

1 Hitachi ID Privileged Access Manager



**Managing the User Lifecycle
Across On-Premises and
Cloud-Hosted Applications**

Securing access to administrator, embedded and service accounts.

2 Agenda

- Hitachi ID corporate overview.
- ID Management Suite overview.
- Securing administrative passwords with Hitachi ID Privileged Access Manager.
- Animated demonstration.

3 Hitachi ID Corporate Overview

Hitachi ID is a leading provider of identity and access management solutions.

- Founded as M-Tech in 1992.
- A division of Hitachi, Ltd. since 2008.
- Over 900 customers.
- More than 11M+ licensed users.
- Offices in North America, Europe and APAC.
- Partners globally.



4 Representative Hitachi ID Customers

Financial 	Healthcare 	Communications
Government 	Manufacturing 	Education
Pharmaceuticals 	Retail/Consumer 	Transportation
Technology 	Resources and Energy 	Food & Beverages

5 ID Management Suite



6 Securing Privileged Accounts

Thousands of IT assets:

- Servers, network devices, databases and applications:
 - Numerous.
 - High value.
 - Heterogeneous.
- Workstations:
 - Mobile – dynamic IPs.
 - Powered on or off.
 - Direct-attached or firewalled.

Who has the keys to the kingdom?

- Every IT asset has sensitive passwords:
 - **Administrator passwords:**
Used to manage each system.
 - **Service passwords:**
Provide security context to service programs.
 - **Application:**
Allows one application to connect to another.
- Do these passwords ever change?
- Who knows these passwords? (ex-staff?)
- Audit: who did what?

7 Project Drivers

Organizations need to secure their most sensitive passwords:

Compliance:	<ul style="list-style-type: none"> • Pass regulatory audits. • Compliance should be sustainable.
Security:	<ul style="list-style-type: none"> • Eliminate static passwords on sensitive accounts. • Create accountability for admin work.
Cost:	<ul style="list-style-type: none"> • Efficient process to regularly change privileged passwords. • Simple and effective deactivation for former administrators.
Flexibility:	<ul style="list-style-type: none"> • Grant temporary admin access. • Emergencies, production migrations, workload peaks, etc.

8 Participants in PAM

Hitachi ID Privileged Access Manager works by *randomizing* privileged passwords and *connecting* people and programs to privileged accounts as needed:

Privileged accounts	Get new, random passwords daily or at the desired frequency.
IT Users	Must sign into HiPAM when they need to sign into administrator accounts.
Services	Are automatically updated with new passwords values.
Applications	Use the HiPAM API instead of embedded passwords.
Security officers	Define policies regarding who can connect to which privileged account.
Auditors	Monitor access requests and privileged login sessions.

9 HiPAM Impact

<i>Feature</i>	<i>Impact</i>	<i>Benefit</i>
Randomize passwords daily	Eliminate static, shared passwords.	Disconnect former IT staff.
Controlled disclosure	Control who can see passwords.	The right users and programs can access privileged accounts, others cannot.
Logging & Reporting	Monitor password disclosure.	Accountability. Faster troubleshooting.
Encryption	Secure passwords in storage and transit.	Physical compromise does not expose passwords.
Replication	Passwords stored on multiple servers, in different sites.	Survive server crashes and site disasters.

10 Understand and Manage the Risks

A privileged access management (PAM) system becomes the sole repository of the most important credentials.

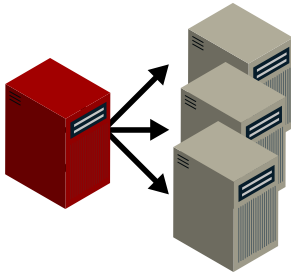
<i>Risk</i>	<i>Description</i>	<i>Mitigation</i>
Disclosure	<ul style="list-style-type: none"> Compromised vault → security disaster. 	<ul style="list-style-type: none"> Encrypted vault. Strong authentication. Flexible authorization.
Data Loss	<ul style="list-style-type: none"> Destroyed vault → IT disaster. 	<ul style="list-style-type: none"> Replicate the vault.
Non-availability	<ul style="list-style-type: none"> Offline vault → IT service interruption. 	<ul style="list-style-type: none"> One vault in each of 2+ sites.

Customers must test failure conditions before purchase!

11 Randomizing Passwords

Push

random passwords to systems:

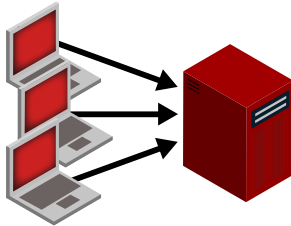


- Periodically (e.g., between 3AM and 4AM).
- When users check passwords back in.
- When users want a specific password.
- On urgent termination.

• ***Suitable for servers and PCs on the corporate network.***

Pull

initiated by user devices:



- Periodically.
- Random time-of-day.
- Opportunistically, when connectivity is available.

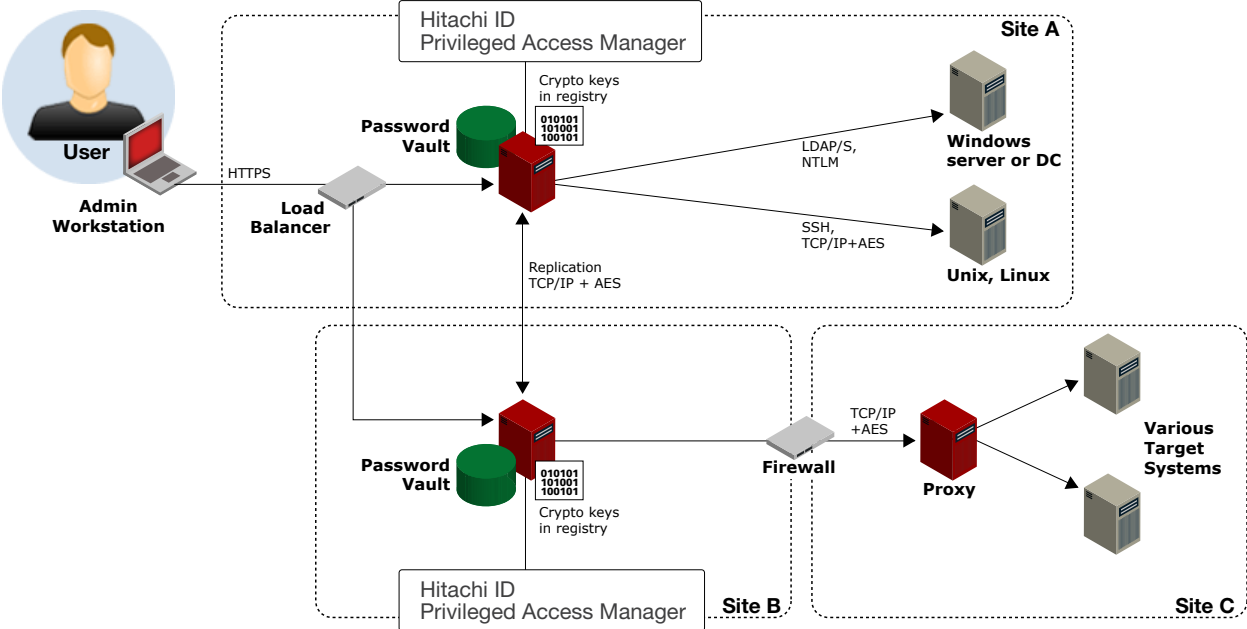
• ***Suitable for home PCs and on-the-road laptops.***

12 Authorizing Access to Privileged Accounts

Two models: permanent and one-time.

<i>Permanent ACL</i>	<i>One-time request</i>	<i>Concurrency control</i>
<ul style="list-style-type: none">• Pre-authorized users can launch an admin session any time.• Access control model:<ul style="list-style-type: none">– Users ... belong to– User groups ... are assigned ACLs to– Managed system policies ... which contain– Devices and applications• Also used for API clients.	<ul style="list-style-type: none">• Request access for any user to connect to any account.• Approvals workflow with:<ul style="list-style-type: none">– Dynamic routing.– Parallel approvals.– N of M authorizers.– Auto-reminders.– Escalation.– Delegation.	<ul style="list-style-type: none">• Coordinate admin changes by limiting number of people connected to the same account:<ul style="list-style-type: none">– Can be >1.– Notify each admin of the others.• Ensure accountability of who had access to an account at a given time.

13 Fault-Tolerant Architecture



14 Included Connectors

Many integrations to target systems included in the base price:

<p>Directories: Any LDAP, AD, WinNT, NDS, eDirectory, NIS/NIS+.</p>	<p>Servers: Windows NT, 2000, 2003, 2008, Samba, Novell, SharePoint.</p>	<p>Databases: Oracle, Sybase, SQL Server, DB2/UDB, Informix, ODBC.</p>
<p>Unix: Linux, Solaris, AIX, HPUX, 24 more.</p>	<p>Mainframes, Midrange: z/OS: RACF, ACF2, TopSecret. iSeries, OpenVMS.</p>	<p>HDD Encryption: McAfee, CheckPoint.</p>
<p>ERP: JDE, Oracle eBiz, PeopleSoft, SAP R/3 and ECC 6, Siebel, Business Objects.</p>	<p>Collaboration: Lotus Notes, Exchange, GroupWise, BlackBerry ES.</p>	<p>Tokens, Smart Cards: RSA SecurID, SafeWord, RADIUS, ActivIdentity, Schlumberger.</p>
<p>WebSSO: CA Siteminder, IBM TAM, Oracle AM, RSA Access Manager.</p>	<p>Help Desk: BMC Remedy, SDE, HP SM, CA Unicenter, Assyst, HEAT, Altiris, Track-It!</p>	<p>Cloud/SaaS: WebEx, Google Apps, Salesforce.com, SOAP (generic).</p>

15 Application and Service Accounts

Unattended programs on Windows

- Services, Scheduled Tasks, IIS Anonymous Access, etc.
 - Run in the context of a named user.
 - Are started with that user's ID and password.
 - Hitachi ID Privileged Access Manager updates the appropriate OS component after every password change.
-

Applications

- Eliminate embedded passwords via secure API to the vault.
 - API authentication using one time passcode + client IP.
-

16 Infrastructure Auto-Discovery

Find and classify systems, services, groups, accounts:

List systems	Evaluate import rules	Probe systems
<ul style="list-style-type: none"> • From AD, LDAP (computers). • From text file (IT inventory). • Extensible: DNS, IP port scan. 	<ul style="list-style-type: none"> • Manage this system? • Attach system to this policy? • Choose initial ID/password. • Manage this account? • Un manage this system? 	<ul style="list-style-type: none"> • Local accounts. • Security groups. • Group memberships. • Services. • Local svc accounts. • Domain svc accounts.

- Hitachi ID Privileged Access Manager can find, probe, classify and load 10,000 systems/hour.
- Normally executed every 24 hours.
- 100% policy driven - no scripts.

17 Alternatives to Displaying Passwords

<i>Launch session (SSO)</i>	<ul style="list-style-type: none"> • Launch RDP, SSH, etc. from Hitachi ID Privileged Access Manager web UI. • Plug-ins for additional programs/protocols. 	<ul style="list-style-type: none"> • Password not disclosed at all. • User is connected directly without further proxy.
<i>Temporary ACL change</i>	<ul style="list-style-type: none"> • Place user's AD account in a local security group (Windows). • Place user's public SSH key in .ssh/authorized_keys file (Unix). • Manipulate /etc/sudoers files (Unix). 	<ul style="list-style-type: none"> • No password involved. • Native logging references the user's own account.
<i>Copy</i>	<ul style="list-style-type: none"> • Place password in user's OS copy buffer. • Clear buffer after N seconds. 	<ul style="list-style-type: none"> • Allows user to paste the password into an e-mail, text, file, etc. • Password not directly disclosed.
<i>Display</i>	<ul style="list-style-type: none"> • Reveal the cleartext value of password on screen. • Clear display after N seconds. 	<ul style="list-style-type: none"> • Appropriate for managing off-line, console login devices.

18 Test Safety Features

To prevent a security or an IT operations disaster, a privileged password management system must be built for safety first:

Unauthorized disclosure

- Passwords must be encrypted, both in storage and transmissions.
- Access controls should determine who can see which passwords.
- Workflow should allow for one-off disclosure.
- Audit logs should record everything.

Data loss, Service Disruption

- Replicate all data – a server crash should be harmless.
- Replication must be real time, just like password changes.
- Replication must span physical locations, to allow for site disasters (fire, flood, wire cut).

- These features are mandatory.
- Failure is not an option.
- Ask Hitachi ID for an evaluation guide.
- Evaluate products on multiple, replicated servers.
- Turn off one server in mid-operation.
- Inspect database contents and sniff network traffic.

19 HiPAM Unique Technology

<i>Multi-master</i>	<ul style="list-style-type: none"> • Built-in replication easy to setup and no extra cost. • Geographically distributed for maximum safety. • All nodes active: efficient and scalable.
<i>Connectors</i>	<ul style="list-style-type: none"> • Over 110 connectors, out of the box. • Also supports mobile devices.
<i>Workflow</i>	<ul style="list-style-type: none"> • Dynamic routing to multiple authorizers. • Built-in reminders, escalation, delegation.
<i>AD/LDAP groups</i>	<ul style="list-style-type: none"> • Manage groups that authorize access. • Requests, approvals, SoD policy, certification, reports.
<i>Session monitor</i>	<ul style="list-style-type: none"> • Record keystrokes, video, webcam, more. • Workflow controls search, playback.
<i>SSO</i>	<ul style="list-style-type: none"> • Launch RDP, SSH, SQL, vSphere and more. • Temporary trust: Windows groups, SSH keys.

20 Request one-time access

Animation: ../pics/camtasia/hipam-71/1-request-access.cam4

21 Approve one-time access

Animation: ../pics/camtasia/hipam-71/2-approve-request.cam4

22 Launch one-time session using a privileged account

Animation: ../pics/camtasia/hipam-71/3-privileged-login-session.cam4

23 Request, approve, play recording

Animation: ../pics/camtasia/hipam-71/7-view-playback.cam4

24 Report on requests for privileged access

Animation: ../pics/camtasia/hipam-71/hipam-06-admin-reports.cam4

25 Summary

Hitachi ID Privileged Access Manager secures privileged accounts:

- Eliminate static, shared passwords to privileged accounts.
- Built-in encryption, replication, geo-diversity for the credential vault.
- Authorized users can launch sessions without knowing or typing a password.
- Infrequent users can request, be authorized for one-time access.
- Strong authentication, authorization and audit throughout the process.

Learn more at Hitachi-ID.com/Privileged-Access-Manager