, managing, and recording all sessions, with the ability to lock and terminate suspicious sessions
- Providing additional context to user access requests by considering the day, date, time, and location
- Implementing advanced segmentation by routing all remote access sessions through the Password Safe proxy

These capabilities ensure that all access to cloud assets is segmented, protected, monitored, and audited.

4. ENFORCE LEAST PRIVILEGE & JUST-IN-TIME ACCESS CONSISTENTLY

Privileges are necessary for IT admins and other users to do their jobs and for applications and other non-human accounts, systems, and assets to properly operate. It's well established that administrator privileges, or even temporary admin accounts, provide attackers with the means to land and expand within the cloud environment. Privilege that is not properly locked down also runs afoul of an increasing number of regulations. By limiting privileges to the minimum necessary, you can achieve drastic results in enterprise risk reduction, and improve compliance posture.

The problem is that employees, vendors, other users, and non-human accounts are routinely given excessive access and permissions to cloud systems and data that can go unmonitored. Additionally, the administrative management consoles for cloud, virtualization, and DevOps platforms administer over the entire cloud infrastructure and provide superuser privileges that can be exercised at tremendous scale. For instance, the consoles provide the ability to instantly spin up thousands of virtual machines—and each of these comes with its own privileged account and privileged security gaps that need to be managed. Restricting access to and within the control plane is paramount to having a secure, stable cloud environment.

Native cloud (i.e. Azure PIM), open source (i.e. sudo), and ad hoc tools are often used by IT teams to "get by," but these are all inadequate in addressing privileged access security for server and desktop environments.

Typical shortcomings of these tools include:

- Inability to get up and running in just hours, with user-based policies
- Lack of an integrations framework allowing organizations to quickly create integrations
- Lack of advanced application control and protection
- Inability to monitor activity within scripts or third-party applications
- Deficiencies in oversight, forensics, and auditing: lack of file integrity monitoring, log security, or the ability to record sessions and keystrokes for audits
- Lack of broad platform support—meaning many overlapping tools are required to administer across a heterogeneous environment

BeyondTrust Endpoint Privilege Management delivers the world's most comprehensive privilege elevation and delegation (PEDM) capabilities. The solution can securely delegate tasks and authorization across cloud, hybrid, virtual, and on-premises environments, including AWS, Azure, Google Cloud, and more. The solution is comprised of the following two products:

- Privilege Management for Windows & Mac
- Privilege Management for Unix & Linux (also includes Active Directory Bridging)

BeyondTrust Endpoint Privilege Management is a preventative endpoint security solution, allowing you to easily remove admin rights and perform passwordless administration. The solution dynamically provides permissions only to the systems, applications, and data that users need – not the human account. BeyondTrust enables you to not only restrict and secure access to the cloud control planes, but to also finely manage the privileged activities performed using agent or gateway technology in the data plane.

BeyondTrust Endpoint Privilege Management also includes advanced application control and protection capabilities. This means our customers can implement the standard features expected of application control solutions, while also gaining advanced protection against zero-day threats and even fileless attacks that may leverage legitimate applications.

Leading analysts, such as in Gartner's Critical Capabilities Report for PAM, have also recognized BeyondTrust as having the broadest approach for applying just-in-time (JIT) privileged access management. Rather than having privileges enabled and always-on (also called persistent or standing privileged access), thus always ripe for misuse or abuse, BeyondTrust enables privilege elevation on an as-needed basis and for only the finite duration of time needed.

A dynamic, JIT access model reduces the threat surface, sharply curtailing the ability for privilege escalation attacks and lateral movement, while minimizing the risk of threats, such as phishing and ransomware, to land and expand. JIT PAM for user accounts is also a natural administrative model for serverless environments. For more information on how BeyondTrust enables JIT PAM, download The Guide to Just-In-Time Privileged Access Management.

Additionally, passwordless administration removes the needs for any passwords to ever be used in this JIT model. Passwordless administration refers to granting privileges to the application and not the user. This eliminates the need for your users to authenticate with an admin privilege and removes the ability for admin privileges to be exploited, by associating privileges with tasks.

Cloud errors play a huge role in cloud breaches (i.e. bucket leaks) and outages. BeyondTrust's solution can prevent and mitigate these types of errors through the combination of its least privilege and command filtering capabilities. For instance, BeyondTrust Privilege Management for Unix & Linux has a policy language that can elevate commands via least privilege and inspect all the options and switches (including what is embedded in scripts). This allows it to identify malformed or inappropriate commands.

With Privilege Management for Unix & Linux, users are assigned commands they are allowed to execute, they can run elevated without the need for sudo or root, and the contents of the commands can be checked for potentially malicious activity. All of the commands typed, scripts executed, and screen output is logged for future auditing and forensics. Correctly applied, these capabilities can protect cloud environments from experiencing outages, such as the one resulting from "the $150 million typo" that was mentioned earlier in this paper.

BeyondTrust Endpoint Privilege Management protects cloud endpoints, users, and assets by:

- Enforcing true least privilege across all cloud assets, users, endpoints, and sessions
- Enabling passwordless administration by dynamically elevating access as needed for tasks and applications
- Exercising granular control over applications, commands, files, and scripts to prevent or mitigate errors, eliminate privilege sprawl, and reduce the attack surface
- Replacing or augmenting native or open source tools (i.e. sudo) by layering on capabilities that resolve the security, auditing, and administration deficiencies of those tools
- Monitoring and indexing all privileged sessions, including all commands typed, for quick discovery during audits (Privilege Management for Unix & Linux only)
- Consolidating audit logs and centralizing reporting across all your server domains
- Auditing and reporting on changes to critical policy, system, application and data files to prevent tampering
- Proactively reducing exposure to advanced fileless malware and trojans through context-aware Trusted Application Protection
- Providing QuickStart (workstyle) Templates, which enable customers to achieve a least privilege posture within days (Privilege Management for Windows & Mac only)

5. SECURE DEVOPS INFRASTRUCTURE

DevOps tends to exacerbate the most dangerous areas of risk in the cloud. With agility and self-service core traits of DevOps, it's unsurprising that shadow IT is rampant. Users in these environments also tend to have high levels of privilege. Passwords are commonly embedded in tools, code, and in repositories, like GitHub.

CI/CD and DevOps toolsets, such as Jenkins, Chef, Puppet, and Ansible commonly leverage and interface with cloud resources. The consoles for these tools, their interactions, and the service accounts created, must all be managed and monitored at the velocity and scale required of DevOps practices.

Managing credentials and applying the principle of least privilege are important to control authorized access to development, management, DevOps, and production systems, while granting only required permissions to appropriately build machines and images.

BeyondTrust enables and secures DevOps environments in the cloud in the following ways:

- BeyondTrust Endpoint Privilege Management enforces granular least privilege across each privileged session and account in the DevOps and CI/CD toolchain. The solution's application control also helps put visibility, control, and security around shadow IT.
- BeyondTrust DevOps Secrets Safe enforces password security best practices for privileged users and DevOps pipeline orchestration processes, while enabling peak DevOps agility. The solution can remove hardcoded credentials embedded in service accounts, applications, and code and replace them with dynamic secrets.
- BeyondTrust Password Safe can discover and secure DevOps secrets and other credentials, while also enforcing boundaries between dev, test, and production systems, providing added protection via segmentation. The solution also layers on advanced monitoring and management over every privileged session, providing unsurpassed scalability for concurrent managed sessions.

6. MONITOR & MANAGE OF EVERY SESSION INVOLVING PRIVILEGED ACCESS

Session monitoring is absolutely essential to ensure security, auditability, and accountability over privileged activity in cloud environments. Yet, native cloud capabilities for session monitoring and management are either absent, immature, or infeasible to implement.

While some techniques can monitor other protocols or API-based access to the cloud, only session monitoring can capture the real-time behavior of users. And, if the users know they are being recorded (or shoulder-surfed electronically), the deterrent alone may be enough to curb some malicious behavior.

Regulatory compliance mandates are increasingly requiring that certain types of sessions—such as privileged sessions on sensitive systems—have full auditability (logging, activity monitoring, etc.). Session monitoring provides the future documentation needed to review, analyze, and determine if the session was authorized, contained malicious behavior, and was appropriately conducted. This includes video recording of graphical sessions, full text output for terminal-based sessions, and keystroke logging of user input.

BeyondTrust solutions for Privileged Password Management and Secure Remote Access can enable organizations to monitor and manage sessions at the scale of hundreds or thousands of concurrent sessions.

BeyondTrust capabilities around session monitoring and management include:

- Monitoring and managing any session involving privileged access—whether in the cloud, on-premises, employee, or vendor
- Recording and inspecting in real-time (for pattern matches) all text on the screen, processes launched, titles in application frames, and keystrokes, while automatically excluding manually entered passwords and secrets
- Pinpointing anomalous sessions and automating workflows to terminate, or pause/lock the session until a determination is made whether or not that activity is appropriate
- A critical list of out-of-the-box capabilities to monitor for potentially inappropriate database commands, lateral movement, sensitive operating system commands, and other suspicious behavior

7. BRINGING IT ALL TOGETHER

The more complex your infrastructure, the more important for your team to have fewer, but more powerful, tools to administer and manage. Simplifying your management approach helps reduce complexity and errors, while making it easier to see and address any gaps. It's also essential that your tools are compatible and integrate with the rest of your IT and security ecosystem. A standalone tool with no integration, realistically, has a finite life until that problem is resolved.

Unify Privilege Management Over Your Entire Cloud & On-Premises Environment

At BeyondTrust, we simply call this Universal Privilege Management (UPM). Our solutions are designed to continuously discover, secure, and audit every privileged account, asset, and session - everywhere.

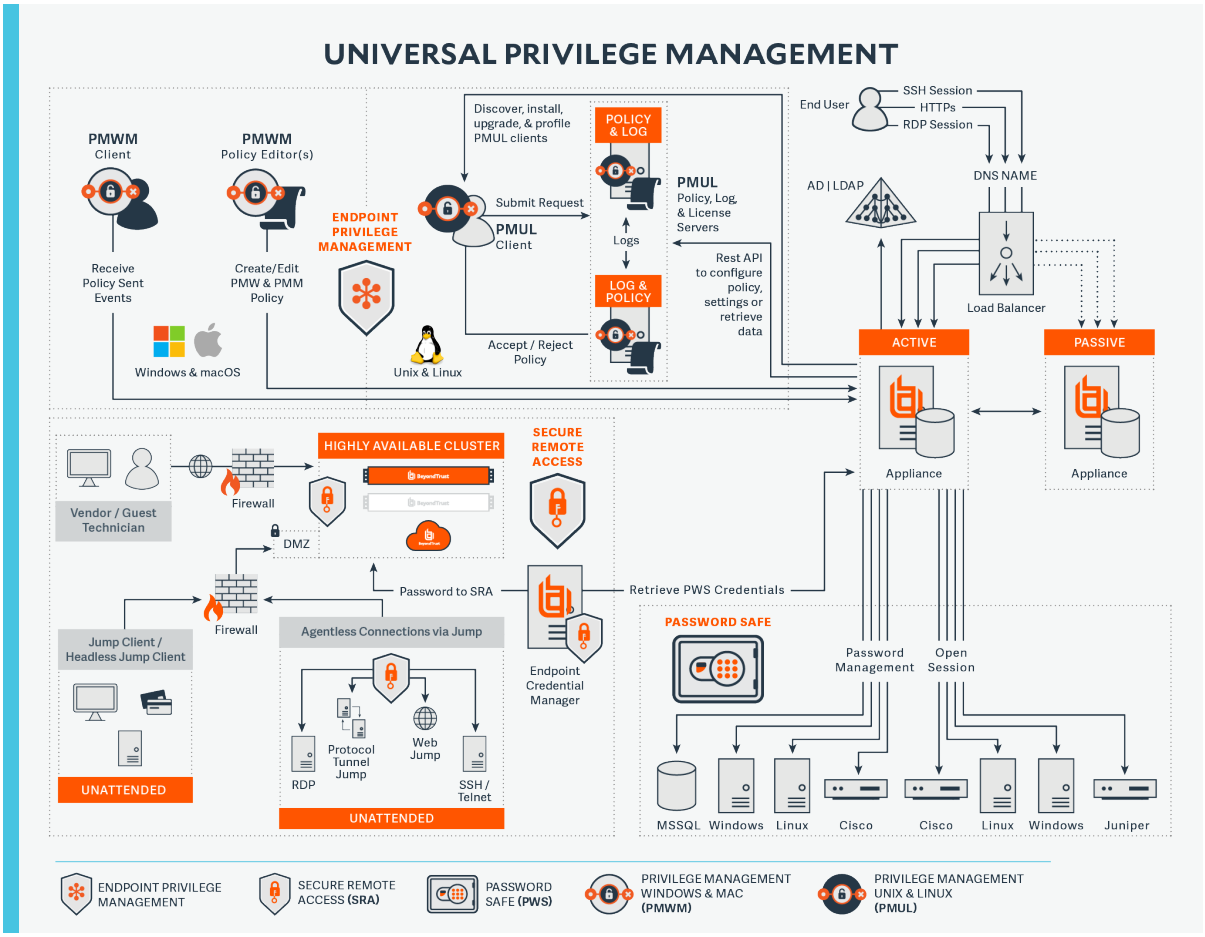


Figure 9: BeyondTrust PAM Architecture

Utilize the BeyondTrust PAM platform to consistently manage your entire universe of privileges across on-premises and cloud assets.

BeyondTrust provides the world's broadest platform coverage as part of our universal privilege management approach. The following is a partial list of cloud-based environments that our solutions support:

IaaS / PaaS

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud
- RackSpace
- GoGrid

SaaS

- Microsoft Office 365
- Box
- Dropbox
- Salesforce
- Workday

Social (SaaS)

- Facebook
- Instagram
- LinkedIn
- Pinterest
- Twitter
- XING

Unify Management of Privileged & Non-Privileged Identities

While IAM solutions, including those native to the various cloud environments, offer such capabilities as single sign-on, user provisioning/deprovisioning, role-based user management, access control, and governance, they lack the ability to granularly manage privilege and monitor session activity.

Bi-directional IAM and privileged access management integration is imperative to holistically manage, secure, and audit identities, accounts, and roles to ensure activity is appropriate. BeyondTrust integrates with numerous identity management providers, enabling organizations to benefit from holistic visibility and management of identities.

Additionally, BeyondTrust provides Active Directory (AD) Bridging capabilities via our Endpoint Privilege Management solution. AD Bridging enables single sign on across Windows, Unix, Linux, and macOS environments by extending Microsoft's Active Directory to non-Windows platforms, enabling SSO.

Integrate with the Rest of the Security & IT Ecosystem

An investment in BeyondTrust is an investment in your entire technology stack. Our solutions integrate and have synergies with major ITSM, SSO, MFA, IDAM (via SCIM), SIEM, RPA, DevOps, threat intelligence, and other tools.

4

Fast-Track Cloud Protection with the BeyondTrust PAM Platform

Organizations that correctly scope their cloud deployments and identify and address gaps with enterprise-class tools will continue to reap the many benefits of the cloud. BeyondTrust addresses crucial cloud security, visibility, and management gaps and can help secure your cloud-based resources and identities from privileged attack vectors.

BeyondTrust protects your entire cloud environment by:

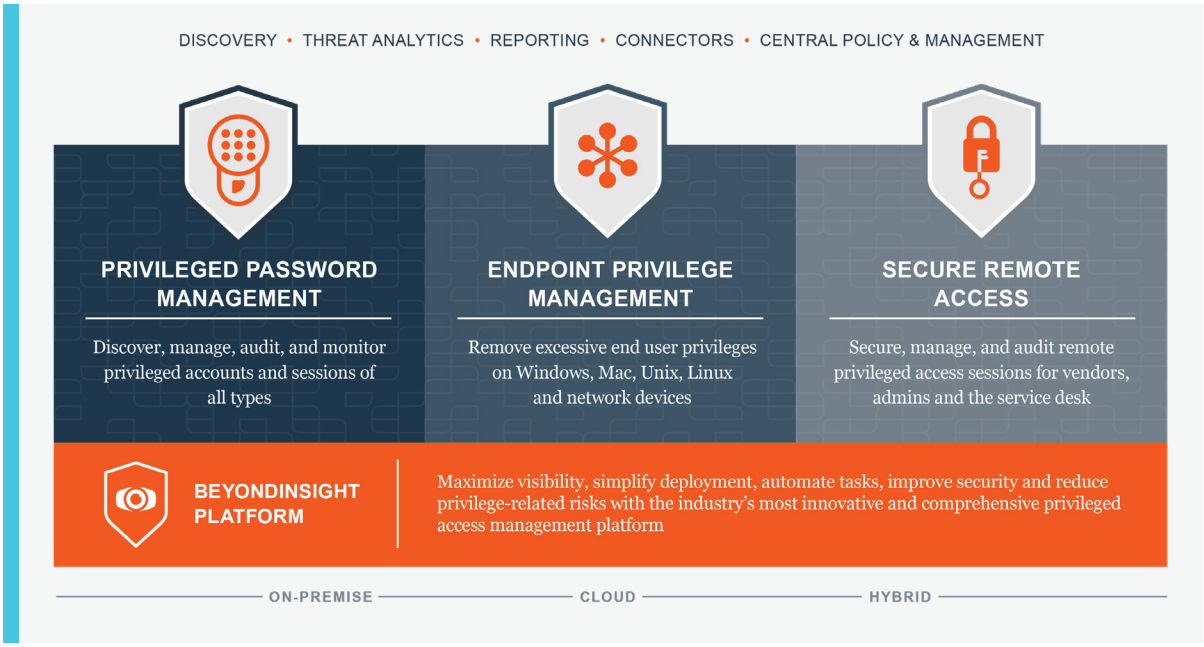
1. Continuously discovering and onboarding privileged accounts and cloud instances
2. Enforcing credential security best practices across every human and non-human account, including implementing zero trust architectures
3. Reducing the number of users with privileged access
4. Restricting the privileges any user, application, service, or asset has for access and automation
5. Preventing and mitigating human-based errors in privileged access
6. Condensing the window of time during which privileges can be executed, and thereby abused, by applying the principle of just-in-time access
7. Enforcing segmentation of the cloud environment and securing/proxying remote access to cloud management consoles and to computing resources
8. Robustly managing and monitoring every privileged session and providing certification for regulatory compliance
9. Providing a single, centralized platform for all privilege management activity that is architected to integrate with the rest of your security and information technology ecosystem

Finally, unlike other privilege management solutions that can take many months to properly configure, BeyondTrust solutions help you rapidly reduce risk.

BeyondTrust solutions can be deployed in the cloud, on-premises, or via a hybrid model to address your organization's unique needs. Privileged Password Management, Endpoint Privilege Management, and Secure Remote Access can each be deployed individually, or you can combine multiple BeyondTrust solutions for maximum privilege control and risk reduction. The solutions can each be managed via the BeyondInsight platform, which centralizes administration, reporting auditing, and more.

The BeyondTrust PAM Platform

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions.



The complete BeyondTrust solution allows you to address the entire journey to Universal Privilege Management to drastically reduce your attack surface and threat windows.

By uniting the broadest set of privileged security capabilities, BeyondTrust simplifies deployments, reduces costs, improves usability, and reduces privilege risks.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network. Learn more at

beyondtrust.com