KuppingerCole Report

EXECUTIVE VIEW

by Martin Kuppinger | January 2019

SSH.COM PrivX

SSH.COM PrivX is an innovative solution for privileged access to sessions running on hosts in the cloud and on premises. Based on short-lived certificates and a policy- and role-based, automated access control, it is targeted at agile IT environments such as DevOps environments.

by **Martin Kuppinger**
mk@kuppingercole.com
January 2019

Content

Related Research

Leadership Compass: Privilege Management - 72330

Executive View: Universal SSH Key Manager - 71509

1 Introduction

In the age of digital transformation, not only the requirements for IT but also the way IT is done, are constantly evolving. To remain relevant, organizations must reinvent themselves by being agile and more innovative. Emerging technology initiatives such as digital workplace, DevOps, security automation and the Internet of Things continue to expand the attack surface of organizations as well as introduce new digital risks. To stay competitive and compliant, organizations must actively seek newer ways of assessing and managing the security risks without disrupting the business. Security leaders, therefore, have an urgent need to constantly improve upon the security posture of the organization by identifying and implementing appropriate controls to prevent such threats.

Privileged Access Management represents the set of critical cybersecurity controls that address the security risks associated with the use of privileged access in an organization. There are primarily two types of privileged users:

1. Privileged Business Users - those who have access to sensitive data and information assets such as HR records, payroll details, financial information, company's intellectual property, etc. This type of access is typically assigned to the application users through business roles using the application accounts.
2. Privileged IT Users – those who have access to IT infrastructure supporting the business. Such access is generally granted to IT administrators through administrative roles using system accounts, software accounts or operational accounts.

The privileged nature of these accounts provides their users with an unrestricted and often unmonitored access across the organization's IT assets, which not only violates basic security principles such as least privilege but also severely limits the ability to establish individual accountability for privileged activities. Privileged accounts pose significant threat to the overall security posture of an organization because of their heightened level of access to sensitive data and critical operations. Security leaders, therefore, need stronger emphasis on identifying and managing these accounts to prevent the security risks emanating from their misuse.

Available Identity and Access Management (IAM) tools are purposely designed to deal with management of standard users' identity and access and do not offer the capabilities to manage privileged access scenarios such as use of shared accounts, monitoring of privileged activities and controlled elevation of access privileges. Privileged Access Management tools are designed to address these scenarios by offering specialized techniques and unique process controls, thereby significantly enhancing the protection of an organization's digital assets by preventing misuse of privileged access.

While credential vaulting, password rotation, controlled elevation and delegation of privileges, session establishment, and activity monitoring have been the focus of attention for PAM tools, more advanced capabilities such as privileged user analytics, risk-based session monitoring and advanced threat protection are becoming the new norm - all integrated into comprehensive PAM suites being offered. We see a growing number of vendors taking different approaches to solve the underlying problem of restricting, monitoring, and analyzing privileged access and the use of shared accounts.

Among the key challenges that drive the need for privilege management are:

- Abuse of shared credentials;
- Abuse of elevated privileges by unauthorized users;
- Hijacking of privileged credentials by cyber-criminals;
- Abuse of privileges on third-party systems;
- Accidental misuse of elevated privileges by users.

Furthermore, there are several other operational, governance and regulatory requirements associated with privileged access:

- Discovery of shared accounts, software, and service accounts across the IT infrastructure
- Identifying and tracking of ownership of privileged accounts throughout their life-cycle
- Establishing Single Sign-on session to target systems for better operational efficiency of administrators
- Auditing, recording, and monitoring of privileged activities for regulatory compliance
- Managing, restricting, and monitoring administrative access of IT outsourcing vendors and MSPs to internal IT systems;
- Managing, restricting, and monitoring administrative access of internal users to cloud services.

Of the available Privileged Access Management (PAM) technologies, PSM (Privileged Session Management) remains one of the three core technologies that constitute a baseline PAM solution. IT infrastructure, operations, and security leaders are under increased business and regulatory pressure to assess and manage the security risks arising from increased cloud access patterns of IT administrators, third-party vendors, and privileged business users. To meet the security requirements of increased cloud adoption, PSM technology over the past few years has undergone a major transformation of its on-premises only approach to include the emerging privileged access patterns of an increasing cloud-dominated IT environment. PAM vendors are continuously adding native cloud-ready features to their PSM technology in order to address the security risks of administrative access to cloud platforms and services.

SSH.COM is one of the solution providers in the PAM space, focused primarily on delivering secure, privileged access to cloud and on premises services without the need to reveal passwords using an integrated session management capability. Offering Tectia SSH Client/Server for secure SSH connections and Universal SSH Key Manager for managing SSH keys, SSH.COM offers PrivX as a separate standalone solution for establishing and managing SSH and RDP sessions to target systems through a client browser. PrivX focuses on setting up secure connections to servers and controlling access within these sessions, without the conventional vaulting of passwords and thereby reducing the overheads commonly associated with the password vaulting approach of existing PAM tools. For a detailed overview of the leading PAM vendors, please refer to the KuppingerCole Leadership Compass on **Privilege Management**[1].

[1] Leadership Compass: Privilege Management (#72330)

2 Product Description

SSH.COM can be described as the company behind the SSH (Secure Shell) protocol that is commonly used for remote host access, specifically in Unix and Linux environments. The company has been founded by the inventor of the SSH protocol and is focused on solutions that are, in a broad notion, centered around this protocol and other means of remote access such as RDP (Remote Desktop Protocol).

The PrivX tool focuses on managing access to privileged sessions and control about these sessions in a lean, scalable way that works well for today's agile environments. In today's IT, setting up servers in the cloud and running DevOps environments with masses of servers and containers is the norm. However, in such dynamic environments, traditional PAM approaches that are focused on managing every server and the privileged access to these servers in a rather static way, tend to fail. Lengthy administrative processes for moving credentials to vaults, rotating passwords, and managing user entitlements for hosts and sessions tend being too slow and costly.

PrivX takes a different approach. Instead of managing administrative accounts, credentials, and entitlements per host, the system acts as the only certificate authority for SSH and RDP access to these hosts and protects session with short-lived certificates. It is the single instance for managing all access. While such single instances are a common approach in PAM environments, commonly used for SSO (Single Sign-On) to privileged sessions, the difference is in the way the sessions are protected. Here we find the innovation that SSH.COM brings to PAM, by using ephemeral certificates for session protection instead of focusing on account protection per combination of host and user.

PrivX works by controlling access based on users/groups that have been defined in, for example, Active Directory and mapping those users to roles in PrivX. PrivX roles then allow users to access specific target hosts in privileged sessions. Users authenticate to the PrivX console. The authentication capabilities support MFA (Multi Factor Authentication), which is essential for privileged access. Users can be automatically mapped from various directory services such as LDAP directories, Microsoft Active Directory, Google Gsuite and AWS Cognito. Furthermore, OpenID Connect is supported to integrate with and provide SSO to AWS Cognito and other 3rd party identity management software. Based on the defined user or group IDs, administrators of PrivX can define which role a user is in and which access to which target hosts is granted. They e.g. can define different roles for system administrators, quality engineers, developers, etc., and grant access to different groups of target hosts. Due to the mapping of such PrivX roles to groups in the directory services, updates in the directory are automatically reflected in PrivX roles.

Obviously, this requires a well-working IAM (Identity and Access Management) that handles user provisioning and assignment of users to groups in the directory services. For smaller environments, customers can rely on the built-in directory services of PrivX. However, IAM is anyway the right place for that part of management, while the PAM approach of PrivX then focuses on just mapping users and groups to roles, entitling the roles for privileged access, and managing the privileged sessions. PrivX maintains partnerships with several IAM vendors.

For non-directory-based access, workflows for approving access requests are supported. The integration with other identity solutions can rely on OpenID Connect. The workflow capabilities include options such

as the four-eye-principle for approvals for granting roles. Furthermore, policies can restrict access of external users and other specific settings. PrivX workflows also include options for time restricted access and floating time windows that make it a good fit for handling subcontractor privileged access.

Other capabilities of the PrivX system include automated discovery of hosts across a variety of on-prem and multi-cloud environments including Microsoft Azure, AWS, Google Cloud and OpenStack, session recording for both SSH and RDP sessions as well as audit and logging for privileged session activities. PrivX Extender a remote component for private cloud environments acts as an intermediary between the on-prem PrivX instance and the remote, cloud-based systems. In an attempt to offer PAM-as-a-service, SSH.COM has recently partnered with Fujitsu to integrate PrivX with Fujitsu's IDaaS offering.

Auditing and logging include integrations into Splunk, Rsyslog, Syslog-ng, Amazon CloudWatch and Azure EventHub for delivering audit data to 3rd party SIEM (Security Information and Event Management) software for alerting and monitoring of privileged activities. While session recording is supported and is straightforward for SSH sessions, it remains fairly limited for RDP sessions, supporting only session playback capability and lacking on advanced search and indexing features within the recorded sessions, e.g. based on OCR or by relating system events to recordings of graphical sessions.

SSH.COM has put specific focus on the support of both cloud environments and on premises environments. PrivX offers deployment scripts for certain DevOps management tools such as Chef and Ansible for faster deployment cycles in DevOps environments.

All features of the UI are available via a REST-based API, allowing customers to fully automate PrivX and integrate PrivX with other management and security tools. SSH.COM PrivX also supports high availability features, including active-active cluster nodes for fail-over, horizontal scalability of clusters by adding nodes, and sticky-session support.

SSH.COM has a defined roadmap for PrivX, focusing on a broader support of protocols (beyond SSH, RDP, and SFTP), advanced IAM integration including more authentication options, and integration with 3rd party security solutions, including DLP (Data Leakage Prevention).

3 Strengths and Challenges

With PrivX, SSH.COM takes an innovative and focused approach on PAM. Instead of managing passwords and other session credentials, PrivX allows users to authenticate against the central PrivX instance and, from there on, builds on short-lived certificates. All access to hosts then runs through PrivX as the certificate authority, which only provides certificates as part of the authorization of users for sessions the users are entitled for. This removes the need for managing passwords and other credentials in vaults but concentrates on session access and monitoring. PrivX furthermore removes the need to install agents on clients and servers. Overall, the concept of PrivX leads to very short deployment times.

With the approach of PrivX, SSH.COM provides capabilities that are suited at environments which primarily rely on SSH access and that are highly dynamic in nature, as today's DevOps environments are. In contrast to other PAM vendors, SSH.COM does not cover the full breadth of PAM capabilities. While some are of little relevance given the PrivX approach, others such as fine-granular control about

entitlements on host (Controlled Privilege Elevation and Delegation Management) or Privileged Behavior Analytics would add value to PrivX. However, the capabilities delivered today allow increasing and managing security of privileged access in cloud and DevOps environments with reasonable effort.

PrivX can act as both a replacement of other PAM approaches and a complementary technology that is used for specific PAM requirements, particularly in DevOps environments. We strongly recommend taking a look at PrivX that offers a unique alternative to standard password vaulting and session management approaches.

Strengths	Challenges
• Efficient approach on managing access to hosts via SSH and RDP sessions • Avoids the effort of managing credentials for privileged accounts by relying on short-lived credentials • Central management of privileged access via roles and policies • High scalability and support for load-balancing • Support for cloud and DevOps environments, targeted at specific requirements of agile IT environments • Integrates with common user directories such as LDAP directories, Gsuite and Microsoft Active Directory, with further integration into identity services via OpenID Connect • Supports session recording and audit logging, including SIEM integration	• Not a comprehensive PAM suite; however, offers an innovative alternative to PSM • Lacks support for advanced PAM capabilities such as Privileged Behavior Analytics • Limited support for windows systems including RDP sessions such as session indexing and activity search

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a leading Europe-based analyst company for identity focused information security, both in classical and in cloud environments. KuppingerCole stands for expertise, thought leadership, and a vendor-neutral view on these information security market segments, covering all relevant aspects like Identity and Access Management (IAM), Governance, Risk Management and Compliance (GRC), IT Risk Management, Authentication and Authorization, Single Sign-On, Federation, User Centric Identity Management, eID cards, Cloud Security and Management, and Virtualization.

For further information, please contact **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstr. 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com