



## PROTECTING UNATTENDED DESKTOPS FROM UNAUTHORIZED ACCESS



### UNATTENDED DESKTOPS ARE A SECURITY RISK

Today, the fastest growing unmanaged risk to the protection of enterprise information assets – patient records, loan applications, financial transactions, and intellectual property is from inside the organization. In fact, research finds that 75% of all fraud and theft is perpetrated by trusted employees and contractors.

In workplace settings where desktops are located in highly accessible areas; shared amongst multiple users; or confined within high security zones, security best practices dictate that users manually lock their desktop to defend against unauthorized access to information assets. Unfortunately, this best practice is easily forgotten or ignored, exposing the organization to the unacceptable risk of a security breach and violation of data protection regulations.

Traditionally, IT professionals have relied on inactivity timers to terminate computer sessions when users step away and fail to manually lock their desktops – if no mouse or keyboard activity is detected over a period of time, the desktop is configured to automatically terminate the user's session.

To date, this approach has been ineffective. Inactivity periods set too short lead to user frustration and inconvenience when sessions are terminated too quickly. Inactivity periods set too long create a serious security gap—exposure to unauthorized access.

However, a new and revolutionary solution to protecting unattended desktops now exists!

### IMPRIVATA ONESIGN® SECURE WALK-AWAY™ – THE ONLY EFFECTIVE SOLUTION FOR PROTECTING UNATTENDED DESKTOPS FROM UNAUTHORIZED ACCESS

Imprivata OneSign Secure Walk-Away closes a critical security gap in the protection of confidential information assets by automating the process of securing the desktop when a user 'walks away'.

OneSign Secure Walk-Away is an add-on to Imprivata OneSign Authentication Management. OneSign Authentication Management replaces weak Windows desktops and remote VPN passwords with a broad range of strong authentication options to enable centralized and flexible authentication management at the desktop, network, application, and transaction-level.

Once a user has securely authenticated to the desktop using OneSign Authentication Management, OneSign Secure Walk-Away uses a combination of computer vision, active presence detection, and user tracking technologies to identify an authenticated user and automatically locks the desktop upon their departure. The result allows employees to do their job without modifying their regular work patterns or burdening them with the task of manually locking the desktop.

OneSign Secure Walk-Away flexibly supports different user workflows, including demanding shared workstation environments where multiple users require constant fast and secure login and logout to information assets.

### BENEFITS

- Protects unattended desktops from unauthorized access
- Takes the burden of desktop security out of the hands of employees
- Non-disruptive to employee workflows
- Prevents users from sharing sessions
- Completely automated, requires no user intervention

## ONESIGN, THE PLATFORM FOR EMPLOYEE ACCESS MANAGEMENT

OneSign Secure Walk-Away is an integrated component of Imprivata's OneSign Authentication Management. OneSign Authentication Management replaces weak Windows desktops and remote VPN passwords with a broad range of strong authentication options—including finger biometrics, proximity cards, smart cards, many national and government ID cards, One-Time-Password tokens, and an employee's physical location, to enable centralized and flexible authentication management at the desktop, network, application, and transaction-level.

OneSign Authentication Management is a module of the OneSign Platform. The OneSign Platform converges authentication and access management, seamlessly integrating strong authentication, application single sign-on, user provisioning, physical access control systems, and event reporting, to enable centralized access policies that enforce every aspect of access across all users, rights, locations, and conditions.

Managed from a single, easy-to-use Web-based administrative console, the Imprivata OneSign platform is delivered in a purpose-built, highly secure and self-contained hardened appliance. Non-invasive to your organization's existing IT infrastructure, OneSign requires no change to user directories, applications, or physical access control systems, and it does not require additional staffing or specialized management skills.

Designed for flexible and rapid enterprise deployment and easy integration, Imprivata OneSign's appliance-based solution dramatically minimizes implementation time, infrastructure needs, and installation costs—accelerating your return on investment and lowering your ongoing support costs.

## TECHNICAL SPECIFICATIONS

### Lighting

- 100 to 5000 Lux
- Evenly diffused lighting

### Processor

- Pentium 4 Hyperthreaded: 2.4 GHz +
- CoreDuo or Core2Duo 1.6 GHz +

### Memory

- 1 GB RAM for Windows XP
- 2 GB RAM for Windows Vista

### Operating System

- Windows XP Professional
- Windows Vista

### Supported Cameras

- Logitech Pro 9000
- Logitech Pro for Notebooks

### Recommended

- Privacy filter



Bringing secure employee access management to companies around the world from our offices in:

Belgium | Germany | Italy | Singapore | UK | USA

1 877 ONESIGN | 1 781 674 2700 | [www.imprivata.com](http://www.imprivata.com)