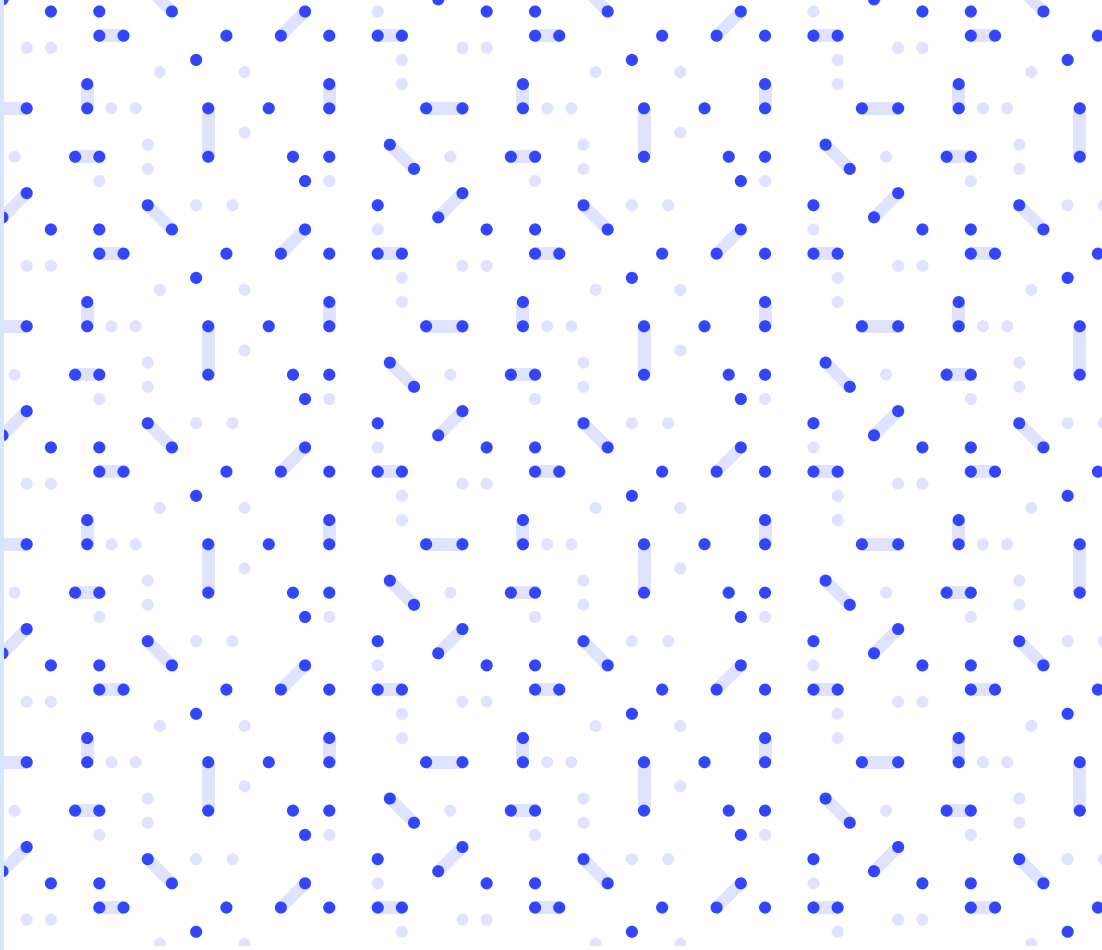
The Future of Cybersecurity is Passwordless and Keyless

White paper

Index



Introduction: From managing the problem to removing it

Every one uses passwords. Also we at SSH Communications Security (SSH) who have pioneered best-of-breed cybersecurity products for a diverse range of use cases for a long time. Our primary goal at SSH is to provide simple and secure privileged access management (PAM), while securing communications between people, systems networks, and applications.

But **cybersecurity needs have evolved greatly** since our founding. The cloud has dramatically altered the cybersecurity landscape, hacking attempts have become more sophisticated, and even the most equipped and established companies continue to experience breaches.

In 1995, the founder of SSH, Tatu Ylönen, witnessed a hacking incident in the Finnish university network that was unprotected. He saw a need and developed a long-awaited solution in the form of the Secure Shell (SSH) protocol to encrypt data transmissions. It now secures millions of transmissions every day.

Passwords date back to the 60s. And just like passwords, SSH keys are access credentials in the SSH protocol. Since both **passwords and SSH keys are permanent credentials that provide access to critical information, both must be managed to mitigate security risks**.

Information protected by these credentials might include:

Just as Tatu saw a need 25 years ago, we see a need today. Despite our best efforts in the cybersecurity industry to manage them, passwords and keys repeatedly cause breaches, increase risks, and management issues.

It's time to alter the way we think about permanent access credentials, by doing away with them entirely. We at SSH have introduced a new wave of passwordless and keyless solutions that eliminate the need for complex and costly SSH key and password management processes.

This white paper explores the numerous benefits of passwordless and keyless solutions and reveal why you are better without keys, passwords, and other permanent credentials.

The future is passwordless and keyless, and it is not a question of "if", but "when" and to "what extent."

We're the problem: How human error impacts cybersecurity

Even the strongest credentials and the most robust security systems are rendered redundant when human error occurs. Wherever passwords and keys pass through human hands, human error (both accidental and malicious) poses a significant risk. Common examples of human error during password and key management include:

- **Sharing of credentials:** Passwords and keys can easily be shared or copied, both within an organization and with third parties. This can lead to exposure and unauthorized access.
- **Insufficient training:** Employees must be trained on the risks associated with poor credential management. Despite infrequent password updates and key rotation, 89% of consumers say they feel secure in their current credential management habits — indicating a gap in credential management training.
- **Neglected policies:** Because passwords and keys do not automatically expire, it is easy to forget to delete your keys at the appropriate time. This leads to the accumulation of rogue keys, and their associated risks, in IT environments. In the case of passwords, this results in passwords being reused across the board or the default password never being updated.

Each of these instances represents a vulnerability that could be exploited by hackers. In fact, **poor password and key security cause an estimated 81% of data breaches**. As Bret Arsenault, Chief Information Security Officer (CISO) of Microsoft, put it: "Hackers don't break in. They log in."

In a passwordless and keyless environment, the user is never required to handle keys or passwords necessary for privileged access. The privileged credential ceases to exist after it has been used to gain access. This eliminates two fundamental sources of risk while making privileged access management processes more streamlined, user- friendly, and cost-effective.

A passwordless approach is also future-proof because it accounts for further advances in technology and the increasingly sophisticated cybercrime we expect to see in the coming years.

Passwordless isn't just the future of enterprise security — it's already here. The iPhone's Touch and Face ID feature, as well as adaptive multi-factor authentication (MFA) that relies on behavior analysis of user activity, are just two examples of existing passwordless security solutions.

In 2022, Gartner placed 'Passwordless Authentication' at the center of its Tech Radar as the most important trend over the next 12 months.

Source: Gartner

How does passwordless and keyless work?

Eliminating passwords has been a long-standing goal in the cybersecurity world, but the term "passwordless" is only just beginning to see real traction in the marketplace. According to Ant Allen, Vice President Analyst in Gartner Research, the past year has "seen a small increase in client inquiries specifically citing 'passwordless'" and other passwordless approaches.

Passwordless isn't necessarily a specific product or technology — it's a goal. Adopting a passwordless approach to cybersecurity requires enterprises to adopt the necessary technologies, products, and services to shrink and eventually eliminate the use of passwords and keys in their organization.

Typically, we rely on passwords, keys, and other "knowledge factors" to gain or grant privileged access. Knowledge factors, as the name suggests, must be known or remembered by their end-users. With passwordless authentication, end-users don't require knowledge factors — instead, they gain access using either:

- **Possession Factors:** Something the end-user "has", like a phone, email account, or magic link.
- **Inherent Factors:** Something the end-user "is", like a fingerprint, eye or facial scan.

End-users will use possession factors, inherent factors, or a combination to unlock a public key, which is provided during registration to your relevant authentication service. This public key interacts with a private key, which contains the necessary secrets for establishing a private connection. The end-user never accesses the private key, allowing for a passwordless experience.

Passwordless authentication is not impervious to hacking — no authentication system is! However, a passwordless approach is considerably safer than relying on knowledge factors. Passwordless credentials are harder to crack, meaning passwordless environments are less prone to cyber-attacks.

Benefits of passwordless and keyless approach

Here are some of the many benefits of taking a passwordless approach to cybersecurity.

Eliminate the problem of weak passwords

In dynamic workplace environments, many employees reuse passwords, create similar passwords, or implement simple passwords. While this proves convenient for the employee, it considerably increases the risk of a password being compromised.

In a passwordless environment, the possibility of employees leveraging weak passwords ceases to be a problem and password rotation is no longer necessary.

No forgotten password requests

Whenever a password is forgotten, the user has to undertake a password recovery process, which can often be time-consuming and disruptive to day-to-day operations. In a passwordless environment, forgotten password requests are a thing of the past, eliminating tedious recovery processes and ensuring rapid, immediate access for all authorized users.

According to Forrester, the annual allocation for password-related support costs in many large US companies exceeds 1 million USD.

Source: Last Pass

Put an end to rotation and lowers support costs

Let's have a show of hands: who enjoys password or encryption key rotation? That's right, no one! But it's been a given that rotation is simply par for the course in password management. Until now.

By removing the need to rotate keys or support password management processes, a passwordless approach greatly minimizes your organization's processing power. This saves you time and resources, in addition to cutting down overall costs.

Let's put this into perspective: one of our customers — a financial institution — performed **over 50,000 key rotations per month**. They were able to manage this hefty task with our key management solution, but when they heard about a better way, they seized the opportunity immediately and began their migration to a keyless paradigm.

No need to store or vault passwords or keys

Another given is password or key storage, which is often referred to as "vaulting" when discussing privileged credentials. Storage is cumbersome and frustrating for many end-users and poses significant potential for error. To effectively store passwords or keys, password storage or vaulting solutions must be kept up-to-date with the appropriate configurations in the server environment.

A passwordless environment eliminates permanent passwords, keys, and credentials altogether, eradicating the need to remember or store them. It also eliminates the labor associated with onboarding passwords to a vault, rotating passwords, and continuously modifying your environment to ensure that vaulting is functioning as it should be.

Improved user experience

In passwordless environments, there's no need to create sufficiently complex passwords, store and remember them, or change them regularly. This improves user experience by eliminating the possibility of forgotten passwords and by providing automatic access for authorized users, which removes the need to input various passwords manually into the user's many tools and platforms.

Passwordless environments deliver a user experience that is ultimately more streamlined, reliable, and secure.

Reduce compliance and breach concerns

With less room for manual error or password mismanagement, passwordless environments greatly reduce compliance concerns like weak, shared, or overused and overlapping passwords or keys.

And because passwords represent a security threat in their own right, with 81% of data breaches caused by poor password and key security, going passwordless reduces more than 80% of your breach risk.

Keep your environment clean

Complexity creates points of failure, and traditional password and key management solutions are rife with complexity and error-prone manual processes. Passwordless environments simplify password, key, and credential management processes, keeping your environment streamlined and dependable.

Get ahead of the game

Like Microsoft, Gartner, and many other organizations in the cybersecurity industry, we at SSH recognize that passwordless is the future.

Uber has their own certificate authority, Facebook has built scalable and secure access with SSH and Netflix has its BLESS. These are some of the most forward-looking companies in the world, and they were looking for ways to solve their access challenges without having to manage keys or passwords.

These tech giants built their solutions in-house. The good news is that we've built a commercial solution that allows you to achieve the same objective, with a fraction of the effort.

Early adopters of passwordless environments will be better able to migrate to passwordless at a pace that suits them and will be ahead of the game by the time we begin to see widespread adoption in the market.

The concept of Zero Trust

A passwordless approach supports the Zero Trust model, which is a framework for securing infrastructure and data with a mind toward modern digital transformation. This security framework requires all users to be authenticated, authorized, and continuously validated before gaining or retaining access.

There are **three fundamental principles of Zero Trust**:

1 Continuous verification

There are no trusted safe zones. Always verify access, for all resources, all the time. Only when risk levels change is workflow interrupted, which allows for continuous verification without sacrificing user experience.

2 Limit the “blast radius”

Minimize negative consequences of external and internal breaches through identity-based segmentation and the principle of least privilege.

3 Automation and real-time processing

There are no trusted safe zones. Always verify access, for all resources, all the time. Only when risk levels change is workflow interrupted, which allows for continuous verification without sacrificing user experience.

How Zero Trust works in the SSH solution framework

Zero Trust security involves using advanced technologies (including identity protection and encryption, risk-based MFA, and robust cloud workload management) to verify user or system’s identity and grant access accordingly.

Zero Trust also supports the continuous monitoring and validation of endpoints. This enables you to consistently and reliably enforce policies that reduce security and compliance risks.

We at SSH focus on passwordless and keyless access management and see that Zero Trust and just-in-time (JIT) access are inseparable. By fostering simple and immediate access to critical data, a passwordless keyless approach makes it significantly easier to adopt the Zero Trust model.

And here’s why:

1 Put a stop to always-on authorizations

Passwords and keys that remain in your system are armed and dangerous, even when stored vaulted. A JIT connection is established by using a certificate that authenticates the user to the target. But this certificate only exists for a short period of time. It then expires automatically, leaving no passwords or keys behind to manage.

2 The number of passwords and keys accumulates, creating complexity

As businesses grow, so do the environments they operate in. Businesses soon realize that instead of managing a few dozen credentials, they are dealing with hundreds or thousands. Vaulting and storing all of them, especially in dynamic multi-cloud environments, is not sustainable.

3 Management complexity incurs costs

By nature, complex systems create inertia, inefficiencies, configuration challenges, and upgrade issues. The more credentials you manage, the greater the number of software components you will typically need to install. Eventually, these challenges require a larger team to run the solution, more processing power to run the system, and more complicated upgrade processes to be undertaken.

4 Every permanent credential is yet another point of trust

The more points of trust you have in your system, the more vulnerable it is to an attack or misconfigurations.

5 Permanent credentials promote an old way to solve modern problems

Let's face it. Many solutions on the market existed when physical servers were the norm and have been retrofitted to work in dynamic multi-cloud environments. These legacy solutions insist on managing the problem instead of reducing its size altogether. Just like the shift from physical to virtual servers made them available just-in-time and temporary, the credentials providing access to them should be equally dynamic and temporary.

Migrating to passwordless and keyless

Passwordless is an exciting new approach to cybersecurity, but migrating from legacy systems may seem daunting. With SSH Zero Trust Suite, you can migrate to a passwordless environment at your own pace.

The solution enables you to continue managing existing keys and passwords while incrementally onboarding existing credentials to the new paradigm. The reality is that some keys and passwords will remain in your system for years to come, so a hybrid approach allows you to continue to manage them without being held back.

We've ensured that the deployment of our solution is non-intrusive, whether you are managing credentials or getting rid of them. There's no need to change your key architecture, server configurations, install agents on the client or the server, or introduce a vast number of error-prone processes to your environment. Our hybrid model keeps your environment clean.

SSH

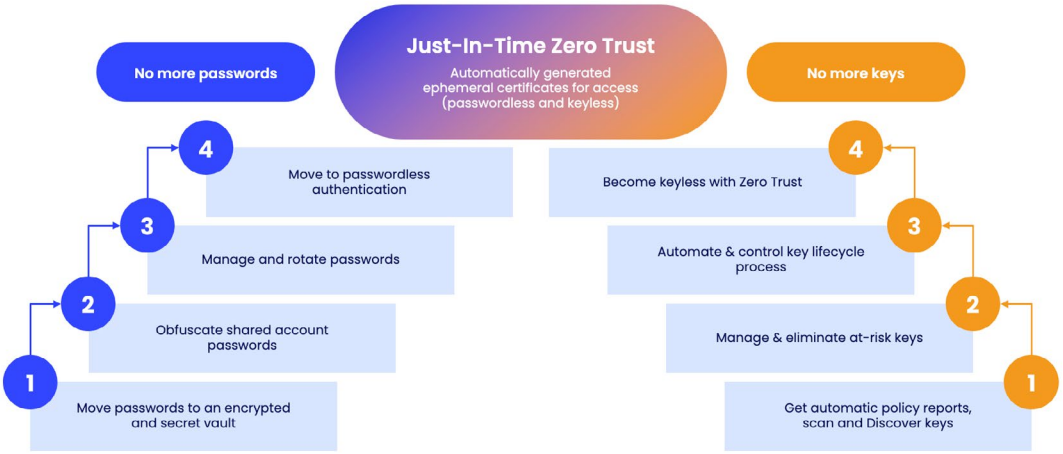
Choose SSH Zero Trust Suite

SSH Zero Trust Suite empowers you to join the passwordless movement and benefit from secure, efficient privileged access management capabilities while you migrate away from your legacy system at a pace that suits you.

Nobody enjoys expensive password vaulting and rotating. Everyone is afraid of losing that one precious "Key to Your Kingdom". Yet businesses manage them to the best of their abilities because most aren't aware that there is a better way.

Now there is. Simply scan and find critical permanent credentials and migrate them to a model where access is granted just-in-time upon establishing the connection, and where privileged users never handle or see the credentials.

The migration process goes like this:

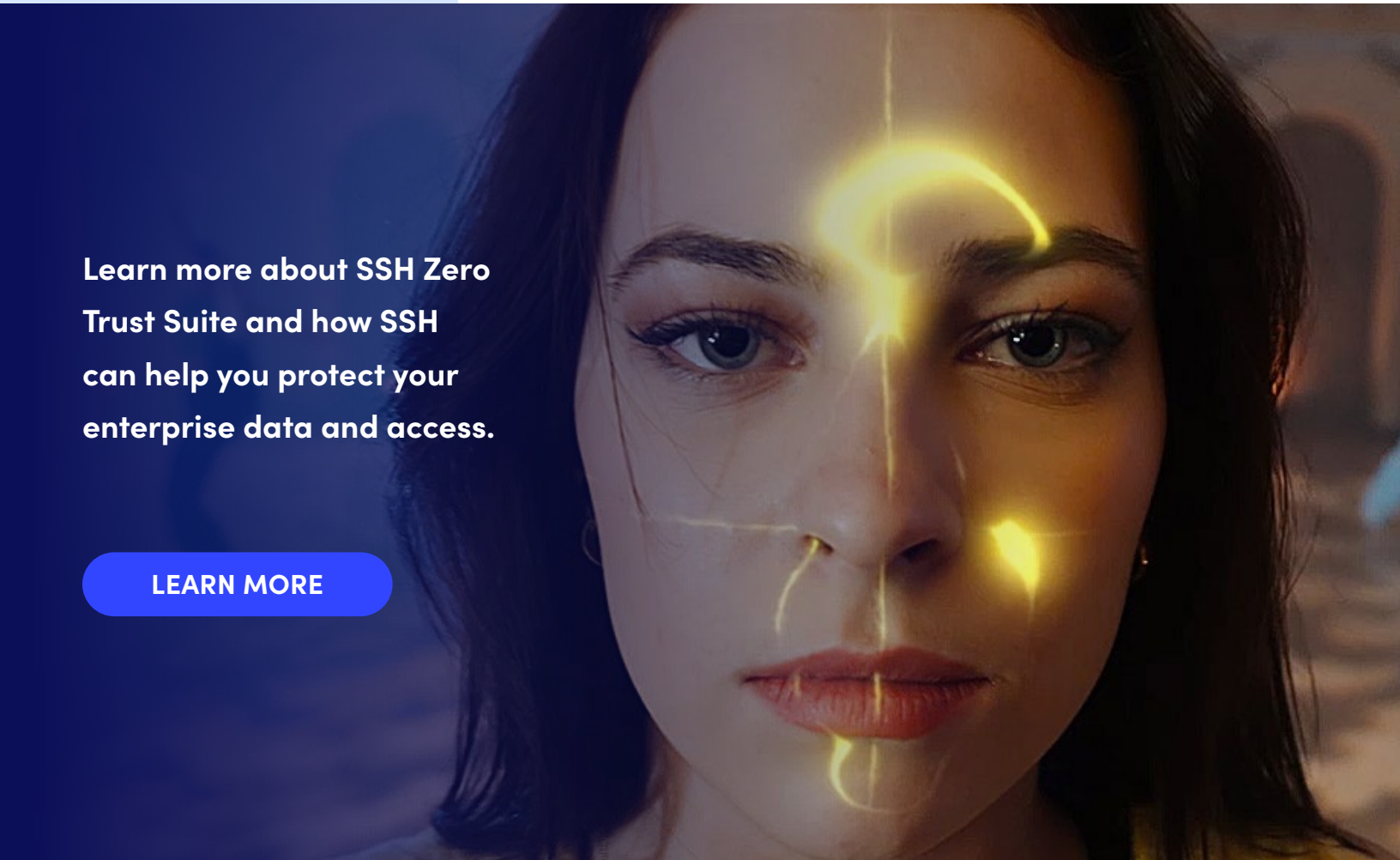


After granting access, the secrets needed to establish the connections simply expire automatically, leaving no passwords or keys to manage, lose, steal, or misuse. When a new connection is made, the process starts all over, making sure no one has always-on authorization to targets.

As the Zero Trust framework states: "Never trust, always verify". Single-Sign-On (SSO) and strong authentication with multi-factor authentication (MFA), security tokens and biometrics are also supported.

Key features of SSH Zero Trust Suite

- Make the use of SSH keys and shared accounts secure by associating them with an identity
- Reduce the attack surface by eliminating rogue, left-behind, weak passwords and SSH keys
- Put an expiration date on SSH keys that are the most common and unmanaged access credentials in large enterprise environments
- Radically reduce complexity of SSH key and password management with nothing to manage
- Vault, rotate, and manage credentials when necessary (passwordless and keyless is not possible in all traditional environments)
- A centralized access platform for all targets
- Onboarding to passwordless and keyless at your own pace
- Ensure just-in-time (JIT), just enough access (JEA) for user-to-target sessions and automated connections to avoid overpermissive access
- Cut down time, resources, and overall costs



Learn more about SSH Zero Trust Suite and how SSH can help you protect your enterprise data and access.

LEARN MORE

We'd love to hear from you!

Get in touch with our experts around the world.

GLOBAL HEADQUARTERS

Helsinki

SSH Communications Security Oyj
Karvaamokuja 2B, Suite 600
00380 Helsinki
Finland
Tel. +358 20 500 7000
info.fi@ssh.com

US HEADQUARTERS

New York City

SSH Communications Security Inc.
66 Hudson Blvd E, Suite 2308
New York, NY, 10001
USA
Tel: +1 (212) 319 3191
info.us@ssh.com

APAC HEADQUARTERS

Singapore

SSH CommSec Pte. Ltd.
6 Raffles Boulevard, Marina Square, #03-308
Singapore 039594
Singapore
Tel. +65 6338 7160
sales.asia@ssh.com

SSH

Let’s get to know each other

Want to find out more about how we safeguard mission-critical access for leading organizations around the world?

We’d love to hear from you.

REQUEST A DEMO