

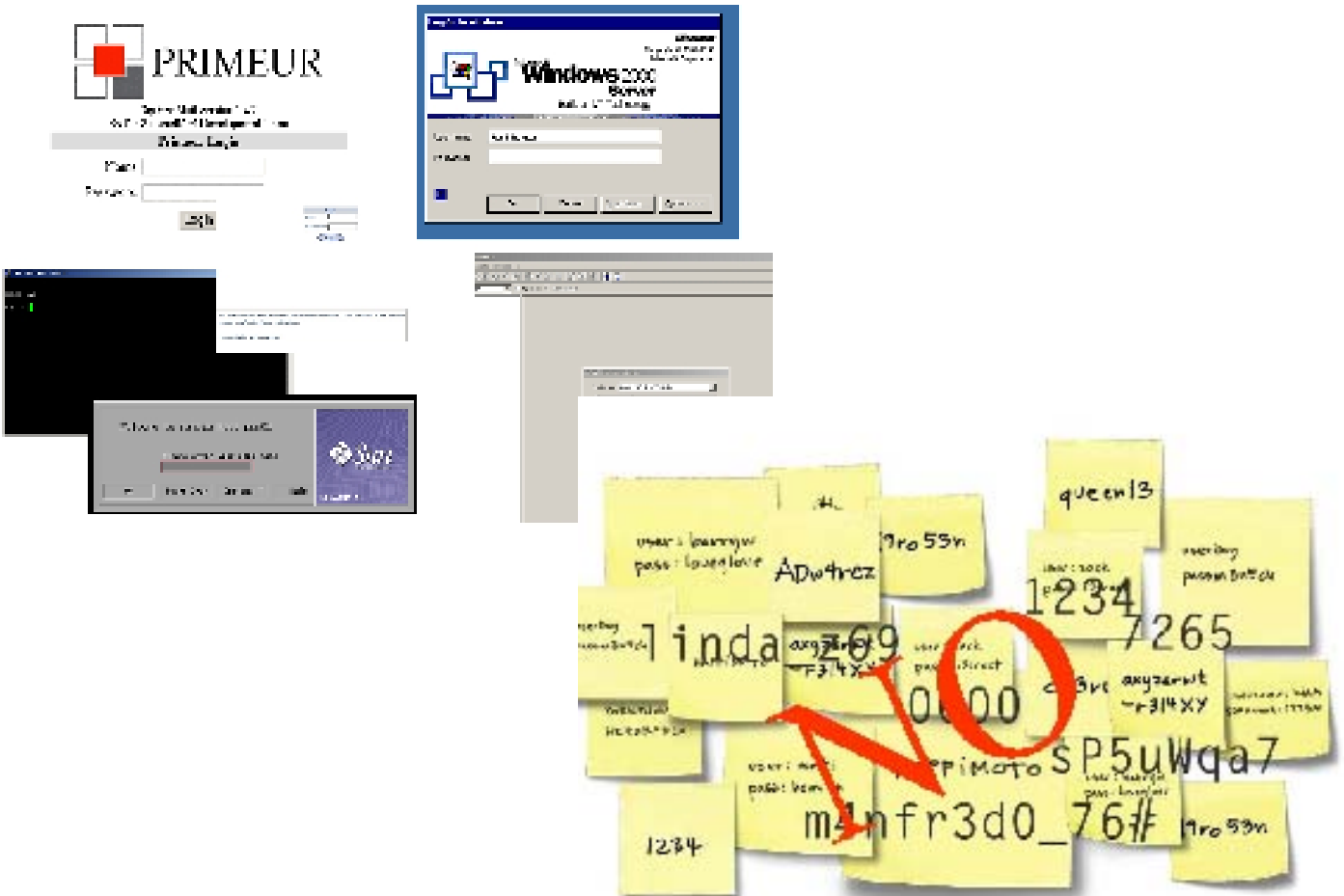
Primeur Security Services

Imprivata OneSign Single Sign-On

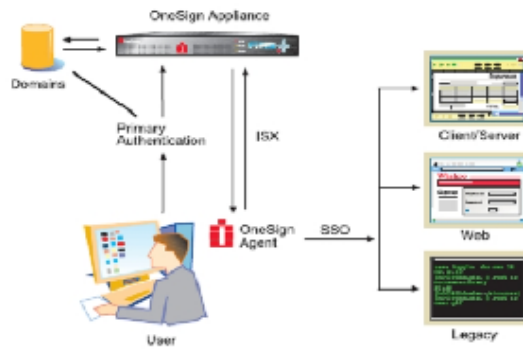
Imprivata® OneSign® makes enterprise single sign-on (SSO) simple and non-intrusive for Web, clientserver, and legacy applications. Packaged as an affordable, easy-to-implement appliance, OneSign uses patent-pending technology to enable SSO without modifying applications. Companies benefit through centralized password administration, lower help-desk costs, increased productivity, and complete compliance.

The OneSign Appliance and Imprivata Secure Exchange (ISX) technology enable companies to quickly deploy simple, automated, SSO services. OneSign requires no modifications to existing applications and no user learning curve. OneSign's native support for multiple authentication methods and centralized password policies allows companies to implement the security that is appropriate for their environments.

Imprivata OneSign is particularly beneficial for IT departments operating a heterogeneous portfolio of applications. Because OneSign replaces multiple passwords and application logon events with a single, centrally-managed user logon, IT's burden is significantly reduced. There's no longer any need to compromise increased security for increased usability. Imprivata delivers both security and convenience within the fully integrated OneSign Appliance.



Single Sign-On Scheme:



Secure Enterprise Single Sign-On

■ SSO for a Broad Set of Applications and Environments

Imprivata OneSign simplifies secure access to Web, client/server, and legacy or host-based applications through a simple network appliance that provides user-centric SSO authentication. SSO-enabled applications can run natively, as a console, a host terminal emulator, in a browser, or through terminal services such as Citrix MetaFrame XP®.

■ Non-Intrusive Appliance

OneSign is a non-intrusive network appliance. The OneSign Agent and Imprivata Secure Exchange (ISX) technology require no changes to applications or directories. OneSign communicates with existing user directories and runs seamlessly on the existing network. OneSign network communication is secure, lightweight, and exception-based. It does not impact network performance. The pair of 1U rack-mounted devices (redundant unit) requires nothing extra to buy or install.

■ No Changes for Users

Successful primary authentication of the enrolled user establishes a private and secure communication session between the OneSign Appliance and the OneSign Agent. Once the user is authenticated, the OneSign Agent receives encrypted user logon credentials and application behavior descriptions from the OneSign Appliance in an application profile. OneSign protects this information for each user in a secure, session-based digital vault on the OneSign Appliance (this is the heart of Imprivata's ISX technology). Users keep their existing network logon procedure, such as Microsoft Windows NT Domain®, MS Active Directory®, or Novell Netware® context.

■ Password Policy

• Strong Password Policy and Password Changes

Imprivata OneSign primary authentication can be tightly integrated with Windows domain and/or Novell Netware authentication. Since one password is easier to secure than multiple passwords, OneSign administrators can implement clear and straightforward security policies across all SSO applications based on users' primary authentication. Imprivata's ISX technology ensures the security of the primary authentication and all OneSign data transport.

• Policy Formats

Imprivata OneSign can generate stronger passwords that conform to any unique application requirements. Custom masks can be created on a per-application basis to allow administrators to configure a password length, mix of characters, specific characters or types for specified locations in the array, and more.

• One-Click User Lockout

Administrators can disable any user from all SSO-enabled enterprise applications and the network desktop logon with a single click. If Imprivata OneSign automated password policies have been implemented, users no longer know their various strong passwords to back-end applications and cannot use out-of-band connections to gain access.

• Self-Service Password Management (SSPW)

Many OneSign customers will use MS Domain or Novell passwords as a primary authentication mechanism for ESSO. OneSign Users can reset their primary domain password by adding this optional self-service mechanism. SSPW management requires the user to enroll shared secret information using personalized questions and answers.



For further information:

sales@primeur.com