

**LOTS OF WORKERS,
MANY APPLICATIONS,
MULTIPLE LOCATIONS...**

**...and you need one smart way to
handle access for all of them.**



IMPRIVATA ONESIGN®

The Converged Authentication and Access Management Platform

THE CHALLENGE: MULTIPLE SECURITY THREATS.

In a world where organizations pride themselves on being “knowledge-driven” and expert users of business intelligence, it’s amazing how little many of us actually know about something just as mission-critical: the security of those vital information assets. See for yourself by answering the following questions:

- *Do you have the same number of active employees and active accounts?*
- *Do you know who is accessing your network and applications?*
- *Do you know which applications users are accessing?*
- *Can you enforce a password policy across all users and locations?*
- *Do you know your password management costs?*
- *Do you have visibility into all disparate systems?*
- *If someone leaves your organization, can you immediately lock down their access to networks and applications?*

If you found yourself answering “no” more than a few times, you’re not alone. The landscape of enterprise security has never been more complex. And what you don’t know **can** hurt you.

“Imprivata’s OneSign is a complete identity and access management security platform that can enable an organization to implement an authentication strategy, single sign-on and now a physical access control system – integrating previously segregated domains.”

- Christopher Paidhrin,
IT Security Compliance Officer,
ACS/Southwest Washington Medical Center

Protecting Your Data from the Insider Threat.

Most of us tend to think of data security in terms of external attackers. But in fact, the biggest threat to your information assets comes from within your own enterprise. Studies have found that 75% of all data fraud and theft is perpetrated by insiders. Yet most organizations have done little to counter internal threats. Every day, in every industry, headline stories highlight the devastating repercussions that can occur when weak or non-existent identity-based access control policies allow even trusted employees to perpetrate fraud and theft – and it is costing organizations billions of dollars.

Demonstrating Compliance.

Countering insider threat isn’t the only high priority item on the data security “to do” list. There’s also the growing need to comply with government and industry regulations regarding data protection. Whether it’s Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley, the Data Protection Act or any of a growing number of industry-mandated regulations, the burden of regulatory compliance increases daily. That means you have to assess your organization’s data security risks; establish data security policies; enforce those policies; and monitor, track, and report employee access. Failure to do so may result in fines or legal action.

Managing Multiple Identities.

Compounding these challenges is the chaos caused by identity proliferation. Each individual employee, contractor and temporary hire associated with your organization has multiple, discrete identities. There’s a network ID, a physical access ID, a remote access ID, as well as multiple internal and external application IDs. Ensuring proper access controls are in place for a single person can mean potentially managing ten or more different identities.

Controlling Authentication and Access.

Another complicating factor: in many organizations, silos of authentication systems and related access policies have accumulated over time to address different levels and degrees of user access. Physical access control systems manage employee access to the workplace or secure zones. Other forms of authentication manage access to the network, often based on employee roles. Some users authenticate using finger biometrics, remote workers often use one-time password tokens, others may use smart cards or a combination

of devices. And for many, a simple and easily compromised password is the only form of user identification to networks and applications.

Gaining Visibility and Control.

Visibility into the “who, what, when, and how” is critical to security, but it’s virtually impossible to connect the dots when each access system within an organization has its own audit trail and access logs. These silos of information make that collection and aggregation of user access activity a monumental effort of time, resources, and costs. And without that comprehensive visibility, you can’t have centralized control.

THE SOLUTION: IMPRIVATA ONESIGN

The authentication and access management experts at Imprivata know what you’re up against. They understood early on that the way to address these critical IT challenges is by converging and unifying the policy for all of your discrete authentication and access management silos into one place. So they developed a solution that enables you to:

- *Manage application passwords and single sign-on to applications*
- *Choose different strong authentications for different users*
- *Map and validate all your users’ different identities*
- *Tie a user’s network access to their physical location*
- *Centrally track and trace all employee access events, across disparate systems, in real time*

It’s called Imprivata OneSign®, an easy, smart, and affordable solution for enforcing secure and compliant employee access to your enterprise information assets. When a password is not strong enough, Imprivata OneSign securely authenticates your users to the network with their choice of a broad range of authentication methods.

OneSign manages each user’s complete collection of application passwords and extends seamless and convenient single sign-on to all of your enterprise applications. That means no more password management headaches, no more frustrated, locked-out users, fewer password resets, and greatly reduced costs and resource requirements at the IT helpdesk.

If you have highly sensitive information assets contained within secure workplace zones or data stores, you can strengthen the security of these assets by locking down access to a network or computer based on a user’s physical presence within the zone.

Along the way, OneSign tracks, monitors, and reports all user access activities across disparate systems. All of which can make regulatory compliance easier to achieve – and demonstrate.

Imprivata OneSign is flexible, offering distinct license modules to address specific enterprise needs:



USERS NEED DIFFERENT STRONG AUTHENTICATION OPTIONS, BUT MANAGING THEM ALL IS THE CHALLENGE.

OneSign Authentication Management replaces Windows and remote access VPN passwords with a broad range of strong authentication options right out of the box. OneSign can mix and match various authentication modalities to provide greater security through flexible user authentication management. Additionally, OneSign’s self-contained environment includes a RADIUS host for handling remote access authentication using passwords or two-factor authentication.



HE HAS EIGHT PASSWORDS, BUT ALL HE HAS MEMORIZED IS THE HELPDESK NUMBER.

OneSign Single Sign-On quickly and effectively solves password management, security and user access issues. OneSign Single Sign-On enables all enterprise applications – legacy, client/server, Windows, JAVA, and Web – without custom scripting, modifications to existing directories, or inconvenient end-user workflow changes.



HE WAS FIRED AND LOCKED OUT OF YOUR BUILDING YESTERDAY, BUT IS ACCESSING YOUR NETWORK TODAY.

OneSign Physical/Logical integrates network and building access systems to provide a single consolidated user identity. You can now implement one comprehensive, converged policy for allowing or denying network access based on a user’s physical location, role, and/or employee status.

THE ADVANTAGE: ALL IN ONE BOX

After devising their ingenious security solution, Imprivata's engineers came up with the perfect form factor: a compact, easy-to-install, tamper-proof, all-inclusive network-based solution. By integrating user authentication, user access, password management and audit data in one easy-to-manage appliance, Imprivata delivers exactly what your company needs – a fast, affordable, fail-safe solution to centrally manage authentication and access policies across your enterprise and around the globe.

Imprivata OneSign simplifies access control while giving you confidence that your data is secure. OneSign strengthens your enterprise security by:

- Enforcing who gets access to corporate networks and applications
- Enforcing password policy across all users
- Providing visibility into all user access activities across disparate systems – both physical and IT
- Providing a comprehensive security infrastructure by integrating physical access with IT and data access

OneSign's appliance-based approach is non-invasive and seamlessly integrates with existing IT infrastructure. No changes are required to user directories, applications, or physical access control systems – nor does it require additional staffing or specialized skills. Deployment is fast and easy, and ongoing maintenance is minimal.

“With Imprivata’s quick to deploy, out-of-the-box solution, we’ve found a way to comply with audit regulations while significantly reducing helpdesk costs and improving employee productivity. Our employees absolutely love the new system...”

- Steve Siress, Network System's Manager,
Enterprise Bank & Trust



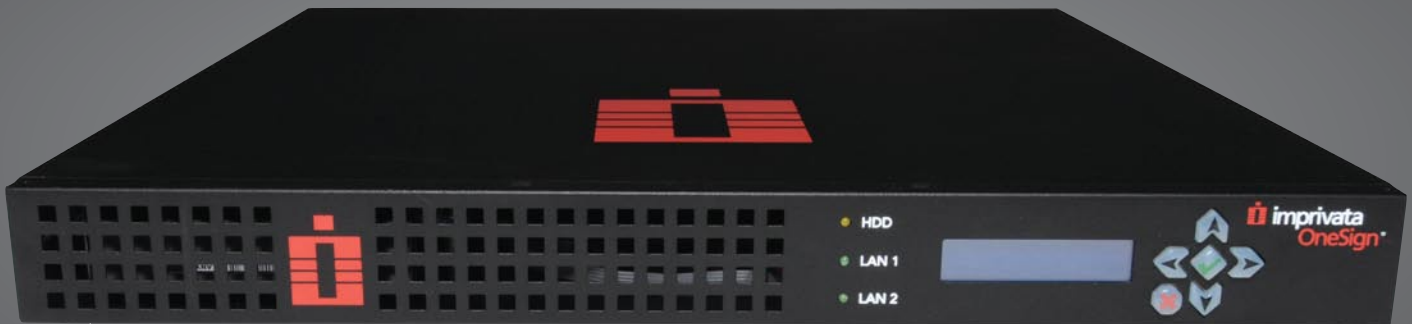
REPORTING

OneSign records all user events – user login, password change, session start/stop, success/failure events, and more – in a centralized log file. This provides a reporting trail accessible to the administrator for audit purposes. User events are collected and consolidated for centralized viewing and reporting.

Pre-established report types are easy to create and manage. Email notification for a variety of system events, including user authentication failure, user lockout, and system failure, can be sent to administrators for immediate issue resolution.

The Platform for 360° of Authentication and Access Security Management

The OneSign platform brings together all of the capabilities you need to ensure 360° of security coverage for your entire organization.



○ SYNCHRONIZING WITH YOUR USER DIRECTORIES

OneSign takes an identity-centric approach by seamlessly synchronizing with all of your LDAP-based directories ensuring all your users are accounted for and enabled for single sign-on and strong authentication, as well as tied to the physical access system events. Because there are no required extensions to your directory schemas, you avoid the risks, complexity, maintainability, and costs associated with changing your underlying directory structure.

○ ENABLING CONTEXT MANAGEMENT

OneSign is designed to work with other productivity tools such as context management in the healthcare environment. Healthcare applications often require a combination of single sign-on with Context Management for speed to patient information. OneSign natively interfaces with Fusion by Carefx® to provide clinicians a seamless login experience with single patient selection.

○ SEAMLESSLY INTEGRATING WITH USER PROVISIONING

OneSign integrates with user provisioning systems for “Day One” employee productivity. OneSign natively interfaces with Courion®, Fischer International™ and IBM Tivoli®, which can provision and de-provision users and application credentials within OneSign. That means there’s no need to distribute application passwords to users. And, everything is managed centrally.

○ SUPPORT FOR ALL LEADING STRONG AUTHENTICATION OPTIONS

Different industries and roles require different strengths and types of authentication. No problem. OneSign supports and provides integrated management right out of the box for one-time password tokens, finger biometrics, smart cards, proximity cards, building access and national and health ID cards. No additional authentication servers. No separate drivers to install.

○ INTEGRATING PHYSICAL ACCESS CONTROL WITH IT SYSTEMS FOR HOLISTIC SECURITY

Integrating your physical and logical access systems with OneSign gives you the power to thwart security breaches before they can occur. OneSign synchronizes with AMAG™, Honeywell®, Lenel®, Nedep®, S2® and Software House® to better secure networks and PCs in sensitive workplace zones. Physical Access Control Systems (PACS) may now act as new “logical access” enforcement points for protecting and locking down sensitive information resources without any added complexity.



ABOUT OUR CUSTOMERS

Imprivata is one of the fastest growing authentication and access companies in the world, with more than 600 customers and 200 reseller and technology partners around the globe. Our customers represent those industries facing today's most challenging regulatory and security issues – including financial services, government, healthcare, life sciences, media, publishing, and utilities.

ABOUT IMPRIVATA

Imprivata is the converged authentication and access management appliance company. The OneSign platform helps organizations safeguard enterprise information assets by enabling secure employee access to networks and applications – improving user productivity and convenience, while reducing the time, risk and cost of complying with data privacy and protection regulations. OneSign has received top ratings in product reviews throughout the industry and has been awarded numerous accolades from leading publications including *Information Security*, *InfoWorld*, and *SC Magazine*.

To discover more about how your organization can benefit from this converged authentication and access management solution, contact Imprivata by calling 1 781 674 2700 or visit us at www.imprivata.com.

“Imprivata OneSign’s platform is a true cost-effective, turnkey solution aiming for ‘360°’ authentication management.”

- Paul De Vroede,
Manager, Telecommunications & Office
Automation, Bridgestone Europe



Securing employee access to desktops, networks, applications and transactions from around the world.

Belgium | Germany | Italy
Singapore | UK | USA

1 877 ONESIGN
1 781 674 2700
www.imprivata.com

Copyright © 2009 Imprivata, Inc.
All rights reserved. Imprivata and OneSign are registered trademarks of Imprivata, Inc. in the U.S. and other countries. The Application Profile Generator and OneSign Agent are trademarks of Imprivata, Inc. All other trademarks are the property of their respective owners.