TECH BRIEF

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

Protecting and Enabling the Cloud

With Privilege and Vulnerability Management Solutions

Table of Contents

Executive Summary

According to the 2016 Gartner Magic Quadrant for Public Cloud Storage Services Worldwide, 80% of cloud breaches through 2020 will be due to customer misconfiguration, mismanaged credentials or insider theft.

Growing use of cloud environments for processing, storage, or application hosting and development has opened up new avenues for would-be hackers or malicious insiders to inappropriately access sensitive data and disrupt organizations. Despite these risks, however, cloud adoption continues to accelerate, with 77% of companies reporting meaningful adoption of the cloud already and believing more processes could be moved to that platform (Cowan). Clearly, organizations must secure access to cloud environments to mitigate security risks while meeting the cost and efficiency demands of hosting more applications and services in the cloud.

This brief describes specific use cases where BeyondTrust privileged access management solutions and vulnerability management solutions protect and enable the cloud, and how BeyondTrust solutions can be hosted in cloud environments.

BeyondTrust *for* the Cloud

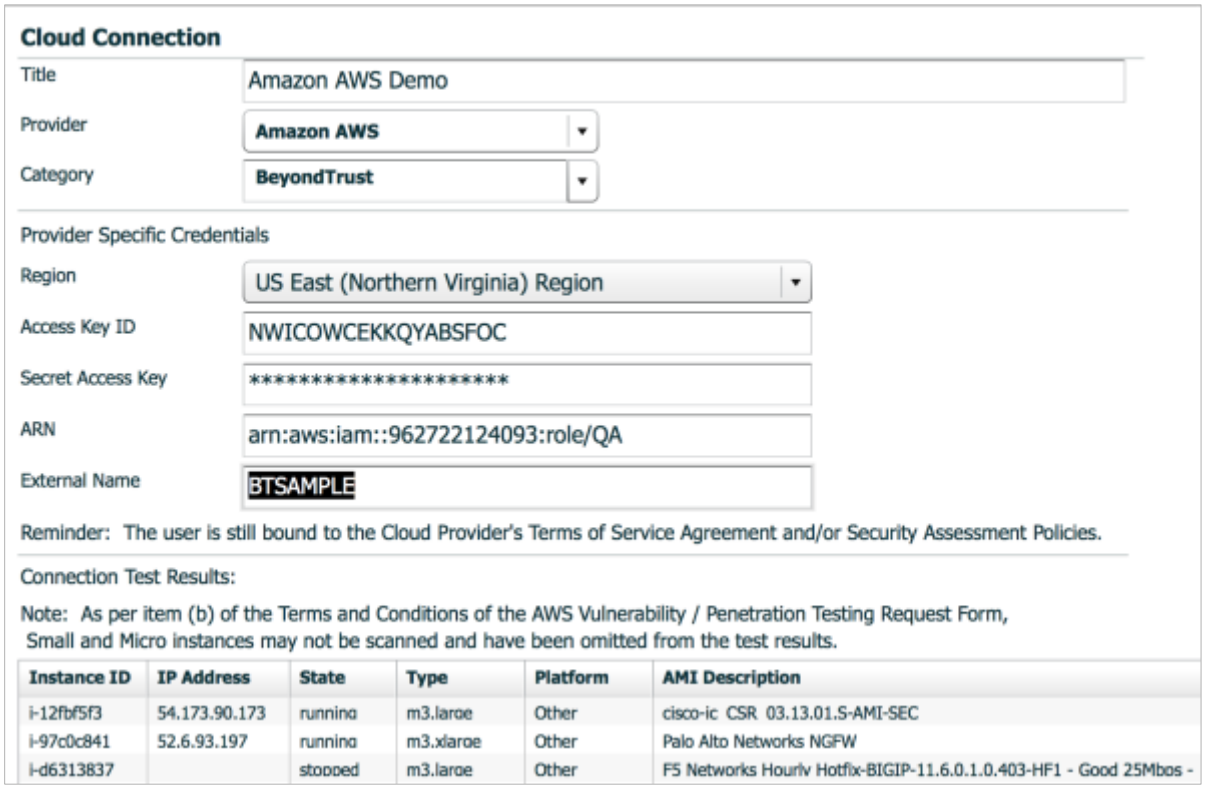
USE CASE: FINDING, GROUPING, AND SCANNING CLOUD ASSETS

Unknown or undermanaged cloud environments 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 of cloud assets. Once cloud instances are found, they must be managed to limit exposure.

BeyondTrust solutions discover all cloud instances in the environment, group cloud assets for secure management, and scan for vulnerability and privilege-related risks using industry unique cloud connector technology.

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



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.

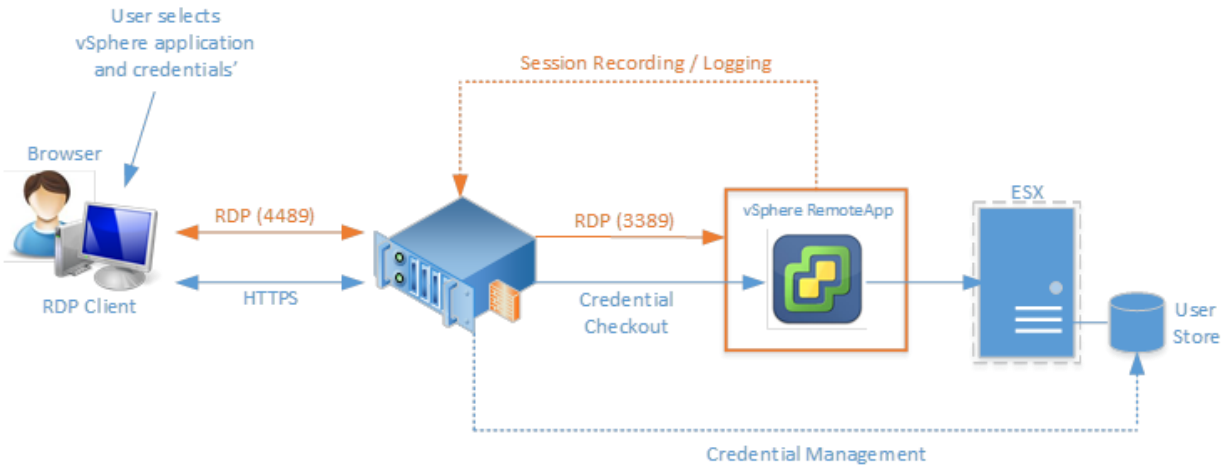
Once cloud assets are found and managed, **Retina CS**, BeyondTrust's solution for enterprise vulnerability management, assesses, reports and remediates vulnerabilities in those cloud environments.

All BeyondTrust solutions that leverage BeyondInsight as their central reporting, management, policy and analytics console benefit from these dedicated cloud connectors. Having this capability reduces risk and ensures that no cloud instances are left unmanaged.

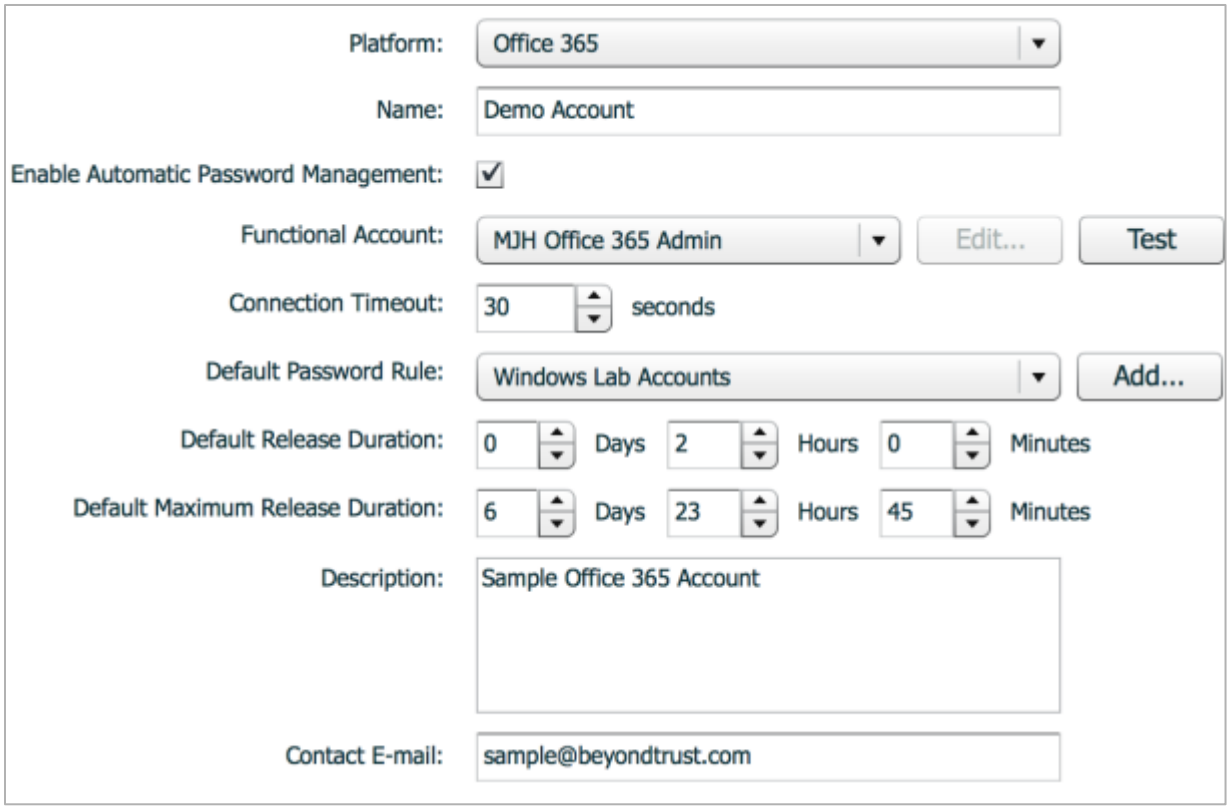
USE CASE: PROTECTING VIRTUAL AND CLOUD MANAGEMENT CONSOLES AND INSTANCES

Cloud and virtualization introduce new super user 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.

BeyondTrust enables tighter control and accountability over cloud management consoles by discovering, onboarding, and managing and cycling passwords, as well as performing session management and reporting on access. This capability is summarized in the diagram below.



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 mitigates the impact of compromises.



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
- Dropbox
- GoGrid
- Google
- Office 365
- Rackspace
- Salesforce
- Workday

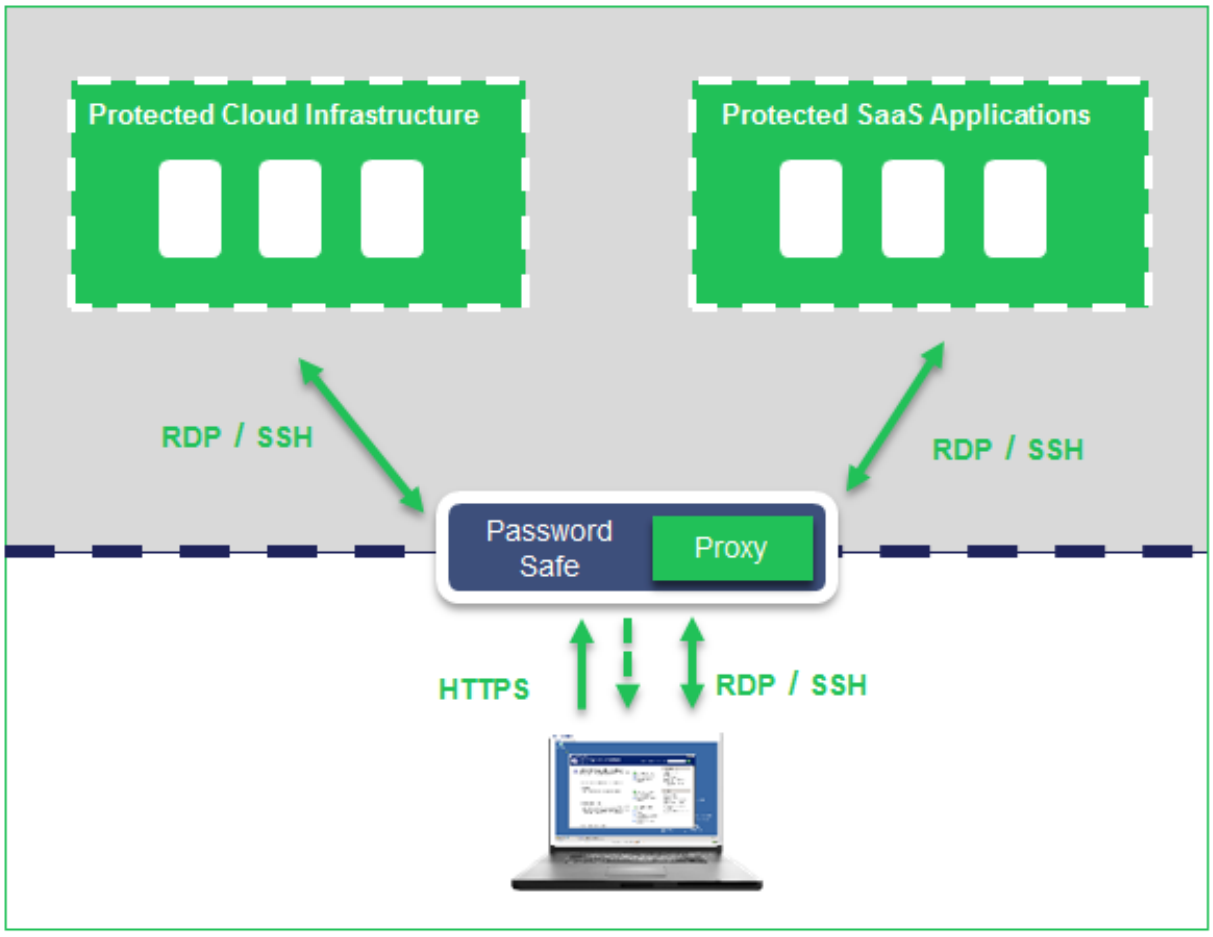
Social

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

USE CASE: USING A CLOUD ACCESS SERVICE BROKER

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 access activities – specifically for privileged accounts and sessions. This capability is summarized in the diagram below.



PowerBroker Password Safe can act as a cloud access service proxy for privileged accounts, enforcing access controls and auditing at a deeper level. Password Safe extends beyond typical CASBs with:

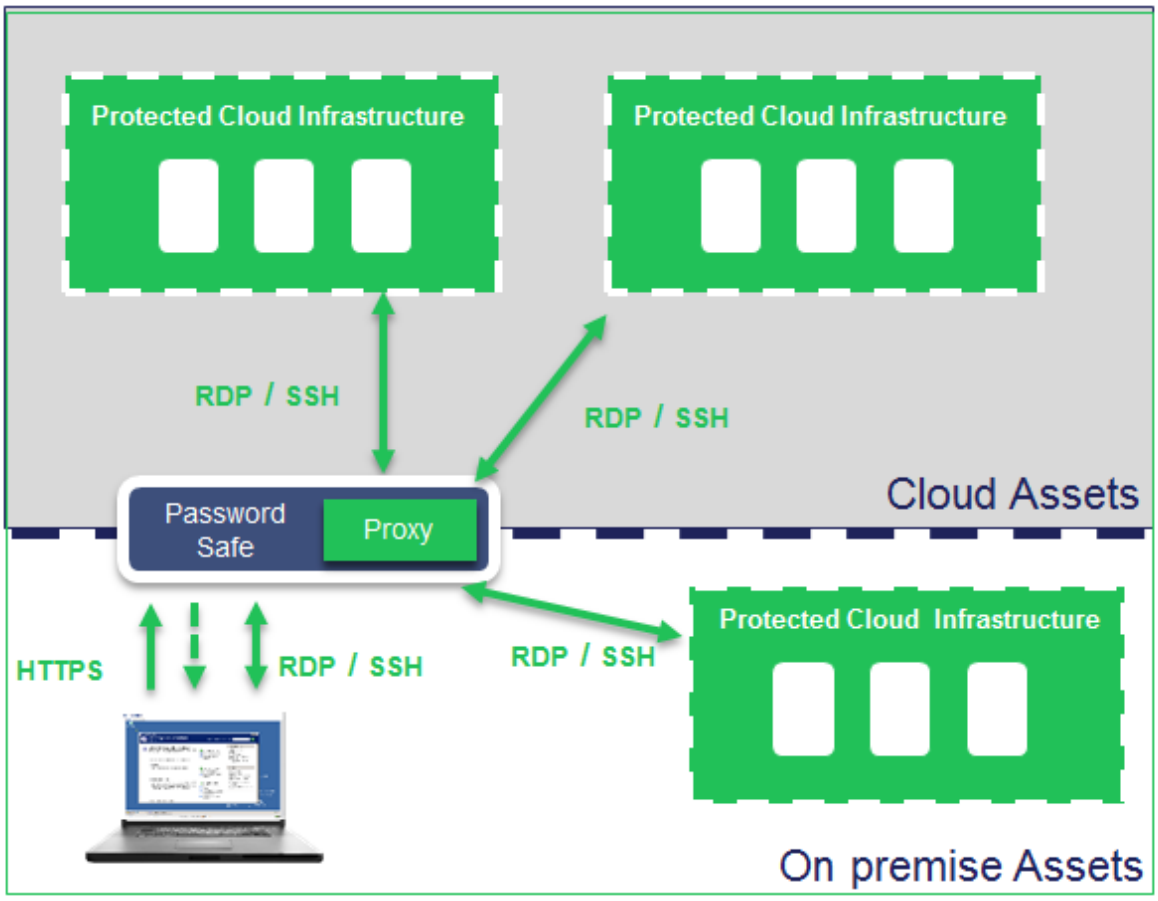
- **Enterprise password management** – Discover accounts, randomize, rotation, and check-in/check-out passwords.
- **Session monitoring, management and recording** – Record privileged sessions in real time via a proxy session monitoring service and enable dual control.
- **Advanced workflow controls** – 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.

BeyondTrust *in* the Cloud

USE CASE: ENABLING PRIVILEGE MANAGEMENT IN A HYBRID CLOUD ENVIRONMENT

BeyondTrust delivers privileged access management capabilities that can be used to securely delegate tasks and authorization across hybrid virtual/on-premises 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.



Following are the four BeyondTrust solutions that can be used in the cloud.

BeyondInsight, the BeyondTrust central management, policy, reporting and analytics platform, delivers multi-tenant capabilities enabling customers to host BeyondInsight in the cloud for business units or MSPs.

Whether BeyondInsight is managing cloud assets, extending your data center, or a hybrid approach, BeyondInsight in the cloud can manage Retina CS, PowerBroker Password Safe, PowerBroker for Unix & Linux, PowerBroker for Windows, and PowerBroker for Mac. This can provide privileged access and vulnerability for assets that have traversed across a dissolving perimeter including cloud assets and mobile devices. By installing BeyondInsight in the cloud, your environment can benefit from having a centralized management console that can communicate with anything from private cloud instances to laptops operating in the field without building infrastructure out in a typical datacenter DMZ.

PowerBroker for Unix & Linux, the industry-standard solution for privilege delegation and Unix and Linux command elevation, can be used in the cloud.

All Unix and Linux systems – including those located in cloud environments – rely on shared and high privileged credentials, with 'root' being the most well-known and the most widely abused. PowerBroker for Unix & Linux allows for the control and audit of all credentials, especially those carrying high privilege capabilities.

The PowerBroker for Unix & Linux architecture allows cloud-specific configurations to be used, or hybrid policies designed, to connect cloud systems and share rights or use their own set of rights depending on where the requesting user and/or system is located. All of the audit data, including a full index of every keystroke entered during captured sessions, are made available via a number of interfaces, with the most popular being BeyondTrust's BeyondInsight dashboard and reporting interfaces. Cloud based Unix or Linux resources have never been so secure because of PowerBroker for Unix & Linux.

PowerBroker for Windows and **PowerBroker for Mac**, the patented solutions for least privilege and application control for Windows and OS X desktops and servers, can be installed in templates used for cloud instances and manage assets beyond the perimeter operating anywhere on the internet. Using BeyondInsight with our PowerBroker endpoint solutions in the cloud allows for laptops, notebooks, tablets, and other devices to participate in privileged access management initiatives and provide visibility into activity via a single dashboard. In

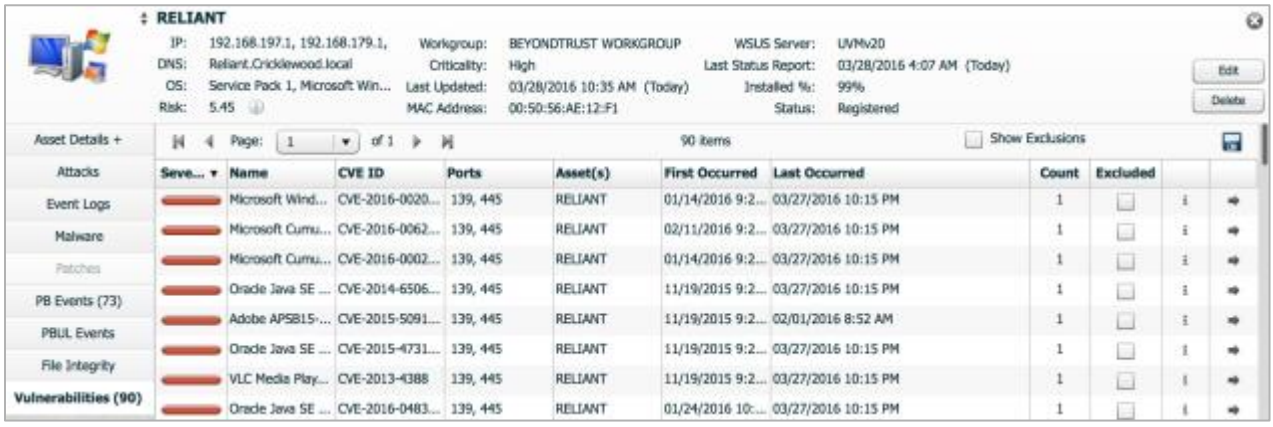
addition, resources in the cloud used for virtually any business function can also ensure that privileged access is never a security risk for your organization.

PowerBroker Password Safe, the BeyondTrust solution for privileged password and session management, is based on the BeyondInsight technology and benefits from all the capabilities it provides from discovery to proxied session management. Deployments in the cloud can secure cloud resources, provide workflows for contractors and employees, and provide attestation of all privileged access to cloud resources.

USE CASE: PERFORMING ZERO-GAP VULNERABILITY ASSESSMENTS FOR HYBRID AND PUBLIC CLOUD INFRASTRUCTURES

The cloud offers opportunities and flexibility for information technology resources to be deployed, scaled, and managed outside of the confines of a traditional datacenter. Many times, these resources are hardened in order to prevent security breaches and are inherently resilient to network based vulnerability assessment scans.

To provide an accurate assessment of these devices requires some inside knowledge for each of the instances (or agent). **Retina CS** offers 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.

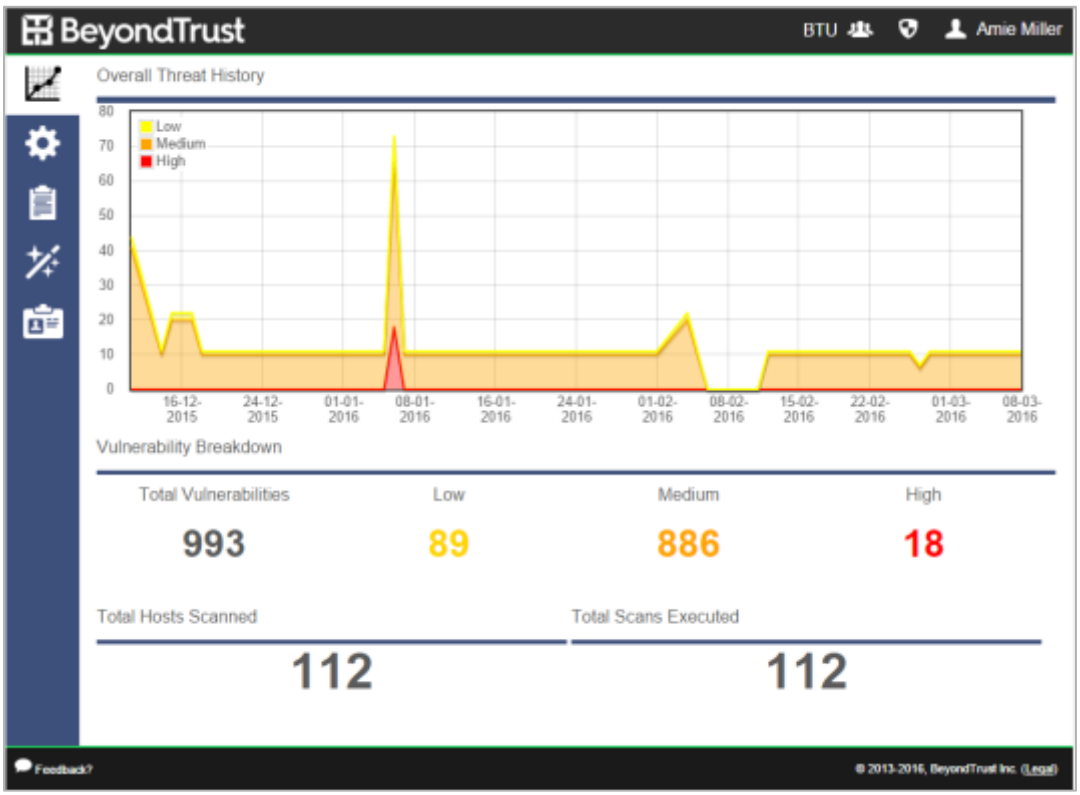


BeyondTrust performs deep inspection and reports back any vulnerability or configuration anomalies.

This approach allows for complete risk assessments, without scanning, and meets security best practices and regulatory initiatives regardless of the asset being in the cloud or on premise.

USE CASE: PERFORMING CLOUD-BASED VULNERABILITY SCANNING

Websites and web-based applications are favorite targets of today's advanced attacks as they are an easy gateway into an organization if not properly protected. BeyondTrust provides security assessments of public-facing network infrastructures and web applications, with **BeyondSaaS**.



BeyondTrust provides a dashboard to easily understand web-based attacks and vulnerabilities.

Having this capability helps to identify perimeter vulnerabilities, understand their potential impact, and provide the intelligence to act to mitigate threats.

Conclusion

To learn more about BeyondTrust solutions for the cloud or in the cloud, 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.