Hitachi ID Privileged Access Manager

hitachi-id.com

Challenges

Security

Elevated-privilege accounts are a prime target for attackers and are subject to abuse and misuse 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 little to no accountability for their actions, which is problematic both for problem diagnosis and forensic audits.

Regulatory Compliance

Government legislation and industry guidelines regarding privacy protection and corporate governance, including PCI-DSS, SOX, EU GDPR, HIPAA and more all demand robust internal controls. This includes control over privileged access, be it privileged accounts or 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 violates policy.

Key Benefits

Hitachi ID Privileged Access Manager secures access to elevated privileges, be they shared accounts, personal administrator accounts, service accounts, embedded accounts or security groups. It replaces static, shared passwords with periodically set, random passwords. Users and applications are strongly authenticated and authorized before gaining access. Audit logs and session recordings create strong accountability for access.

Hitachi ID Systems, Inc.

Securing Access to Privileged Accounts

Hitachi ID Privileged Access Manager secures access to elevated privileges. It eliminates shared and static passwords to privileged accounts and enforces strong authentication and reliable authorization prior to granting access. User access is logged, creating strong 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.

Temporary Access to Accounts and Groups

Users may request access to shared or personal administrator accounts or membership in security groups. Access may be pre-authorized or require approval using the included workflow.

Password Randomization and Vaulting

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

Access Disclosure, not Password Disclosure

HiPAM can launch administrator programs 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.

Session Recording

When HiPAM launches login sessions, it can also capture video, keystrokes and more, creating a forensic audit trail.

Discovery and Analysis of SSH Trust

HiPAM discovers SSH trust relationships and can analyze trust graphs. It can inject temporary trusts to grant access to Unix/Linux systems.

Support for Local Accounts on Mobile PCs

A local agent is included to secure access to PCs that may be turned off, disconnected or moved off-site.

Windows Service Account Password Changes

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

A Secure API to Replace Static, Embedded Passwords

A secure API allows one application to acquire a password for connecting to another. This eliminates plaintext passwords in source code or configuration files.

HITACHI
Inspire the Next

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

Any LDAP, AD, eDirectory, NIS/NIS+

Servers

Windows 2000--2012, Samba, SharePoint

Databases

Oracle, Sybase, SQL Server, DB2/UDB, ODBC, Informix, Progress

Unix

Linux, Solaris, AIX, HPUX, many more

Mainframes

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

Midrange

iSeries (OS400), OpenVMS

ERP

JDE, Oracle eBiz, PeopleSoft, SAP, Siebel, Business Objects

Collaboration

Lotus Notes, Exchange

Tokens, Smart Cards

RSA SecurID, SafeWord, Duo Security, RADIUS, ActivIdentity, Schlumberger

WebSSO

CA SiteMinder, IBM TAM, Oracle AM, RSA Access Manager

Ticket systems

ServiceNow, Remedy, BMC SDE, HP SM, CA, Assyst, HEAT, Altiris, Clarify, Track-It!, RSA Envision, MS SCS Manager

Network devices

Cisco IOS, Juniper JunOS, F5, iLO cards, DRAC cards, RSA cards, etc

Cloud

Salesforce.com, WebEx, Google Apps, Office 365, Concur, AWS, vCloud

Miscellaneous

OLAP, Hyperion, iLearn, Cache, Success Factors, vSphere

Extensible

SPML, SCIM, SAML, SSH, Telnet, TN3270, HTTP(S), SQL, LDAP, ODBC, CSV, Python/web services

Hitachi ID Privileged Access Manager is part of the Hitachi ID Identity and Access Management Suite, which also includes: Identity Manager for governance and administration of identities and entitlements and Password Manager for strong authentication, federation and credential management.

For more information, please visit: http://hitachi-id.com/
or call: 1.403.233.0740 | 1.877.386.0372

HITACHI
Inspire the Next