DATA SHEET

Entrust Cryptographic Security Platform Key Management Vault for PASM

Manage and Control SSH Access Across On-Premises and Cloud Environments.

Overview

Privileged accounts pose a significant risk to your organization. Hackers and malicious insiders can gain access to critical systems and steal sensitive data or cause service disruption. To further add to the risk, privileged accounts and associated access rights are not just granted to employees, but also to vendors, contractors, business partners, and other personnel.

To protect access to privileged systems, Secure Shell, commonly referred to as SSH, is an industry standard protocol used by IT professionals to secure remote login to such systems. Strong cryptographic algorithms protect the security and integrity of the communication channel.

The Entrust Cryptographic Security Platform's Key Management Vault for Privileged Account and Session Management (PASM) ensures privileged accounts are protected by vaulting their credentials. With it, you can control SSH access and usage of administrative and privileged accounts, recording privileged user activity across virtual, cloud, and physical environments.

You can also can give security teams control through centralized visibility and policy enforcement, simplifying the management of SSH access by leveraging corporate identity and access management (IAM) solutions.

Key Features

- Authentication, authorization, and audit control for SSH access with policy enforcement
- Integration with Active Directory (AD) and OpenID Connect (OIDC)/ SAMLv2 identity providers
- Protection of SSH keys
- On-demand and scheduled SSH key rotation
- SSH session recording in text format
- SSH session alerting with command filtering
- Audit data and forensic evidence to support compliance and investigations.
- Deployed as a virtual appliance
- High-availability (HA) support with active-active cluster

Benefits

Protects SSH Access

Achieve authentication, authorization, and audit control (AAA) security for all SSH access:

- Assign SSH access privileges to users and groups
- Enable Active Directory or OIDC Authentication
- Control access to remote hosts using policy-based access control
- Utilize SSH keys to authenticate to remote hosts
- Control and audit SSH access to machines

Reduces Key Risks and Helps Meet Compliance Requirements

Centrally manage and control SSH keys in multi-cloud environments:

- Import, protect, rotate SSH keys in an encrypted vault
- Reduce key sprawl by getting centralized control and visibility of all SSH keys
- Reduce key risks by ensuring continuous compliance with security standards and best practices

Records Sessions and Ensures that No Unauthorized Change is Made

Create a complete record of the user's activity and block unauthorized commands during a privileged session:

- Block specific commands during a session using regular expressions
- Provide a complete audit trail including the user connection, disconnection, and actions performed during a remote session
- Export the session recording as a PDF file

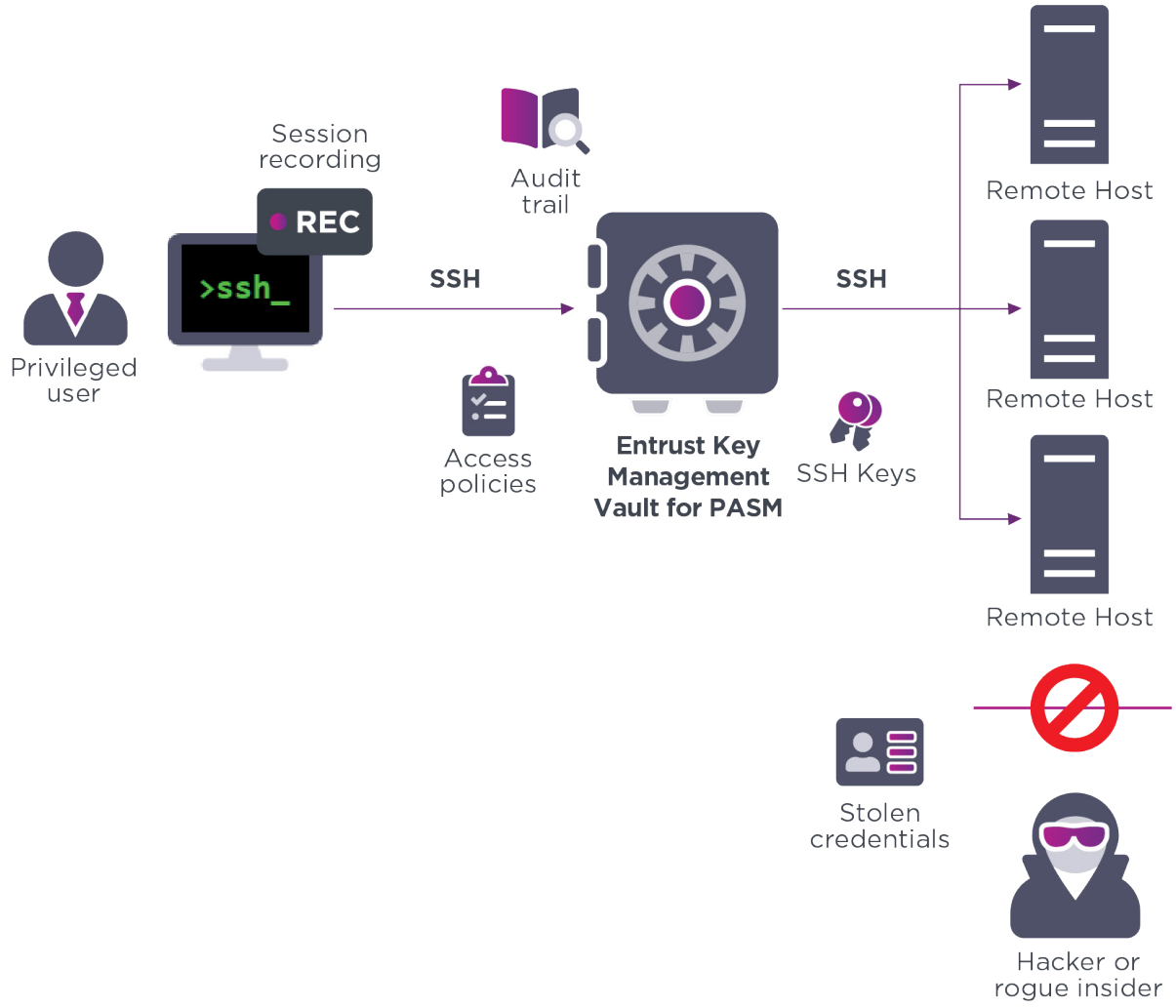
How It Works

Entrust Key Management Vault for PASM centrally manages and enforces access control to servers and systems based on user identity. End-users are authenticated and provided SSH access according to access control policies. All user activity on remote hosts is recorded. The solution requires no agents on the target systems, and therefore has zero footprint on remote hosts.

- The user logs into the platform Key Management Vault for PASM using their Active Directory or vault credentials
- The vault connects to the remote host without divulging any privileged credentials
- Once logged in, the user issues commands on the remote host
- When finished the user ends the session

All user activity on the remote host during the session is recorded by the vault.

How It Works



Highlights

Reduce the Burden of SSH Access and Key Management

SSH keys are continuously being created along with the creation of new workloads without any controls over when or how these keys are used. Managing SSH keys for numerous users and environments can be a painful and time-consuming job for infrastructure administrators.

Key Management Vault for PASM can ease the burden of controlling SSH access and managing SSH keys by leveraging corporate IAM systems for user authentication and authorization.

This enables automatic provisioning of privileges based upon group membership.

All SSH access privileges can be automatically revoked if a system administrator changes roles or leaves the company. Finally, the vault removes the constraint of having to distribute SSH keys to end-user desktops and can automatically rotate keys based on corporate security policy.

ENTRUST
SECURING A WORLD IN MOTION

Comply with Audit Requirements

Meeting audit and compliance requirements does not only entail the auditing of all access to critical systems but also necessitates keeping track of what actions are carried out on remote systems.

For instance, the U.S. Federal Information Security Modernization Act (NIST SP 800-53r4 AC-2, AC-17, and AU13) specifies the need "to monitor the use of account and remote access methods, authorize each type of remote access, route remote accesses through authorized and managed network access control points and ensure that audit records contain necessary information to support the auditing function."

Beyond access control, the vault provides a complete recording of the user's activity during the SSH session. SSH recordings are provided in a searchable format and can be exported for audit or compliance purposes.

Session recordings are securely and centrally stored to make audit activities straightforward, ensure accountability, and improve compliance.

Technical Specifications

Supported Unix/Linux Operating Systems

- CentOS, Red Hat Enterprise Linux, Ubuntu, SUSE Linux Enterprise Server, Oracle Linux, Amazon Linux

Supported Protocols and Client

- All SSH versions and clients

Authentication Methods

- Local password authentication
- Active Directory and LDAP authentication

Management and Monitoring

- Centralized management with Web UI and RESTful API
- Syslog and Splunk integration

Supported Hypervisors for the Key Management Vault

- VMware ESXi 7.0 (HW version 17) and above
- Red Hat KVM 7.8 and above
- AWS, Azure, and GCP (latest Entrust version available in the marketplace)

Prevent or Reduce the Consequences of System Compromise

If an attacker gains access to your virtual machines, they can control the applications running there, all local data, and any connected machines and systems.

Entrust Key Management Vault for PASM can track access of sensitive information that might have been exfiltrated or actions carried out on critical systems that resulted in outages, helping to reduce the impact of an attack and the time to resolve an issue.

Each command in the privileged session is audited and can be forwarded to an SIEM tool. Moreover, the vault has the capability to block specific commands, limiting the ability of attackers to cause damage on IT systems.

Forensic Investigation and Root Cause Analysis

Audit data is captured to support problem resolution as well as for forensic investigation. Session recordings facilitate quicker root cause analysis, shortening the recovery time from outages and server failures. Session recordings are searchable and allow users to search for specific text strings (e.g., find the sessions where a specific file was modified).

VMware Solution (AVS), Google Cloud Platform (GCP)

- Hypervisor support: ESXi, AWS, Azure, KVM, Google Cloud Platform

Deployment Media

- ISO, OVA (Open Virtual Appliance), AMI (Amazon Web Services Marketplace), or VHD (Microsoft Azure Marketplace)

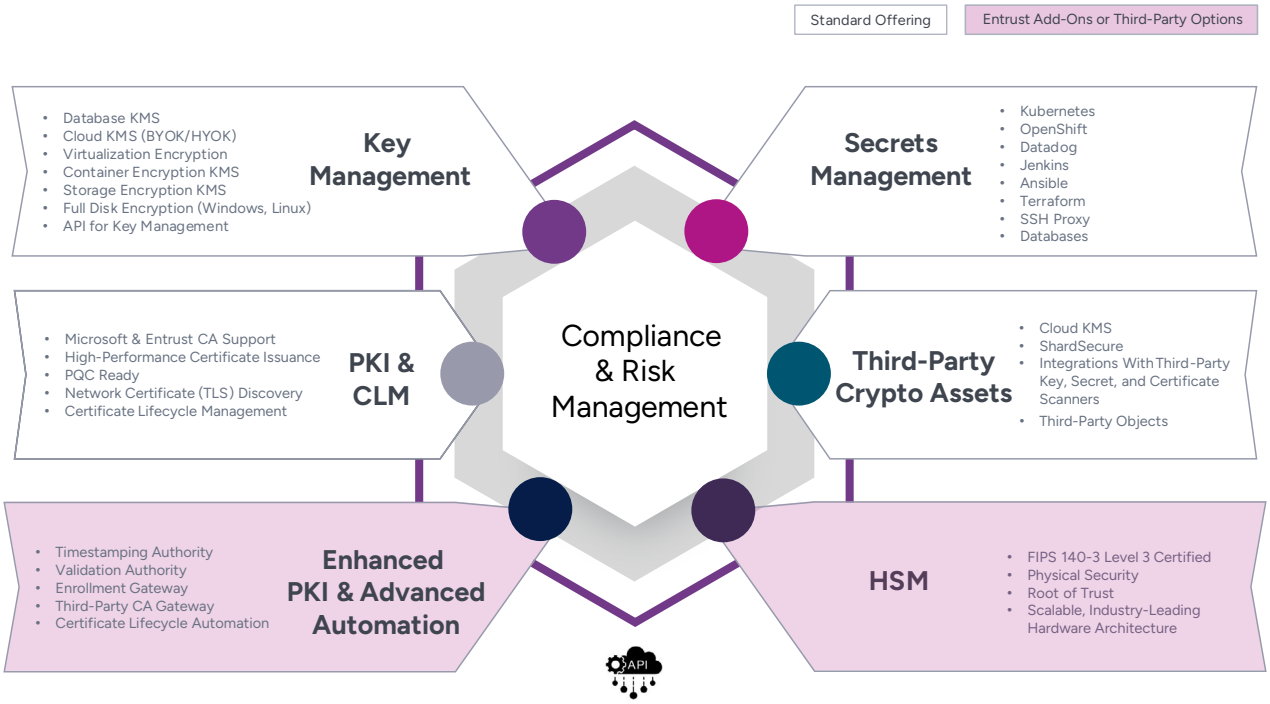
Certifications

- FIPS 140-2 Level 3 compliance via Entrust nShield HSM on premises or as a service

Entrust Cryptographic Security Platform

The Entrust Cryptographic Security Platform provides a comprehensive solution for discovering and managing the lifecycles of certificates, cryptographic keys, secrets, tokens, libraries, protocols, and configurations.

By centralizing cryptographic asset management, it enhances security, helps ensure compliance, and streamlines operations, enabling seamless integration across both on-premises and cloud environments.



entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION