



# Technical Specifications

## CREDANT® Protector

Prevent data leakage and data theft via physical, wireless and storage interfaces

### The Growing Risk of Internal Data Leakage and Theft

Today's enterprises are making internal security – and especially internal access to network resources - their highest IT priority. Unfortunately, the growing number of connectivity options between endpoints and mobile devices is also making internal data access all too easy. In fact, analysts report that over 70% of IT security breaches originate from within the enterprise. Data losses from these breaches now cost US companies over \$50 billion per year.\*

This is why many enterprises are turning to CREDANT Protector, the industry's most secure and easy-to-use endpoint data leakage prevention solution for controlling physical and wireless interfaces, as well as external storage devices. CREDANT Protector monitors real-time data traffic and applies highly granular security policies by domain, group, computer, or user. The solution also offers enforced CD/DVD access control and encryption, hardware keylogger protection, anti-network bridging capabilities and other powerful features.

Designed for a wide range of IT environments, CREDANT Protector can help enterprises:

- Protect their data from leakage and theft
- Eliminate targeted attacks through endpoints and removable media
- Enable connectivity and productivity without compromising security
- Support compliance with regulatory data security and privacy standards

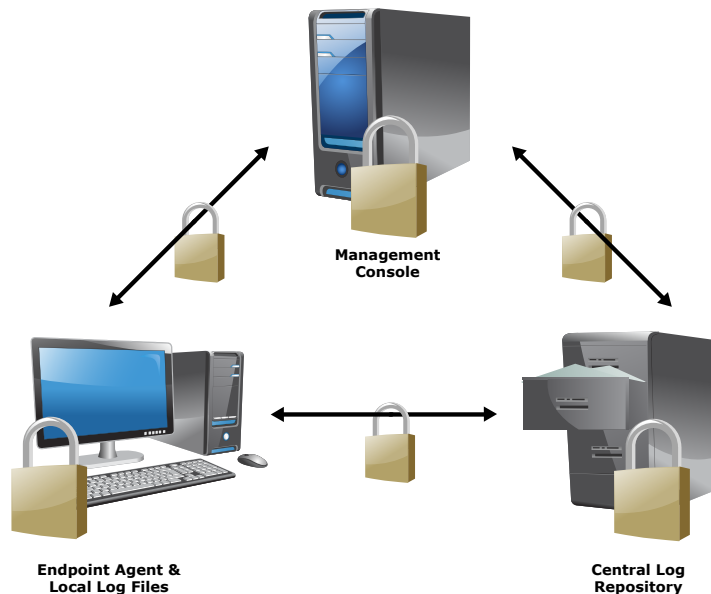
\* Statistics from Vista Research and The Economist.

### Endpoint Data Security Across Multiple Interfaces

CREDANT Protector provides a comprehensive, secure and easy-to-use endpoint data leakage prevention solution across a variety of interfaces.

Physical	Wireless
USB	WiFi
FireWire	Bluetooth
PCMCIA	Infra Red (IrDA)
Secure Digital (SD)	<b>Storage</b>
Parallel	
Serial	
Modem	
Internal Ports	
	CD/DVD Drives
	Floppy Drives
	Tape Drives

CREDANT Protector detects and allows the restriction of devices by device type, model, or even device serial number. WiFi controls are based on the Media Access Control (MAC) address, the Service Set Identifier (SSID), or the network security level.



CREDANT Protector encrypts consoles, agents and all the communications between them

### Ironclad Security Mechanisms

CREDANT Protector includes redundant, multi-tiered anti-tampering features to guarantee permanent control over enterprise endpoints.

- Protection of local polices, logs stored at the client, the central log repository, and all CREDANT Protector-related communications
- Local policies "signed" with unique ID which, if altered, highlights any tampering attempt
- Hashed uninstall passwords required for all users
- Hashed passwords required by local administrators to remove the local agent
- Local client lock-down, preventing further action and sending an alert if unauthorized activity is detected



## CREDANT Protector Architecture

### Highly Customized Security Strategies

At CREDANT Technologies, we understand that different organizations have different technical needs, corporate cultures and business goals. As a result, CREDANT Protector allows administrators to first choose their endpoint security strategy and then implement it in line with their unique organizational requirements.

Using a flexible management console with CREDANT Protector, administrators can:

- Create comprehensive and granular endpoint security policies
- Gain real-time notifications of any activity that needs immediate response through a built-in alerting capability
- Receive alerts via email, SNMP, Syslog, Windows Event Viewer, popup messages and even custom scripts

### Your Advantages With CREDANT Protector

- **Data encryption** – encrypts corporate data on CD/DVDs.
- **Granular control** – detects and restricts data transfers by device, device type, or unique serial number.
- **Data awareness** – inspects files by their types and allows, blocks or restricts the transfer of files to and from external storage devices.
- **Granular WiFi control** – maintains control by MAC address, SSID, or the security level of network.
- **Anti-bridging** – prevents hybrid network bridging by blocking WiFi, Bluetooth, modems, or IrDA while the PC is connected to the wired corporate local area network (LAN).
- **Flexible and intuitive policy management** – defines separate policies for any domain, group, computer, or user. Policies are seamlessly integrated with Active Directory organizational objects.
- **Built-in compliance policies** – includes detailed configurations for achieving security policies that are mapped to specific regulatory compliance standards.
- **Anti-hardware keylogger** – blocks both USB and PS/2 hardware keyloggers.
- **U3 and autorun control** – turns U3 USB drives into regular USB drives while attached to organization endpoints, protecting against auto-launch program by blocking autorun.
- **Interface for content inspection add-on** – examines the “content” before it is allowed to be downloaded to an external storage device.
- **Unique certifications** – for Windows Hardware Quality Labs (WHQL), Operations Security (OPSEC), and Network Access Control (NAC) compatibility.

### Part of a Comprehensive Security Solution

CREDANT Protector works closely with CREDANT Mobile Guardian (CMG), the only security system that can encrypt and secure data on mobile devices across multiple, diverse platforms from a single console.

More than 650 enterprises and government agencies -- including 50 of the Global 500 – rely on CREDANT to ensure security compliance, protect their brand and enhance IT and end-user productivity.

To learn more about CREDANT Technologies and our solutions, visit [www.credant.com](http://www.credant.com).



#### SPECIFICATIONS

##### Supported Operating Systems:

###### CREDANT Protector Client Platforms:

Microsoft® Windows Vista® Ultimate, Enterprise and Business  
Microsoft Windows XP Professional and Tablet PC

###### Supported PDA Platforms for Access Control:

Windows Mobile™ 6.0/6.1 Professional and Standard  
Windows Mobile 5.0 Pocket PC and Smartphone  
Windows Mobile 2003 Pocket PC and Smartphone  
Palm OS® 5.x  
RIM® Java OS 4.0 BlackBerry™ devices  
Apple iPhone

###### Enterprise Server and Management Console Platforms

Microsoft Windows Server 2003 Standard and Enterprise  
Microsoft Windows Server 2003 R2 Standard and Enterprise  
Microsoft Windows XP Professional

##### LDAP Support

Microsoft Active Directory®

##### Supported Databases

MS SQL Server 2000 and 2000 Enterprise Edition  
MS SQL Server 2005, 2005 Express Edition, and 2005 Enterprise Edition