

Protiva™ SmartTMS

Securing and managing USB peripherals while protecting identities, company data and applications



ENTERPRISE > SOLUTION

Perhaps one of the greatest threats to company information is the number of mobile workers carrying sensitive information in and out of the company premises. At times, employees use their personal USB drives to copy or safeguard company information. The real threat is when employees misplace these same portable devices. A report showed that at least 5000 handheld devices including USB drives get left behind each month in New York City taxi cabs alone, while in another survey, British dry cleaners found at least 9000 USB memory sticks forgotten in people's pants pockets.*

How much does data breach cost an organization? In 2009, data breaches cost companies in the U.S. an average of \$204 and £64 in the UK per compromised record. That's an average organizational cost of \$6.75M and £1.68M respectively.** Enterprises are aware that the increased use of USB peripherals represents a serious challenge to the protection of company data and user identities. As the leader in digital security, Gemalto addresses the question of managing these devices, easily and efficiently, thereby protecting two of enterprises' most-precious assets: people identities and sensitive company information.

Protiva™ SmartTMS: centralized management of USB peripherals

The Protiva™ Smart Token Management System (SmartTMS) is a server

> Key features:

- Centrally manage the complete lifecycle of company-issued USB peripherals including binding the token to a user
- Administer and remotely distribute applications, documents and web services
- Enforce security policies on devices including PIN policy and hostile network usage
- Remote PIN recovery
- Remote device locking for lost/stolen devices and revoked access for terminated employees
- Supports multiple OS: Linux, Unix, Windows
- Support for strong authentication through smart cards
- Track and audit token usage, recover and re-issue token

application that centralizes all operations needed to manage and secure enterprise USB peripherals. Applications, data and even web services can be centrally managed by the SmartTMS. This standalone server application is easily installed at enterprises' premises, giving organizations full control and access to a company's USB peripherals and data security policies. In addition, the SmartTMS can be easily integrated into existing company directories and can be customized and automated within specific workflows to meet

companies' needs and adapt to existing public key infrastructures (PKI).

Providing comfort and convenience to users

Unlike most in-house corporate computing tools that employees perceive as a work constraint, the Protiva SmartTMS is a simple security solution that lets enterprises focus on user comfort and convenience. A variety of usage models depending on the type of USB peripherals and workstations used can improve workflow, enable easy access to data and increase user convenience. As a content-oriented device management system, SmartTMS communicates securely with an embedded agent on each USB peripheral in order to easily transmit instructions, security policies and software updates. This facilitates the deployment of mobile services that take full advantage of your company PKI and USB peripherals.

* Separate surveys in 2008 and 2009 carried out by Credant Technologies to gauge the frequency and ease with which mobile devices, such as memory sticks, are lost or forgotten in strange places such as dry cleaners, taxis and other commonly visited locations.

** US and UK reports: 2009 Annual Study: Cost of a Data Breach, benchmark research conducted by the Ponemon Institute

Protiva™ SmartTMS

Securing and managing USB peripherals while protecting identities, company data and applications

Overall advantages and benefit

> Reduced integration costs

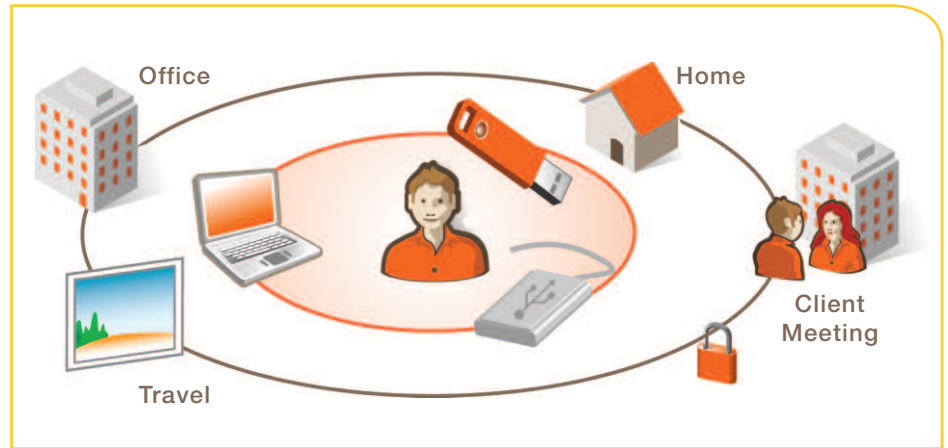
Protiva SmartTMS can be integrated into existing company directories and PKI. The server application requires minimum handling by a designated administrator and/or operator because it can be customized and automated to accommodate an organization's workflow and needs. Templates or device models can be created and later on replicated to users' USB peripherals: setting default configuration, contextual security policy, loading software suite and pre-defined documents. There is no software installation required on users/employees PCs. The server application can customize a single or a fleet of USB peripherals, thus simplifying portable device management.

> Reduced operational risks with managed user identities

SmartTMS protects users and their USB peripherals by binding devices to specific users. Enterprises' security policies are reinforced thereby reducing operational risks. Lost or misplaced USB devices can also be remotely blocked or even destroyed, keeping company data away from unauthorized users. SmartTMS ensures that only authorized company employees can access sensitive data and it can be set to provide status and functional reports for active USB peripherals. Moreover, the server application facilitates the easy enrollment of new users and USB peripherals.

> Leveraging USB peripherals for simplified content management

The SmartTMS is an ideal solution for companies that are looking for secure means of managing data contained in employees' USB drives or mobile devices. It can be used to push and securely update business documents, applications and company websites. Pertinent mobile services can also be deployed for employees who are constantly on-the-go.



Using SmartTMS

> For secure mobile office

For companies that employ personnel who are on-the-go and manage sensitive information, Gemalto's SmartTMS can be used to create a cost-effective portable computing platform with IT-approved corporate application for actions such as secure remote access to company resources. This ensures IT-controlled computing in public or temporary computers and work-from-home environments.

> For secure web services and home banking

For enterprises and banks offering web-based services, Gemalto offers a simple and cost-effective solution to ensure complete control of web transactions and enables companies and banks to authenticate users. SmartTMS supports strong authentication solutions such as smart cards and software certificates, allowing enterprises to verify the origin and ownership of transactions.

SmartTMS for your Smart Guardian

SmartTMS is designed to manage an array of USB peripherals, such as USB keys, secure USB drives, and USB smart tokens that combine flash memory and smart card security.

As the leader in digital security, Gemalto offers highly secure end-user devices that manage individual access to networks, applications and data. Its secure USB tokens protect data by controlling access to the device's flash memory and encrypting the data stored on it. The Protiva Smart Guardian is a zero-footprint personal security device that protects portable data with proven smart card technology. It comes in the form of a USB token. Unlike other secure USB memory products, it provides an unsurpassed level of data protection because all critical functions and cryptographic keys are managed from within the secure environment of the smart card module.

With the SmartTMS and Smart Guardian combined, your company is guaranteed the highest security for your sensitive data.

