Entrust® Securing Digital Identities & Information

Entrust IdentityGuard for Enterprise

Protecting Your Enterprise

When an employee or partner accesses a corporate network through an extranet, remote access gateway (VPN) or Microsoft® Windows® desktop, they have effectively opened a door to the organization's most sensitive assets, intellectual property and customer data. The security of the network and subsequent desktops are only as strong as the authentication method implemented, highlighting the importance of executing this properly.

Coupled with industry mandates like the Red Flag Rules, Sarbanes-Oxley Act (SOX) or the Payment Card Industry (PCI) standard, organizations are being driven to increase the strength of authentication across a much broader user population than ever before.

The most common way of authenticating employees and partners — username and password — is also one of the weakest in use today. Strengthening this type of authentication — typically by mandating long, complex passwords and enforcing frequent changes — often delivers minimal security improvement, yet significantly increases help-desk costs.

The need to provide strong second-factor authentication to wider enterprise populations is increasing. The budgetary challenges highlighted by widely deploying traditional strong authenticators is causing organizations to look for more cost-effective solutions that deliver a flexible approach to increasing security without introducing significant costs.

Entrust IdentityGuard – An Open Versatile Authentication Platform

As an established global leader in layered security strategies, Entrust offers a cost-effective versatile authentication platform that can help organizations protect the identities of employees and partners accessing sensitive enterprise data.

A key component of a layered enterprise security model, the Entrust IdentityGuard versatile authentication platform allows organizations to match the authentication

Product Benefits

- Versatile authentication platform that can be deployed at a fraction of the cost of traditional options
- Widest range of cost-effective authentication methods
- Easy to deploy and manage with a non-invasive architecture
- Protect leading applications like IP-SEC and SSL VPNs, Microsoft Windows desktops and enterprise Web applications like Microsoft Outlook Web Access
- Broad platform support including Microsoft Windows Server 2003, Sun Solaris, AIX and Linux
- Key component of a layered security strategy

SC MAGAZINE BEST BUY

The Entrust IdentityGuard versatile authentication platform was named a "Best Buy" and received a five-star rating from SC Magazine.

strength and mechanism to the amount of risk involved, usability requirements and cost considerations. This enables organizations to apply strong authentication across the enterprise, instead of just a select group of users.

Entrust IdentityGuard seamlessly integrates with existing environments with minimal impact on the user experience. This is advantageous for users accessing the network via remote access, Microsoft Windows desktop or the extranet, which can be used for leading applications like Microsoft Outlook Web Access.

Entrust IdentityGuard Advantages

Range of Strong Authentication Capabilities
Entrust IdentityGuard provides one of the widest ranges of authentication capabilities on the market today. The solution's variety of multifactor authentication options can enable stronger authentication across the enterprise without the need to deploy a one-size-fits-all solution that may not meet the unique requirements found across an organization.

Unmatched in versatility and efficiency, Entrust IdentityGuard delivers a range of authentication capabilities that can enable strong authentication without requiring client-side software, hardware or significant changes to the user experience.

The solution provides authentication methods that require virtually no user interaction, such as device fingerprinting and IP-geolocation. Authentication techniques that don't require a second physical form factor include knowledge-based, username and password, and out-of-band one-time passwords (OTP) via SMS or voice. Finally, the platform also supports authentication factors that require a form factor, which include grid cards, OTP hardware tokens and slim display card tokens.

Entrust IdentityGuard affords a level of choice, flexibility and personalization to both end-users and enterprises. Organizations can choose how they want their users to authenticate depending on user type, risk assessment and the application being used, including remote access, Windows desktop and applications deployed on the extranet.

The platform can be readily extended to other delivery channels, including interactive voice response (IVR) and help-desk systems. The solution's authentication methods do not require specialized hardware or direct hardware connections with the computer, so it can be leveraged across multiple platforms and used in conducting various types of transactions.

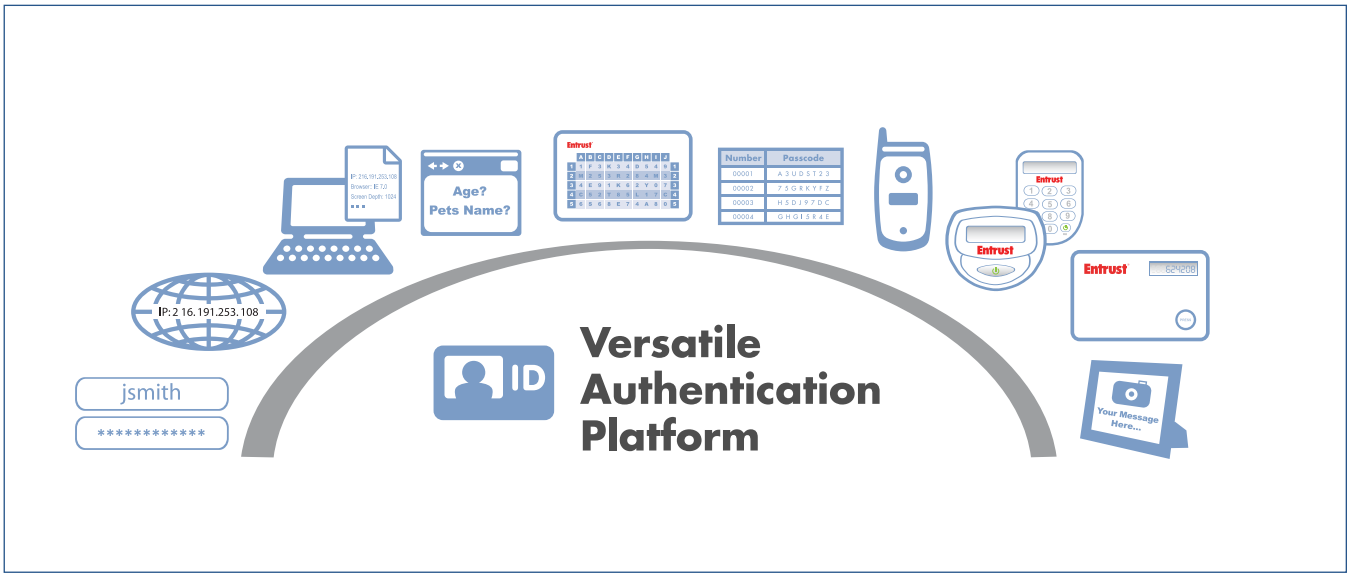

Figure 1: Entrust IdentityGuard provides one of the widest ranges of authentication capabilities on the market today

The range of authentication methods provided by Entrust IdentityGuard is supported by a single administrative layer that allows organizations to manage all users through one point of policy enforcement while being able to tailor the specific authentication policy on a per-user or group basis. The security of the Entrust IdentityGuard versatile authentication platform is built on Entrust's FIPS 140-2-validated cryptographic engine.

Easy to Use
Entrust IdentityGuard enables organizations to choose from a range of authentication options tailored to meet the unique requirements of their users.

The platform provides the capability to manage everyday authentication in the enterprise with one type of highly usable authentication, such as grid, and leverage another option, such as knowledge-based authentication, for applications like self-service user-recovery. All authenticators are administered through one central Web-based console, making management simple and efficient.

For organizations leveraging strong authentication for Microsoft Windows desktops, users are able work both on and offline, making it a true enterprise application for users on the go.

Non-Invasive, Open Platform
The Entrust IdentityGuard versatile authentication platform is designed to work within an organization's environment with little impact to the existing infrastructure. It does not require additional client or server software for VPN remote access, interoperating with various leading IP-SEC and SSL VPN applications from Nortel, Cisco, Checkpoint, Juniper Networks, F5 and more. The solution even includes 802.1x native support.

For Microsoft Windows authentication, Entrust IdentityGuard requires a small footprint client that provides the Entrust IdentityGuard grid challenge as a second step to Microsoft Windows authentication. For Web applications, organizations can leverage standard Web service APIs to directly integrate into an enterprise portal, or use a standard ISAPI filter to protect leading applications like Microsoft Outlook Web Access.

The solution leverages current user repository — whether it is LDAP, Active Directory or a database — and is architected to address the high scalability needs of large organizations.

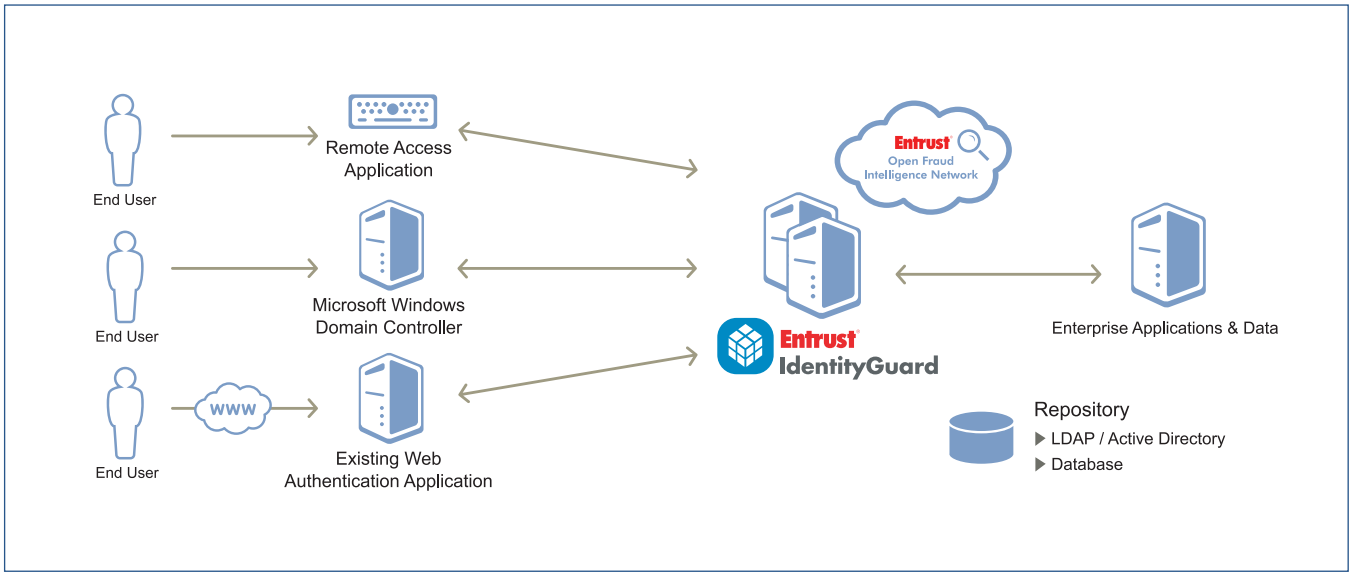

Figure 2: Entrust IdentityGuard Enterprise Architecture

Easily Extends to Address Consumer Security
What makes Entrust IdentityGuard unique is its ability to provide strong authentication to both enterprise and consumer environments. Not only can it be used to provide security for enterprise applications, but also can be extended to provide highly usable, cost-effective multifactor authentication to multimillion-user deployments that are common on the Internet today.

Product Architecture
The Entrust IdentityGuard server can run as a stand-alone authentication server or be deployed into leading application servers, including IBM and BEA, interfacing to the current sign-on application via Web services. This allows rapid integration with current applications whether they are built on J2EE, .NET or legacy platforms.

In addition, Entrust IdentityGuard leverages existing repositories for storing identity information instead of mandating new expensive instances, including supporting leading LDAP directories such as Sun One, Microsoft Active Directory and Novell, and databases from Oracle, IBM and Microsoft.

In addition to the built-in Web-based console for managing all user and policy activities, administrative actions can be easily integrated into current processes via a broad set of Web service APIs.

More Information

For more information on Entrust IdentityGuard, contact the Entrust representative in your area at 888-690-2424 or visit www.entrust.com/identityguard.

About Entrust

Entrust [NASDAQ: ENTU] secures digital identities and information for consumers, enterprises and governments in 1,700 organizations spanning 60 countries. Leveraging a layered security approach to address growing risks, Entrust solutions help secure the most common digital identity and information protection pain points in an organization. These include SSL, authentication, fraud detection, shared data protection and e-mail security. For information, call 888-690-2424, e-mail entrust@entrust.com or visit www.entrust.com.

Entrust® Securing Digital Identities & Information