SSH

Solution brief

Zero Trust Suite for secure communications and access

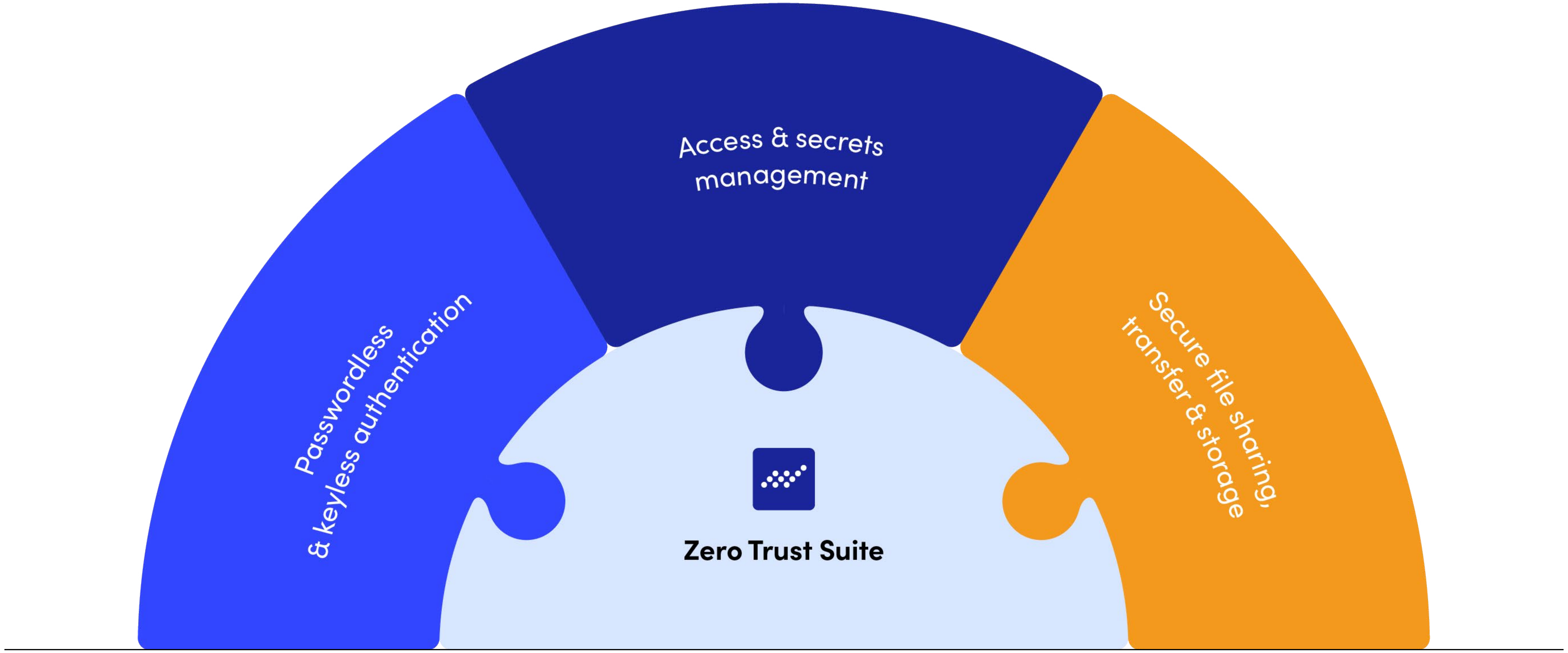
Keyless. Passwordless. Frictionless. Share, transmit, and store files securely. Manage access, secrets and shared credentials. All with SSH's modular Just-in-Time Zero Trust Suite software.

Contents

What is Zero Trust Suite?

Zero Trust Suite is a modular software solution that helps organizations to:

- Manage access and secrets in critical communications
- Authenticate to targets just-in-time without passwords or keys
- Manage, vault, and rotate credentials when necessary
- Securely share, transmit, and store sensitive information between people and applications



Typical challenges in interactive and automated connections and information sharing

Risks

- Operational service downtime
- Intellectual property and customer data theft
- Open Web Access
- Losing reputation as a company
- Disclosing sensitive information

Productivity

- Time and labour-intensive access provisioning processes – removal after use? (AlwaysOn <-> JIT, JEA)
- Too many different systems to maintain
- Security slows down operations
- Secure remote and 3rd party access
- Collaborating on sensitive information with third parties

Compliance

- Security audit failure (Industry regulations; NIS2, GDPR, SOX Cobit, PCI DSS, ISO27001, IEC62443, EO14028,...)
- Lacking up-to-date security audit reports
- Incomplete access governance
- More keys than passwords and PAMs can't handle them - PAM bypass
- More keys than passwords and controls can't handle them

Security

- Password pandemonium
- Shared credentials in the wrong hands
- Security system bypass
- Visibility: Who/what has access to what & when?
- Sender and recipient verification when sharing confidential data
- Application-to-application connections lack proper oversight

Secrets sprawl
– keys and passwords everywhere

Most companies understand the importance of managing passwords. They are also aware that a subset of passwords is particularly armed and dangerous: privileged passwords grant root or admin access to mission-critical hybrid cloud, apps, network devices, systems, and infrastructures.

Yet, 80% of data breaches start with misuse of privileged credentials, including shared credentials. Why? We believe there are three main reasons:

1 Over-dependency on permanent credentials like passwords

Passwords are being generated by the thousands and then being managed with complex processes, like vaulting. This process requires changes to the server estate, configuration files, and typically the clients, increasing system complexity and requiring constant changes to the environment. Constant changes and complexity create problems.

Let's put this into context. A customer was rotating 12,000 passwords an hour which is 184,000,000 passwords a year. Just because you can do something, it doesn't mean you should.

Even using one-time passwords (OTP) means creating them, vaulting them, and rotating them every time access is made. Vaulting and rotating credentials is an attempt to make them temporary.

2 Ignoring critical shared credentials for access closing: SSH keys

Even if a company has all their passwords managed, vaulted, and rotated, they are often alarmed to learn that 80% of their credentials are rogue. SSH keys are an access credential in the Secure Shell protocol that still powers the secure internet as we know it. They typically outnumber passwords by the ratio of 10 to 1 in IT environments.

Security controls like traditional privileged access management (PAM) solutions are built to manage passwords, and SSH keys are functionally different. Therefore, PAM solutions only handle 20% of all keys – in the best-case scenario. We know this because all our SSH key management customers have a traditional PAM deployed in-house, but they found them lacking in key management.

Skillful staff and malicious actors also use SSH keys to bypass PAM.

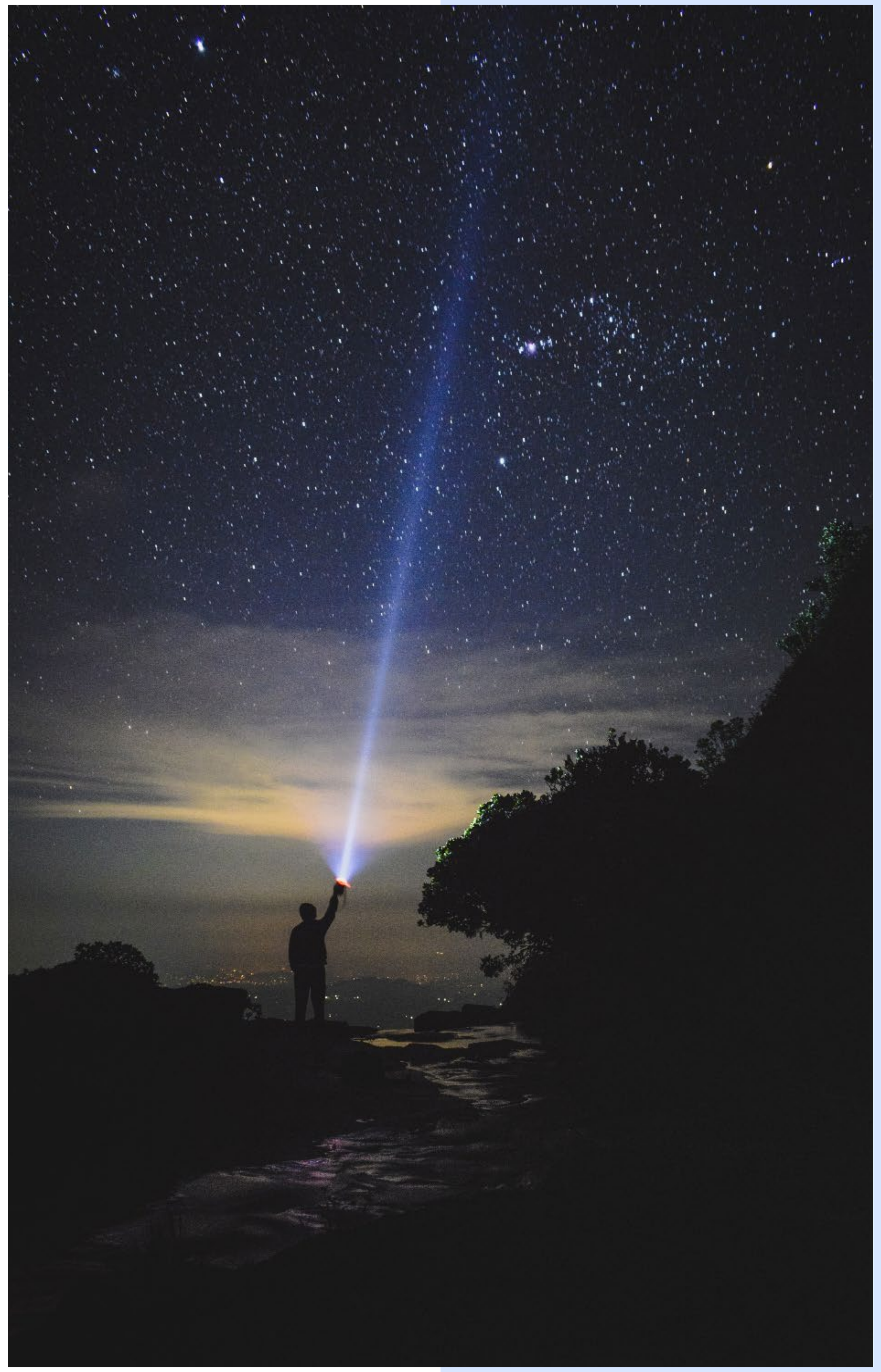
If your SSH keys are not managed, you are simply not managing your shared credentials at an acceptable level.

Let's put this into context. A customer discovered that they had more than a million SSH keys unmanaged in their environment. That's a lot of uncovered attack surface.

3 Relying only on legacy methods, like vaulting and rotating

The go-to method to manage passwords and keys for more than 15 years has been to vault and rotate them. This method has not disappeared and is still needed. However, it is no longer the most secure and efficient way to manage your secrets.

Temporary is the new black. Privileged access, (cloud) hosts, assigned roles in projects, and consultant tasks have nowadays a short lifecycle. But the secrets needed to grant access are way too often permanent (like passwords and keys).



Files gone wild – sharing sensitive data with unsanctioned tools between people and applications

Companies and organizations routinely need a way to share sensitive files between internal networks or outside their organization. Often these files are being sent using regular business applications like Outlook or Gmail or stored in services like Sharepoint or Google Drive. However, these everyday applications were not built with the need to handle data that is critical to your operations in mind. They were not designed with privacy, security and auditability built-in. Their encryption when data is sent over networks is not sufficient for sharing confidential, restricted, or secret information. And they do not allow automated file transfers between servers or applications when large, automated batch file need to travel between organizations.

Point solutions may solve a part of the problem but their management and use become a pain if every communication context requires a different solution. If a user needs to learn a different logic when sending secure emails, signing documents, working in a secure workspace or collecting information from forms, the risk of human error increases, usability decreases, and traceability becomes more challenging. It's even worse if the recipient need to make configuration changes to their systems to be able to communicate. Moreover, maintaining multiple solutions with different core architecture makes the life of your IT department all the more miserable.

The solution: Start your journey toward password-less and keyless and secure communications authentication with Zero Trust Suite

SSH keys and passwords should be managed from a single solution. Managing, vaulting, and rotating credentials is important and necessary. This is because customer environments can't be migrated overnight to something new, and some environments are so legacy that traditional methods are necessary.

But storing and rotation is just the first step. We at SSH can disarm the risk of always-on privileged credentials like passwords and keys and eliminate the pain of having to rotate and vault them.

We can get you started on a journey towards a passwordless and keyless future where the authentication to access a target is made just-in-time for the session – and that authentication expires automatically without the need to explicitly revoke it.

There are no passwords or keys to manage, every session is verified each time it's made, and users never see or handle any credentials. This is true Zero Trust and the foundation of our Zero Trust Suite.

Protect your installed base and secure your future with our solution.

> “
>
> **There are no passwords or keys to manage, every session is verified each time it's made, and users never see or handle any credentials.**

How does Zero Trust Suite work?

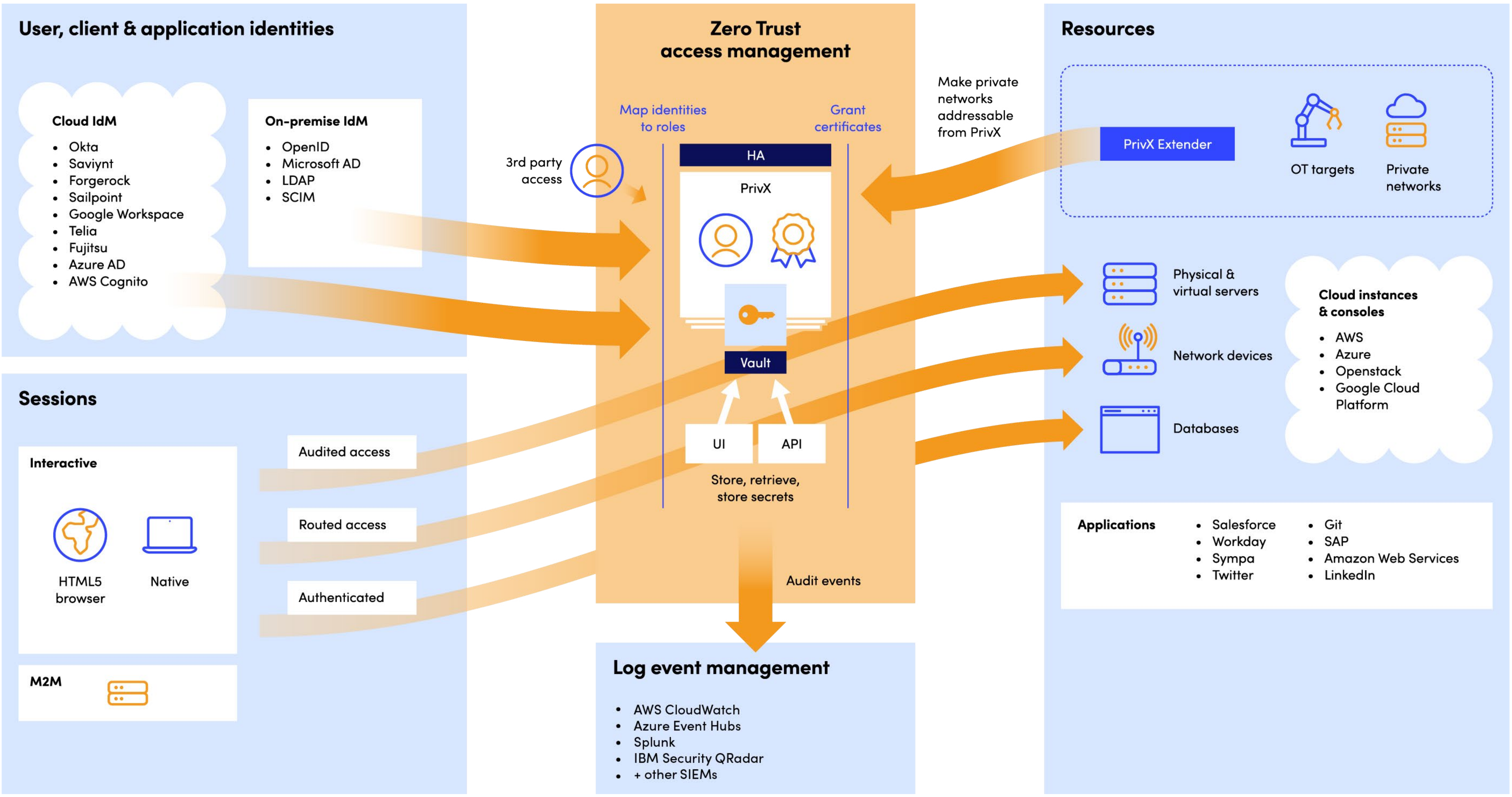
Zero Trust Suite consists of three software modules: **1. access management module**, **2. access closing and SSH key management module**, and **3. secure communications module**.

Access management module (called PrivX)

The PrivX module acts as a gateway between users (human or machine) and resources/targets.
The resources could be, for example, on-premises, physical or virtual servers, or network appliances. PrivX also supports access to multi-cloud environments or targets that are part of isolated sites/networks, which is typical for operational technology. (For these targets, we offer PrivX Extender.)
Supported connections include RDP, SSH, VNC, HTTP, but also web targets (e. g. managing access to DevOps tools, like GitHub).

1. Access based on identity

Users (human as well as machine IDs) and user groups are maintained in identity and access management systems (IAM, IGA, or IDM), Active Directory (AD)/ Lightweight Directory Access Protocol (LDAP), or through OpenID Connect (OIDC) providers. These systems contain up-to-date information about who (identities/ users/group) is authorized to access what targets and when.



User, client & application identities

Cloud IdM

- Okta
- Saviynt
- Forgerock
- Sailpoint
- Google Workspace
- Telia
- Fujitsu
- Azure AD
- AWS Cognito

On-premise IdM

- OpenID
- Microsoft AD
- LDAP
- SCIM

Sessions

Interactive

HTML5 browser

Native

M2M

Audited access

Routed access

Authenticated

Zero Trust access management

Map identities to roles

Grant certificates

3rd party access

HA

PrivX

Vault

UI

API

Store, retrieve, store secrets

Audit events

Make private networks addressable from PrivX

Log event management

- AWS CloudWatch
- Azure Event Hubs
- Splunk
- IBM Security QRadar
- + other SIEMs

Resources

PrivX Extender

OT targets

Private networks

Physical & virtual servers

Network devices

Databases

Cloud instances & consoles

- AWS
- Azure
- Openstack
- Google Cloud Platform

Applications

- Salesforce
- Workday
- Sympa
- Twitter
- Git
- SAP
- Amazon Web Services
- LinkedIn

2. Sync with AD/LDAP and targets

PrivX hosts roles and maps them to identities. It ensures that it is always in sync with user identities and user groups for any changes in AD/LDAP or OIDC systems. PrivX also stays in sync with the state of the global cloud estate for any changes, when hosts are spun up or down.

3. Role-based access

PrivX maps the user information containing the right identity and authorization to the right role. Therefore, all access to critical targets is granted using role-based access controls (RBAC). Since roles rarely change, and the information between the role and identity is always up-to-date, this approach reduces manual work.

4. Just-in-time, Zero Trust authentication

When a user logs into browser-based PrivX UI (using SSO and MFA if needed), they can only see and select the targets available to them, restricted by their role. The user does not handle or see any access secrets at any point, instead the authentication is done automatically in the background, and access is granted just-in-time. The secrets needed for the connection are contained within ephemeral certificates, which expire automatically after establishing the session, leaving no secrets behind to be managed.

If ephemeral certificates are not available, PrivX utilizes other authentication methods, like using a public key or passwords. In these cases, PrivX vaults and rotates the secrets.

5. Audit trail

PrivX allows auditing, tracking, and monitoring of every session, and the related information can be automatically sent to external systems (i.e., SIEMs) for alerting and reporting. Even when using shared accounts, PrivX creates a trace of the individual who made the connection. Sessions can also be recorded for forensics.

6. Integrations REST API

Application Programming Interfaces (API)/Software Development Kits (SDK) can be used for customized integrations. Examples of these include integrations to ticketing systems, behavior analytics solutions, and Information Technology Service Management (ITSM).

Access closing and SSH key management module (called UKM)

To manage SSH keys at scale, our Zero Trust Suite includes the Universal SSH Key Management (UKM) module.

1. Discovery and risk assessment

UKM connects agentlessly and scans your entire server estate to create an inventory that accurately represents a trust map of your SSH access. UKM discovers and records user accounts, and password- and SSH key-related data. It evaluates SSH access, records failed and successful logins, and then maps them to the actual keys used.

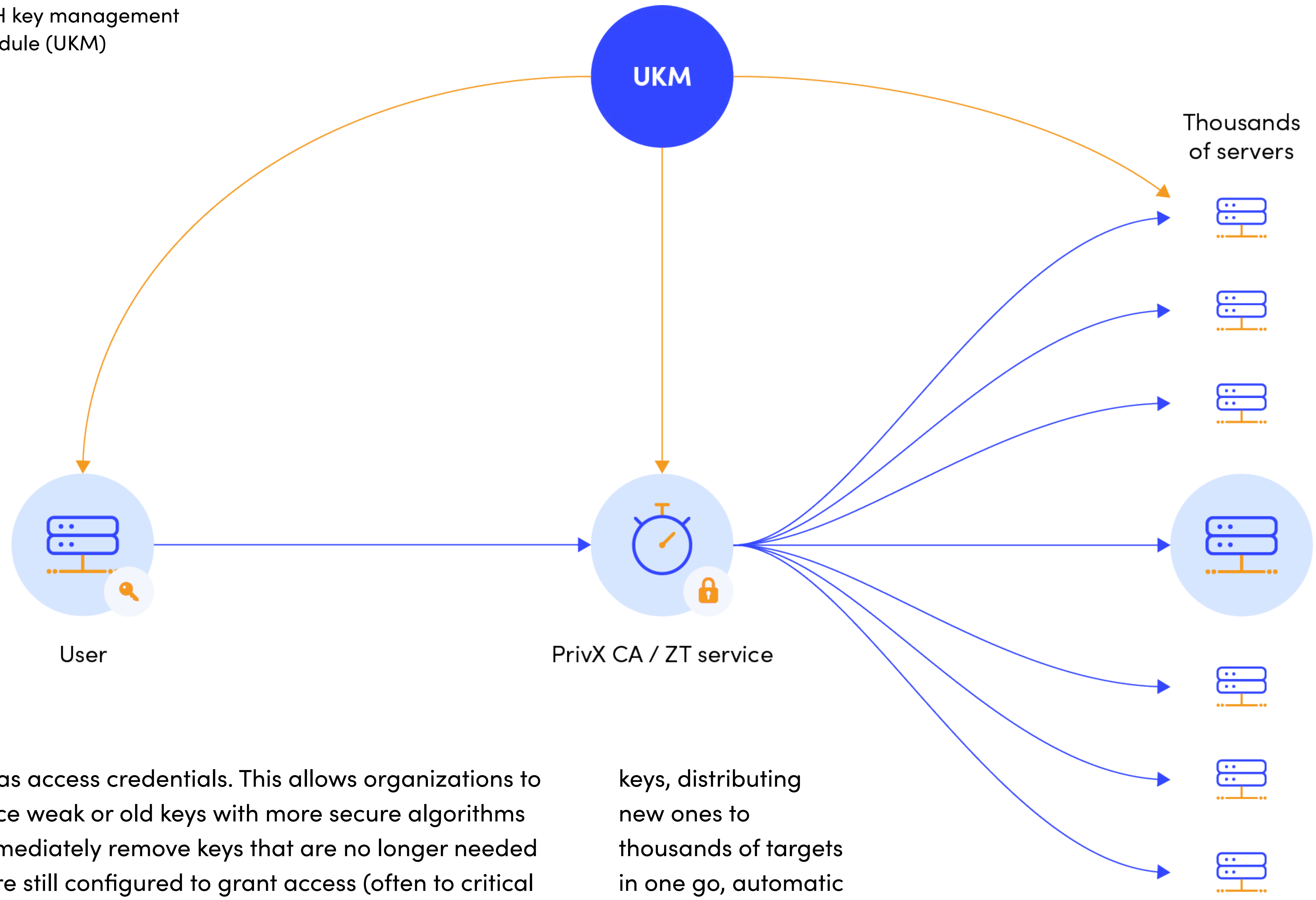
Once SSH key assets are discovered, UKM can identify best practices and regulation-violating credentials such as SSH keys using insecure cryptographic algorithms, granting access from non-production to production environments, keys no longer needed but granting unauthorized access, and more.

UKM further helps discover the use of quantum-vulnerable algorithms used within SSH, the de-facto protocol used for establishing secure communications for remote administration, configuration, and automation on-prem or in the cloud.

2. Reduce SSH key complexity and risks with UKM

Using the collected account and SSH key data, UKM can provide assessment of at-risk keys as well as determine which keys are in active use and which are no longer used as access credentials. This allows organizations to replace weak or old keys with more secure algorithms or immediately remove keys that are no longer needed but are still configured to grant access (often to critical infrastructure).

▼ SSH key management module (UKM)



UKM provides reports for internal and external auditors with up-to-date evaluation and executive summary on the level of compliance with regulations and standards such as NIST, PCI-DSS, etc.

3. Manage and automate SSH key management lifecycle

After at-risk credentials have been tackled, organizations are left with keys that are in use and needed. UKM helps perform systematic monitoring and control of the environment in a centralized platform, offering a single pane of glass view. It allows hardening of existing SSH keys, distributing new ones to thousands of targets in one go, automatic rotation when keys are too old, and removal when keys are no longer needed or are bypassing existing controls.

UKM automates the full lifecycle of SSH cryptographic keys and simplifies the effort of staying compliant. UKM includes maker/checker capabilities to provide approval flows for all key-related operations, full auditing as well as integration with ticketing tools, SMDB server inventory systems, and HSM devices. UKM also integrates with AD, Azure AD, and various identity providers via SAMLv2 protocol to ensure user directory integration and MFA.

4. Migrate to Zero Trust keyless access

It is important to point out that SSH key management is a never-ending process. Newly rotated keys eventually get too old, keys that provided authorized access eventually become unauthorized when personnel changes positions, others leave the organization, or otherwise the access is no longer necessary. The inherent property of SSH keys is never expiring, which means that they will continue to grant access until they are explicitly removed.

UKM provides the most comprehensive automated key management capabilities on the market, but with the steady increase in SSH key usage for access, automation, and configuration, our Zero Trust Suite offers a better way to administer SSH access that is aligned with the demands of the future.

Once the SSH key estate is under control, UKM module provides mechanisms to automatically and transparently migrate SSH access – to radically reduce the overhead of managing permanent SSH keys and move to keyless, just-in-time Zero Trust access with short-lived certificates.

The UKM module uses its knowledge from the previously mentioned trust map to successfully move access away from keys. The shift from SSH keys to ephemeral certificates via PrivX as the authentication method is done transparently to the underlying applications that rely on the SSH connectivity. This ensures that the shift does not require changes in the infrastructure or the applications themselves.

> “
>
> **UKM helps perform systematic monitoring and control of the environment in a centralized platform, offering a single pane of glass view.**

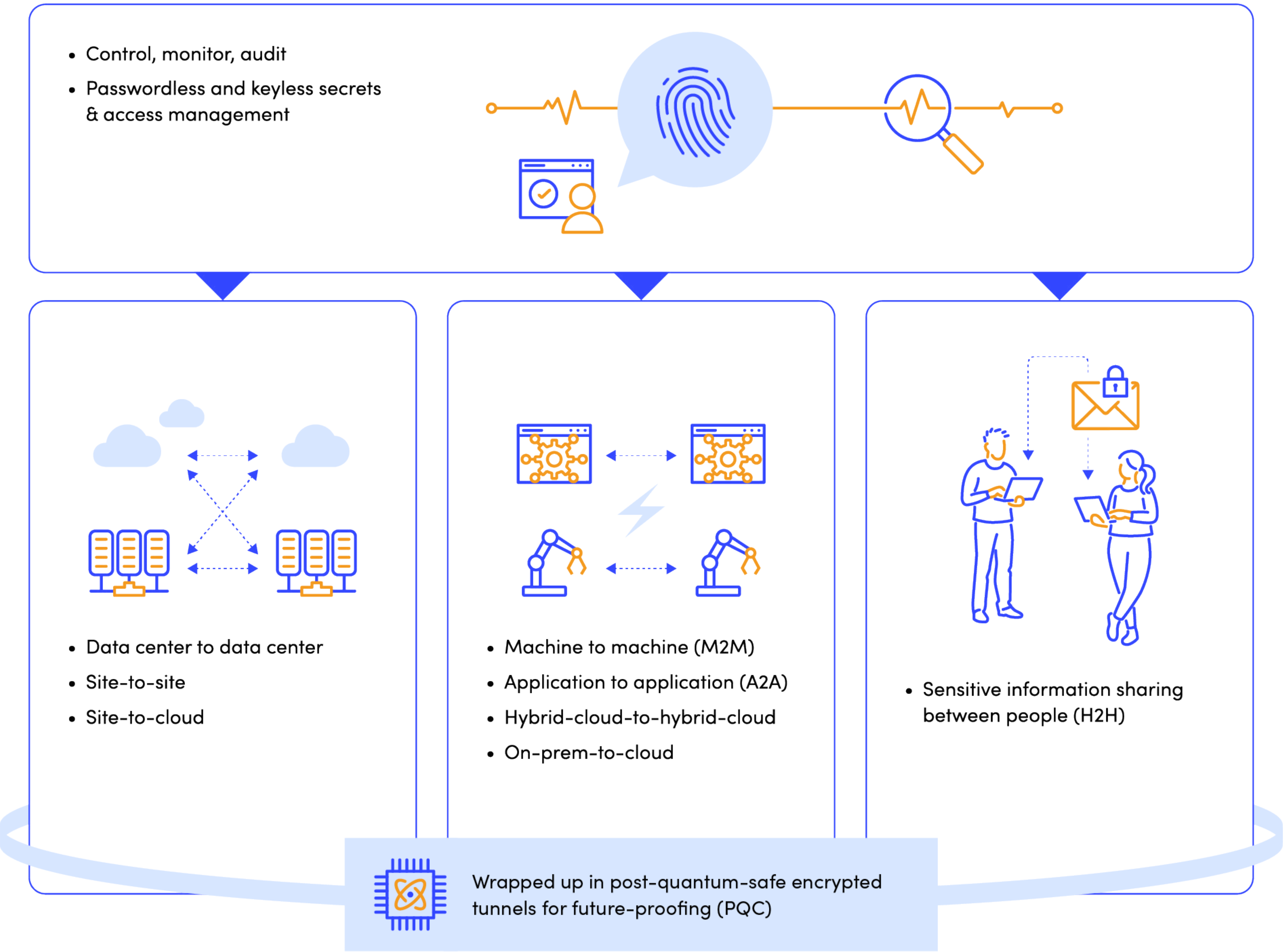
Secure communications module

Our secure communications module helps you answer the following questions when sharing, transmitting, or storing sensitive information:

- Where is your sensitive data stored?
- Who or what (applications) have access to it?
- Who is actually accessing it?
- When is it being accessed?
- How is it being accessed?

The module allows organizations to centralize their interactive and automated data sharing into a single solution. The benefits include:

- Routinely share sensitive files between internal stakeholders and third parties without the risk of data disclosure
- Handle data that is critical to business operations with a security-first mindset
- Enforce strict control and policies when sensitive data is in transit or being accessed
- Apply various authentication methods, including passports, bank IDs, or a range of multi-factor authentication (MFA) methods
- Verify the sender and recipient when data or documents are being shared or transmitted in a true Zero Trust fashion
- Restrict access from read-only to editing – or just to notifications of actions
- Allow highly secure workspaces and data collection forms for confidential projects
- Sign confidential documents with tamper-proof security
- Produce a solid audit trail of activities for any action
- Enjoy high availability for file sharing
- Routinely automate file transfers for batch jobs or massive data transfer need



- Control, monitor, audit
- Passwordless and keyless secrets & access management

- Data center to data center
- Site-to-site
- Site-to-cloud

- Machine to machine (M2M)
- Application to application (A2A)
- Hybrid-cloud-to-hybrid-cloud
- On-prem-to-cloud

- Sensitive information sharing between people (H2H)

Wrapped up in post-quantum-safe encrypted tunnels for future-proofing (PQC)

Path to passwordless and keyless

SSHerlock is an SSH key and post-quantum resilience discovery and audit self-service tool that can scan your entire SSH key estate and identify policy and compliance violations related to SSH keys.

Learn more & get SSHerlock for free →

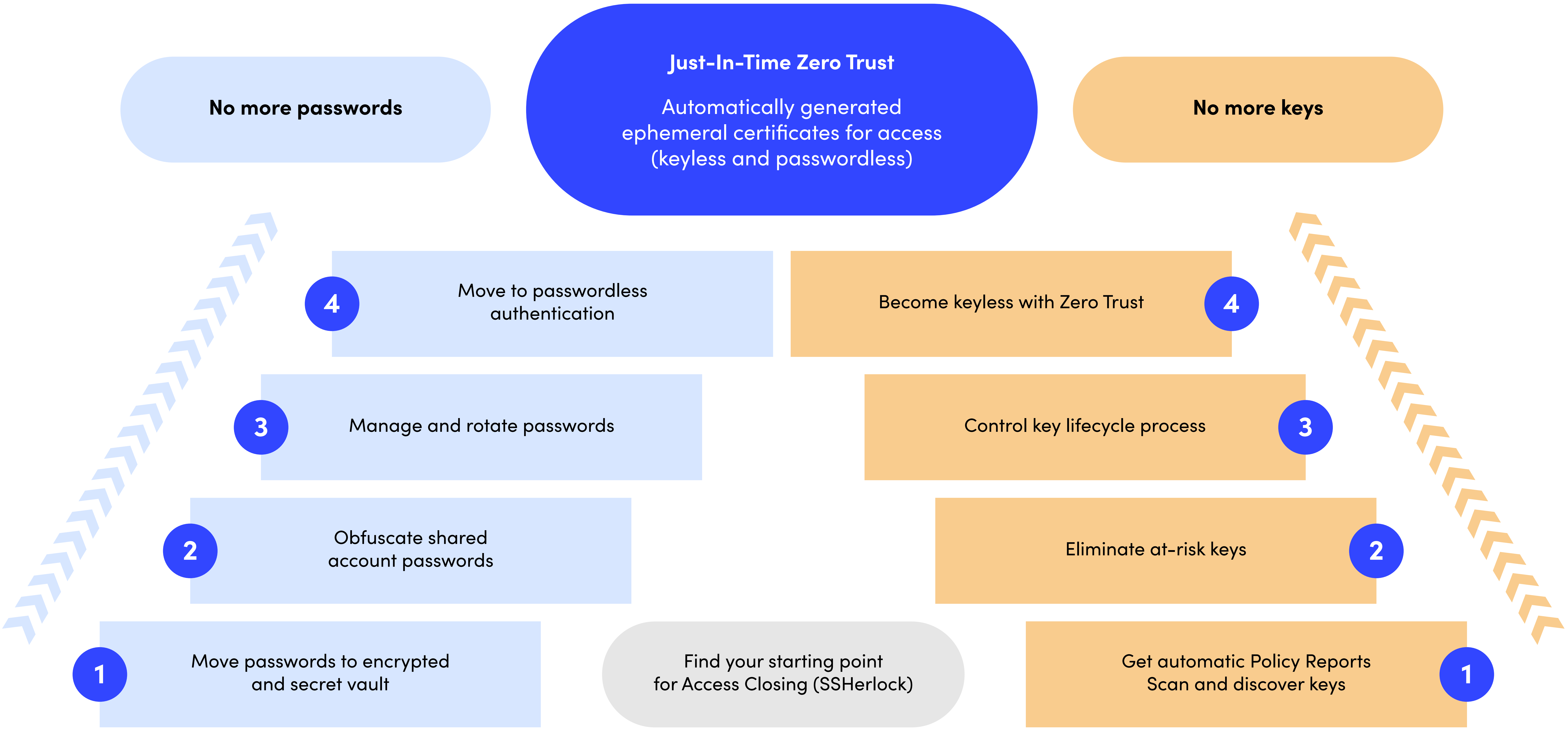
The journey to passwordless and keyless authentication doesn’t happen overnight but is a gradual process. Our customers typically go through these steps when embarking on their journey. What is your maturity level?

1. Basic
Your passwords are secured in an encrypted and secret vault. Your keys are scanned and discovered with reports demonstrating the state of your SSH key estate.

2. Intermediate
Shared account passwords are obfuscated to prevent their easy misuse. You have the means to reliably eliminate rogue, risky, and obsolete keys.

3. Advanced
You are managing and rotating your passwords in a systematic fashion in your environment. You can control your SSH key lifecycle process in an automated fashion.

4. Expert
You have migrated to passwordless authentication that leaves no passwords to be managed. You have migrated to keyless authentication that leaves no keys to be managed.



No more passwords

Just-In-Time Zero Trust

Automatically generated ephemeral certificates for access (keyless and passwordless)

No more keys

4 Move to passwordless authentication

Become keyless with Zero Trust 4

3 Manage and rotate passwords

Control key lifecycle process 3

2 Obfuscate shared account passwords

Eliminate at-risk keys 2

1 Move passwords to encrypted and secret vault

Find your starting point for Access Closing (SSHerlock)

Get automatic Policy Reports
Scan and discover keys 1

Benefits

Stop security control bypass

Achieve access closing by managing all your secrets, including passwords, keys, and tokens, and stop security control bypass with unauthorized SSH keys or shared credentials.

Prevent misuse of shared credentials

Shared accounts and SSH keys don't have identities. With the keyless and passwordless approach, access secrets are hidden from your users from end to end, but you always have full visibility and know who has access to what.

Utilize on-demand access and auto-revocation

Provide just enough access (JEA) just-in-time (JIT) to the right target for the right duration to the right identity. Prevent always-on, too broad, or unauthorized access by making all access temporary by default and access revocation automatic. Vault credentials only when necessary.

Ramp up security, save on costs

The passwordless and keyless approach leaves no credentials behind to be managed, rotated, or vaulted. What doesn't exist cannot be stolen or shared, nor it needs to be managed. Reduce costs by radically reducing complexity and simplifying processes.

Centralize secure communications

Handle all your interactive and automated file sharing and transmission needs consistently and coherently from a single solution.

Collaborate securely

Turn on government-grade security for your business collaboration with our solution. Stay secure when sharing, signing, collaborating on or collecting sensitive data.

Stay compliant

Demonstrate compliance and adherence to regulations with a solid audit trail of activities and strong identity for every access.

Protect human as well as machine connections

Identify and manage access to human-to-machine, machine-to-machine, and application-to-application connections alike. Manage also machine-generated credentials.

Minimize changes to your environment

Permanent passwords and keys are not only a risk, but they also clutter up your environment, even when under management. With the keyless and passwordless approach, you can minimize the changes to your environment, bringing it closer to an immutable infrastructure.

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