

## CREDANT Solutions for PCI DSS Compliance

The success of most businesses today depends on safeguarding cardholder data.



### CREDANT SOLUTION

*CREDANT Mobile Guardian (CMG) ensures that PCI DSS encryption and security requirements are consistently and efficiently enforced – regardless of where the cardholder data resides.*

#### Only CMG enables organizations to:

- › Encrypt and secure cardholder data across multiple, diverse platforms from a single console.
- › Create automatic audit trails that offer proof of end-to-end data security.
- › Provide a transparent end-user interface that supports user productivity while keeping data safe.

*CMG's Intelligent Encryption provides centrally-managed, highly scalable and architecturally flexible security to manage all data endpoints. With CRE DANT, organizations can:*

- › Protect cardholder data from leaving the organization unprotected on USB flash drives or other forms of removable media.
- › Provide confidentiality, privacy and auditing of data residing on any endpoint.
- › Protect sensitive data from unwarranted access, thus reducing risk of internal breaches.

### Regulatory overview

PCI DSS is a global security program created to reduce risks to PCI members, merchants, service providers and consumers. The standard is based on 12 data-centric requirements that combine the use of data encryption and end-user access control with activity monitoring and logging. For compliance, support is mandated for all 12 requirements.

### The compliance challenge

Over one billion people worldwide use payment cards to support commercial transactions in almost every business around the world. [Source: PCI Security Standards Council] The use of these cards has created enormous opportunities for businesses. However, the value of the information associated with these payment cards — commonly referred to as “cardholder data” — has also prompted a growing number of attacks on this data.

Attacks include hacking by outsiders, the physical theft of storage media and illegal activities by company employees. The growing number of remote users — often with laptops, handhelds, smartphones, USB drives and CD-DVDs— has compounded the risk of these security breaches. A single employee can walk out of an office with literally millions of credit card numbers stored on a memory device.

For compliance, PCI DSS states that organizations must develop and maintain secure systems and applications that protect cardholder data ... implement strong access control measures ... track and monitor all access to network resources and cardholder data ... regularly test security systems and processes ... maintain an information security policy ... and maintain a policy that addresses information security.

### CREDANT

More than 700 enterprises and government agencies — including 50 of the Global 500 — rely on CRE DANT to ensure security compliance, protect their brand and enhance IT and end-user productivity.