Hitachi ID Privileged Access Manager

hitachi-id.com

Challenges

Security

High risk accounts are a prime target for attackers and may be abused or misused by authorized users. Static, shared and plaintext passwords can be compromised by departed employees or malicious software. When authorized users sign into shared accounts, there is no accountability for their actions, which is problematic both for troubleshooting and for forensic audits.

Regulatory Compliance

Government legislation and industry guidelines regarding privacy protection and corporate governance, including PCI-DSS, SOX, EU GDPR and HIPAA demand robust internal controls. This includes control over privileged access, be it administrator accounts or membership in security groups.

Coordination

Changing passwords on shared accounts is difficult, as is changing service account and embedded passwords. Manual processes are time consuming, error prone and costly, but failure to change passwords creates vulnerabilities and often violates policy.

Key Benefits

Hitachi ID Privileged Access Manager secures access to high risk accounts and groups. It replaces static, shared passwords with periodically changing random values. Users and applications are strongly authenticated and authorized before gaining access. Audit logs and session recordings create strong accountability for access.

Securing Access to Privileged Accounts

Hitachi ID Privileged Access Manager secures access to high risk accounts and groups. It eliminates shared and static passwords and enforces strong authentication and reliable authorization prior to granting access. User access is logged, creating forensic-level accountability.

Strong Authentication, Authorization

HiPAM integrates with corporate directories to identify users. It can either leverage existing 2FA solutions, such as tokens or smart cards, or introduce its own 2FA, via a smart-phone app. User access may be pre-authorized or subject to a request-approval workflow.

Password Randomization and Vaulting

HiPAM randomizes passwords on a schedule and after each login session. Passwords are stored in an encrypted, replicated credential vault that protects against data loss and service interruption.

Access Disclosure, not Password Disclosure

HiPAM can launch administrator tools on behalf of users and inject credentials from its vault. Sessions can be established directly from the user's PC, or via VDI or HTML5 proxy servers.

User-friendly Single Sign-On

Users sign into the HiPAM portal and from there can request access to one or more accounts or groups. Users launch sessions right from the portal, without having to sign in again for each session (as is the case with "jump server" products). HiPAM can also be used to run commands across multiple systems -- a great time saver.

Smart Phone Access

Users typically sign into HiPAM with a PC to request and approve access and to launch login sessions. HiPAM includes apps for Android and iOS and a mobile proxy, making it possible to establish SSH and RDP sessions from any location at any time.

Session Recording, Search and Replay

When HiPAM launches login sessions, it can capture video, keystrokes and more, creating a forensic audit trail. Recordings can be viewed in real time or after the fact. User privacy is protected with keystroke censorship and request/approval workflow to protect search and playback.

Discovery and Analysis of SSH Trust

HiPAM discovers SSH trust relationships (.ssh/authorized_keys files) and can analyze trust graphs. It can inject temporary trust relationships access on Unix/Linux systems, as an alternative to password injection.

Hitachi ID Systems, Inc.

HITACHI
Inspire the Next

Local Accounts on Servers and PCs

HiPAM secures access to both directory and local accounts. An optional agent is available for installation on Windows systems, to manage passwords on frequently unreachable systems, such as laptops.

Windows Service Accounts

When HiPAM randomizes Windows service account passwords, it notifies SCM, the Scheduler, IIS and other Windows OS components of the new password, to ensure uninterrupted service.

Embedded Accounts

A secure API allows applications to securely and reliably retrieve managed passwords. A fingerprint of both applications and their runtime environment is computed as an authentication mechanism. Alternately, HiPAM can inject new passwords into services, registry entries, configuration files and more, to integrate with applications that cannot be modified to leverage the HiPAM API.

Auto-discovery of Systems and Accounts

HiPAM can automatically discover systems, look up appropriate credentials, connect and scan for accounts, groups and services. Discovered systems and accounts are automatically assigned to policies based on import rules.

Analytics and Dashboards

Built-in reports and dashboards can monitor the behaviour of individual users, access to systems and overall activity. A risk model flags unusual patterns prior to access and in post-facto reviews.

Included Connectors

Directories

Active Directory and Azure AD; any LDAP; NIS/NIS+

Databases

Oracle; SAP ASE and HANA; SQL Server; DB2/UDB; Hyperion; Caché; MySQL; OLAP and ODBC.

Server OS: X86/IA64

Windows: NT thru 2016; Linux and *BSD.

Server OS: Unix

Solaris, AIX, HP-UX and many others.

Server OS: Mainframes

z/OS with RAC/F, ACF/2 or TopSecret.

Server OS: Midrange

iSeries (OS400); OpenVMS and HPE/Tandem NonStop.

ERP, CRM and other apps

Oracle EBS; SAP ECC and R/3; JD Edwards; PeopleSoft; Salesforce.com; Concur; Business Objects and Epic.

Messaging and collaboration

Office 365; Google Apps; Cisco WebEx, Call Manager and Unity.

Tokens, smart cards and 2FA apps

Any RADIUS service or SAML IdP; Duo Security; RSA SecurID; SafeWord; Vasco; ActivIdentity and Schlumberger.

Web access management and SSO:

CA SiteMinder; IBM Security Access Manager; Oracle AM; RSA Access Manager and Imprivata OneSign.

Help desk incident management (ITSM):

ServiceNow; BMC Remedy, RemedyForce and Footprints; JIRA; HPE Service Manager; CA Service Desk; Axios Assyst; Ivanti HEAT; Symantec Altiris; Track-It!; MS SCS Manager and Cherwell.

Server health monitoring

HP iLO, Dell DRAC and IBM RSA.

HR / HCM

WorkDay; PeopleSoft HR; SAP HCM and SuccessFactors.

Extensible / scriptable:

CSV files; Google Sheets; SCIM; SSH; Telnet/TN3270/TN5250; HTTP(S); SQL; LDAP; PowerShell and Python.

Hypervisors and IaaS

AWS; vSphere and ESXi.

Network devices

Cisco IOS PIX and ASA; Juniper JunOS and ScreenOS; F5 BigIP; HP Procurve; Brocade Fabric OS and CheckPoint SecurePlatform.

Filesystems and content platforms

Windows/CIFS/DFS; SharePoint; Samba; Hitachi Content Platform and HCP Anywhere; Box.com and Twitter.

Security Incident / Event Management:

Splunk; ArcSight; RSA Envision and QRadar. Any SIEM supporting SYSLOG or Windows events.

Infrastructure and vulnerability managers

Qualys; McAfee ePO and MVM; Cisco ACS; ServiceNow ITAM; HP UCMDB; Hitachi HiTrack.

Hitachi ID Privileged Access Manager is part of the Hitachi ID Identity and Access Management Suite, which also includes: Identity Manager to manage users and groups and Password Manager for strong authentication, federation and credential management. For more information, please visit: https://hitachi-id.com/ or call: 1.403.233.0740 | 1.877.386.0372

HITACHI
Inspire the Next