Hitachi Solutions

Zero Trust Security

User Access Security Offer

Security for Today. Powered by Microsoft. Based on Zero Trust.

Today's cloud environment can be a hostile place. It's time to assume that everyone, inside or outside the network, could be a threat to your business-critical applications and data. With the stakes so high, you can't rely on a standard network perimeter to assess trust anymore.

The answer? Zero trust. In a zero trust security model, people are the new perimeter, and identity is the core of maintaining a secure environment. In fact, Gartner has forecast that as many as 60 percent of VPNs in place today will be replaced by a form of zero trust technology by 2023.

Hitachi Solutions can design and implement a zero trust framework that establishes a dynamic and digital identity-based perimeter that ensures you can manage risk, improve compliance, and proactively detect and prevent threats. Our scalable, innovative zero trust user access security implementation offer gives you the confidence you need in an end-to-end security platform. We'll guide and advise and do the heavy lifting, so you can remain focused on building your business.

The Principles of Zero Trust

Just because it's behind a corporate firewall doesn't mean it's safe. You need zero trust to:

- **Verify explicitly.** Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.
- **Use least privileged access.** Limit user access with just in time and just enough access (JIT/JEA) to protect data and productivity.
- **Assume breach.** Minimize blast radius for breaches and employ a security strategy to prevent lateral movement.

Reimagining Security with Zero Trust

Hitachi Solutions' phased zero trust user access security implementation centers on strong user identity, device health verification, validation of application health, and secure, least-privilege access to corporate resources and services.

Our security experts work with you to understand your current security environment, baseline your potential needs, and build a zero trust roadmap based on:

Identity
Make it harder for attackers to acquire and use stolen credentials, using Azure Active Directory and conditional access tools to help secure your users, service accounts and devices.

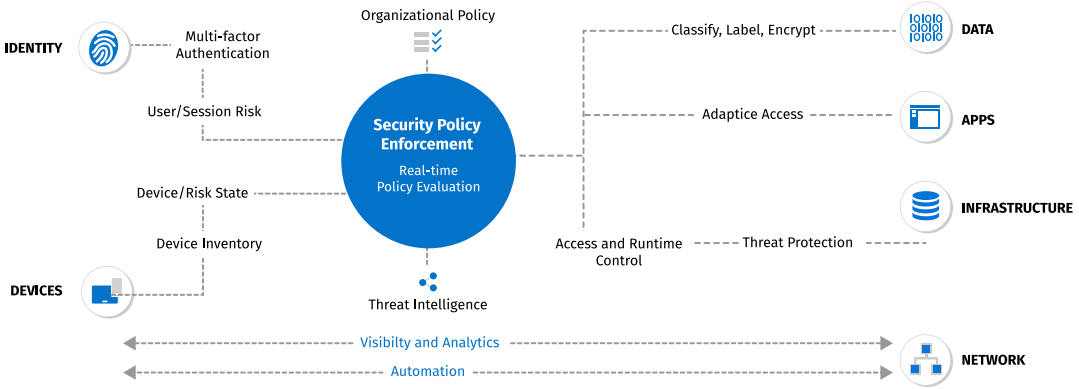
Endpoints
Ensure your support staff is more efficient by providing visibility into devices accessing the network and ensuring compliance before granting access. We'll guarantee all devices, and their installed apps meet security and compliance requirements.

Data
Protect your data at rest to maintain confidentiality, integrity, and availability across all workloads, using Defender for Cloud tools to automatically classify data in Azure SQL and implement controls.

Applications
Configure policy management for controlled access to all cloud apps and resources. You'll get A quick and easy access to compliance data for every application that gets accessed from your environment.

Network
Reduce your total cost of ownership related to security infrastructure by reducing the burden on IT to manage networks and upgrades. We'll work with you to move beyond traditional network security with micro-segmentation, real-time threat detection, and end-to-end encryption.

Infrastructure
End the struggle to assess, prevent, enforce, and govern privileged access and permissions across your hybrid and multi-cloud environments. We'll help you right-size permissions and consistently enforce least-privilege principles to reduce risk using continuous analytics to help prevent security breaches and ensure compliance.



Zero trust: extending throughout the entire digital estate and serving as an integrated security philosophy and end-to-end strategy

The Business Value of Zero Trust

User access security allows you to explicitly verify users, devices, and data retrieval with centralized detection and response. Other benefits of engaging Hitachi Solutions to help you establish a zero trust architecture include:

- Provides secure employee network access to support work from anywhere without draining IT resources and budgets
- Realizes cost savings through the simplification of the security stack
- Strengthens defenses to detect and respond to threats in real time
- Reduces third-part licensing costs for security tooling

We Can Help

Hitachi Solutions has decades of experience supporting clients in many industries with migration and implementation of Azure Cloud security solutions. Our skilled team of security experts have attained advanced certifications from Microsoft as part of the Azure Migration and Modernization Program (AMMP) in both hybrid cloud security and threat protection. Couple that with our many Azure-based advanced certifications, and we are uniquely prepared to help you develop and implement a security solution that supports and extends your business transformation goals. Let's get started.

Powered by Microsoft

A complete zero trust security solution is powered by state-of-the-art Microsoft security technologies and includes the deployment of:

- Microsoft Endpoint Manager
- RBAC, Azure AD Conditional Access
- Intune MDM/MAM
- Cloud App Security, Data Classification, Labeling
- Network Segmentation and Protection Design
- SIEM/SOAR Enablement
- Azure Policy Assignment

An expert-led journey through Azure-based zero-trust security concepts and implementation

Talk to us about Zero Trust security today!

Email Us NA.Marketing@hitachisolutions.com

Call Us 888.599.4332

Connect with Hitachi Solutions to learn more about our team and our story!

Follow Us