HITACHI
Inspire the Next

Hitachi ID Bravura Discover delivers a powerful risk and threat assessment for both IAM and PAM solutions to get your organization on the right track – quickly.

DATA SHEET

Hitachi ID Bravura Discover

Reveal your risks and threats with the most accurate, fastest, and in-depth risk and threat assessment report for both identity and privileged access with the Hitachi ID Bravura Discover, a critical layer of the Hitachi ID Bravura Security Fabric.

In the age of ransomware attacks when you need to create a zero trust environment, the only one who can protect your organization is the one who controls access to your systems and networks. Hitachi ID Bravura Discover gives you proactive control of your identity and privileged access security. By building an ecosystem based on data and metrics, Hitachi ID Bravura Discover will recommend automatic fixes to close security gaps when it matters most, helping your organization:

Gain Fast and Accurate Visibility

Quickly pinpoint and correct the root cause of identity and access breaches by combining Hitachi ID Bravura Discover with an automation-first approach to identity and access management (IAM). Hitachi ID Bravura Discover reveals your identity and privileged access risks and threats with the fastest, most accurate in-depth risk and threat assessment, complete with resolution recommendations.

It's the first level of insight you need to identify IAM process vulnerabilities, so you can develop an impactful automation plan that seals security gaps. This automation-first mindset makes digital transformation real and lets your organization move faster and more effectively.

Identify Risks Below the Surface

Security is an ongoing process starting with discovering vulnerabilities, automating impacted areas, and using certification for a configuration check. A focus on discovery while implementing automation helps you detect potential attacks and enables quick protection for your identity and access solution.

Hitachi ID Bravura Discover scans your systems at-scale to discover accounts, groups, entitlements, and associated metadata beyond Windows and Linux to uncover the most critical and hidden vulnerabilities.

The Hitachi ID Bravura Security Fabric has the technological and architectural building blocks with decades of proven reliability to manage and protect your entire digital identity and access infrastructure from malicious attackers. It encompasses all of the Hitachi ID Bravura solutions including Identity, Privilege, Pass, and Group with the Hitachi ID Bravura Discover threat detection and response (TDR) layer together in a singular, powerful platform.

It identifies risks to accounts and potential configurations to your environment, including discovery of domain accounts that are members of risky groups, universal and application reports, cloud systems like ServiceNow, Salesforce, and other common and well-known platforms.

Securely Scale Your Organization

To address security threats there are typically two paths forward. Take a certification snapshot in real time or address the root cause of the problem with automation. The latter allows you to manage tens of thousands of systems efficiently and effectively to expand business operations and scale your organization.

When you take an access certification approach, it creates a lag between seeing who has access and deciding what to do about it – that could mean disaster. Move quickly to protect your organization and confidently scale provisioning in real time with automation. Use certification as a spot check mechanism to ensure automation is protecting and governing as intended.

Dive Deep Into Impact and Guided Recommendations

The Hitachi ID Bravura Discover Identity Graph presents a centralized view of your organization's attack surface to audit, compare, and benchmark your IAM maturity. The Hitachi ID Bravura Identity Graph report of your organization's consolidated risks and threats tracks all identity and access authorizations and inheritances with substantial depth and results. It highlights relationships and risks in both common and privileged scenarios – between your users, their accounts, groups, computers, and more. This in-depth report allows you to easily find non-compliant accounts, empty groups, accounts with expired passwords, accounts with broad reach and lots of relationships to groups, at-risk computers and subscribers, and additional potential vulnerabilities.

For each risk and threat uncovered, dive deeper into the Hitachi ID Bravura Discover Community to get a more comprehensive description of the threat, potential impact, and guided resolution recommendations. Through business process evaluation, you can then determine which resolutions to adopt and as you put mitigations in place, your risk model will automatically adapt.

Hitachi ID leverages decades of experience to deliver the industry's only single platform Identity, Privileged Access, and Password Management solution, resulting in rock-solid reliability, performance and scalability.

Integrate and Inspect Across the Largest Ecosystem

With Hitachi ID Bravura Security Fabric you can quickly weave the patterns of functionality your organization needs to protect against new or continual threats. As you uncover additional risks and your roadmap evolves, use the Hitachi ID Bravura Security Fabric to turn services on or off and automate them without installing and deploying other products.

Hitachi ID Bravura Discover, part of the Bravura Security Fabric, includes integration with the largest organic suite of connectors; developed, implemented, and maintained by Hitachi ID over the last two decades. Hitachi ID Bravura Discover universal reporting also performs discovery and inspection across the broadest range of applications.

Develop a More Meaningful Project Plan

Beyond discovering risk, you can get a comprehensive understanding of your organization's current state and take inventory of what you already have. Hitachi ID Bravura Discover lets you complete the first step of a well executed IAM program to accurately prioritize work to fix the problems and reduce exposure.

Once you know the risks, you can identify weak or strong areas and build a more meaningful solution design. Our partners can help you develop a strategy and project plan to drive focus on systems and process implementation that will mitigate top risks and increase return on your identity and privileged access investments.

Minimum Requirements: Intel Xeon or similar CPU. Multi-core CPU, Dual core. 16GB RAM – 32GB or more per server, 600GB HD storage in an enterprise RAID configuration, and one Gbit Ethernet NIC. Windows Server 2019 (Version 10.0.17763.1397) including updates to 09-2020. Docker version 19.03.11 or higher.

Hitachi ID