Authomize and Ping Identity

Securing Identity and Access Privileges Better Together

The combination of Authomize's Cloud Identity and Access Security Platform with Ping Identity's authentication authority hub enables customers to ensure effective security access across all their apps and cloud services

The Challenge

Securing access privileges for identities across all your applications and cloud services is becoming increasingly difficult as organizations scale their operations across multiple cloud services.

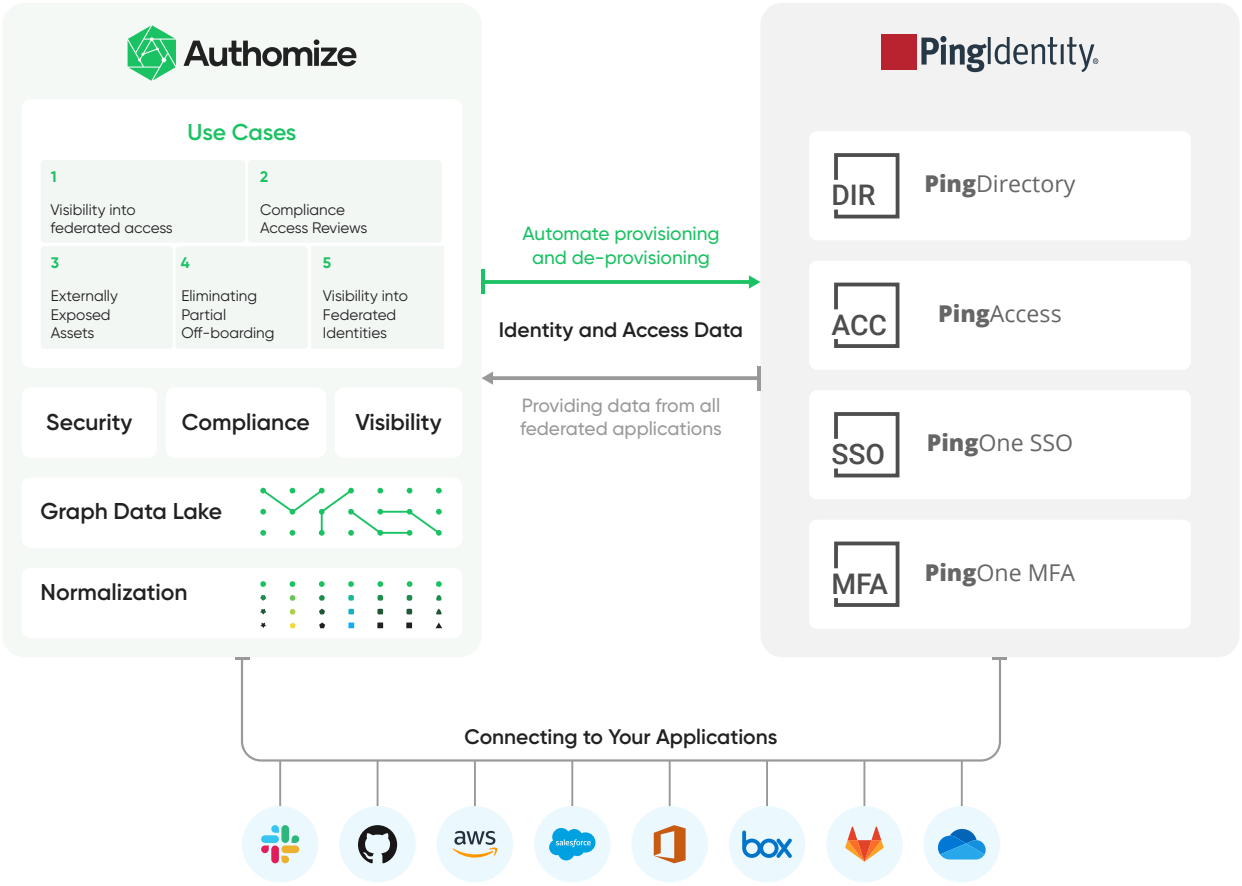
At the same time, the demands from the current security environment and compliance requirements require organizations of all sizes to implement comprehensive solutions that provide them with the visibility and control over all their identities, access privileges, and assets, regardless of the cloud environment.

Authomize Offers

- One-click integration for rapid, easy deployment and a faster time to value
- Ensure effective access and achieve secure Least Privilege
- Centralized full-stack Cloud Platform (IaaS, SaaS, Data, XaaS)
- Streamline Compliance Access Reviews (SOC 2, CSA STAR, SOX)
- Continuous monitoring with granular visibility

The Solution

By combining Ping Identity's best-of-breed authentication and access management solution with Authomize's Cloud Identity and Access Security Platform, organizations can achieve fine-grained visibility over effective access and implement risk mitigation controls that they need to ensure secure usage of their cloud services.



Authomize

The Cloud Identity and Access Security Platform

Authomize continuously monitors your identities, access privileges, assets, and activities to secure all your apps and cloud services. We enable organizations to mitigate IAM risk with unprecedented visibility and granular control across all apps and cloud services (IaaS, Saas, Data).

Our proprietary SmartGroups Machine Learning technology maps and understands who has specific access privileges, which assets can be accessed by who, and how those access privileges are being used. This extensive data-driven visibility provides detailed context that allows for actionable alerting on risks, policy violations, and more efficient compliance operations that enhance business continuity and security.

Ping Identity

Ping Identity provides a comprehensive identity and access management (IAM) platform with flexible deployment options for centralized adaptive multifactor authentication, single sign-on (SSO), and access management for workforce, customer, and partner identities.

The PingOne Cloud Platform enables companies to achieve Zero Trust identity-defined security and more personalized, streamlined user experiences.

Access Security Continuity: Authomize + Ping Identity Benefits

As a leader in identity security, Ping empowers their customers to manage their enterprise's access, providing unparalleled control and trust over all identities in the organization.

Building on Ping's authentication services, Authomize provides the next step in the Access Security Continuity chain, enabling customers to secure their access privileges on a granular level across all of their applications and cloud services (IaaS, SaaS, Data).

Integrating Authomize with Ping Identity's authentication hub creates end-to-end coverage of the access control plane, enabling frictionless yet secure logins and ensuring that every identity has the right-sized level of access to applications and cloud services to achieve Least Privilege. Our adaptive Machine Learning engine constantly assesses and prescribes the exact level of access to equip identities with the access privileges they need while continuously reducing the attack surface.

Use Case #1

Detect Hidden Over-Privilege Cloud Risks

A common challenge that organizations face in limiting access privileges in line with Least Privilege is in how they manage their groups. Take for example an R&D team leader who has admin privileges in AWS is then added to another group for managers that unintentionally gives her admin rights in Salesforce. This person would now be over-privileged and present a higher risk to the organization because the potential damage from their identity is expanded if compromised or if they become a malicious insider.

With visibility across all apps and cloud services, Authomize can detect and alert that this legitimate, verified user is over-privileged in other environments inside the organization and offer actionable remediation recommendations to regain Least Privilege and mitigate the risk with a better security posture.

Use Case #2

Compliance Access Reviews

Completing Access Reviews for compliance audits are challenging, especially as the scale and complexity of the identities and access privileges grow. Organizations struggle to finish on time and avoid rubber stamping their reviews, all risking their ability to remain compliant.

Authomize enables organizations to meet their requirements by:

- Matching the right reviewers with the access privileges to be reviewed
- Providing data-driven recommendations using SmartGroup Machine Learning for approving/rejecting privileges
- Offering a centralized platform for managing the whole process, tracking campaigns, and nudging reviewers when needed
- Automating up to 40% of the approvals to cut the workload on reviewers
- Producing human-readable, detailed reports that auditors trust

Use Case #3

Externally Exposed Assets

With easy collaboration at the heart of the cloud, sharing assets like files externally with 3rd-party partners is a common practice. However, when it comes time to revoke access to the externally shared resource, most either forget to close it or leave it open for convenience's sake. Adding to the challenge is the fact that solutions that only track identities lack the visibility over the assets' access privileges' usage and cannot see who outside the organization has access to the resource.

With total fine-grained visibility over the identities, access privileges, assets, and activity, Authomize knows who retains access, even if they are not part of the organization. Continuous monitoring of security policies, including those that allow users to set guardrails to alert when an asset has not been accessed over a given time period, helps to close the gaps in your threat surface and mitigate risk of exposure.

Use Case #4

Eliminating Partial Off-boarding

An employee leaving the organization presents a higher risk as they may retain some of their access privileges and can use them to cause harm. This can often happen when those privileges are not provisioned through the primary identity management system.

Ping Identity provides easy to manage control over all of your federated identities, streamlining the process of off-boarding a user.

Authomize identifies all identities and access privileges associated with a user, both those that are federated through Ping and any locally created users, and can merge any disparate identities to avoid such incidents from occurring. By providing the comprehensive visibility over effective access, continuous monitoring for policy violations, organizations can ensure that employees are fully removed from all assets and company identities.

Next Steps

Learn more about how Authomize's Cloud Identity and Access Security Platform can extend the value of your PingOne authentication authority hub, request a demo or contact your Ping representative.

REQUEST A DEMO