KuppingerCole Report

EXECUTIVE VIEW

By Martin Kuppinger

February 01, 2022

Hitachi ID Bravura Security Fabric

Enterprise IAM suites today need to meet an ever-growing list of IT requirements, which includes process automation, self-service, and identity-related administration and governance capabilities. Hitachi ID offers a well-integrated all-in-one IAM package that can meet these enterprise business requirements.

By **Martin Kuppinger**
mk@kuppingercole.com

Content

1 Introduction

Digital identity was a primary attack vector in nearly all the headline-grabbing data breaches of the last few years. Bad actors, such as fraudsters, state agents, and even malicious insiders or contractors, start by getting access to user accounts, then searching for administrative or service accounts to take over in order to exploit the elevated privileges that they possess. Whether the attackers' goal is stealing credit card information, health records, or intellectual property, their Techniques, Tactics, and Procedures (TTPs) almost always include compromising passwords and using privileged accounts.

Passwords remain an all-too-common authentication method for getting access to a user, group, shared, administrative, and service accounts even today. Managing passwords securely has never been more important.

Regulatory compliance is another factor driving the adoption of privileged access management solutions. For example, in Germany, the "IT-Sicherheitsgesetz" (IT Security Law) requires critical infrastructure operators to adopt a stronger security posture and report security incidents to the government. In the US, federal laws such as Sarbanes-Oxley mandate segregation of duties (SoD).

Traditional IAM systems are designed to provision, authenticate, authorize, and store information about users. User accounts are also defined; users are assigned to groups; users receive role or attribute information from an authoritative source. IAM systems are generally composed of user identities stored in directories, credentials, authenticators, authentication, and authorization services for Single Sign-On (SSO) and Web Access Management (WAM), identity federation for cross-domain support, and identity lifecycle and access governance functions.

IAM systems are generally deployed in an inward-facing way to serve a single enterprise. Over the last decade, many enterprises have found it necessary also to store information about business partners, suppliers, and customers in their own enterprise IAM systems, as collaborative development and e-commerce needs have dictated. Many organizations have built extensive identity federations to allow users from other domains to get authenticated and authorized to external resources. Traditional IAM scales in well-defined environments containing up to hundreds of thousands of users.

The growing need for APIs is driven by the need to meet emerging IT requirements such as hybrid environments that span across on-premises, the cloud, even multi-cloud environments, which support the different functional requirements of B2E, B2B, and B2C, as well as the ability to select these capabilities a la carte as needed. By exposing key IAM functionality via APIs, workflow and orchestration capabilities can span across multiple environments as well as providing DevOps support through automation.

Hitachi ID Systems was founded as M-Tech in 1992 in Calgary, Canada. Their first password management product – P-Synch – was released in 1995. In 2008, the company was purchased by Hitachi and became known as Hitachi ID Systems. Hitachi ID focuses on identity, credential, entitlement management, as well as

access governance. Hitachi ID Systems has offices in North America, Europe, and the APAC region with partners globally. With over 1, 300 licensed customers worldwide serving more than 14.5 million users, Hitachi ID is an established and respected solution developer in the Identity and Access Management (IAM) space.

2 Product Description

Hitachi ID Bravura Security Fabric

Hitachi ID Bravura Security Fabric comprises Hitachi ID Bravura Identity, Hitachi ID Bravura Pass, Hitachi ID Bravura Discover, Hitachi ID Bravura Group, and Hitachi ID Bravura Privilege. It is an integrated set of enterprise class products focused on process automation and access governance in traditional business-to-employee (B2E) and business-to-business (B2B) contexts, especially for organizations subject to strict privacy protection or corporate governance regulations. Hitachi ID Bravura Security Fabric customers include Fortune 500 corporations spanning the automotive, consumer, finance, energy/resources, manufacturing, pharmaceutical, retail, and healthcare as well as in the higher education, and government/military industries.

The Hitachi ID Bravura Security Fabric builds on a common set of components such as database, connectors, discovery functions, multi-factor authentication (MFA), admin UI, or high availability features. It also provides a consistent API across all individual components.

Hitachi ID Bravura Identity

Hitachi ID Bravura Identity's core capabilities include the management of user identities and entitlements such as creating, modifying or deleting accounts, as well as assigning and revoking individual access rights and group memberships on various integrated systems. HiIM also includes a hierarchical model of groups and roles.

Hitachi ID Bravura Identity can scale up to manage identities and groups in directories containing millions of identities and hundreds of thousands of groups. It supports all major directories including LDAP services, Azure AD and Active Directory as well as many other types of account repositories, both on-premises and cloud-hosted. It also supports real-time detection and response to changes made in Microsoft Active Directory. Additionally, password policy enforcement in Microsoft Azure Active Directory is supported, including checks against Microsoft’s global list of banned passwords or checking against own lists of compromised passwords.

Hitachi ID Bravura Identity offers more than 120 connectors for various types of systems including mainframes (e.g. RACF); midrange (e.g. iSeries); Microsoft Exchange and Office 365; SQL databases; ERP systems including Oracle JDE, PeopleSoft and, SAP ECC; hard tokens such as RSA SecurID and, SafeWord, as well as MFA apps such as Duo Security, Ping and Okta; and WAM systems including CA SiteMinder, IBM Tivoli Access Manager, and Oracle Access Manager. The list of connectors is growing continuously, with, amongst others, Jira, Kubernetes or Blue Prism having been added recently.
Hitachi ID Bravura Identity can also manage identities and entitlements on systems that support standards-based administration, using SCIM and SPML.

Every change processed by Hitachi ID Bravura Identity goes through a workflow process, which supports

validation, calculation, authorization and audit history as well as auto-approve or reject a change request, or invite individuals to make approval decisions. Workflows can also be used for manual fulfillment in cases where a connector is not available or not yet deployed. Workflow capabilities leverage process definitions, analytics, roles, SoD, and other policy constructs The Hitachi ID Bravura Identity can also crowd source identity attribute cleanup, by leveraging the access recertification workflow to not just review if someone should have an entitlement, but to also review identity attributes such as department code, phone number, charge code, etc. are accurate and to make corrections if needed. Access governance and entitlement management functions are based on user requests and approval workflows, which can be automated, where appropriate. Both the request portal an Hitachi ID Bravura Identity workflow system facilitate secure best practices such as segregation of duties, including over nested entitlements such as are found in AD groups or SAP ECC T-Codes/Profiles/Roles. Another capability are time-based entitlements that allow for granting entitlements only for a defined period, including support for periodical mass approvals and other unique features.

Analytics within Hitachi ID Bravura Identity can be used for evaluating roles and entitlements, for example, finding oversubscribed roles that are too coarse-grained, or finding unused roles that could be eliminated. Analytics can also be used for monitoring compliance using policies such as SoD or ophan accounts and remediating issues discovered - via feedback from analytics to requests. In addition, an advanced role/user cluster discovery mechanism is included, which organizations can used to suggest roles and user class definitions based on discovered data about existing users, their attributes and their already-assigned entitlements. In the recent release, enhanced capabilities for role governance have been added, to support the full lifecycle of roles including approvals of role changes, and for enabling organizations to delegate out the modeling of roles to application owners or business departments.

Hitachi ID Bravura Identity provides both end-user and administrative portals, including system dashboards, not only from computer browsers but also mobile access via smartphone apps for both Android and iOS. Mobile access is facilitated by a cloud-hosted mobile-specific proxy server which allows phones attached to public carrier networks to reach on-premises Hitachi ID Bravura Identity instances, without exposing Hitachi ID Bravura Identity to a public URL, where it might be attacked by malicious actors.

Hitachi ID Bravura Pass

Hitachi ID Bravura Pass has a number of features related to credential management and federation, in addition to the eponymous password management. For passwords, it provides synchronization between systems. When passwords expire, users can be prompted to update them on their Windows infrastructure and Active Directory. Hitachi ID Bravura Pass can then pick up the password change, verify that it meets password policies, and propagate the change to other configured systems, including other ADs, LDAP services or any other account repository, on-premises or cloud-hosted that maintains local passwords. It allows user self-service reset of passwords and PINs for operating systems, applications, and even PCs during boot-up sequence. Users can create personal password vaults to store unmanaged credentials, such as those used to sign into consumer service as an example.

Also, access to password self-service is given throughout for onsite and offsite OS login screens, pre-boot to unlock OS with an encrypted drive, as well as via smart phone (BYOD) even where the HiPM web portal

is not accessible via a public URL is supported.

The product ships with a Telephone Password Manager module that allows users to make a voice phone call to reset passwords, PINs, and to unlock an encrypted drive whose pre-boot password was forgotten. The Telephone module has limited text-to-speech and speech-to-text capabilities, and can integrate with PBX and VOIP systems. An optional module is available for biometric voice print verification of callers to this system. The self-service and telephone reset options can significantly help reduce help desk costs.

Beyond passwords, Hitachi ID Bravura Pass can manage RSA SecurID tokens, cryptographic certificates, smart cards, security question/answer profiles, biometric samples, as well as unlocking encrypted drives and OS logins. Supported operations include clear/reset PIN, enable/disable token, and challenge/response for drive unlock. Some operations, such as PIN resets on smart cards, require client-side hardware (card reader) and software (browser extension).

Hitachi ID Bravura Pass is also capable of managing enrollment to help drive user adoption and ROI. It can do this through identification of user that should enroll, inviting them periodically until enrollment is complete. Enrollment is used to collect answers to security questions, biometric samples and to link accounts as well as MFA factors to user profiles. Self-service enrollment can be used to update identity data such as asking users to provide a personal e-mail address or phone number or to review data such as their home mailing address as examples.

Hitachi ID Bravura Pass can also serve as an authentication and authorization gateway to SaaS and other SAML-capable applications, including Amazon AWS, Salesforce.com, WebEx, Google Apps, Office 365, and Concur. It includes both a SAML 2.0 Identity Provider and an application launchpad. Every product in the Hitachi ID Bravura Security Fabric includes both the ability to leverage existing MFA mechanisms as well as its own MFA smart phone app. The combination of federated access and MFA are used to harden SaaS logins. Hitachi ID Bravura Pass has many useful built-in reports, such as lists of users, utilization data, event logs, and statistical analysis by user or service.

Hitachi ID Bravura Privilege

Hitachi ID Bravura Privilege stores and secures administrative, embedded, and service account passwords. It randomizes and stores passwords in an AES encrypted vault, which can then be accessed by users or groups according to an administrator assigned policy. To ensure that even passwords with the same text don’t have the same hash, a random 128-bit salt is used prior to encryption. User and group membership can be ingested from an existing account repository, most commonly Active Directory, allowing for simplified administration. Vaulted passwords are injected into administrative tools login screens to provide users with single sign-on while minimizing password disclosure.

Hitachi ID Bravura Privilege can also require multi-factor authentication (MFA) before users can request, approve or launch access. There are 5 main methods PAM uses to allow users access to elevated privileges:

- Password disclosure: Display to the authorized user, or add the password to the user’s copy buffer.

- Direct connection: Launch the administration program on the user's PC and inject credentials into that program, so that it automatically signs into the managed account without user input.
- Proxy connection: Connect the user through a proxy server, which is running the administration program. Both VDI-based proxies (which can run any administration tool) and HTML-based proxies (which render SSH or RDP sessions only) are provided, with no restriction on the number of such proxies that an organization may deploy. Proxies eliminate software dependencies on the authorized user's device and can overcome network path limitations from the user's device to the managed endpoint.
- Privilege elevation: Elevate the access rights of the user's non-privileged account so that it can temporarily perform privileged functions on the managed system. This may be via SSH trust relationships or temporary membership in security groups.
- Run commands: Similar to Windows "Run As" or Linux "sudo", but with the option of running one set of commands across many systems at once.

Hitachi ID Bravura Privilege supports password rotation for administrative, embedded, and service accounts. To eliminate security risks due to passwords embedded in scripts and applications, PAM provides a password retrieval API. Developers can code their scripts and apps to use the Hitachi ID Bravura Privilege API, which fingerprints the calling program and runtime environment prior to providing a password to a backend service. This removes a significant risk, since malicious actors often search for high privilege accounts and passwords in scripts. To address the risks of static accounts on service accounts, Hitachi ID Bravura Privilege can automatically discover which services run in the security of which accounts and facilitates both scheduling password changes and injecting new (and random) passwords back into service infrastructure that needs these passwords to launch services, scheduled jobs and more.

At an enterprise level, Hitachi ID Bravura Privilege provides automation for onboarding of endpoints, in order to scale up deployments. It ingests systems inventory data from available sources, such as a CMDB, and applies rules to connect to and manage credentials to shared or high privilege accounts on these systems.

Elevated privilege sessions can be recorded to create strong accountability and comply with regulations in some jurisdictions (e.g., Singapore). If users attempt to disable recording, Hitachi ID Bravura Privilege can shut down the session and send alerts. Recordings use the following methods: IE/ActiveX controls; browser extensions for Chrome, Opera, or Firefox; or one-time generated executable files sent to administrators' desktops. Recording is also available in proxied login sessions (HTML or VDI proxies). The ability to audit user activity, including video capture and keylogging consistent across all these brokered login mechanisms.

In cases where IT "ticketing systems" are in place, Hitachi ID Bravura Privilege can integrate directly with "ticketing systems" such as ServiceNow or Remedy. For example, Hitachi ID Bravura Privilege can be configured to require that elevated privileges are only granted as part of an assigned trouble-ticket workflow.

To compensate for common Privileged Access Management usability problem, such as users forgetting their password, Hitachi ID Bravura Privilege provides additional features such as the ability to check out

multiple accounts simultaneously, run commands against multiple accounts on multiple systems, give single sign-on across multiple accounts to users and to connect users to login sessions directly, rather than via a jump server, which can improve performance. Moreover, users can initiate login sessions with only a web browser from any device type, including their smart phone, for RDP and SSH logins.

A newly added feature is the Web Session Manager, which allows controlling privileged access to browser-based applications such as web applications and cloud services. User access is controlled via strong authentication and optional, additional security checks such as captchas, to ensure that only the authorized user can access.

Hitachi ID Bravura Privilege has a number of pre-configured reports, including history, active, and pending requests and check-outs. The information available can be used for audits and investigations. Hitachi ID Bravura Privilege can also send event information to SIEM via the SYSLOG protocol.

Hitachi ID Bravura Group and Bravura Discover

Additionally, there are two more components. One is Hitachi ID Bravura Group, which complements Hitachi ID Bravura Identity. In addition to the usual people identity management functions, Hitachi ID Bravura Group can also manage the lifecycles of group objects, which means that it can create and delete security groups, mail distribution lists and similar objects, not just assign and revoke them.

The other component is Hitachi ID Bravura Discover, which surfaces organizational risks, by discovering key environments, compiling an inventory, highlighting risks, and suggesting mitigations. Such risks include, amongst others, password risks or risks due to misconfigurations in the Privileged Access Management space.

Integrations

The Hitachi ID Bravura Security Fabric is designed for open integration. It ships with over 200 connectors to directories, systems, and applications where it can manage user accounts, passwords, and entitlements. It also includes connectors to popular ticketing systems, SIEM applications, e-mail systems, 2FA, and smart card systems. A web services API allows third party applications, such as IVR systems or service catalogs, to submit change requests and lookup user profile or entitlement data.

Integrations with custom applications are possible using scriptable connectors. Included connectors are suitable for different classes of application technology using API bindings, SSH sessions, SQL scripts, Web services, Windows and Unix CLI programs as some examples.

Hitachi ID provides connectors for many common LDAP directories, SQL databases, mainframe security products, midrange systems, ERP applications, collaboration/e-mail platforms, 2FA tokens and smart cards, WebSSO systems, help desk / ticketing systems, HDD encryption products, and SaaS applications. Connectors are also available to popular SaaS platforms and hardware devices such as routers, switches, load balancers or server health monitoring systems. In addition, connectors to the most common hypervisors, both to broker administrative logins to the hypervisor consoles (e.g., VMWare, AWS, etc.) and to enumerate and manage access to credentials within guest VMs.

Deployment Models

The Hitachi ID Identity and Access Management Suite can be deployed locally on Windows infrastructure or hosted in the cloud on popular IaaS platforms. Hitachi ID also offers the system as a service hosted on Amazon AWS. Hitachi ID Bravura Security Fabric components run on Windows Server, IIS, and Microsoft SQL Server. It can be installed using conventional software or virtualized on popular hypervisors supporting Windows server VM. Each application server normally has its own private database instance with replication between application nodes provided out-of-the-box. This facilitates deployment in environments that need load-balanced, highly available, geographically distributed, and horizontally scaled architectures. Most Hitachi ID customers deploy from 2 to 5 replicated application servers, usually spanning at least two data centers and at least two metro areas. When delivered as a service, Hitachi ID selects AWS availability zones based on customer location and jurisdiction and deploys a minimum of three application nodes, three database instances over two or more regions.

3 Strengths and Challenges

Hitachi ID Bravura Security Fabric provides a well integrated set of IAM and PAM products covering authentication (including 2FA), credential management, privileged access management (PAM), password management and synchronization, access governance, compliance, identity lifecycle, group lifecycle and federated SSO. It includes a wide range of connectors to managed systems and applications, ticketing systems, SIEM platforms and authentication services, making integration easier.

Hitachi ID Bravura Identity not only provides the core functionality of most identity management systems but also includes some other interesting features such as group lifecycle management, SoD over nested entitlements and crowd-sourced identity data cleanup. Workflows are available to facilitate most common tasks, from access governance to entitlement management functions as examples.

One of Hitachi ID's driving principles is to help customers reduce deployment and technical support costs while providing a full IAM solution. The self-service password and entitlement request features exemplify this, as does the Telephone Password Manager module and smartphone app. By enabling users to handle resetting passwords and PINs themselves either on-site or remotely via a mobile device, not only are help desk calls decreased, but also the users can get rapidly back to being productive.

Hitachi ID Bravura Privilege is very comprehensive and mature, covering all the critical areas of PAM. Good workflow capabilities are derived from the shared codebase with Identity Manager. IT users are provided advanced features that allow them the ability to work on multiple accounts simultaneously and connect to login sessions with various mechanisms as needed. Brokered logins to privileged accounts are available from any device in any location, for the requesting user using strong authentication. Hitachi ID Bravura Privilege supports the management of different classes of privileged accounts, including administrator, embedded and service accounts and includes advanced features such as just-in-time (JIT) entitlement assignment, session monitoring, automated endpoint onboarding, access request risk scoring and client application fingerprinting.

Hitachi ID Bravura Security Fabric is geared toward solving fundamental challenges that all medium to large enterprises have in the identity and privileged access management spaces. It provides numerous connectors between identity infrastructure components and enterprise systems, including support for SaaS platforms and legacy mainframe, midrange, and older Unix platforms. It also provides an authentication portal for in-house and popular SaaS apps.

Hitachi ID

Strengths

- Well integrated IAM and PAM solution with advanced features
- Adds additional features such as group management and discovery of inventory and risks
- Can be deployed on-premise or in the cloud (IaaS or managed SaaS)
- Large number of connectors to operating systems, applications, and SaaS
- Comprehensive and mature capabilities in all core areas of PAM
- Very useful advanced features and tools included with product licenses
- Cost-reducing self-service features are built-in
- Modern UI and consistent architecture and UI across all components
- Consistent set of APIs for integration, orchestration, and customization of components

Challenges

- Still relatively low visibility in the overall IAM market, despite high maturity and broad functionality of solutions
- Does not support FIDO or OIDC authentication out of the box
- While solutions can be implemented independently, the benefit increases with opting for the full Bravura Security Fabric

4 Related Research

Executive View: Hitachi ID Privileged Access Manager - 80030
Leadership Compass: –Access Governance & Intelligence – 80098
Leadership Compass: Identity Governance & Administration – 80516
Leadership Compass: Identity Fabrics – 80514
Leadership Compass: Privileged Access Management - 80636

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.