



## Background

This large bank manages assets of \$16.8 billion and has been meeting the financial services needs of individuals and businesses in the Midwest, primarily in Missouri, Kansas, Illinois, Oklahoma and Colorado, for over 140 years. The bank has 5,200 employees, 360 locations, and an IT department consisting of 380 employees that support MVS, UNIX, and Windows operating systems across a mainframe, 500 servers, 30 LPARs, and 6,500 endpoints.

**“One of the things that I love about CREDANT—besides the fact that we love the product—is their unique customer service level.”**

## Challenges

The bank wanted to:

- Prevent losing sensitive data contained on desktops, laptops, PDAs, and USB drives
- Minimize the impact on end users
- Streamline ongoing administration by using a single management console with a consolidated view across platforms and device types
- Ensure full recovery of encrypted data
- Stay ahead of the regulatory curve and have adequate time to evaluate solutions before being forced to make a quick decision

**IT Manager**  
A large Midwest bank

## Solution

The bank is using CREDANT Mobile Guardian (CMG) software for endpoint data protection.

## Results

CREDANT enabled the bank to:

- ✓ Safeguard data with little to no increase in administrative burden
- ✓ Maximize operational productivity for routine tasks such as trouble shooting devices and recovering data
- ✓ Fully recover encrypted data upon operating system (OS) corruption, device failure, and human error
- ✓ Eliminate the impact to end users by avoiding the pre-boot login authentication process required by full disk encryption products
- ✓ Support all required platforms and device types using one solution with a single management console and consolidated enterprise-wide view
- ✓ Phase deployment to augment internal learning and user acceptance



## Business Problem

Each year the bank had four or five laptops that “walked” (were stolen or lost). The potential to lose sensitive data on laptops, desktops, PDAs, and USB drives drove IT to further secure its environment—before it was a regulatory requirement. The bank wanted data encryption because it was the only satisfactory means of satisfying the question, *what if we lose a laptop*.

In addition to strong data security, the bank’s requirements included:

- **Single, central console to view & manage security across endpoint platforms:** The bank’s IT department already had many applications to administrate. Adding multiple, platform-specific consoles to manage one application was not acceptable due to the increase in complexity and administrative burden.
- **Minimal Impact to End Users:** The bank wanted to avoid adding complicated, non-industry-standard processes that might frustrate end users and increase help desk calls.
- **Fast, Reliable Data Recovery:** The bank needed the ability to recover encrypted data—with minimal impact to IT & end user productivity.
- **Easy Administration & Strong Customer Support:** The bank wanted to minimize the amount of management and technician time needed to support the application after the initial rollout and set up.

## Why CREDANT?

The bank initially focused on the full disk encryption (FDE) vendors, but quickly migrated towards CREDANT’s more data-centric, policy-based encryption technology. Why? The bank found CREDANT’s approach to be different in every way—from a “listening-based” sales process to a unique way of solving the problem to the quality of the product to the ongoing customer support. From a business justification perspective, the bank selected CREDANT Mobile Guardian because the product provided:

- **A single, cross-platform management console** which significantly reduced ongoing administrative burden. (The FDE solutions required multiple consoles for multiple device platforms)
- **Fast, easy data recovery** to ensure smooth day-to-day operations. (The FDE solutions did not have the ability to recover encrypted data in the event a device’s OS became corrupted.)
- **Phased deployment** for a more gradual and controlled implementation. (The FDE solutions did not support phased deployment, only an “all or nothing” approach.)
- **Breadth of platform support.** (The FDE solutions did not support PDA or USB platforms.)

## Benefits

CREDANT’s product quality, customer support, and vision combined with the company’s ability to address client needs and adapt to technology change were the keys reasons why the bank initially chose and remains committed to the CREDANT solution.

## Competitive Advantage: Stayed Ahead of the Regulatory Curve

While regulatory compliance is a significant business driver in the financial services industry, the bank made the decision to implement additional IT security to prevent the loss of sensitive data prior to regulatory mandates. This enabled the bank to gain competitive advantage because IT was not restricted by tight time constraints and was never in a position where a decision had to be made because of looming deadlines.

## Phased Deployment Maximized Control

Rather than being forced to implement everything all at once, a phased rollout enabled the bank’s IT staff to learn as they went, adjust as needed, anticipate and answer frequently asked questions, and proactively communicate across the enterprise to educate and set expectations. The phased deployment gave IT complete yet flexible control over the entire implementation process—minimizing the impact to end users and all but eliminating incremental calls to the help desk.

## Fast, Reliable Data Recovery—Every Time!

With CREDANT, the bank has always been able to recover data when devices or processes have failed—typically in 20 minutes or less. Even when the bank accidentally lost encryption keys by failing to follow its own policy, CREDANT was able to help the bank fully recover its data.

## Proactive Customer Support

The bank found CREDANT Technologies’ first line of customer support extremely knowledgeable, able to answer hard questions, and solve technical problems at a much quicker rate than the bank had experienced with other IT vendors. At no time throughout the evaluation, implementation or ongoing production phases of the project did the bank have to call CREDANT to escalate an issue. CREDANT proactively escalated issues and provided status updates rather than requiring the bank to initiate or make these types of requests.

## Minimal Impact to End Users

By not using a full disk encryption solution, the bank was able to avoid pre-boot login authentication, which was a non-standard process and a massive change for the end user community. CREDANT’s industry standard user authentication process was non-invasive and easy for end users to understand.

## Easy Ongoing Administrative Management

The bank found CREDANT Mobile Guardian extremely easy to implement and support. The team was able to quickly move on to other projects while having somebody to support the CREDANT application on a day-to-day basis—without requiring a lot of management time.