



Background

Founded in 1975, American Systems is one of the largest employee-owned companies in the United States with 1500 employees, 21 office locations, and 125 field sites. Based in the Washington, D.C., suburb of Chantilly, Virginia, the company provides systems engineering, technical, and managed services to government and private sector customers.

Challenges

In addition to adding strong data security, American Systems wanted:

- Transparent encryption operations to prevent end users from selectively implementing security.
- Robust key management for centralized, company-controlled access to encryption keys.
- Reliable data recovery to fully recover encrypted data as device usage and personnel changed.
- Easy integration with existing IT infrastructure to leverage existing IT investments.
- Minimal impact to end users and IT process to ensure ongoing operational productivity.

Solution

American Systems is using CREDANT Mobile Guardian (CMG) encryption software on 600 laptops, BlackBerrys, and desktops to protect data residing on endpoint devices and on the internal network.

Results

CMG's strong yet flexible data security enabled American Systems to:

- ✓ Silently and automatically encrypt data to reduce risk and heighten customer confidence
- ✓ Centrally store encryption keys in a secure database rather than in a file share or end user device
- ✓ Fully recover encrypted data upon contractor/employee departure, hardware failure, or human error
- ✓ Seamlessly integrate with RSA SecurID and Active Directory
- ✓ Add data security with little to no impact to end user or IT productivity

“CREDANT has been excellent in fulfilling our enterprise security requirements and does not hinder end users’ ability to perform daily functions. CREDANT is a big part of our company’s security initiative and an excellent vendor with top-of-the-line customer support.”

Wesley Ward
Information Security Manager
American Systems



Business Problem

American Systems does a lot of work with the federal government and has access to secret data, plans, and documentation. The company has many contract and mobile workers, so IT is faced with multiple, daily personnel changes and a high, constant risk of mobile device theft / loss. The company wanted to encrypt data contained on mobile devices and on the internal network to minimize risk and gain competitive advantage. The company also wanted to become SOX and HIPAA compliant (even though regulatory compliance was not legally required) to better emulate their customers' environments.

Why CREDANT?

American Systems selected CREDANT because CREDANT Mobile Guardian (CMG) provided:

- **Strong, transparent data protection** that automatically and consistently enforced security policy.
- **A secure, centralized, database to store encryption keys** which ensured the company not the end user controlled encryption keys and that the keys were not kept on a file share or an end user's PC.
- **100% data recoverability** to provide operational continuity and accommodate daily personnel change.
- **Seamless integration with RSA SecurID and Active Directory** which avoided extra passwords, unnecessary expense, and end user training on modified pre-boot authentication processes.
- **Nominal impact to end users and IT processes** because applications did not have to be decrypted to access data files or perform routine diagnostic activities (FDE products incurred extra overhead and latency from encrypting/decryption application files).

Benefits

CREDANT is very important to the overall security strategy of American Systems. By adding strong data protection, CMG has enabled the company to become SOX and HIPAA compliant while creating competitive advantage (CMG enabled the company to win business they might not have won, improve existing customer relationships, and avoid potential customer loss). If given the choice, American Systems would choose CREDANT again and recommend them to another company.

Strong Data Protection

Immediately after deployment, two of the company's field techs had their car broken into and their laptops stolen. Since the data was protected with CMG, the data was useless to the thieves. CMG prevented the thieves from using any kind of password crack utility to get access to the SAN database or registry to retrieve log in credentials or to crack those credentials and spoof the network. In addition, CMG's easy to use web console and reporting capabilities enabled American Systems to prove that the data was protected. IT simply looked up the machine's ID (or the DCID), verified that CMG was installed on it, and identified authorized users for the device.

Reliable Data Recovery, Effortless Maintenance, & Responsive Customer Support

Due to the way CMG manages encryption keys, American Systems has always been able to recover encrypted data – even after an employee or contractor has left the company. The solution is easy to maintain because it is highly automated and requires little to no end user training or IT management time. In addition, CREDANT's technical support has been very effective, knowledgeable, and eager to help – even if the AS team had an issue due to something being overlooked by one of the staff members.

Painless Integration with Minimal Impact to End Users & IT Processes

CMG was seamlessly integrated with existing tools such as RSA SecurID authentication and Active Directory. As a result, American Systems did not have to modify end user log in processes or IT diagnostic and repair procedures. End users log in with existing Active Directory credentials, have immediate access to their data, and work as usual. End users do not know data is being encrypted and do not see CMG running in the system tray. There have been no user complaints, no PC performance issues, and no problems accessing encrypted data or opening PST files.