Bravura Security

Global Semiconductor Manufacturer Secures Thousands Of Sensitive Passwords

CASE STUDY

Challenge: The manual administrator password change process created productivity and risk problems.

Solution: The company selected Bravura Security Privileged as the only solution able to manage thousands of passwords while ensuring both security and fault tolerance.

Outcome: Automating passwords reduced costs and increased security through cryptographic measures and replication across data centers.

INDUSTRY
Manufacturing

REGION
North America

PRODUCT
Bravura Security Privileged

This Bravura Security customer is one of the largest semiconductor design and manufacturing companies in the world. The global corporation had revenues of over $30 billion US more than fifteen years ago, employing 100,000 people, and was ranked among the world's 100 most powerful brands by Millward Brown Optimor. A Global Semiconductor Manufacturer driven to create bold advancements in technology that lead to positive change and a better, more interesting world.

Due to this customer's policies, Bravura Security is unable to disclose the customer's name.

The Challenge

Securing intellectual property and keeping plans confidential is crucial to success in the semiconductor industry. Chip design and fabrication companies must protect their own data, adhere to contractual obligations to protect customer and partner data and must comply with legislative requirements regarding corporate governance and privacy protection.

Bravura Security's customer, a global semiconductor company, needed a more effective way to secure and manage data distributed over thousands of servers.

The customer knew that effective management of local administrator passwords is critical to securing data. This required that local administrator passwords be changed regularly and immediately changed whenever an IT worker with elevated privileges left the company. The existing, manual process to change administrator passwords posed both productivity and risk problems, taking up to three days to respond to staff terminations.

To address these challenges, the company required a reliable, secure, scalable and efficient solution that could randomize passwords across thousands of servers on a regular basis. It needed to streamline the process for responding to IT worker departure. It also needed to authenticate, authorize and audit access to sensitive passwords and operate across firewalls and to manage isolated servers.

The Solution

Following an evaluation of available products, the company selected Bravura Security Privileged as the only solution able to manage thousands of sensitive passwords while ensuring both security and fault tolerance.

Bravura Security Privileged secured thousands of company servers by randomizing local administrator passwords daily. Proxy servers were installed on over 50 network segments, allowing Bravura Security Privileged to cross over firewalls. Bravura Security Privileged was integrated with thousands of Windows, Microsoft SQL Server, Oracle and Linux servers.

Bravura Security at a Glance

Bravura Security is the only industry leader delivering identity and privileged access management across a single platform to ease implementation as your IAM and PAM roadmaps evolve.

The Solution

The enterprise-class solution for securing local administrators, service accounts and application passwords randomized each password daily and required IT staff to acquire the passwords they need using a secure web application. Its core capabilities, including over 70 connectors, enabled it to randomize passwords on most common systems and applications with built-in replication of data and configuration between servers. This allowed the organization to ensure high availability, even when individual servers or whole data centers go offline. A proxy server, enabled it to connect to target systems isolated by firewalls. The client software enabled secure passwords on thousands of workstations.

IT staff signed into Bravura Security Privileged with pre-existing credentials, such as a Windows password or an RSA SecurID token. Bravura Security Privileged notified programs such as the Windows Service Control Manager of new passwords. Applications used an Bravura Security Privileged SOAP API to retrieve passwords they needed to connect to databases or directories.

The Outcome

Coordinating high volume password changes without impacting the availability of applications can be difficult. Mission-critical passwords must be secure, even when the network is under attack and unavailable, even when hardware crashes or data centers suffer disasters. Password storage must be hardened and ultra-reliable.

Using Bravura Security Privileged, this customer secured thousands of sensitive passwords. Bravura Security Privileged produced cost savings for the customer by reducing the human effort required to change passwords, both regularly and after the departure of IT staff.

At the same time, the customer was able to avoid disruptive and costly manual password change processes. Automation and password storage became increasingly secure through cryptographic measures and replication across data centers.