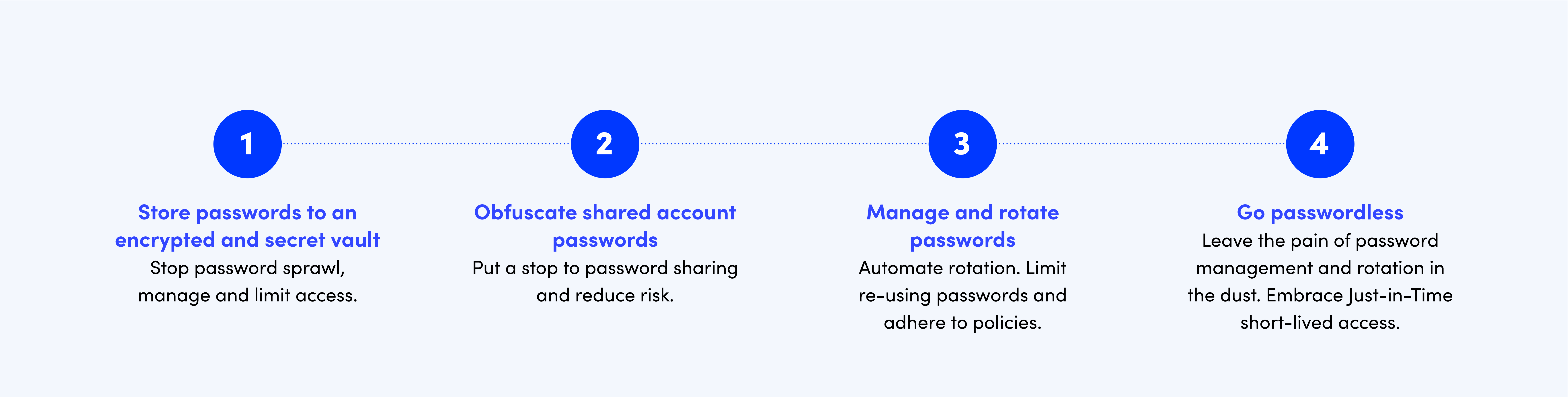
SSH

Solution brief

Passwordless identity validation and access management for critical infrastructures and IT

Joint solution by SSH and Beyond Identity:
Passwordless MFA access with continuous verification

The challenge



1

Store passwords to an encrypted and secret vault

Stop password sprawl, manage and limit access.

2

Obfuscate shared account passwords

Put a stop to password sharing and reduce risk.

3

Manage and rotate passwords

Automate rotation. Limit re-using passwords and adhere to policies.

4

Go passwordless

Leave the pain of password management and rotation in the dust. Embrace Just-in-Time short-lived access.

Journey to passwordless authentication for privileged users

Constantly evolving cyberattacks have all but eliminated traditional security perimeters and trusted zones. Instead, organizations are moving from static 'moat-and-castle' models to more dynamic Zero Trust approaches where there are no trusted users, connections or devices.

Ephemeral multi-cloud environments, remote work and third-party access requirements have also increased the need to think beyond risky shared or static credentials in favor of more dynamic and agile solutions.

The journey from the endpoint device to the superuser accessing a company's critical infrastructure needs to be identifiable, trackable, manageable, secure, and fluid.

For this reason, continuous monitoring, continuous verification, and dynamic controls have taken the centre stage in identity and access management (IAM) and privileged access management (PAM).

With a joint solution, Beyond Identity and SSH can continuously verify each identity, device and session and guarantee that the user privileges and entitlements are limited to the minimum required to complete the task at hand. This approach aligns with the Zero Trust approach, since permanent, long-standing authorizations disappear from the equation in favor of verifying the legitimacy of each device, user and privileges for each session.

Zero Trust from endpoint to the cloud

For every authentication request, the Beyond Identity Authenticator captures 90+ user and device security signals from the exact device making the request. These signals are then validated by the Beyond Identity policy engine so you can enforce risk policies including step-up authentication prior to login for adaptive security.

Passwordless authentication is significantly more secure, reduces user friction, and saves organizations time, effort, and money. Instead of passwords, passwordless authentication uses something they have or something they are, none of which is stored by the provider.

Beyond Identity leverages the technology built into modern devices to provide secure authentication, through biometrics and the Trusted Platform Module.

PrivX, Zero Trust Just-in-Time privileged access Management (PAM)

PrivX is a scalable, cost-efficient, and highly automated hybrid PAM solution that supports hybrid and multi-cloud environments. The solution increases security and operational efficiency by providing centralized access to mission-critical targets for superusers and privileged users without any credentials left behind. With PrivX, access to on-prem, hybrid, or cloud environments is managed centrally – all under one roof.

PrivX allows organizations to move to secure and cost-efficient passwordless authentication while supporting password vaulting and rotation when still needed – allowing businesses to migrate at their own pace.

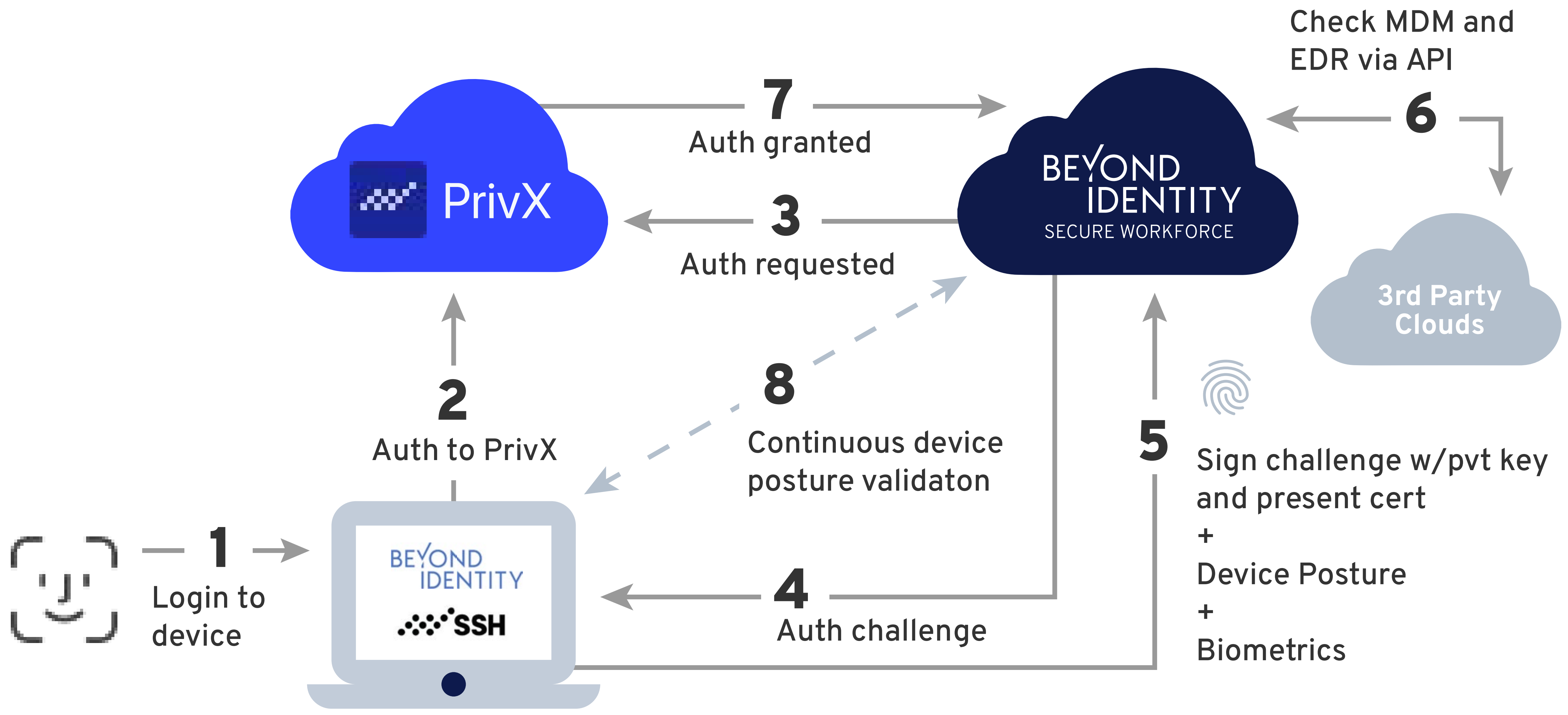
In a PrivX's Zero Trust model, connections are established using ephemeral certificates that are created just-in-time for the session and expire automatically shortly afterwards, leaving no credentials behind to manage, lose, share or rotate (see the four steps to passwordless access above).

Additionally, PrivX syncs with Active Directory and automatically maps existing identity groups. Users are then granted access based on their roles (role-based access control, RBAC), rather than identities. PrivX automatically grants just enough access to the right users, at the right time, for the right duration of time, and with the right level of privilege.

The solution in a nutshell

The joint solution by Beyond Identity and SSH prevents credential-based breaches by ensuring user and device trust with strong, biometric authentication and eliminating passwords and encryption keys. With it, you grant only the right level of access to the right target at the right time for the right person in a true Zero Trust fashion. The solution continuously validates user identity and device security throughout the session and terminates at-risk connections, increasing the security posture of critical IT and OT environments.

Joint solution: Zero passwords and Zero Trust.



What it does

The PrivX and Beyond Identity integration ensures only strongly validated users with currently active permissions can gain and maintain access to target services. It also ensures that users are only able to gain and maintain access to target services using endpoint devices that remain within device security policies.

How it works

When PrivX is integrated with an IAM solution, it continuously monitors users' rights and permissions to access targets. For example, if the role of a developer accessing a resource changes during a session, PrivX automatically closes and prevents all connections that were granted for the removed role. Since changes made in directory services are automatically reflected in the roles in near real-time, the joiners, movers, and leavers -process is automated too.

But the concept of continuous monitoring and response is taken even further with this integration. When Beyond Identity is added to the mix, the initial user authentication combines two very strong user authentication factors - cryptographic passkeys and biometrics – to provide a very high level of trust in the user identity.

Beyond Identity also adds device trust checks. During each authentication request, Beyond Identity's authenticator works in conjunction with its cloud-based policy engine. The system validates the user's identity with frictionless MFA (passkeys + biometrics). The authenticator captures user behavior and device security signals, enabling Beyond Identity's policy engine to determine whether the endpoint meets security requirements prior to allowing access. After the initial authentication transaction, Beyond Identity continues to collect and evaluate user and device security signals and if needed, can command PrivX to drop the user Session and target connections. For example, if the device's security posture decreases (e.g. the user turns off the firewall, or changes another security setting).

Architecture

The joint solution created by combining PrivX and Beyond Identity Authenticator is a state-of-art example of modern Zero Trust concept in real life - continuously assess user permissions, validate user identity, confirm device security, and respond by revoking access if needed.

The diagram shows the architecture and authentication flow of the Beyond Identity and PrivX integration. The products share a common source for user identities and roles.

When the user accesses PrivX, Beyond Identity prompts the user for their biometric factor (proving possession of an authorized device) and conducts an asymmetric cryptographic transaction to prove the private key on the device matches the public key in the Beyond Identity cloud. This approach cryptographically binds the user identity to their device.

The user's private key is securely stored in the Trusted Platform Module (TPM) built into the device and cannot be moved. After proving that device owner is in possession of the device, with the device biometric, the system conducts an X.509 certificate exchange to confirm the user identity.

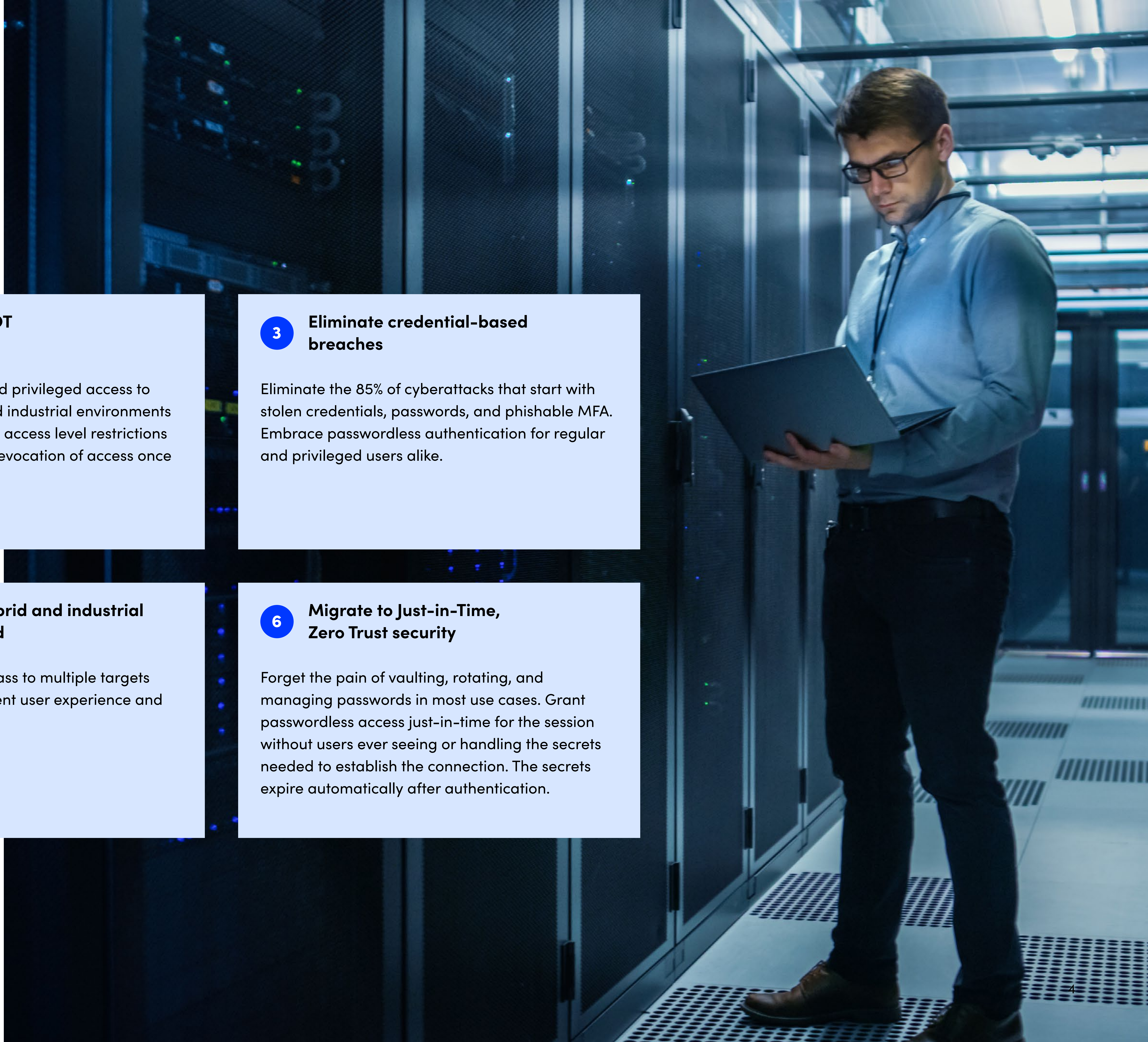
In sensitive environments where the role-based access to hosts and targets is based on privileges, this extra layer of security makes a lot of sense. The privileged user is not only treated according to his roles, but also according to the fact that login is only accepted from a specific device, owned by this privileged user.

Beyond Identity's cloud-based Policy Engine continuously monitors user behavior signals and the security posture of the device. The Beyond Identity authenticator natively collects endpoint security posture data and additional signals are collected from various 3rd party systems, such as Device Management and End-Point detection and response (EDR) software. The signals are combined to form a risk-policy based decision whether access is granted or not and then continuously re-evaluated to ensure the user and device should maintain access.

For example, the access could be denied if the Anti-virus is not running, the device firewall or lock screen is turned off. If the change occurs during a session, the user can be prompted to provide the biometric authentication again.

The joint solution includes a mechanism for the Policy Engine to instruct PrivX to terminate user sessions based on observed changes in the security posture of the client device.

Benefits



1 Endpoint trust with strong authentication

Verify users and devices with modern multi-factor and/or biometric authentication built for zero trust. Ensure compliance with fine-grained security checks, immutable event logs and privileged sessions recordings – or even monitoring.

2 Protect IT and OT infrastructures

Grant verified, role-based privileged access to valuable targets in IT and industrial environments with workflow approvals, access level restrictions per task and automatic revocation of access once the job is done.

3 Eliminate credential-based breaches

Eliminate the 85% of cyberattacks that start with stolen credentials, passwords, and phishable MFA. Embrace passwordless authentication for regular and privileged users alike.

4 Enforce risk-based continuous authentication

Capitalize on real-time user and device risk signals to make dynamic access decisions at time of authentication and continuously thereafter.

5 Multi-cloud, hybrid and industrial targets included

Enjoy a single pane of glass to multiple targets in IT and OT with consistent user experience and uniform auditing.

6 Migrate to Just-in-Time, Zero Trust security

Forget the pain of vaulting, rotating, and managing passwords in most use cases. Grant passwordless access just-in-time for the session without users ever seeing or handling the secrets needed to establish the connection. The secrets expire automatically after authentication.

Background

About SSH

SSH is a defensive cybersecurity company with a mission to secure critical data and communications between systems, automated applications, and people. SSH product portfolio is developed to defend business secrets and access to them – now and in the future.

With SSH teams in North America, Europe, and Asia along with a global network of certified partners – SSH is the pioneer in secure communications serving customers for 25+ years. From large financial institutions and governments to operational technology and critical infrastructure.

The company's shares (SSH1V) are listed on Nasdaq OMX Helsinki.

ssh.com

About Beyond Identity

Beyond Identity prevents credential-based breaches by ensuring user and device trust and eliminating passwords – the single largest source of ransomware and other cyberattacks. Only Beyond Identity's cloud-native Universal Passkey Architecture delivers secure and frictionless multi-factor authentication that continuously validates user identity and device security, making user adoption easy and advancing their journey toward Zero Trust Security.

Industry leaders like Snowflake, Unqork, and Roblox rely on Beyond Identity to solve their access security challenges so they can deliver safe and efficient digital experiences for their customers, employees, partners and contractors.

beyondidentity.com

SSH

Helsinki
Global and EMEA headquarters
SSH Communications Security Corp.
Karvaamokuja 2B, Suite 600
FI-00380 Helsinki
Finland
Tel. +358 20 500 7000
info.@ssh.com

New York City
AMER headquarters
SSH Communications Security Inc.
66 Hudson Blvd E, Suite 2308
New York, NY, 10001
USA
Tel. +1 781 247 2100
info.us@ssh.com

Singapore
APAC headquarters
SSH CommSec Pte. Ltd.
24 Sin Ming Lane, #03-99 Midview City
Singapore 573970
Singapore
Tel. +65 6338 7160
sales.asia@ssh.com

The information in this document is provided “as is” without any warranty, express or implied, including without any warranties of merchantability, fitness for a particular purpose and any warranty or condition of non-infringement. SSH Communications Security products are warranted according to the terms and conditions of the agreements under which they are provided. SSH Communications Security may make changes to specifications and product descriptions at any time, without notice. SSH® and NQX™ are a registered trademark or trademarks of SSH Communications Security Corporation and are protected by the relevant jurisdiction-specific and international copyright laws and treaties. Other names and marks are the property of their respective owners.