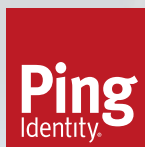




# Fast-track your digital transformation with a modern enterprise identity program

Building end-to-end Zero Trust solutions for information security with Ping Identity, SailPoint and BeyondTrust





Organizations are embracing the cloud to create new digital services for their employees and customers, making it easier to do business anytime, anywhere. But while the cloud makes things simpler for users, it's a different story for information security professionals.

According to a recent ESG survey, 33% of respondents said that maintaining security consistency across data centre and cloud environments was their biggest challenge.

In the past, IT had a defined network perimeter: trusted systems lived within your firewall, while anything outside was suspect. Today, it's impossible to make such clear distinctions. Instead, you need to take a Zero Trust approach: trust no one until verified, add extra layers of protection for privileged access where possible, and architect your systems to detect threats and minimize impact if a breach occurs.

A foundation of Zero Trust is identity. With the dissolution of traditional network perimeters, identity has become the primary and most critical line of defense that can span all users and devices. You need to be able to monitor and actively manage every aspect of the identity and access management lifecycle.

## KEY INFORMATION SECURITY CHALLENGES

Information security professionals are in short supply, and most organizations find it difficult to hire and retain talent with the right experience and skills. Moreover, threats are constantly evolving, and even the top professionals struggle to stay up to date, especially when they are constantly fighting security incidents on a daily basis.

The most effective way to empower security teams and get the most benefit from limited resources is to adopt best-in-class technology with built-in automation and AI. However, that technology has to work with your teams, not against them. If mismatched tools make it difficult to automate processes, your people will bear the burden. And if your systems don't work together seamlessly, it becomes difficult to analyze events or ensure the right balance between appropriate security and a frictionless user experience.

Ping Identity, SailPoint and BeyondTrust each offer best-of-breed standalone solutions that provide key components of a modern, Zero Trust enterprise identity program. With seamless integration between their platforms, you can quickly and easily assemble the solution you need to solve today's information security challenges.

### CAN YOUR INFORMATION SECURITY TEAM ANSWER THESE QUESTIONS?

**Who** is logging in – where, how, and on what device?

Which systems are they **authorized** to access?

What specific **privileges** do they currently have?

What privileges **should** they have in their current role?

## BUILDING A MODERN ENTERPRISE IDENTITY PROGRAM

Together, Ping Identity, SailPoint and BeyondTrust provide the three foundational components of a modern enterprise identity program.

## IDENTITY AND ACCESS MANAGEMENT FROM PING IDENTITY

The PingOne Cloud Platform offers a comprehensive solution for registering, verifying, authenticating, authorizing, and monitoring users as they access your systems. It provides an authentication authority that acts as the single mechanism for users to access all their applications via single sign-on (SSO)—minimizing the number of credentials that users need to manage, and reducing the risk of lost passwords and system lockouts.

With intuitive workflows to help users set up multi-factor authentication, the platform can increase security and reduce the risk of unauthorized access by linking authentication to the user's smartphone or other physical access tokens. It can also leverage biometrics such as fingerprint scans or facial recognition to add an extra layer of security, and provides monitoring and risk analysis tools to detect suspicious activity, such as a user attempting to log in at unusual times or via an unknown device.

## IDENTITY SECURITY FROM SAILPOINT

SailPoint Identity Security solutions simplify the management of digital identities throughout their lifecycle—from onboarding new starters and moving employees into new positions, to revoking access when people leave the organization.

As soon as an employee record is created or deleted in your core HR system, SailPoint can automatically provision or de-provision user accounts in the appropriate systems. It also provides user-friendly workflows to allow personnel to reset passwords or request access to additional systems, and keeps a full audit trail of approvals and changes to access rights.

In addition, SailPoint helps with ongoing management of job roles, using artificial intelligence to assess how users' access patterns and requirements are changing over time, and helping you make smarter decisions about which roles should have access to which systems.



## PRIVILEGED ACCESS MANAGEMENT FROM BEYONDTRUST

It's estimated that approximately 80% of hacking-related security breaches involve the misuse of privileged credentials, such as admin or root passwords. Managing and controlling the explosion of privileges across the enterprise presents an ongoing challenge.

BeyondTrust's Universal Privilege Management platform enables trusted access across your organization by securing and managing privileges across every user, session, and asset by implementing comprehensive layers of control and monitoring, significantly reducing the risk of privileged credentials being leaked or used inappropriately.

BeyondTrust goes beyond just managing privileged credentials in a vault. It also offers secure remote access and endpoint management solutions to allow properly authorized users to access privileged systems, without needing to give them direct access to the credentials themselves. As a result, it becomes easier to maintain the principle of least privilege: users only have the minimum access they need to do their job, and additional privileges can be temporarily granted or revoked when necessary on a Zero Trust basis.

## BENEFITS OF A MODERN ENTERPRISE IDENTITY PROGRAM

The combination of Ping Identity, SailPoint, and BeyondTrust helps you fortify your security posture and be confident the right users have the right access. Together, the solutions enable you to strike a balance between security and convenience for all privileged and non-privileged users, demonstrate compliance with confidence and ease, and maintain an access audit trail for every identity.

### LEARN MORE

Contact your local Ping Identity, SailPoint or BeyondTrust representative to learn more, or reach out to arrange a demonstration:

[www.pingidentity.com/en/platform.html](http://www.pingidentity.com/en/platform.html)

[www.sailpoint.com](http://www.sailpoint.com)

[www.beyondtrust.com/solutions](http://www.beyondtrust.com/solutions)

## KEY BENEFITS

### INCREASED VISIBILITY

Ensure secure, authenticated logins and appropriate entitlements for privileged or non-privileged users based on their current role and responsibilities

### GREATER GOVERNANCE AND CONTROL

Meet regulatory requirements by knowing who has access to your critical applications and document your processes to prove compliance

### SEAMLESS & SECURE ACCESS FOR ALL USERS

Ensure secure, authenticated logins and appropriate entitlements for every type of user based on their current role and responsibilities

### ENTERPRISE-PROVEN TECHNOLOGY

Trusted by the world's largest enterprises, we seamlessly integrate to extend customer investments, increase productivity and deliver an optimal end user experience.

