HITACHI
Inspire the Next

The First Step to Zero Trust Security

Start With Rock-Solid Identity and Access Management

DATA SHEET

In a modern age of heightened threats, a zero trust security model for your identity and privileged access program is the ultimate best practice—though it may be difficult to attain. Reduced trust, with centralized controls and policies enforced through automation, is a sustainable stepping stone you can achieve on your zero trust journey.

Achieve reduced trust with an integrated platform

A reduced trust security model that includes layers of authentication, identity, governance, and privilege, can be best achieved with a singular platform—the Hitachi ID Bravura Security Fabric. It is the only fully integrated platform and framework that enforces automated policy settings across multiple access management disciplines to achieve a reduced trust model. From your workforce to your entire tech stack and soon IoT devices, it ensures the right people have access to the right resources at the right time regardless of their location, device or network.

With the Hitachi ID Bravura Security Fabric, your organization can weave protective identity and privileged access management patterns using combinations of Hitachi ID Bravura Pass, Identity, Privilege, Group and Discover. It provides continuous, progressive and adaptive access models and policies with the speed, breadth and depth only one platform can provide. From adaptive authentication with granular authorization, to automated lifecycle administration, and excellent audit mechanisms for your entire workforce and tech stack ecosystem, the Hitachi ID Bravura Security Fabric has your reduced trust model covered.

As new threats or your roadmap evolves, our singular platform allows you to turn services on or off without installing other products that improve IT security, support internal controls or regulatory compliance, and lower access administration and costs. More than holistic protection for your data, reduced trust also delivers greater enterprise risk visibility, the highest possible level of security assurance, and support for hybrid IT including multicloud IT infrastructure.

Target identity as the control surface for your environment

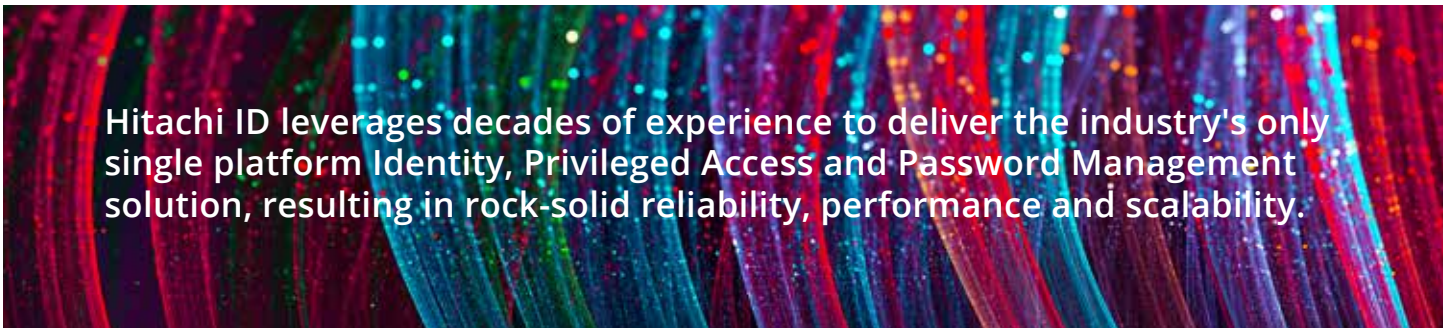
A foundational component of your reduced trust model is the configuration of policies that govern credentials to enforce adaptive authentication and protect against credential-focused cyber attacks. Your organization should strive to include all applications within the scope of its zero trust model. However like many organizations, there may be hundreds or thousands of applications and services that lie in use outside of your existing identity and privileged access program. Optimally, each application should have its own security and access strategy for password management, federated authentication, randomizing administrative accounts, or Just in Time (JIT) access.

The Hitachi ID Bravura Security Fabric offers four types of zero trust authentication to authenticate identities through local applications, cloud or on-premises directories, and federated approaches that give application administrators a choice about what option best meets compliance for their specific applications. Hitachi ID Bravura Pass, a credential & authentication management solution for hybrid IT solutions, synchronizes and periodically changes credentials to enhance password security. Hitachi ID Bravura Pass enables federated single sign-on that makes logins more convenient, secure and enforces a strong password policy. On the path to zero trust, the most secure approach is to enable a federated authentication solution using SAML which Hitachi ID Bravura Identity offers. Hitachi ID Bravura Identity provides robust lifecycle control and management, including onboarding and offboarding, for identities with automation through rules, policies, workflows, and APIs for full customization. Requiring additional verification, such as multi-factor authentication (MFA), helps add yet another protection against internal and external threats.

Take stock of all the identities that challenge your trust

With an ever expanding ecosystem of identities vying for your trust, your organization needs to take stock of all of the assets you need to manage in your

© 2021 Hitachi ID Systems, Inc. All rights reserved.
All other marks, symbols and trademarks are the property of their respective owners.



identity and privileged access operations. Your reduced trust model can only be cohesive and complete when you have an exhaustive understanding of your entire environment. Many organizations manually audit, inventory and report access leaving the potential for human error or worse, interference.

The Hitachi ID Bravura Security Fabric and Hitachi ID Bravura Identity auto-detection provides near instant visibility of all accounts, groups, group memberships and more from every system integrated into the platform. It auto-detects and produces an inventory of all identities that need to be brought into governance. Hitachi ID Bravura Identity also includes an incremental list of any identities that are new, added, changed, or have moved since the last auto-detection. Through simple automated collection of entitlement information, you significantly reduce the trust that would otherwise underpin your entitlement ecosystem.

Minimize always-on access and privilege to reduce risk

Eliminate always-on access and privileges as part of your reduced trust model. Remove unnecessary or unused accounts and permissions and rely on Hitachi ID Bravura Identity and Hitachi ID Bravura Privilege to enable policy-driven processes that minimize standing access and privileges. Enabling zero standing privileges provides audited and brokered access to your data at the time and within the scope needed to complete the work at hand. Though you can trust users have the accounts they need, adding automated policies helps reduce trust chains and overall risk. Adding certification to the process is a regular safety maintenance best practice with managers periodically verifying rights and access for the task at hand.

Hitachi ID Bravura Privilege enables policy-driven processes that manage JIT access for users who need additional temporary or shared account access. It activates just enough privileges to perform only the desired task and promptly revokes those privileges once the activity is complete, reducing the attack surface to the window during which the privileged access is active.

Beyond auto-detecting all identities and changes, the Hitachi ID Bravura Security Fabric detects newly elevated privileges and changes made out of band to enable proactive governance and mitigate risk. The Hitachi ID Bravura Security Fabric auto-detect process is massively multi-threaded, able to list, classify and probe over 10,000 systems per hour and is typically scheduled to run every 24 hours to manage and minimize your attack surface.

Govern security exceptions with automated policies

Organizations would prefer perfect security policies that drum up complete adherence. In reality, security has a dynamic formula to mitigate risk that may often include exceptions. In a, 'trust but verify first' culture, security exceptions become the rule. Automated policies minimize exceptions so only the true outliers need additional management. Tracking exceptions enables you to track how your organization's overall risk is trending and use that insight to fine tune security policies that are out of step with systems or processes.

Monitor and mitigate your attack surface

To further reduce exposure to your systems and data, the threat detection and response component of the HItachi ID Bravura Security Fabric—Hitachi ID Bravura Discover presents a birds-eye view of your organization's current attack surface so you can begin developing a more meaningful solution design. Beyond Active Directory, Windows, Mac, Linux, and Public Cloud Service, Hitachi ID Bravura Discover extends discovery to include your organization's HR and ERP systems and reporting databases. Hitachi ID Bravura Discover scans all of your systems at-scale to discover accounts, groups, entitlements, and metadata to help you prioritize work to fix the problems. We can help drive focus on implementations that will mitigate risks and increase return on your identity and privileged access journey to zero trust that begins and ends with rock-solid identity and privileged access management at every level.

© 2021 Hitachi ID Systems, Inc. All rights reserved.
All other marks, symbols and trademarks are the property of their respective owners.