1 Hitachi ID Privileged Access Manager

Securing access to administrator, embedded and service accounts

Temporary, secure and accountable privilege elevation.

2 Agenda

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

Hitachi ID delivers access governance and identity administration solutions to organizations globally.
Hitachi ID IAM solutions are used by Fortune 500 companies to secure access to systems in the enterprise and in the cloud.

- A division of Hitachi, Ltd. since 2008.
- Over 1200 customers.
- More than 14M+ licensed users.
- Offices in North America, Europe and APAC.
- Global partner network.
4 Representative customers
5 Hitachi ID 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?
- Plaintext in configuration files?
- Who knows these passwords? (ex-staff?)
- Who made what changes, when and why?
7 Project drivers

Organizations need to secure their most sensitive passwords:

| Compliance         | • Pass regulatory audits.  |
|                    | • Compliance should be sustainable.  |
| Security           | • Eliminate static passwords on sensitive accounts.  |
|                    | • Create accountability for admin work.  |
| Cost               | • Efficient process to regularly change privileged passwords.  |
|                    | • Simple and effective deactivation for former administrators.  |
| Flexibility        | • 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 Privileged Access Manager when they need to sign into administrator accounts.  |
| Services            | Are automatically updated with new passwords values.  |
| Applications        | Use the Privileged Access Manager 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

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

10  Understand and manage the risks

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

<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized Disclosure</td>
<td>• Compromised vault → security disaster.</td>
<td>• Encrypted vault. • Strong authentication. • Flexible authorization.</td>
</tr>
<tr>
<td>Data Loss</td>
<td>• Destroyed vault → IT disaster.</td>
<td>• Replicate the vault.</td>
</tr>
<tr>
<td>Non-availability</td>
<td>• Offline vault → IT service interruption.</td>
<td>• One vault in each of 2+ sites. • Multiple network routes.</td>
</tr>
</tbody>
</table>

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.

**Pull** initiated by user devices:
- Periodically.
- Random time-of-day.
- Opportunistically, when connectivity is available.

- *Suitable for servers and PCs on the corporate network.*
- *Suitable for off-site laptops, systems in a DMZ.*
## 12 Authorizing access to privileged accounts

Two models: permanent and one-time.

<table>
<thead>
<tr>
<th>Permanent ACL</th>
<th>One-time request</th>
<th>Concurrency control</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Pre-authorized users can launch an admin session any time.</td>
<td>• Request access for any user to connect to any account.</td>
<td>• Coordinate admin changes by limiting number of people connected to the same account:</td>
</tr>
<tr>
<td>• Access control model:</td>
<td>• Approvals workflow with:</td>
<td>– Can be &gt;1.</td>
</tr>
<tr>
<td>– Users ... belong to</td>
<td>– Dynamic routing.</td>
<td>– Notify each admin of the others.</td>
</tr>
<tr>
<td>– User groups ... are assigned ACLs to</td>
<td>– Parallel approvals.</td>
<td>• Ensure accountability of who had access to an account at a given time.</td>
</tr>
<tr>
<td>– Managed system policies ... which contain</td>
<td>– N of M authorizers.</td>
<td></td>
</tr>
<tr>
<td>– Devices and applications</td>
<td>– Auto-reminders.</td>
<td></td>
</tr>
<tr>
<td>• Also used for API clients.</td>
<td>– Escalation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– Delegation.</td>
<td></td>
</tr>
</tbody>
</table>
13 Fault-tolerant architecture

User

Credential vault

Load balancer

HTTPS

Site A

Hitachi ID Privileged Access Manager

Replication TCP/IP + AES

Site B

Hitachi ID Privileged Access Manager

Firewall

TCP/IP + AES

Managed endpoints

Site C

Windows server or DC

Unix, Linux

TCP/IP + AES

HTTPS

Various protocols

© 2019 Hitachi ID Systems, Inc. All rights reserved.
**14 Included connectors**

<table>
<thead>
<tr>
<th>Directories:</th>
<th>Databases:</th>
<th>Server OS – X86/IA64:</th>
<th>Server OS – Unix:</th>
<th>Server OS – Mainframe:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory and Azure AD; any LDAP; NIS/NIS+ and eDirectory.</td>
<td>Oracle; SAP ASE and HANA; SQL Server; DB2/UDB; Hyperion; Caché; MySQL; OLAP and ODBC.</td>
<td>Windows: NT thro 2016; Linux and *BSD.</td>
<td>Solaris, AIX and HP-UX.</td>
<td>RAC/F, ACF/2 and TopSecret.</td>
</tr>
</tbody>
</table>

Server OS – Midrange: iSeries (OS400); OpenVMS and HPE/Tandem NonStop.

<table>
<thead>
<tr>
<th>ERPS, CRM and other apps:</th>
<th>Messaging &amp; collaboration:</th>
<th>Smart cards and 2FA:</th>
<th>Access managers / SSO:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle EBS; SAP ECC and R/3; JD Edwards; PeopleSoft; Salesforce.com; Concur; Business Objects and Epic.</td>
<td>Microsoft Exchange, Lync and Office 365; Lotus Notes/Domino; Google Apps; Cisco WebEx, Call Manager and Unity.</td>
<td>Any RADIUS service or SAML IdP; Duo Security; RSA SecurID; SafeWord; Vasco; ActiveIdentity and Schlumberger.</td>
<td>CA SiteMinder; IBM Security Access Manager; Oracle AM; RSA Access Manager and Imprivata OneSign.</td>
</tr>
</tbody>
</table>

Help desk / 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.

<table>
<thead>
<tr>
<th>PC filesystem encryption:</th>
<th>Server health monitoring:</th>
<th>HR / HCM:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft BitLocker; McAfee; Symantec Endpoint Encryption and PGP; CheckPoint and Sophos SafeGuard.</td>
<td>HP ILO, Dell DRAC and IBM RSA.</td>
<td>WorkDay; PeopleSoft HR; SAP HCM and SuccessFactors.</td>
</tr>
</tbody>
</table>

Hypervisors and IaaS:
AWS; vSphere and ESXi.

<table>
<thead>
<tr>
<th>Mobile management:</th>
<th>Network devices:</th>
<th>Filesystems and content:</th>
<th>SIEM:</th>
</tr>
</thead>
<tbody>
<tr>
<td>BlackBerry Enterprise Server and MobileIron.</td>
<td>Cisco IOS PIX and ASA; Juniper JunOS and ScreenOS; F5 BigIP; HP Procurve; Brocade Fabric OS and CheckPoint SecurePlatform.</td>
<td>Windows/CIFS/DFS; SharePoint; Samba; Hitachi Content Platform and HCP Anywhere; Box.com and Twitter.</td>
<td>Splunk; ArcSight; RSA Envision and QRadar. Any SIEM supporting SYSLOG or Windows events.</td>
</tr>
</tbody>
</table>

Management & inventory:
Qualys; McAfee ePO and MVM; Cisco ACS; ServiceNow ITAM; HP UCMDB; Hitachi HiTrack.

<table>
<thead>
<tr>
<th>Extensible / scriptable:</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSV files; SCIM; SSH; Telnet/TN3270/TN5250; HTTP(S); SQL; LDAP; PowerShell and Python.</td>
</tr>
</tbody>
</table>

**15 Types of privileged accounts**

<table>
<thead>
<tr>
<th>Shared Administrative</th>
<th>Embedded</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Interactive logins used by humans.</td>
<td>• One application connects to another.</td>
<td>• Run service programs with admin or limited rights.</td>
</tr>
<tr>
<td>• Client tools: PuTTY, RDP, SQL Studio, etc.</td>
<td>• DB logins, web services, etc.</td>
<td>• Windows requires a password.</td>
</tr>
<tr>
<td>• May be used at a physical console.</td>
<td></td>
<td>• Scheduled tasks, IIS, DCOM, SCM, etc.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Challenges:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Access control.</td>
</tr>
<tr>
<td>• Audit/accountability.</td>
</tr>
<tr>
<td>• Single sign-on.</td>
</tr>
</tbody>
</table>
16 Infrastructure auto-discovery

Find and classify systems, services, groups, accounts:

<table>
<thead>
<tr>
<th>List systems</th>
<th>Evaluate import rules</th>
<th>Probe systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>• From AD, LDAP (computers).</td>
<td>• Manage this system?</td>
<td>• Local accounts.</td>
</tr>
<tr>
<td>• From text file (IT inventory).</td>
<td>• Attach system to this policy?</td>
<td>• Security groups.</td>
</tr>
<tr>
<td>• Extensible: DNS, IP port scan.</td>
<td>• Choose initial ID/password.</td>
<td>• Group memberships.</td>
</tr>
<tr>
<td></td>
<td>• Manage this account?</td>
<td>• Services.</td>
</tr>
<tr>
<td></td>
<td>• Un manage this system?</td>
<td>• Local svc accounts.</td>
</tr>
</tbody>
</table>

• 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 Access disclosure mechanisms

<table>
<thead>
<tr>
<th>Launch session (SSO)</th>
<th>Temporary entitlement</th>
<th>Copy buffer integration</th>
<th>Display</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Launch RDP, SSH, vSphere, SQL Studio, ...</td>
<td>• Group membership (AD, Windows, SQL, etc.).</td>
<td>• Inject password into copy buffer.</td>
<td>• Show the password in the UI.</td>
</tr>
<tr>
<td>• Extensible (launch any CLI).</td>
<td>• SSH trust (.ssh/authorized_keys).</td>
<td>• Clear after N seconds.</td>
<td>• Clear after N seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

| Active-active | • Trivial to setup, no add'l cost, minimal effort to recover from disaster.  
|              | • Geographically distributed: maximum safety. |
| User friendly | • Strong login (2FA) followed by single sign-on (launch many sessions).  
|              | • Request multiple accounts, launch multiple sessions without re-authenticating.  
|              | • Direct and proxy connections. |
| Not just passwords | • Temporary group membership.  
|                | • SSH trust injection.  
|                | • Suspend/resume cloud based VM (lower cost of cloud). |
| Robust workflow | • Reminders, escalation, delegation, concurrent invitations.  
|                | • Not limited to "two keys" scenario. |
| IAM included | • Manage AD, LDAP groups that determine who has access.  
|              | • Requests, approvals, SoD policy, certification, reports. |

20 Request privileged account

Animation: ../../pics/camtasia/suite11/hipam-request-password.mp4

21 Approve one-time access

Animation: ../../pics/camtasia/suite11/hipam-approve-request.mp4

22 Launch approved RDP to Windows

Animation: ../../pics/camtasia/suite11/hipam-launch-rdp-approved-request.mp4
23  Request and launch PuTTY to Linux

Animation: ../../pics/camtasia/v10/hipam-linux-preauth.mp4

24  Request, approve and play recording

Animation: ../../pics/camtasia/suite11/hipam-view-playback-nb.mp4

25  Report on requests for privileged access

Animation: ../../pics/camtasia/v10/hipam-admin-reports.mp4

26  Password display

Animation: ../../pics/camtasia/v9/pw-disp-scaled-1/pw-disp-scaled-1.mp4

27  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