Protecting and Enabling the Cloud
With Integrated Privileged Access Management and Vulnerability Management Solutions

An 8-Step Best Practices Approach
Table of Contents

Table of Contents .................................................................................................................. 2

Executive Summary ............................................................................................................... 3

Cloud Security Best Practices ................................................................................................. 3

- Discovery and Inventory of Cloud Assets ........................................................................ 3
- Scan for Vulnerabilities and Misconfigurations ................................................................. 5
- Gain Accountability and Control Over Passwords to Virtual and Cloud Management Consoles and Instances .................................................................................................................. 6
- Segment Networks by Using a Cloud Access Service Broker (CASB) ......................... 9
- Enable Privilege Management in a Hybrid Cloud Environment ..................................... 11

The BeyondTrust Best Practices Solution for Protecting and Enabling the Cloud .......... 12

- Mapping BeyondTrust Solutions to Secure Cloud Best Practices ................................. 13

The PowerBroker Privileged Access Management Platform ............................................. 14

Next Steps & Cloud Security Infographic ............................................................................ 14

About BeyondTrust ............................................................................................................. 15

Executive Summary

According to Gartner, 80% of cloud breaches through 2020 will be due to customer misconfiguration, mismanaged, credentials or insider theft.

As cloud ecosystems evolve, and IT perimeters expand and become more complex, it’s increasingly critical to ensure visibility and security across hybrid cloud environments. Unknown, or undermanaged, cloud environments can create significant security gaps that open up networks to security breaches, data loss or corruption, intellectual property theft, and regulatory compliance issues. How can organizations securely enable the cloud for business agility, and unify security controls with their on-premise assets without sacrificing control?

This guide describes specific use cases where BeyondTrust’s integrated privileged access management solutions and vulnerability management solutions protect and enable the secure adoption of the cloud by unifying policy, management, reporting, and analytics across on-premise and cloud environments. This approach will ensure that organizations can meet stringent security and compliance controls over cloud usage, while achieving business agility goals.

Cloud Security Best Practices

DISCOVERY AND INVENTORY OF CLOUD ASSETS

Undermanaged or unknown (shadow I.T.) cloud instances can create a significant security gap that opens networks to security breaches, data loss, intellectual property theft, and regulatory compliance issues. The first step in getting control over cloud assets is discovery. Once cloud instances are found, they must be managed to limit exposure.

BeyondTrust solutions perform continuous discovery and inventory of assets across physical, virtual, and cloud environments, ensuring that only properly configured and approved assets are available and used in your environment.
BeyondInsight, BeyondTrust’s unified platform for privilege and vulnerability management, includes dedicated cloud connectors for:

- Amazon Web Services (AWS)
- GoGrid
- Google Cloud
- Microsoft Azure
- Microsoft Hyper-V
- Rackspace
- IBM SmartCloud
- VMware

### Cloud Connection

<table>
<thead>
<tr>
<th>Title</th>
<th>Amazon AWS Demo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider</td>
<td>Amazon AWS</td>
</tr>
<tr>
<td>Category</td>
<td>BeyondTrust</td>
</tr>
</tbody>
</table>

Provider Specific Credentials

<table>
<thead>
<tr>
<th>Region</th>
<th>US East (Northern Virginia) Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Key ID</td>
<td>&lt;your_access_key_id&gt;</td>
</tr>
<tr>
<td>Secret Access Key</td>
<td>************</td>
</tr>
<tr>
<td>ARN</td>
<td>arn:aws:iam::XXXXXXXXXX</td>
</tr>
<tr>
<td>External Name</td>
<td>BeyondTrust</td>
</tr>
</tbody>
</table>

Reminder: The user is still bound to the Cloud Provider’s Terms of Service Agreement and/or Security Assessment Policies.

Connection Test Results:

Note: As per item (b) of the Terms and Conditions of the AWS Vulnerability / Penetration Testing Request Form, Small and Micro Instances may not be scanned and have been omitted from the test results.

<table>
<thead>
<tr>
<th>Name</th>
<th>Instance State</th>
<th>Public IP Address</th>
<th>Private IP Address</th>
<th>State</th>
<th>Type</th>
<th>Platform</th>
<th>AMI Description</th>
</tr>
</thead>
</table>

Figure 1: 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, organizations can quickly group them into Smart Groups for easier management. Smart Groups and role-based access allow teams to assess and manage cloud instances according to an organization’s unique business needs.
Just as important to cloud asset discovery is the management of supporting containers, for example Docker images deployed throughout the environment. Common attributes to scan for in Docker images and containers include:

- Basic image data: OS identification, repository tag, image ID; and where available, image size, creation date, and image author
- Enumerations: Services, processes, ports, certificates, users and user groups, and the network stack
- Installed software packages
- Registry and system files

Having this data will improve the visibility over Docker container usage and potential risks.

**SCAN FOR VULNERABILITIES AND MISCONFIGURATIONS**

Once cloud assets are found and managed, Retina CS, BeyondTrust’s solution for enterprise vulnerability management, provides continuous vulnerability assessment and remediation guidance of the infrastructure across physical, virtual and cloud environments, as well as continuous configuration and hardening baseline scanning across physical, virtual, and cloud-deployed assets.

While these resources are hardened in order to prevent security breaches and are inherently resilient to network-based vulnerability assessment scans, BeyondTrust provides vulnerability assessment agent capabilities for the Retina Host Security Scanner (RHSS) to provide a deep inspection into an instance and report back any vulnerability or configuration anomalies to BeyondInsight. This agent can be provisioned as a part of the instance template to ensure the asset is secured and remains un-tampered with during its lifecycle.
Figure 2: BeyondTrust performs deep inspection and reports back any vulnerability or configuration anomalies.

Having this integrated capability reduces risk, ensures that no cloud instances are left unmanaged (even without network scanning), and ensures configurations are consistent and properly hardened across cloud and on-premise resources against best practices from NIST, STIGS, USGCB, CIS, and Microsoft.

GAIN ACCOUNTABILITY AND CONTROL OVER PASSWORDS TO VIRTUAL AND CLOUD MANAGEMENT CONSOLES AND INSTANCES

Cloud and virtualization introduce new superuser consoles into the mix. Consoles such as those for Amazon AWS and Office 365 provide administrators with tremendous control, enabling them to modify, delete, and add new servers, often with just a few clicks. The AWS Console, for example, is also a de facto procurement system, enabling administrators to instantly order additional systems, storage, and network resources. Corporate accounts for Facebook, LinkedIn, or Salesforce are the same – inappropriate access can severely damage a firm’s reputation resulting in significant financial loss. Controlling and auditing access to these shared accounts ensures that all privileged activity is associated with a unique identity and ensures that all passwords are properly managed and rotated across the cloud environment.
Shared accounts are only part of the problem, though. Removing hard-coded passwords in cloud tool configurations, build scripts, code files, test builds, and production builds should be prioritized, as these embedded application credentials represent open backdoors to critical systems.

Securely storing privileged account credentials, requiring a simple workflow process for check-out, and monitoring privileged sessions limits lateral movement in the case of a compromise and provides a secure audit trail for forensic purposes.

BeyondTrust enables tighter control and accountability over cloud management consoles by discovering, onboarding, and managing passwords (such as enforcing rotation and other best practices), as well as performing session management and reporting on access. This capability is summarized in the diagram below.

![Diagram](image)

*Figure 3: PowerBroker discovers, onboards and manages access to cloud credentials.*

**PowerBroker Password Safe**, the BeyondTrust solution for privileged password and session management, enables the storage and session management for administrative credentials to cloud platforms, as well as social networks, with dedicated cloud connectors. Having this capability ensures tighter control and accountability over powerful credentials, which reduces the likelihood and the impact of compromises.
Figure 4: Password Safe enables the secure storage and management of cloud credentials.

Password Safe currently supports the following cloud and social platforms:

**Cloud**
- Amazon AWS
- Azure
- Box
- Dropbox
- GoGrid
- Google
- Office 365
- Rackspace
- Salesforce
- Workday

**Social**
- Facebook
- Instagram
- LinkedIn
- Pinterest
- Twitter
- XING
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 improves on CASB functionality by providing a single tunnel to control and audit cloud sessions – specifically for privileged accounts and interactive sessions. This capability is summarized in the diagram below.

**Figure 5: Utilizing PowerBroker as a single tunnel to cloud sessions enables tight control and audit of all activity.**
**PowerBroker Password Safe** can act as a cloud access service proxy for privileged accounts, enforcing access controls and auditing at a deeper level. By employing integrated multi-factor authentication, adaptive access authorization, and session monitoring, Password Safe extends beyond typical CASBs with:

- **Enterprise password management** – Discover accounts, randomize, rotation, and check-in/check-out passwords.

- **Session monitoring, management, and recording** – Record privileged sessions in real-time via a proxy session monitoring service and enable dual control.

- **Advanced workflow controls** – Provide additional context to requests by considering the day, date, time, and location when a user accesses resources to determine their ability to access those systems.

- **Advanced segmentation** – Route all remote access sessions through the PowerBroker Password Safe proxy for management, reporting, and enforce segmentation from authorized connectivity and attack.

These capabilities ensure that all access to all cloud assets are segmented, protected, monitored and recorded for auditing purposes.
ENABLE PRIVILEGE MANAGEMENT IN A HYBRID CLOUD ENVIRONMENT

In a cloud context, the principle of least privilege is important to restrict access to development, management and production systems, while granting only required permissions to appropriately build machines and images. BeyondTrust delivers privileged access management capabilities that can be used to securely delegate tasks and authorization across hybrid virtual/on-premise environments. With unified policy, management, reporting, and analytics across both on-premise and cloud environments, organizations can meet the stringent auditing demands on cloud usage. This capability is summarized in the diagram below.

Figure 6: Utilize PowerBroker as a single solution to manage privileges across both on-prem and cloud assets.
The BeyondTrust Best Practices Solution for Protecting and Enabling the Cloud

The BeyondTrust solution for secure cloud enablement discovers all cloud instances in the environment, groups cloud assets for consistent privilege management, and scans for security vulnerabilities and privilege-related risks. By unifying policy, management, reporting, and analytics across both on-premise and cloud environments, organizations can meet stringent security and compliance controls over cloud usage, while achieving business agility goals. The figure below depicts an eight-step best-practices approach for securing and enabling the cloud.

![Diagram: BeyondTrust’s 8-step best practices approach to securing and enabling the cloud.](image)

*Figure 7: BeyondTrust’s 8-step best practices approach to securing and enabling the cloud.*
## MAPPING BEYONDTRUST SOLUTIONS TO SECURE CLOUD BEST PRACTICES

### Table 1: How BeyondTrust Solutions Map to Secure Cloud Best Practices

<table>
<thead>
<tr>
<th>Secure Cloud Best Practice</th>
<th>How BeyondTrust Solutions Help</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Discover &amp; Inventory</strong></td>
<td><strong>Retina Enterprise Vulnerability Management</strong> performs continuous discovery and inventory of assets across physical, virtual and cloud environments, ensuring that only properly configured and approved assets are available and used in your environment.</td>
</tr>
<tr>
<td><strong>2. Scan for Vulnerabilities</strong></td>
<td>Retina provides continuous vulnerability assessment and remediation guidance of the infrastructure across physical, virtual, and cloud environments.</td>
</tr>
<tr>
<td><strong>3. Scan for Configuration Compliance</strong></td>
<td>Retina performs continuous configuration and baseline scanning against industry configuration guidelines and best practices from NIST, STIGS, USGCB, CIS, and Microsoft, across servers and code/builds in physical, virtual, and cloud-deployed assets. Retina automates and streamlines auditing and reporting, and ensures configurations are consistent and properly hardened across on-prem and cloud assets</td>
</tr>
<tr>
<td><strong>4. Gain Accountability Over Shared Accounts</strong></td>
<td><strong>PowerBroker Password Safe</strong> controls and audits access to shared accounts and improves accountability by ensuring that all credentials are properly managed and rotated across the environment, and that all audited activity is associated with a unique identity.</td>
</tr>
<tr>
<td><strong>5. Eliminate Hard-Coded Passwords</strong></td>
<td>Password Safe controls access to scripts, files, code, embedded application credentials, and hardcoded passwords, including removing hardcoded passwords in cloud management consoles. Here, Password Safe reduces risk by closing backdoors to critical systems.</td>
</tr>
<tr>
<td><strong>6. Enforce Appropriate Credential Usage</strong></td>
<td>Password Safe eliminates administrator privileges on end-user machines, securely stores privileged account credentials, requires a simple workflow process for checkout, and monitors privileged sessions. This reduces risk by limiting lateral movement in the case of a compromise, and by providing a secure audit trail for forensic purposes.</td>
</tr>
<tr>
<td><strong>7. Segment Networks</strong></td>
<td>Password Safe utilizes a secured jump server with multi-factor authentication, adaptive access authorization, and session monitoring for access that needs to cross trust zones. This enables IT teams to segment access based on the context of the user, role, application, and data being requested, and reduces risk by minimizing the “line of sight” access that attackers have into internal systems.</td>
</tr>
<tr>
<td><strong>8. Restrict Privileges</strong></td>
<td><strong>PowerBroker Endpoint Privilege Management</strong> and <strong>Server Privilege Management</strong> solutions grant only required permissions to appropriately build machines and images, and deploy, configure, and remediate production issues on machines and images.</td>
</tr>
</tbody>
</table>
The PowerBroker Privileged Access Management Platform

BeyondTrust’s solutions for secure cloud are part of the PowerBroker Privileged Access Management Platform – an integrated solution to provide control and visibility over all privileged accounts and users. By uniting best-of-breed capabilities across on-premise, virtual, and cloud platforms that many alternative providers offer as disjointed tools, the PowerBroker platform simplifies deployments, reduces costs, improves system security, and closes gaps to reduce privileged risks.

Next Steps

To learn more about BeyondTrust solutions for securing cloud, visit us on the web, request a free trial or contact us today.
About BeyondTrust

BeyondTrust® is a global cyber security company that believes preventing data breaches requires the right visibility to enable control over internal and external risks.

We give you the visibility to confidently reduce risks and the control to take proactive, informed action against data breach threats. And because threats can come from anywhere, we built a platform that unifies the most effective technologies for addressing both internal and external risk: Privileged Access Management and Vulnerability Management. Our solutions grow with your needs, making sure you maintain control no matter where your organization goes.

BeyondTrust's security solutions are trusted by over 4,000 customers worldwide, including over half of the Fortune 100. To learn more about BeyondTrust, please visit www.beyondtrust.com.