SSH.COM

WHITEPAPER

From Permanent Credentials to Ephemeral Certificates

Lean privileged access management for streamlined operations, better business speed and improved security

Executive Summary

Connecting privileged users with assets in a complex and fast-moving environment

Traditionally, privileged access has been divided into two categories: those who have access to mission critical or highly-sensitive data and those who manage that access.

With traditional privileged access management (PAM) solutions, you grant that access per user and per host.

However, since the digital world is changing at lightning speed, companies are hard-pressed to find all the required skills and expertise in-house, no matter how big, small or versatile they are.

Organizations today therefore need external help, new types of job roles, temporary workforces, 3rd parties of 3rd parties, etc. All of a sudden, you have a disparate groups of people requiring privileged access to all kinds of environments for different periods of time and needing it now.

PrivX, a lean, zero-trust access management tool, offers a modern solution. Organizations can deploy this agentless solution in minutes, and streamlined ephemeral certificate authentication replaces cumbersome and risky permanent credentials.

The Back-end In Turmoil

The back-end is also in a constant state of change. First, there was a shift from physical to virtual servers, where one physical server hosts multiple virtual instances, and today organizations are shifting workloads to the cloud and oftentimes using multiple cloud service providers at once. This creates a complex hybrid hosting environment. The latest development is that your hybrid servers might host multiple containers, further complicating the landscape!

As if all this wasn't enough, there's the dimension of time. The time that a particular instance stays available for access just keeps getting shorter. Ideally, virtual servers are ramped up and down as per need, so that you only pay for what you use. With clusters of containers, the access might exist only as long as it takes to complete a mathematical calculation. Often that time is measured in milliseconds!

Then there's the product development cycle. Gone are the times when companies released two software updates per year. In today's fast-paced industry, you may update your product multiple times a day! We also have a bonus feature: the introduction of new regulations, such as the General Data Protection Regulation (GDPR). Any time someone handles sensitive data, companies need to demonstrate a justified reason for doing so. And a rock-solid audit trail to boot.

> **Only 19.8% of enterprises have 3rd party risk management at recommended levels**
>
> —Hong Kong Enterprise Cyber Security Readiness Index report

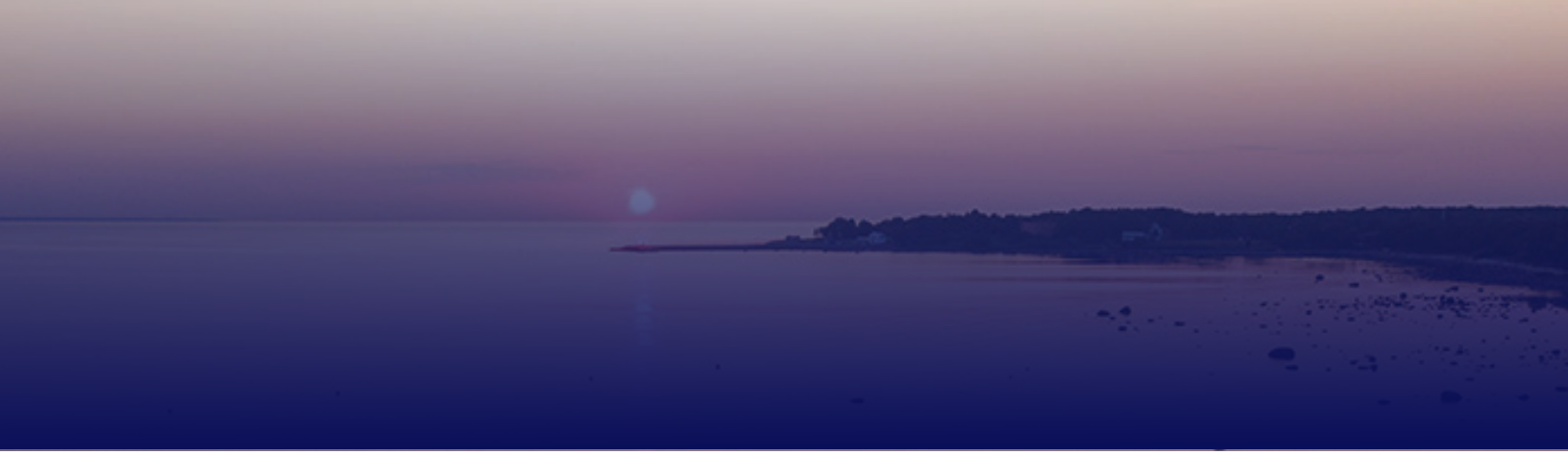
Permanent Access Credentials Are Dead

Most traditional PAM solutions are designed to support permanent access credentials. Their problem is that they are too static and slow to configure, in addition to being too easy to leave behind. When you pair that with the fact that the-

1. number of people who have privileged access has exploded
2. access needs are often short-lived
3. hybrid and multi-cloud environments are under constant change
4. and your software developers want to work at the speed of cloud

...traditional solutions introduce too many obstacles.

We have seen the results. Companies lose track of who can access what resources and what those people are doing there. Furthermore, companies waste a lot of money when developers wait for access while admins work to grant that access. Based on our calculations, every three minutes it takes to access resource can cost a large company somewhere near half a million dollars a year.



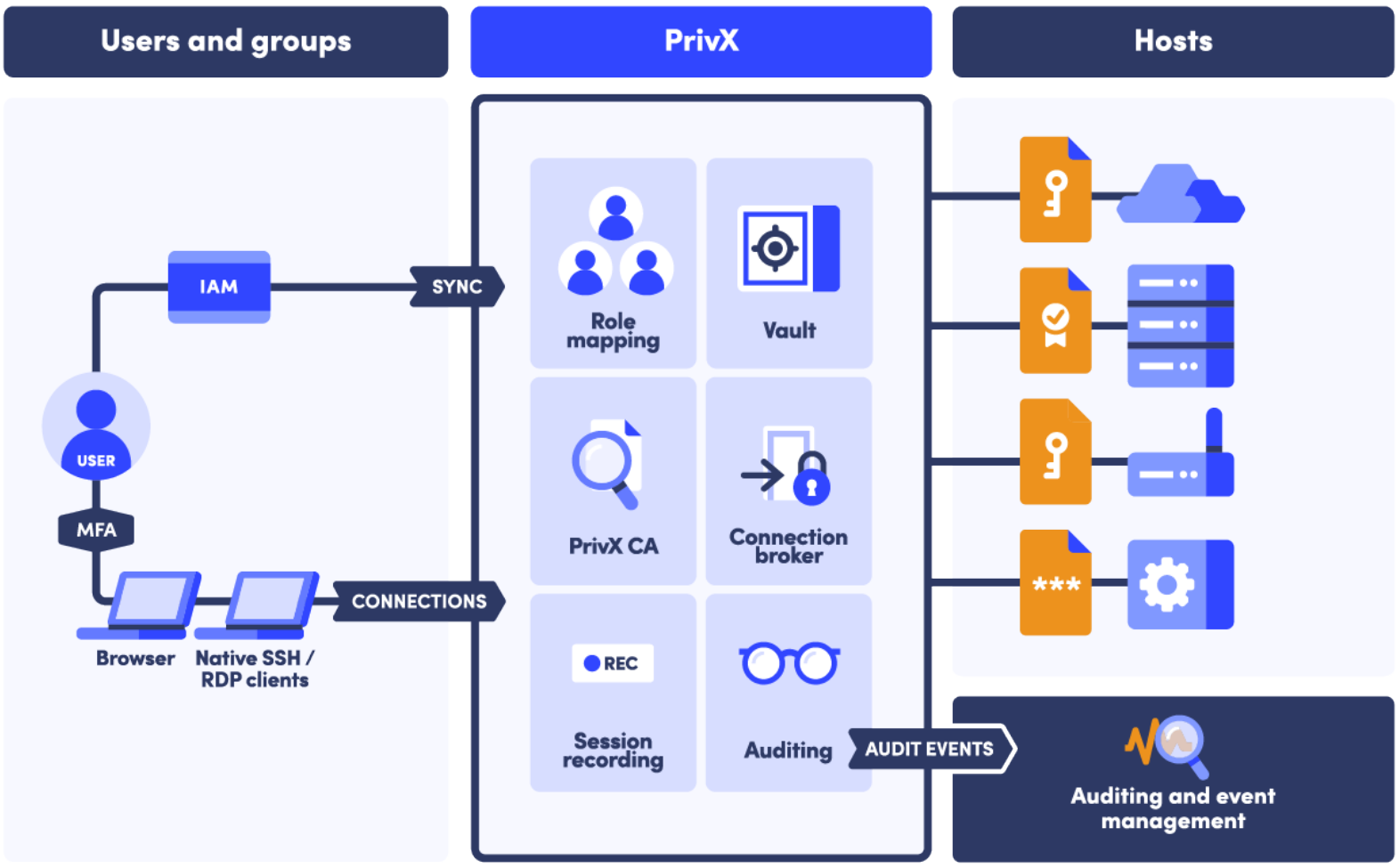
What are the shortcomings of traditional PAM in today's environment?

No matter how much the world changes, you still need to manage who is allowed to access mission critical data in your organization. There are a lot of PAM solutions in the market, but they rely largely on technology that was relevant a decade or more ago. They are not built for the age of the cloud. Some problems include:

- a hefty price tag for enterprise deployment
- deployment times in months or years and still resulting in unfinished deployments
- hard-to-maintain endpoint agents on clients and hosts
- creating and maintaining a duplicate directories for privileged users
- storing permanent access credentials in a vault and rotating their passwords
- poor fit for multi-cloud and DevOps where legacy methods are almost ideologically opposed
- poor fit for sysadmins, database administrators, technicians and software developers who need access faster that it can be granted

The Solution

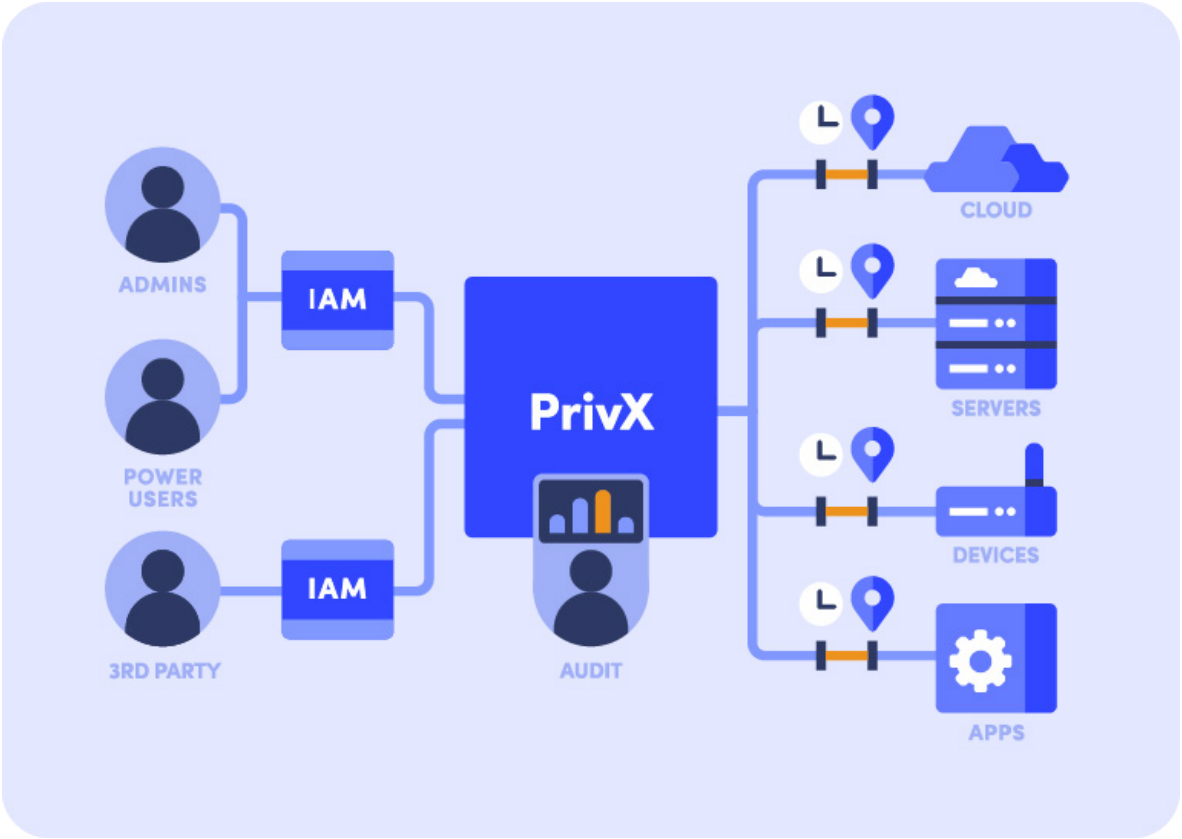
Credentialess And Ephemeral Access



It’s time to rethink the entire access paradigm

We believe in keeping a lot of the traditional PAM functionality but re-designing the way it is used and set up.

That is why we developed PrivX. It is an access authority that stands between users and hosts and builds a permanent trust relationship between them. All privileged traffic is directed through the access authority that stays immune to changes in your front-end and back-end.



No permanent privileged access to anyone

We don't believe in permanent access credentials. Even if you protect them carefully, they can be stolen, forgotten or duplicated. Instead, PrivX uses ephemeral certificates that exist only as longs as they are needed to authenticate privileged connections - and then disappear automatically.

Credentialess access

In fact, we believe that privileged access to hybrid and multi-cloud environments is best created without using any type of access credentials. All the privileged users just log in to PrivX, the access authority, and they gain entry to the appropriate environment without using any type of access credentials.

On-boarding & off-boarding made easy

The result of RBAC is that on-boarding, off-boarding and changing roles or devices does not have any effect on privileged access management: if a user is added to or removed from the IMS, her privileged access status is accordingly automatically updated.

Cloud asset auto-discovery

Your IT administrator needs to set up the access role configurations to your multi-cloud environment only once. New cloud instances are autodiscovered automatically after that. Your multi-cloud environment can change, you can scale your host needs up or down, and you are kept up-to-date on the state of your global cloud inventory automatically.

3rd party & external workforce secured and tracked

PrivX comes with detailed logging and session recording for playback. This gives you the confidence to work with the 3rd parties of your choice, as regardless of their security policies or devices, every privileged connection is properly logged and accounted for.

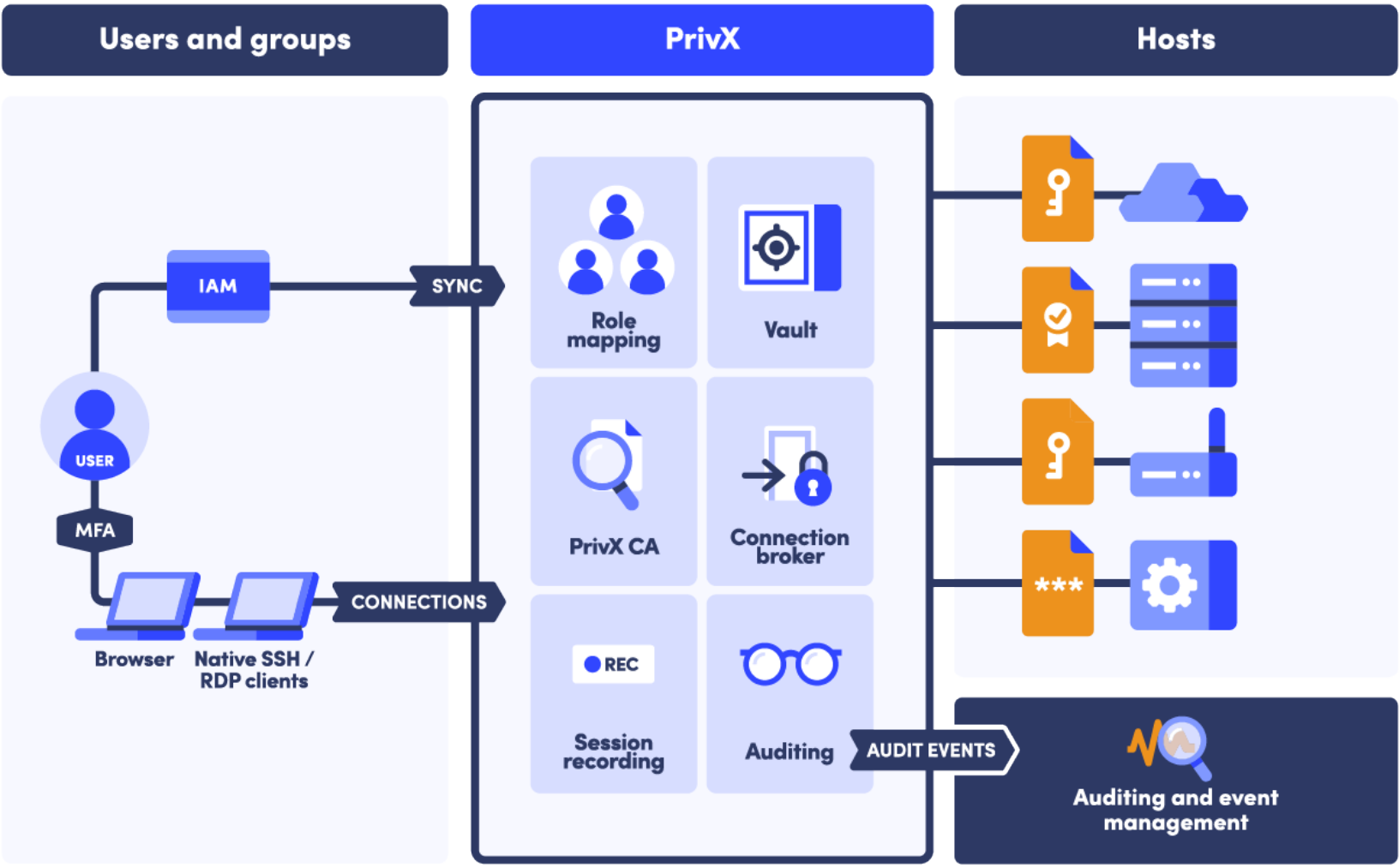
No duplicate directory for privileged users

We believe in role-based access control (RBAC) where access is no longer managed per individual user but per access role. User identities are already defined in your corporate directory (AD/LDAP) or identity management system (IMS). Since those identities are already in groups, PrivX fetches them automatically for your admin. All your admin needs to do is to associate those groups with their level of access.

No agents to install, configure or update

This is what makes the infrastructure truly nimble. It frees your entire development team to focus on working instead of managing or waiting for access. Since you only have the central access authority that updates automatically, there are no obsolete or vulnerable software components n the cloud or on your users' devices. This is a huge improvement to both convenience and security.

Elastic cloud access gateway for ephemeral access



How does PrivX work?

Identity Management and User Authentication

PrivX integrates with existing identity management solutions for user authentication. The supported identity management solutions include:

- LDAP
- Google G Suite
- Microsoft Active Directory (AD)
- Azure Active Directory (AD) via Graph API
- OpenID Connect (OIDC) Identity Providers (e.g. AWS Cognito, Okta, Ubisecure)

This means that your existing tools and user management processes don't have to be changed. Users are managed in the existing IAM solution, and PrivX will authenticate the users with the existing system. Once authentication is done, PrivX fetches the user's attributes from the IAM so that it can map users to their roles based on the role configuration.

PrivX can integrate into multiple IAM systems at the same time. This makes it easier to manage heterogeneous, complex environments.

Roles

PrivX controls access to the target system based on user roles, which are created based on rules. The rules for particular roles are generated according to security policies and access requirements. PrivX fetches the rules for each role from the IAM system, and uses them to determine proper authentication. This system alleviates setting up access for each individual user and enables streamlined updates to groups of users.

Access by ephemeral certificates

With PrivX, the primary method of authorizing sessions is with ephemeral certificates. The connections are established using existing encryption protocols (SSH/RDP/HTTPS), but the primary method of access authorization of the user to the target host is based various industry-standard certificates. Even if the target server does not support certificate-based access, there are other options available.

HOW DO EPHEMERAL CERTIFICATES WORK

The access is also called 'credentialess', since on establishing the connection the user does not handle access credentials at all. Instead, the user logs in to PrivX each time he or she wants to establish a remote connection without having permanent authorization to the environment.

In ephemeral certificate-based authorization, the target systems are accessed without the need for permanent access credentials, explicitaccess revocation or traditional SSH key management. For each session, the ephemeral certificate:

- is issued from the Certificate Authority (in this case PrivX), which serves as the trusted third party
- is based on various industry-standard methods, the chief example being the short-lived X.509 certificate
- encodes the target user ID for security
- has a short lifetime (5 minutes) after which it autoexpires

USER ACCESS CONFIGURATION

PrivX controls access to the target system based on user roles, which are created based on rules. The rules for particular roles are generated according to security policies and access requirements. PrivX fetches the rules for each role from the IAM system and uses them to determine proper authentication. This system alleviates setting up access for each individual user and enables streamlined updates to groups of users.

TARGET SYSTEM ACCESS CONFIGURATION

The target systems must be configured to support credentialess access. The configuration is static, meaning that it needs to be done only once when the servers are provisioned. Credentialess access does not change if user roles/job functions change or users are added or removed from the identity management system. The target systems must be re-provisioned only if there are changes in the roles and their mappings to the operating system level accounts that define which access roles have the right to perform which functions on the target server.

The configurations that allow credentialess access are like templates that serve a function. This means that multi-cloud instances (such as Amazon Web Services, Microsoft Azure, Google Cloud or OpenStack) can be scaled up and down at will, but the templates remain immune to the changes and continue to provide access as per purpose, for example, access to financial data, system databases, production environment etc.

EPHEMERAL CERTIFICATES IN CONJUNCTION WITH SECURE PROTOCOLS

OpenSSH certificates
The SSH access is implemented with OpenSSH certificates. The certificates encode the user roles and the SSH server configuration on the target server maps the roles into the operating system level accounts.

Windows RDP access
The Windows RDP access is implemented with a virtual smart card. PrivX acts as the smart card in RDP authentication. The smart card's certificate is created on-demand when the user opens the RDP connection. The certificate is enrolled for an ephemeral keypair which is discarded after the authentication has been completed. The virtual smart card authentication is fully automated and invisible for the end users.

HTTP(S)
The user makes a connection to a sandboxed browser which then browser establishes the HTTPS connection to the target resource. PrivX creates a web-access credential and authenticates the session from the browser sandbox; the new credential is never stored in the browser, target host or on the client. The user never handles the credential used to access the target resource.

The target host can be configured to only allow access from the sandboxed browser that PrivX creates, and vice versa.

Non-certificate access
If the target server does not support OpenSSH, RDP or HTTP(S) certificates, PrivX uses role keys instead. The role keys are standard SSH keypairs. The public key associated with the role key is configured for the file that defines which private keys are allowed to access the target host, and the corresponding private key is held in PrivX's secure key storage. The user will never get access to the private key that is associated with the role. Users can only use it indirectly via PrivX to authenticate and authorize the access, based on their access role defined in PrivX.d vice versa.

Conclusion

Today's fast-paced and complex IT environment requires agile security solutions. SSH.COM delivers PrivX, a lean zero-trust access management solution, which offers a modern alternative to traditional PAM, and is ideally suited to today's rapid-fire DevOps applications and hybrid, multi-cloud environments.

Ephemeral certificate authentication avoids password and credentials management, adding convenience and security, while the agentless deployment scheme results in faster deployments. RBAC and simple integration with existing identity management systems further facilitate implementation, and deployment time is measured in days rather than months.

LEARN MORE

Finland

SSH Communication Security Oyj
Karvaamokuja 2 B 00380 Helsinki
www.ssh.com
+358 20 500 7000
info.fi@ssh.com

USA

SSH Communication Security, INC.
434 W 33rd Street, Suite 842
New York, NY, 10001, USA
www.ssh.com
+1 781 247 2100
info.fi@ssh.com

Hong Kong

SSH Communication Security LTD.
35/F Central Plaza, 18 Harbour Road
Wan Chai
Hong Kong
www.ssh.com
+852 2593 1182
info.fi@ssh.com