Access Governance and Identity Administration Solutions

The Hitachi ID Identity and Access Management Suite is an integrated solution for identity administration and access governance. It streamlines and secures the management of identities, groups, entitlements and credentials across systems and applications, on-premises and in the cloud. It also includes strong authentication via a mobile app and single sign-on to federated applications, at no extra cost. Organizations deploy the Hitachi ID Suite to strengthen controls, meet regulatory and audit requirements, improve user experience and reduce access administration and IT support cost.

The Hitachi ID Suite consists of three products, which may be deployed individually or together. Hitachi ID solutions can be delivered for installation on-premises or as a cloud-hosted, managed service (SaaS).

Identity Manager

Hitachi ID Identity Manager is an integrated solution for managing identities and groups across systems and applications. With Identity Manager, organizations move access changes out of IT to a mix of automated, HR-driven processes and request/approval workflows driven by business users. The end result is access granted appropriately and revoked on time, in support of internal controls and in compliance with regulations.

Identity Manager includes an automation engine that responds to changes in systems of record, a request portal, a workflow used to invite stake-holders to approve requests, complete tasks or review access, access certification, role-based access control, segregation of duties policy, risk scores and extensive reports, dashboards and analytics.

Password Manager

Hitachi ID Password Manager is an integrated solution for managing credentials across multiple systems and applications. It simplifies the management of passwords, tokens, smart cards, security questions, certificates and biometrics. Password Manager lowers IT support cost and improves the security of login processes.

Password Manager includes password synchronization, self-service password and PIN reset, federated access, enrollment of security questions and biometrics and self-service unlock of encrypted filesystems.

Privileged Access Manager

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.

Privileged Access Manager includes automatic discovery and classification of systems and accounts, password randomization and vaulting, pre-authorized access and one-time access requests, single sign-on to administrator login sessions, changes to service account passwords, an API to replace embedded passwords, session recording with search and playback. In addition to managing passwords, Privileged Access Manager can assign temporary group memberships and SSH trust relationships.
All Hitachi ID products share a common infrastructure and can be co-installed in a single logical instance. They share a scalable, active-active, geographically distributed architecture, connectors, a single management console, smart phone apps and an associated mobile proxy, built-in multi-factor authentication as well as the ability to leverage existing 2FA solutions.

**Included Connectors**

**Directories**
- Active Directory and Azure AD; any LDAP; NIS/NIS+

**Databases**
- Oracle; SAP ASE and HANA; SQL Server; DB2/UDB; Hyperion;
- Cache; MySQL; OLAP and ODBC.

**Server OS:**
- X86/IA64
- Windows: NT thru 2016; Linux and *BSD.
- Unix
- Solaris, AIX, HP-UX and many others.

**Server OS: Mainframes**
- z/OS with RACF; 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**
- Microsoft Exchange, Lync and Office 365; Lotus Notes/Domino;
- 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; Activedirectory and Schumlerberger.

**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.

**PC drive encryption:**
- McAfee; CheckPoint; Microsoft BitLocker; Symantec Endpoint
  Encryption and PGP and Sophos SafeGuard.

**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;
- HTTPS; SQL; LDAP; PowerShell and Python.

**Hypervisors and IaaS**
- AWS; vSphere and ESXi.

**Mobile device management:**
- BlackBerry Enterprise Server and Mobileiron.

**Network devices**
- Cisco IOS PIX and ASA; Juniper JunOS and ScreenOS; FS 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.