appviewx

Solution Brief

Simplifying SSH Lifecycle Management with AppViewX AVX ONE SSH

SSH: Securing Remote Access at Scale

SSH, or Secure Shell, has been a trusted protocol for decades, enabling developers, system administrators, and security teams worldwide to access remote systems securely. Its strong encryption and authentication mechanisms make it indispensable for secure file transfers, port forwarding, tunneling, and automation, safeguarding digital trust across enterprise networks.

SSH Keys and Certificates

SSH machine identities come in two forms: **SSH keys** and **SSH certificates**. Both authenticate users and systems across enterprise networks.

SSH keys are cryptographic key pairs (public and private) used to authenticate users or systems to an SSH server. Each key must be individually generated and provisioned on target servers or devices, then rotated regularly, and eventually removed to revoke access. SSH keys are stronger than password-based authentication. However, as SSH keys can be created on-the-fly and have no expiration date, it often leads to large volumes of unmanaged, stale, or overly privileged keys that persist for years, creating security and compliance risks.

SSH certificates take a more modern approach. They bundle a public key with identity information (like a user or service name), access permissions, and an expiration date, all digitally signed by a central Certificate Authority (CA). The private key remains securely on the client machine, while servers trust the CA to validate the certificate—similar to verifying an ID card. Because certificates automatically expire, they reduce the risk of long-lived, unmanaged SSH access. However, they must be renewed and managed efficiently to avoid disruptions.

Although SSH certificates are emerging as a more secure, scalable, and industry-tested alternative, SSH keys are still the most common method today.

Despite SSH's critical role in secure network operations, SSH management has not kept pace with the speed and scale of modern business. SSH keys proliferate quickly, manual processes still dominate, and organizations often struggle with key sprawl, visibility gaps, and unmonitored access. The result is operational inefficiency, compliance challenges, and elevated security risk.

As SSH keys grant the highest levels of access, effective SSH lifecycle management is essential not just for security, but for protecting systems, ensuring compliance, and preserving digital trust.

> **Today, the (SSH) protocol is used for managing more than half of the world's web servers and practically every Unix or Linux computer, on-premises and in the cloud.**
>
> -SSH.COM

Challenges with SSH Management

1. SSH Key Sprawl

Unlike SSL/TLS certificates, SSH keys never expire. Over time, they multiply across enterprise systems, leaving many keys dormant, forgotten, and difficult to track. Without a centralized management system, maintaining visibility over potentially millions of keys becomes a major challenge for security teams.

Because SSH keys don't expire, they continue granting access to critical systems and applications unless explicitly revoked. When unmanaged, they present a significant security risk: attackers can steal or misuse these keys to access production servers, firewalls, and databases, moving laterally across networks undetected.

Administrators also struggle to rotate keys or remove inactive ones due to limited visibility into their dependencies and configurations. As a result, stale and stray keys accumulate over years, creating a growing attack surface. Beyond the security risk, unmanaged SSH keys often lead to policy violations, failed audits, and costly regulatory penalties.

2. Manual Key Lifecycle Management (KLM)

Provisioning, rotating, and removing SSH keys are essential steps in managing their lifecycle. Yet performing these operations manually remains a persistent challenge for security teams.

Manually provisioning user or client keys individually to every target server is tedious, time-consuming, and highly error-prone. Tracking and managing keys in spreadsheets quickly becomes unmanageable at scale. For example, when employees leave the organization or move between departments, their access must be revoked immediately. Doing this manually—checking every server and deleting each associated key—requires enormous effort.

Manual processes also hinder crypto-agility. As new SSH-related threats emerge, replacing or upgrading SSH keys through manual workflows can take months of extensive planning and effort, leaving critical systems vulnerable during the transition.

3. Lack of Control

SSH keys can be created by anyone with system access using simple commands, leading to uncontrolled key generation and ad-hoc provisioning. This often results in key sprawl and keys with excessive privileges, expanding the attack surface.

Weak keys are another concern—many are generated with outdated algorithms or low bit-length, making them easy targets for attackers. In addition, keys are frequently shared between users or across multiple servers, further increasing the risk of exposure.

Compliance adds another layer of complexity. Regulations such as GDPR, HIPAA, PCI DSS, and Sarbanes-Oxley impose strict requirements for managing access credentials, including SSH keys. Meeting these mandates requires visibility, standardized processes, and centralized control to govern, monitor, and audit key usage.

Yet, most security teams still rely on manual oversight—from key generation and configuration to access control privileges and rotation policies. This manual approach often leads to inconsistencies, security gaps, and compliance failures, leaving organizations vulnerable.

How AppViewX AVX ONE SSH Simplifies SSH Lifecycle Management

AVX ONE SSH automates, orchestrates, and secures the lifecycle of SSH machine identities across the enterprise. Through complete visibility, end-to-end automation, and policy-driven controls, AVX ONE SSH helps organizations eliminate key sprawl, reduce risk, ensure compliance, and govern privileged access at scale. Delivered as a SaaS-first solution, it can also be deployed on-premises if needed.

Visibility for Mitigating Key Sprawl

- **Smart Discovery**

  Being aware of all the SSH keys across complex environments, detecting suspicious/shared/orphaned/weak keys, in order to promptly delete or invalidate them, is essential to prevent key theft or misuse. AVX ONE SSH helps scan and discover all SSH keys (and certificates) across clients and hosts spread across hybrid and multi-cloud infrastructures on an on-demand or scheduled basis. Automated discovery helps ensure that no keys or certificates are left undetected and unmanaged, mitigating the security risks of stale and stray keys. Automated discovery also eliminates the manual overhead of searching for SSH keys across complex environments, which is inefficient and often error-prone.

- **Inventory**

  As SSH keys are large in number and often generated and configured frequently, maintaining full visibility of all the keys is critical to reduce key sprawl and prevent key theft or misuse. AVX ONE SSH consolidates all the discovered keys (and certificates), clients, hosts as well as client/server configurations in an accurate and up-to-date inventory. It also maps trust relationships of keys to associated users, hosts, servers and service accounts to understand access, minimize risk, and enable successful key rotations. Granular visibility into key trust relationships and centralized control help monitor and manage SSH keys at scale confidently.

- **Risk Intelligence**

  Key-related insights, such as key status, age, trust relationships, access privileges, and crypto-standards help detect key issues and proactively mitigate SSH-related security threats. AVX ONE SSH offers a unique Risk Dashboard that helps summarize risk and trend analysis to monitor the status of keys (inactive, rogue, or weak keys) and configurations for detecting anomalies. The dashboard also flags SSH keys that are newly created out of band or shared with other users to help remediate them with one-click remediation.

Automation for Centralizing Management and Improving Security Posture

- **SSH Lifecycle Automation and Risk Remediation**

  AVX ONE SSH automates SSH key lifecycle management end-to-end. Key requests, rollouts, rotations, and deletions are all automated to significantly lower the overhead and risk of manual SSH lifecycle management. Orphaned or weak keys can be deleted, and new keys can be generated in a single click for instant risk remediation. Automation also allows bulk provisioning of keys to grant bulk access to multiple servers in a group. The process is simplified by organizing servers or hosts into Infrastructure Access Groups.

- **Automation Workflows, Self Service, and Integrations**

  Another powerful feature of AVX ONE SSH is the custom or out-of-the-box automation workflows it offers. These workflows help automate and streamline complex processes like key rotations. AVX ONE SSH also provides self-service capabilities supported by role-based access control, where users can efficiently request or generate keys and manage access needs.

  AVX ONE SSH provides direct integrations with IAM and DevOps tools. This helps automatically onboard and update SSH keys and ensure they are provisioned and deleted seamlessly.

Policy Control for Maintaining Continuous Compliance

- **SSH Lifecycle Policies and Governance**

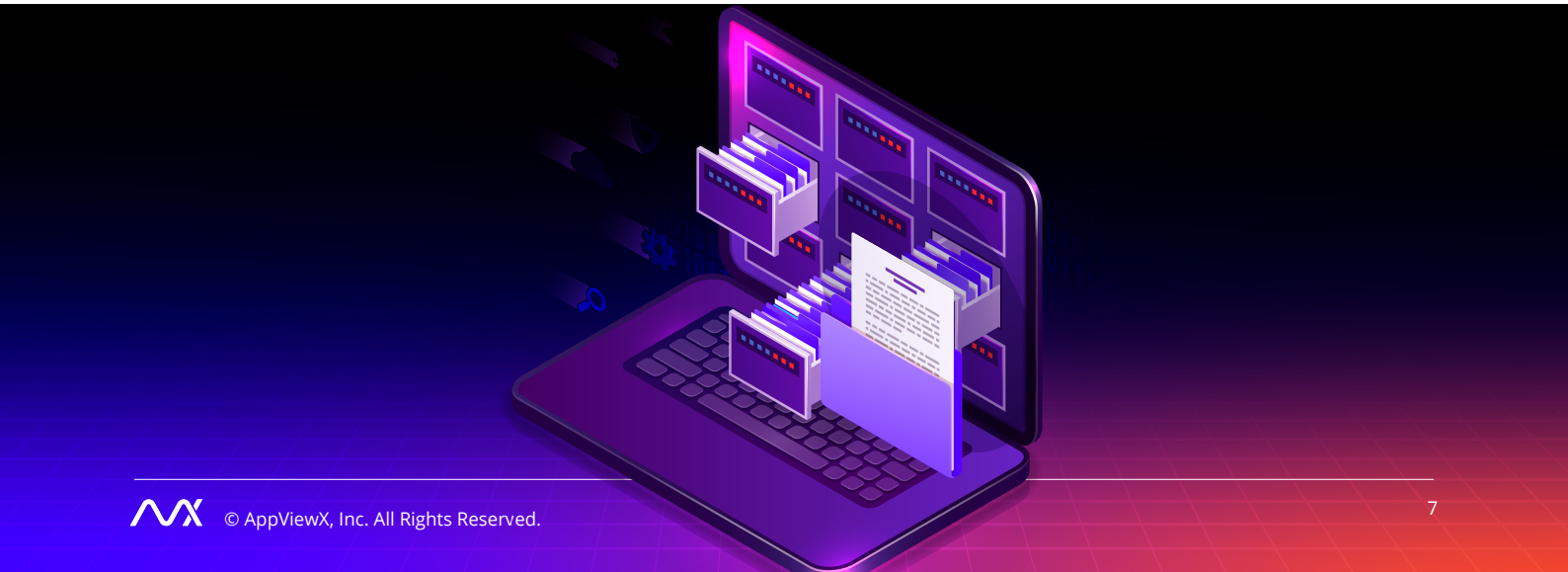
  All keys are not created equal. Some protect access to mission-critical application systems, while others protect access to less-important testing environments. It is important to restrict and control access to systems by enforcing appropriate policies. AVX ONE SSH allows you to group keys based on functionality and set policies around key and certificate generation, approved crypto standards (i.e. key lengths and algorithms), regular key rotations, as well as time-bound access to ensure consistent processes and compliance with industry and regulatory standards. Zero-touch policy enforcement removes the need for human intervention, ensuring policies are applied automatically and consistently across the enterprise.

- **Role-Based Access Control**

  AVX ONE SSH allows you to implement role-based access control (RBAC) to authorize and restrict SSH management and access at a granular level. You can group hosts to automatically delegate SSH access for users and groups, reducing the risk of privilege sprawl and unauthorized access.

- **Risk Assessments and Audit Support**

  AVX ONE SSH also provides regular risk assessments, detailed reporting, and audit trails or logs to help streamline internal and external compliance audits. Risk intelligence and continuous monitoring help spot anomalies or irregularities in the system, remediate them in time, and ensure continuous compliance with regulations and mandates, such as PCI DSS, GDPR, and HIPAA, as well as security standards such as NIST, MITRE, and others.



Why AVX ONE SSH

Zero Trust Security

Eliminate blind spots and backdoors by centrally managing all SSH machine identities. Ensure secure SSH access across hybrid multi-cloud environments to prevent unauthorized entry and lateral movement.

Higher Operational Efficiency

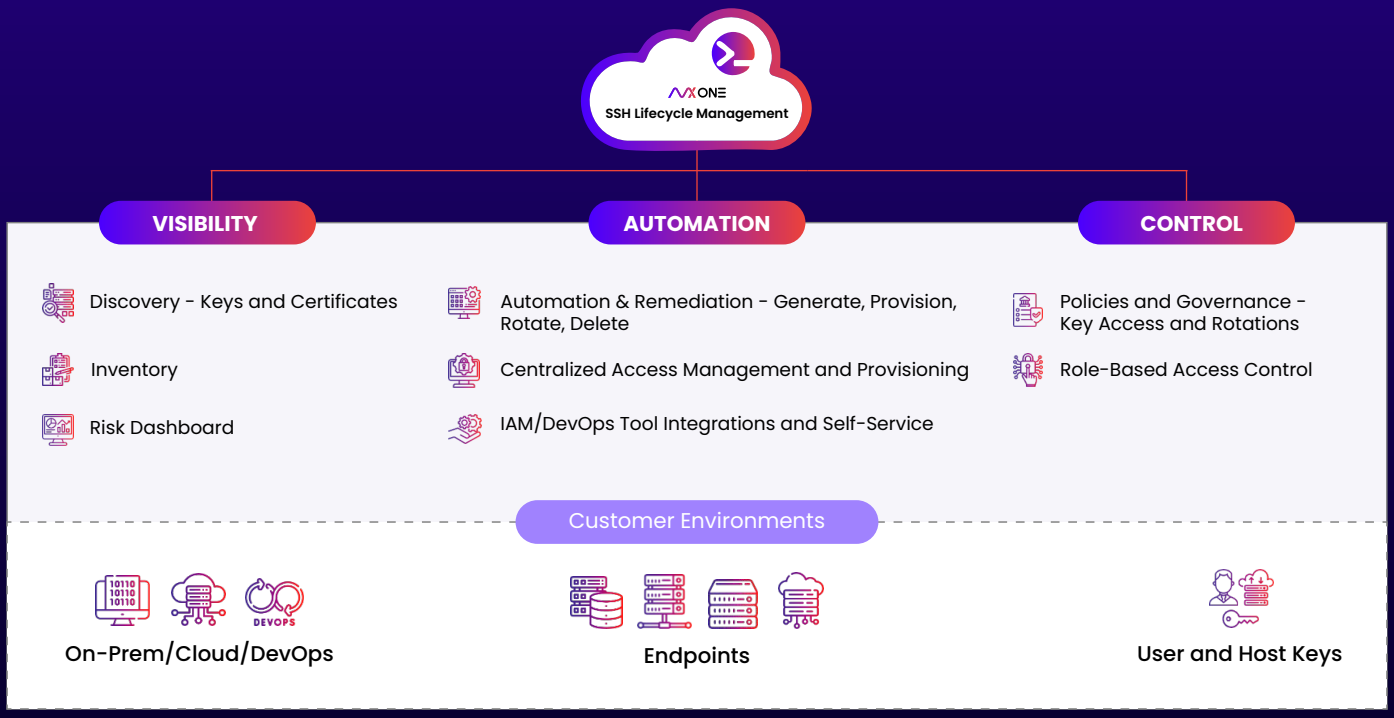
Streamline SSH lifecycle management through automation, self-service, and powerful integrations.

Continuous Compliance

Enforce policies and standardize SSH lifecycle management to simplify audits, close compliance gaps, and protect against regulatory penalties.

Crypto-Agility

Rapidly adapt SSH infrastructure to evolving cryptographic standards, minimizing exposure to emerging threats and ensuring long-term resilience.



AVX ONE SSH Lifecycle Management

AVX ONE SSH – Flexible Deployment Models

AVX ONE SSH is part of the AppViewX AVX ONE Platform and has flexible deployment options, including:

- **SaaS Deployment**
  Available as a service, AVX ONE SSH is fully managed and updated by AppViewX. Customers can directly set up an account and start using it immediately. The advantage of deploying the SaaS version of AVX ONE SSH is that customers see instant value, require minimum on-prem hardware or maintenance, and always have the most updated version of the product.

- **On-Prem and Hosted Deployment**
  AVX ONE SSH can also be deployed within a customer-managed environment, including hypervisor-based VMs, private clouds, or public clouds using AWS, GCP, Microsoft Azure, and others. As AVX ONE SSH is a Kubernetes-based application, it can also be installed in a managed Kubernetes environment like EKS, AKS, GKE, RedHat Openshift, Rancher, and others.

Security simplified with AppViewX

AppViewX is trusted by the world's leading global organizations to ensure application availability, security and compliance with centralized visibility and control of public key infrastructure (PKI) and application delivery services across complex hybrid multi-cloud environments. The AppViewX Platform enables self-service automation and orchestration for NetOps, DevOps, SecOps and application teams to quickly and easily translate business requirements into automation workflows that improve agility, harden security, enforce compliance, eliminate errors, and reduce cost.

Make visibility the cornerstone of your protection mechanism.
www.appviewx.com/live-demo

appviewx

City Hall, 222 Broadway
New York, NY 10038

info@appviewx.com
www.appviewx.com

+1 (206) 207-7541
+44 (0) 203-514-2226