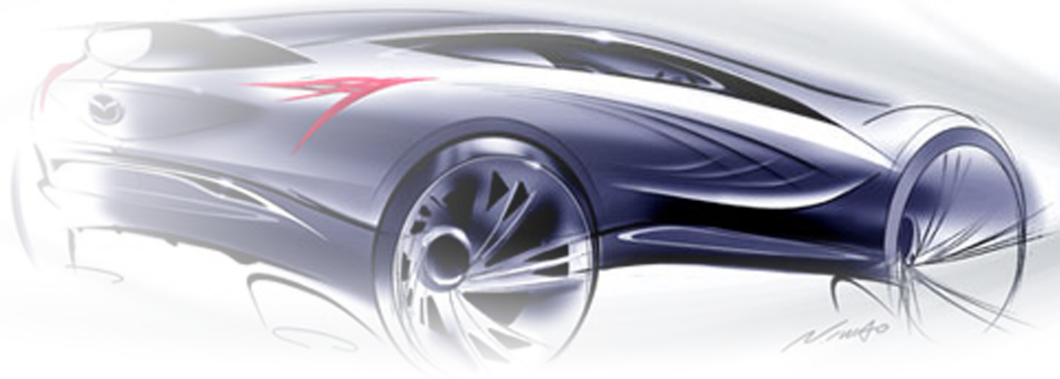




MAZDA



Wave Systems' EMBASSY® software and Seagate self-encrypting hard drives help Mazda North American Operations achieve Japan's Sarbanes Oxley (J-SOX) compliance.

Mazda North American Operations

Industry
Automotive

Benefits Summary

- Protects mobile data in minutes
- “Built in” encryption minimizes setup and support costs
- Centralized management of computer security policies
- Proof of compliance with data protection regulations for J-SOX and Japan's Personal Information Protection Act (JPIPA)

Forty years ago, Mazda first challenged the Big Three American automakers on their own shore, when its R100 coupe arrived in style as the first rotary-powered car ever to spin four wheels on American pavement. Since then, the Japanese automaker has demanded further attention and respect by introducing legendary vehicles like the RX-7 and the MX-5 Miata.

That level of achievement is no accident. In a market driven by uncompromisingly high expectations, Mazda's brand has survived and thrived because it practices a commitment to excellence and customer satisfaction at every level of its global organization... including data security.

THE CHALLENGE:

Protect customer personal identifiable information and confidential business information on employee laptops scattered across North America without overburdening in-house IT resources.

With responsibility for all research and development, sales and marketing, parts and customer service operations on the North American continent, Mazda North American Operations (MNAO) represents the company's largest division outside Japan. Based in Irvine, California, the business sells or leases Mazda cars, trucks, minivans and SUVs through some 900 dealerships scattered throughout the US, Canada and Mexico.

With that much ground to cover, MNAO relies on 200 highly mobile field staff who, in turn, rely heavily on their laptop computers. Additional laptops frequently traveled and went home with Irvine-based employees, who worked in MNAO's corporate legal, finance and personnel departments.

“The likelihood that one of these laptops could eventually become lost or stolen is very high,” said Kai Sookwongse, Department Manager for MNAO's Infrastructure Services. “And the cost of the laptop is very small compared with the data stored on it.”

Such data might include personal information about employees and customers, future product plans, pricing and cost information or information concerning legal matters. Initial attempts to protect the data on MNAO's laptops relied on software-based full-disk encryption. The logistics of flying field reps to Irvine to install software on their laptops, however, was problematic to say the least.

A software rollout just for MNAO's 200 field reps would impose three days of downtime for each of them, Sookwongse explained. It generally required a two-day roundtrip for reps to either send or bring the laptop to MNAO's IT department in Irvine, and a third to prepare and encrypt the hard drive. That could translate into as many as 600 days of lost productivity just for the field staff alone. Installing FDE software would also require dedicated IT staff time ranging between four and six hours per laptop, which translates into an additional per laptop cost of \$200 to \$350.

Consequently, MNAO was only able to rollout software-based FDE to a limited number of users operating out of the Irvine office, where Sookwongse and his team are based.

Half measures, however, don't align well with Mazda's corporate vision. Recognizing the risk to its customers, employees and brand, Mazda's HQ in Japan issued a global security policy that required full-disk encryption (FDE) on all laptops storing confidential data.



Simplifying Encryption and Authentication

Case Study

Further motivation came from the Japanese government, in the form of J-SOX, a framework for internal controls on financial reporting by public companies and Japan's personal privacy laws.

J-SOX is very similar to the Sarbanes Oxley legislation passed in the US, in that it requires regulated companies to perform risk assessments, implement appropriate risk mitigation and establish incident response measures. In practical terms, these collective events meant MNAO needed to apply FDE to all company laptops, beginning with the 600 machines in active use. That, however, introduced a new problem for Sookwongse.

"My team didn't have the resources to convert everyone in a software-based FDE deployment," he said. "It would have been cost prohibitive to go out and do this."

THE SOLUTION:

Seagate Momentus FDE.2 self-encrypting hard drives managed with Wave System's EMBASSY Trusted Drive Manager and EMBASSY Remote Administration Server (ERAS).

Through MNAO'S partnership with Dell Inc, Sookwongse and his staff traveled every year to a Dell Briefing Center in Austin, Texas. It was there he learned about the computer-maker's work with Seagate — a pioneer of self-encrypting drives — and Wave Systems, a leading provider of encryption management software to offer customers turnkey solutions for data security.

The packaged solution appealed to Sookwongse, for several reasons. The most immediate was that MNAO received new laptops with Seagate drives and Wave software built right in, which eliminated IT's need to install and encrypt every machine's hard drive.

Also, important was the fact that Seagate's hard drive technology simply imparted a higher degree of security than software-based solutions. Wave's Trusted Drive Manager, a client application that activates the on-board security features of Seagate's encrypting drives, provides authentication that is stronger than Windows® and enables a secure erase feature that allows for the safe retirement or disposal of machines and drives. The technology immediately enforces policy-based access controls when the PC is powered on.

Plus, Wave's EMBASSY Remote Administration software (ERAS) provided Sookwongse with centralized administration of users, credentials and access rights, and helped MNAO establish policy-based access controls and proof of compliance under J-SOX.

Wave's technology also supports single sign-on to Windows, providing a friendly and familiar user experience. Integration with Windows password update allows the drive access policies to be automatically updated with Windows, ensuring compliance to company password policies.

THE BENEFITS:

Minimized time and expense to secure sensitive and confidential data on laptop computers. Plus, centralized management ensures policy-based access controls and proof of compliance.

The built-in security of Seagate's hard drives delivered a tremendous advantage in terms of time. Each laptop's initial set up on the Wave server (ERAS) took 15 minutes, said Sookwongse. That's a fraction of the four to six hours required to install software-based FDE solutions. Plus, since MNAO leases laptops from Dell on a two-year cycle, the business can order pre-installed, hardware-based FDE on new machines.

"When J-SOX emerged, we realized that installing encryption software would be a prohibitively expensive task," said Sookwongse. "A major part of our decision to go with this solution is that Dell simply replaces current laptops with new machines in which the drive is already encrypted."

Whether pre-installed or not, Dell's bundled solution significantly reduced the time and costs MNAO dedicated to encrypting laptops — not only for the first installation, but on subsequent occasions as well when machines required maintenance or repair. "When users had issues with their systems, we would typically repair it and then re-encrypt the drive again," Sookwongse explained.

Wave's ERAS technology further provided Sookwongse with remote management of MNAO hard drives scattered across North America. ERAS enables centralized administration of users, credentials and access rights. Through its native integration with existing directory structures and policy-distribution mechanisms, assigning users and policies can be performed within the directory framework, which dramatically simplified MNAO's deployment.

Wave's support of Windows® single sign-on and password synchronization was something that benefited both IT staff and end-users alike. This feature means end users need remember only one password to secure both the contents of a laptop's hard drive and its active Windows profile, which simplifies the task of securing their laptops.

"While we had the software FDE solution, there was no remote administration support for users who had forgotten their password," said Sookwongse. "This feature saved our help desk a lot of hassles."

Finally, and most importantly, hardware-based FDE enabled by Seagate and powered by Wave protects *all of the data* stored on MNAO's laptops. The decryption key is protected by hardware, making it impervious to software attacks, such as malware and rootkits. Wave's software securely stores user access control policies in a protected area of the hard drive, ensuring only authorized users have access to protected data.

In addition, Wave's ERAS software creates secure audit logs including specific drive security profiles to further aid compliance both with the firm's internal policies and Japanese frameworks, like J-SOX.