INFO~TECH
RESEARCH GROUP

# SSH PrivX:
# A Modern Approach to Privileged Access Management

**Carlos E. Rivera**
Principal Advisory Director,
Info-Tech Research Group

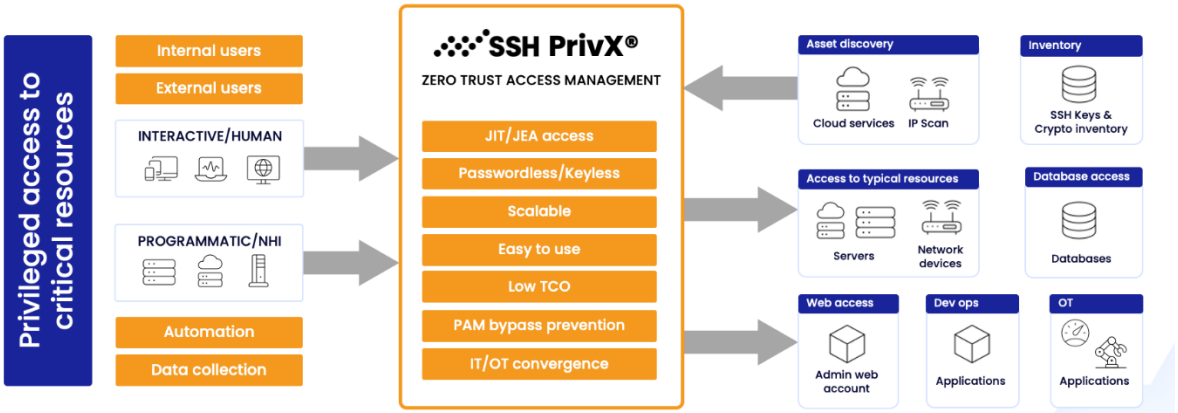
Managing privileged access securely across IT, operational technology (OT), and cloud environments is one of the most pressing concerns for many IT and cybersecurity professionals today. SSH PrivX, developed by SSH Communications Security, offers a solution rooted in zero trust principles to address this challenge. This tech note explores SSH PrivX in detail, covering its background, features, unique aspects, and overall merit as a PAM tool.

## Short Description of the Vendor and Company History

SSH Communications Security was established in 1995 by the creator of the Secure Shell (SSH) Protocol, a foundational technology for secure remote access often used for shell access in Unix and Linux operating systems. With over 30 years in the cybersecurity field, the company has built a reputation for delivering reliable, secure communication solutions. Based in Helsinki, Finland, where its R&D team of approximately 50 employees is located, SSH Communications Security also maintains offices in New York and Singapore. The company employs around 140 people globally, reflecting a modest, focused operation.

Historically, SSH Communications Security has leveraged its expertise in the SSH Protocol to develop a range of products. Today, it organizes its offerings into three primary business areas: system security, represented by PrivX; network security products, known as NQX; and security solutions for human interaction or cooperation, branded as SalaX. The development of SSH PrivX began around 2017, marking a shift toward addressing modern privileged access management (PAM) needs with a zero trust approach. This long-standing experience in secure access technologies underpins the company's current efforts with PrivX.

## PrivX – Preventing Unauthorized Access



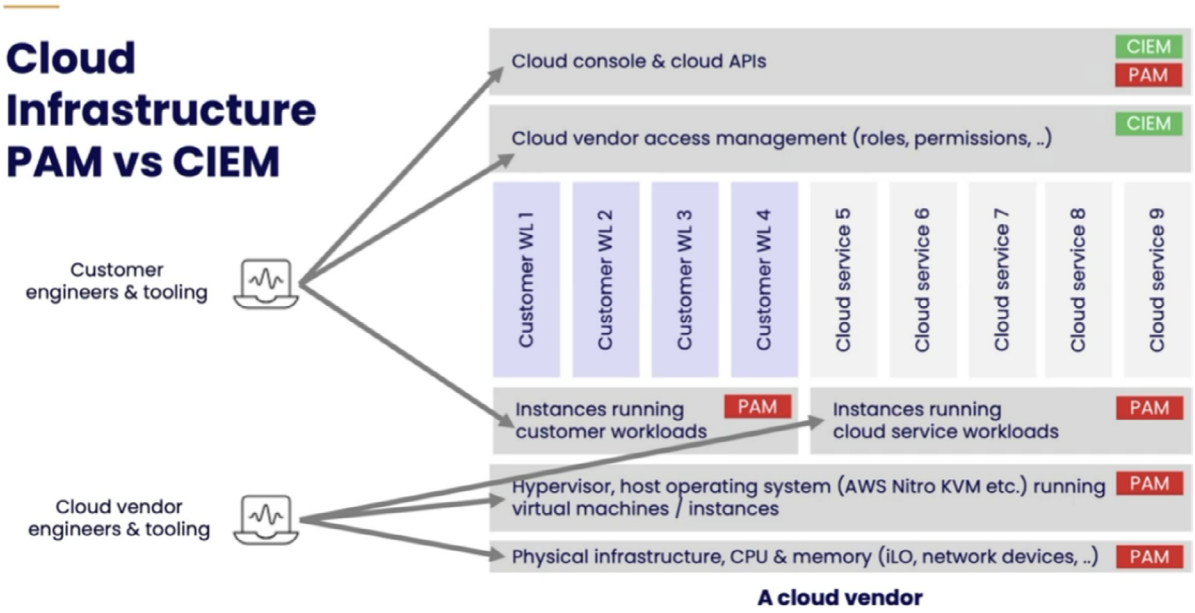

Source: SSH, Analyst Briefing January, 2025

# Product Overview and Value Proposition

SSH PrivX is a PAM solution designed to administer secure access to critical systems across IT, OT, and cloud environments. Introduced around 2017, it was built from scratch with a zero trust architecture, meaning it does not assume trust based on a user's location or network. Instead, it verifies every access request, aligning with contemporary security demands where traditional, perimeter-based models fall short.

The value proposition of SSH PrivX centers on enhancing security while streamlining access management. It replaces traditional passwords with short-lived certificates, reducing risks tied to credential theft, weak passwords, or phishing attempts. This certificate-based approach also simplifies administration by automating credential issuance and revocation. PrivX also has a secrets vault for vaulting and rotating passwords if passwordless access (certificate-based) is not viable and provides granular access control, enabling organizations to specify not just who can access systems but what they can do once connected – down to individual commands or actions. This precision supports compliance with regulatory standards, particularly in industries with stringent requirements.

PrivX also emphasizes auditing and monitoring, supporting privileged session management (PSM) capturing detailed logs of user activities for accountability and forensic analysis. Another significant component is its SSH key management functionality, which addresses the common problem of unmanaged SSH keys by discovering and securing them, aiding the transition to a zero trust environment.




Source: SSH, Analyst Briefing January, 2025

# Core Features

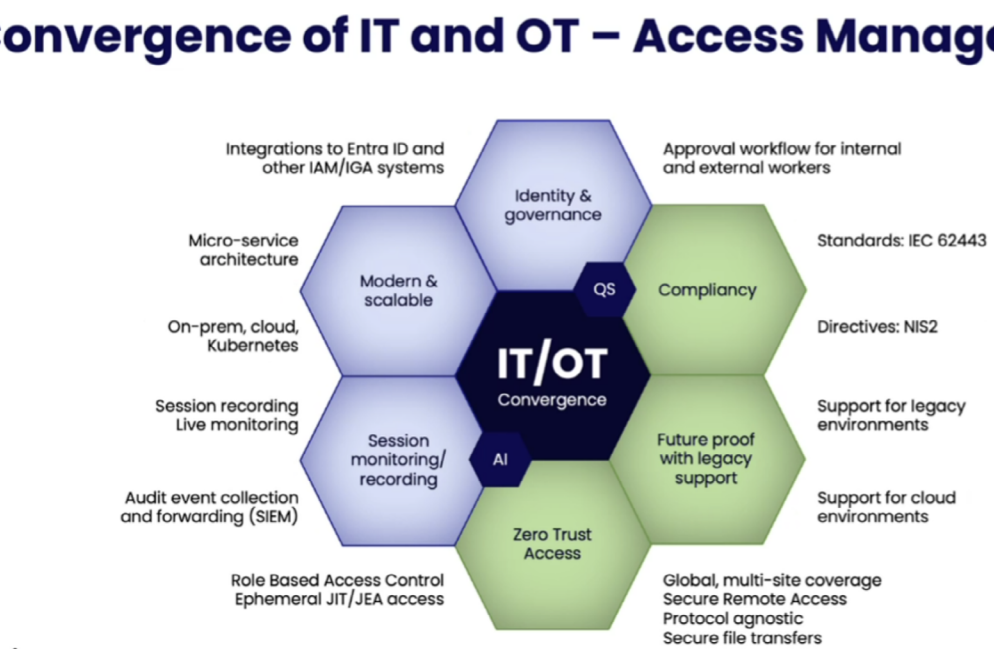
SSH PrivX offers a comprehensive set of features to manage privileged access effectively. These core capabilities underpin its ability to secure diverse environments:

- **Zero Trust Approach:** PrivX assumes no inherent trust, verifying each access request regardless of the user's origin.
- **Certificate-Based Authentication (CBA):** By using short-lived certificates instead of passwords, PrivX eliminates common vulnerabilities associated with password management. Certificates are generated and revoked automatically, reducing manual effort. This helps meet regulatory requirements such as EO 14028 and M-22-09.
- **Granular Access Control:** The solution allows organizations to define detailed access policies, restricting users to specific actions on target systems. For

instance, in an SSH session, access might be limited to certain commands or directories, minimizing the risk of misuse.

- **PSM:** PrivX records and allows you to monitor all privileged sessions, including keystrokes and interactions, creating a searchable audit trail. This supports compliance audits and helps investigate incidents efficiently.
- **SSH Key Management:** The tool scans for existing SSH keys, manages their lifecycles, and ensures secure usage, addressing a frequent security gap in many organizations.

These features collectively enable SSH PrivX to secure both interactive user access and application-to-application (A2A) connections. For interactive access, users authenticate through PrivX, which issues a certificate for temporary system access. For A2A scenarios, PrivX manages application credentials via APIs and integration with secrets vaults, ensuring secure communication without hardcoding sensitive data.



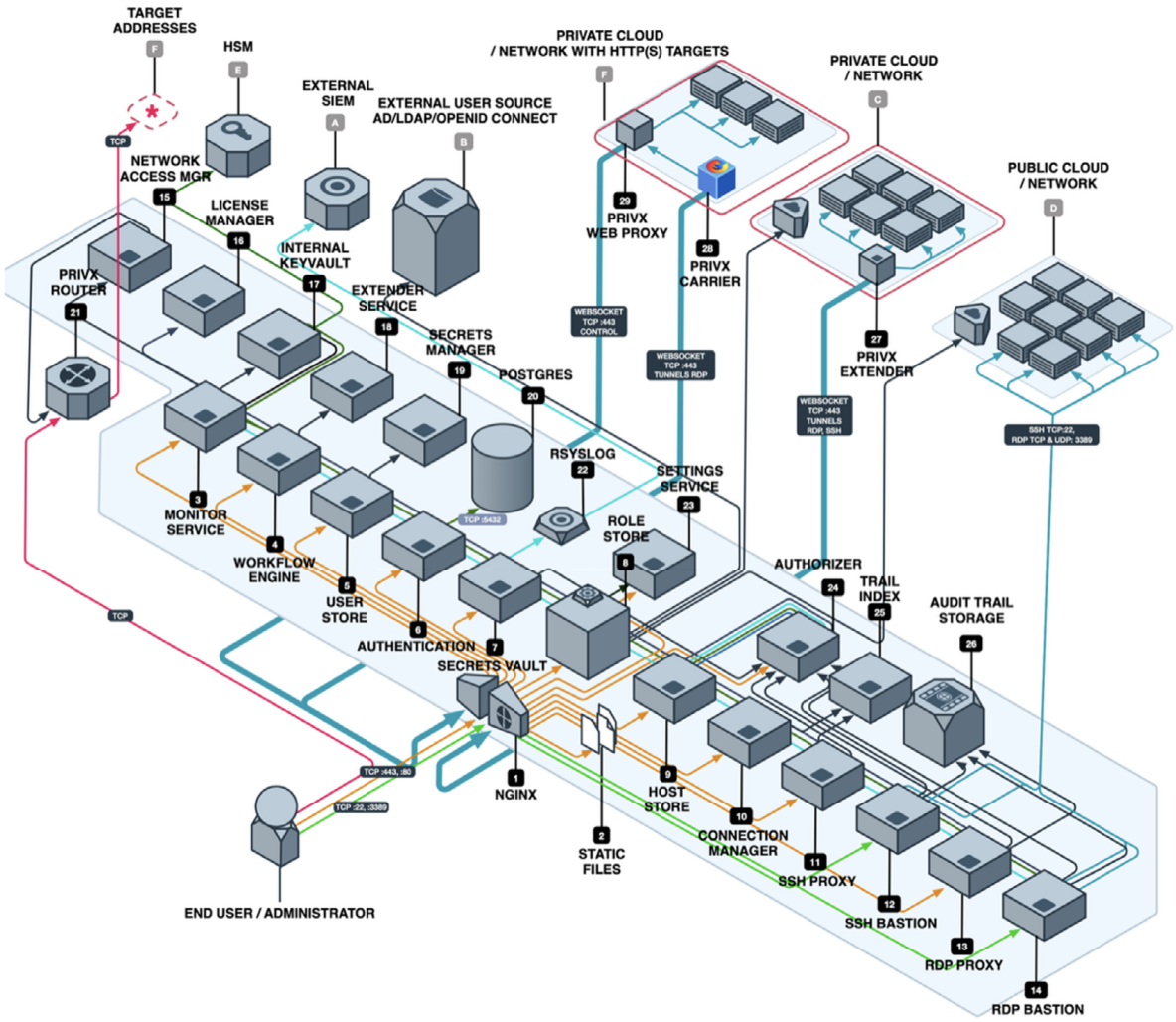

Source: SSH, Analyst Briefing January, 2025

# Differentiating Features

While SSH PrivX shares common ground with many of the other PAM solutions, several aspects distinguish it in the market. One notable differentiator is its dual focus

on IT and OT environments. Many PAM tools cater primarily to IT systems, but PrivX extends its reach to operational technology, critical in sectors like Manufacturing or Energy. It leverages the Purdue model, a framework for industrial control systems, by mapping user roles to specific levels of the OT hierarchy. This ensures that access aligns with operational needs, such as granting a technician access to field devices but not higher-level systems. Network extender components further enable secure connections to OT networks using protocols like SSH, RDP, VNC, proprietary automation protocols, and web access protocols, while imposing time-based approvals for safety and compliance.

Another distinguishing factor is PrivX's microservices architecture. Built with Golang (Go) and deployed in Kubernetes, PrivX supports scalability, zero downtime upgrades, and rapid updates, with a release cycle of six to seven weeks. This modern design allows for autoscaling and flexible deployment, adapting to varying organizational

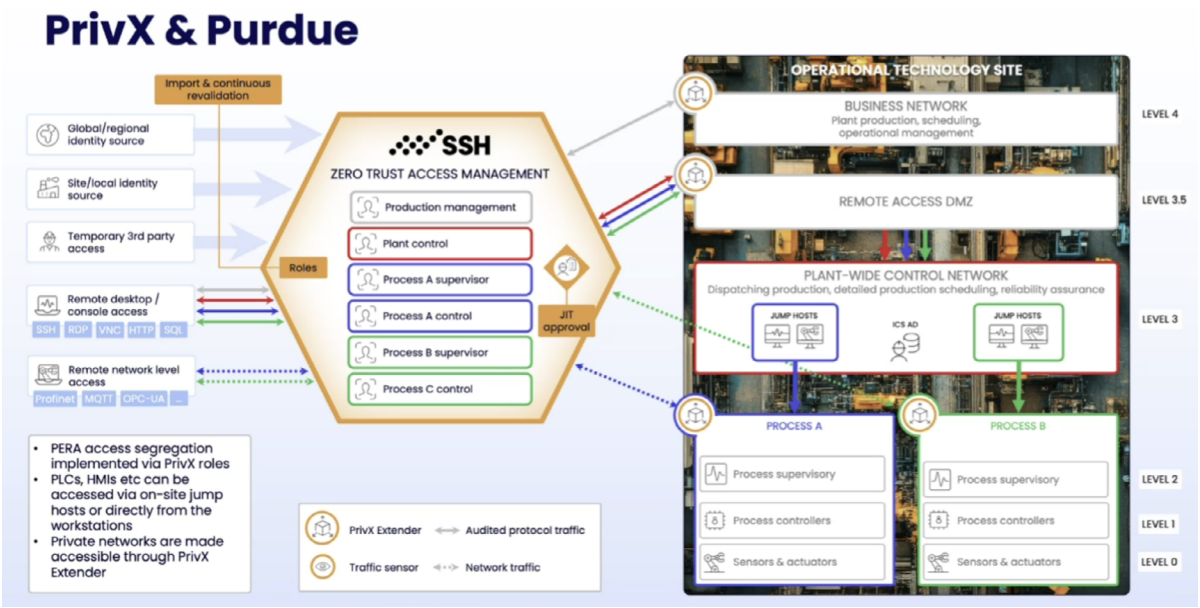


demands. The use of REST APIs and logical components such as its PostgreSQL database, deployable on-premise or in the cloud with services like Amazon RDS, enhances its technical versatility.

PrivX also stands out with its just-in-time (JIT) PAM. Unlike solutions that grant persistent privileges, PrivX provides zero standing privileges (ZSP). This reduces the attack surface by eliminating standing privileges that could be exploited. Additionally, its support for a broad range of protocols – beyond SSH and RDP to include web applications, databases, and custom protocols – makes it adaptable to diverse infrastructures.

Another breakthrough PrivX feature is dynamic, JIT, quantum-safe, site-to-site connectivity without the need to open permanent connections. In this model, the site admin allows access by opening a quantum-safe tunnel on demand, and the remote worker opens the connection to the target using role-based access control (RBAC).

In OT contexts, PrivX facilitates discovery by deploying sensors to identify devices and protocols, providing visibility into existing systems. This capability, combined with its integration of IT and OT security, positions it as a practical choice for organizations bridging these domains.




Source: SSH, Analyst Briefing January (2025)

# Our Take

SSH PrivX presents a compelling option for organizations seeking to secure privileged access across IT, OT, and cloud environments. Its zero trust foundation, reliance on CBA, and granular control over user actions address key security challenges effectively. The comprehensive auditing and SSH key management tools further strengthen its appeal, offering both compliance support and practical risk mitigation.

What sets PrivX apart is its ability to serve both IT and OT use cases, supported by its alignment with the Purdue model and network extender features. The modern microservices architecture ensures it can scale and evolve quickly, while the JIT access approach reflects a proactive stance on reducing vulnerabilities. The versatility in protocol support also broadens its applicability, making it suitable for varied operational needs.

The backing of SSH Communications Security, with its decades of experience and the original SSH protocol's inventor at its helm, adds a layer of credibility. The company's focus on R&D suggests a commitment to keeping PrivX relevant amid changing security demands. That said, potential adopters should weigh its merits against their specific requirements. The solution's technical sophistication and deployment options – on-prem or cloud-based – may require careful planning, particularly in complex or highly regulated settings. Organizations must assess whether its features align with their infrastructure and operational priorities.

Overall, SSH PrivX demonstrates significant merit as a PAM solution. Its thoughtful design and alignment with zero trust principles and zero standing privileges make it a strong candidate for organizations aiming to enhance security without sacrificing efficiency. Based on its documented capabilities, it earns consideration as a reliable tool in the PAM space.