

MARVELL

Marvell Implements SecureAuth IdP and Streamlines its Remote Access Workforce

Marvell's technological prowess is fueling the digital age. It is renowned as a global leader in semiconductors and ships more than one billion chips a year. Its components are in more than 200 million smartphones as well as leading tablets, TVs, stereos, and other digital entertainment systems. Despite the innovation transforming our digital world, Marvell was using legacy RSA tokens to grant remote access for 3,500 employees who access its Juniper virtual private network (VPN).

Business Challenges

When Todd Holloway, senior manager of Information Security at Marvell, joined the company, updating the access management policy was his first priority.

"We had a team of IT personnel whose main function was being the help desk for employees," stated Holloway. "The amount of global resources spent on reconfiguring and monitoring tokens was unnerving. The IT team was often busy shipping new tokens to replace lost or damaged tokens."

Transition from a hard token to a more cost-effective alternative was needed. Software solutions were eliminated since installation on each employee's laptop would be a logistics nightmare. Holloway sought a solution that would not require any hardware or software installation and could simply authenticate identities and grant access from a secure browser. Most important, the access control solution would need to be minimally intrusive and be cost effective to implement across the company's entire workforce of 7,200 employees.

"We had a team of IT personnel whose main function was being the help desk for employees. The amount of global resources spent on reconfiguring and monitoring tokens was unnerving. The IT team was often busy shipping new tokens to replace lost or damaged tokens."

— **Todd Holloway, Senior Manager of Information Security, Marvell**



Overview

Industry

- + High Tech

Environment

- + Over 7,000 employees worldwide access Juniper VPN using two-factor authentication via hard token and leveraging Active Directory identity data

Challenges

- + Reducing administrative overhead
- + Self-service browser based solution

Solution

- + SecureAuth IdP
 - Multi-factor authentication
 - Single Sign-On

Benefits

- + Combined single sign-on and multi-factor authentication in one product
- + Self-service and easy to use two-factor authentication
- + 50% reduction in cost
- + Quick and easy deployment

The Solution

Marvell chose SecureAuth IdP for its ability to provide secure access to their Juniper VPN using multi-factor authentication and single-sign-on (SSO). SecureAuth IdP is the only token-less platform that is easily configured to mutually authenticate both the user and server.

Rapid implementation across the entire Marvell workforce was remarkably easy because SecureAuth IdP used the credentials already stored in Marvell's on-premise directory. This gave Marvell immediate use of the identity governance standards and profiles residing in Active Directory to secure access to their Juniper VPN.

SecureAuth IdP's architecture configured seamlessly with Marvell's SAML (Security Assertion Markup Language) application server. SAML is regarded as the open-source identity standard and has become the de facto identity management standard.

Integration and transition for Marvell employees was easy. Employees seeking remote access simply log on, and enter a one-time password, and their credentials are authenticated.

"Usually when IT implements an organizational-wide change, you hear grumbling, but employees were glad to finally be rid of their tokens and were pleasantly surprised how easy the SecureAuth IdP solution authenticated and granted access to the Marvell VPN. I'm confident with the high level of security, control, and scalability with SecureAuth IdP. I am also pleased with the best-in-class service and support we've received from the SecureAuth team."

— **Todd Holloway, Senior Manager of Information Security, Marvell**

In less than four months, Marvell deployed a browser-based identity access management solution that offered two-factor authentication and SSO for all 7,200 employees — at a 50 percent cost savings over RSA tokens. With the amount of research and development, and planning and implementation that Marvell invests with next-generation consumer electronic devices, their identity governance and access management policies now leverage leading-edge access control technology with SecureAuth.