

# The Ubiquitous Password Problem

*How 3 companies are solving it with SSO*



Step 1 of 3: Recognize Screen  
To learn the screen, please use your mouse to drag the magnifier and drop it on the screen of this application.  
Learn Screen



#### Server information

OneSign Server process running  
Number of requests handled by OneSign Server since start  
Average Server response time

# Why Have Passwords Become so Problematic?

*In 2000*

*Today...*

	<i>In 2000</i>	<i>Today...</i>
<b>User Convenience</b>	The average corporate user had 2 passwords	Average user has 10-15 passwords to remember
<b>Regulatory compliance</b>	NO regulations	SOX, HIPAA, GLBA, PCI, FFIEC, Global issue
<b>Password Security</b>	90% of companies had no password policies	Companies are either: thinking about; trying to; or have implemented PW policies
<b>Control over information access</b>	Access limited to within the enterprise	ASP's, third-party web applications, remote users

# The Truth About Passwords

- **“Good” Passwords are designed to be user unfriendly**
  - Simple passwords are weak
  - Complex passwords are stronger but difficult to remember
  - Confusion across numerous passwords
- **Social engineering can defeat most password security**
  - Using the same password for all applications
  - Sticky note reminders for credentials
- **Password change events cause loss of productivity**
  - Average user maintains 7-10 changing passwords
  - 30% of Help Desk calls relate to forgotten or incorrect passwords
  - Average of 45 minutes lost productivity
- **Roaming and remote users constantly re-enter credentials**
- **Passwords are not “free”**



# What is Enterprise Single Sign-On (ESSO)?

*A single authentication to the network providing seamless access to a full range of enterprise applications, including:*

- **Windows/Client Server**
  - Java, VB, etc.
  
- **Legacy Applications**
  - Terminal emulators, Command line, Telnet, etc.
  
- **Web Applications**
  - Including 3rd party hosted/ ASP





# How are people solving the Password Problem?



**Step 1 of 3: Recognize Screen**

To learn the screen, please use your finger to drag the magnifier and drop it on the screen of this application.

Learn Screen



## Server information

OneSign Server process running  
Number of requests handled by OneSign Server since start  
Average Server response time

# Bridgestone Europe

## ■ Summary

- European Division of the world's largest tire manufacturer
- Over 11,000 employees across eight factory locations
- HQ in Brussels

## ■ Problem

- Too many passwords
- Large heterogeneous environment – resulting from lots of M&A
- Over 50 core applications, including SAP and Oracle
- Wide range of user security requirements – both internal and external access

## ■ Initial objectives

- Simplify access to applications
- Provide greater user convenience

# Bridgestone Europe

## ■ Requirements

- Integrated 2-Factor authentication
- Ease of configuration and roll-out
- Low cost of on-going management and maintenance

## ■ Results with Imprivata OneSign

- Fast deployment with appliance, low on-going maintenance
- Rolled out to 3500 users
- Complete SSO to all their applications with no scripting
- Deployed Fingerprint biometric and Vasco OTP token 2-factor authentication for increased security
- Very happy users

## ■ Unexpected Benefits

- Was able to address JSOX regulations for audit and compliance
- Solution moved from convenience to critical need

# Renasant Bank

## ■ Summary

- \$3.6B asset financial institution
- Regionally focused, based in Tupelo, Mississippi
- Over 70 community banking, insurance, mortgage and financial services offices

## ■ Problem

- Time spent *Learning, Resetting and Managing* passwords was directly impacting lender's ability to meet customer service goals

## ■ Initial objectives

- Provide secure unique passwords for each individual lending application
- Improve user productivity



# Renasant Bank

## ■ Requirements

- Affordable solution with fast deployment
- Easily extensible to branch offices
- Ability to be managed in-house

## ■ Results with Imprivata OneSign

- 30 minute initial set-up time
- Rolled out to over 1,000 users
- SSO to over 20 applications
- Password resets fell by over 82% in the first year of use
- Near zero on-going maintenance, managed by existing IT staff

## ■ Unexpected Benefits

- Better utilization of licensed software
- Reduction in overall IT budget by 5%
- OneSign is now the litmus test for any new IT solution



# Parkview Adventist Healthcare

## ■ Summary

- State-of-the-art acute care hospital
- Based in Brunswick, Maine
- Recognized in 2006 as a national award winner in healthcare service quality

## ■ Problem

- Heterogeneous HIS environment – increasing complexity of multiple systems
- Clinician frustration of constantly logging in/out of critical applications
- Rising help desk costs

## ■ Initial Objectives

- Reduce clinician password burden
- Strengthen access security
- HIPAA compliance



*Dr. Robert Aranson, Parkview Adventist*

# Parkview Adventist Healthcare

## ■ Requirements

- East to install and run
- Low cost to implement and maintain
- Integrated 2-Factor strong authentication
- Ability for clinical users to share workstations

## ■ Results with Imprivata OneSign

- Deployed in 2 days
- Rolled out to 300 users with integrated fingerprint biometric 2-factor strong authentication for increased security
- SSO to all critical applications
- High user satisfaction

## ■ Unexpected Benefits

- Compliance with HIPAA privacy mandates
- Patient bedside medication verification



*Dr. Robert Aranson, Parkview Adventist*

**“Imprivata provided the company with the 360 degree solution needed to solve SSO integration issues, password problems, and provide a platform for strong authentication.”**

Paul De Vroede, Manager Office Automation & Telecommunication,  
Bridgestone Europe

**“The solution began paying for itself immediately. And there is virtually no IT overhead. Initially it took 20-40 minutes to set up each application, and then it truly became a system we almost forget is in place.”**

James Hayes, VP Network Operations  
Renasant Bank

**“Two 1U servers and you are done. It plugs right into your active directory and you are live”**

Bill McQuaid, AVP and CIO  
Parkview Adventist Medical Center



# Common Lessons from the field

- **User adoption will make or break you – make it easy**
- **Choose an IT champion within the user community**
- **Design to streamline user workflow**
- **Provide a choice of authentication modes for users/roles**
- **Standardization of devices will help you**
- **You can never have too much communication/ education/promotion surrounding your implementation**
- **Educating everyone once and one way is not enough  
Keep in close contact with users – appreciate and incorporate their feedback**
- **Holding the users' hands can take some time but can help keep you employed**

# OneSign

## Seamless, Integrated Capabilities

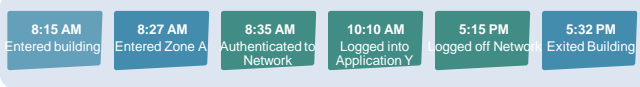
### Authentication Management



### Single Sign-On/Password Mgmt



### Monitoring and Reporting



### Location-based Authentication



Which clinician accessed what, when, and *from where*



# Questions?

# Authentication – Its all about identifying the user



## What you know:

- Passwords
- Strong passwords



## What you are:

- Fingerprint
- Iris scans



## What you have:

- ID Tokens
- Smart Cards
- Passive Proximity Cards
- Active Proximity Cards



## Where you are:

- Converged logical-physical access
- RFID tags

***Technology is only part of the solution – understanding your user requirements is critical***