Entrust® Securing Digital Identities & Information

Securing Your Digital Life

Entrust IdentityGuard for Enterprise

Protecting Your Enterprise

When an employee or partner accesses the corporate network through an extranet, a remote access gateway (VPN) or Microsoft® Windows® desktop, they have effectively opened a door to the corporate network and its data. The security of the network and that of the desktop is only as strong as the method users are authenticated, highlighting the importance of executing this properly. Coupled with industry mandates like the Payment Card Industry (PCI) requirement for protecting sensitive card holder data, 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 forms of authentication used today, and has been subject to numerous forms of proven password attacks. Strengthening this type of authentication, through mandating complex long passwords and enforcing frequent changes, often delivers minimal security improvement, yet significantly increases help-desk costs. Although deployed in small projects — typically remote access — in most organizations, the need to extend strong authentication to a wider audience is increasing. The budgetary challenges highlighted by widely deploying traditional strong authenticators is causing organizations to look for a more cost-effective solution that delivers 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.
The Entrust IdentityGuard solution allows organizations to layer security across a diverse range of enterprise users, transactions and applications. This enables organizations to apply the right level of strong authentication across the enterprise, instead of a select group of users. Entrust IdentityGuard seamlessly integrates with existing environments with minimal impact on the user experience accessing the network via remote access, the Microsoft Windows desktop, or the extranet that

Product Benefits

- Versatile authentication platform that can be deployed at a fraction of the cost of traditional options
- Wide range of cost-effective methods that can be used across the entire enterprise
- 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

may be used for leading applications like Microsoft Outlook Web Access. Designed with enterprise security requirements in mind, Entrust IdentityGuard can provide layered security and a broad range of authentication options — including the industry-first $5 Entrust IdentityGuard Mini Token — all at a single, low price.[1]

Entrust IdentityGuard Advantages

Range of Strong Authentication Capabilities
Entrust IdentityGuard delivers a range of versatile authentication options that can enable stronger authentication across the enterprise without the need to deploy a one-size-fits-all solution that may be cost-prohibitive. This includes machine, grid-based, knowledge-based, time-synchronous Entrust IdentityGuard Mini Tokens or mobile authentication, along with mutual authentication to authenticate the Web site to the user. Organizations can choose how they want their users to authenticate depending on user type and the application being used, including remote access, Windows desktop and applications deployed on the extranet.

Entrust IdentityGuard 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.

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 engines.

[1] Entrust IdentityGuard Savings Calculator

Figure 1: Entrust IdentityGuard delivers a range of highly deployable versatile authentication options for consumers

Easy to Use
Entrust IdentityGuard enables organizations to choose from a range of flexible options, all of which are familiar to end-users. Independent usability tests have shown 100 percent success rates for Entrust IdentityGuard in the enterprise, a good representation of how easy it is for users to authenticate to sensitive applications.[2] The Entrust IdentityGuard versatile authentication platform enables organizations to manage everyday authentication in the enterprise with one type of highly usable authentication, such as grid, and leverage another option, such as knowledge authentication, for applications like self-service user recovery. 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.

Easier to Deploy
Entrust makes it easier for organizations to deploy strong authentication to end-users, regardless of the type chosen. For grid authentication, delivering cards to end-users is a seamless process, leveraging standards-based output formats for either in-house printing or production through Entrust's turnkey service. Entrust IdentityGuard Mini Tokens do require delivery of a physical device, but organizations can leverage established processes for seamless delivery of the devices. For all other types of authentication, there is nothing physical to distribute, making deployment rapid and efficient. As Entrust IdentityGuard delivers a range of authentication methods for a single, low price, the ongoing management of users through a single platform that does not charge on a per-method basis can make ongoing administration simpler and more straightforward.

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. 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 Services APIs to directly integrate into an enterprise portal, or use a standard ISAPI filter to protect leading applications like Microsoft Outlook Web Access. As a versatile authentication platform, Entrust IdentityGuard 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.

Easily Extends to Address Consumer Security
What makes the Entrust IdentityGuard versatile authentication platform 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 it can also be extended to provide highly usable, cost-effective versatile authentication to multimillion-user deployments that are common on the Internet today.

[2] Entrust IdentityGuard Usability Study, May 2005

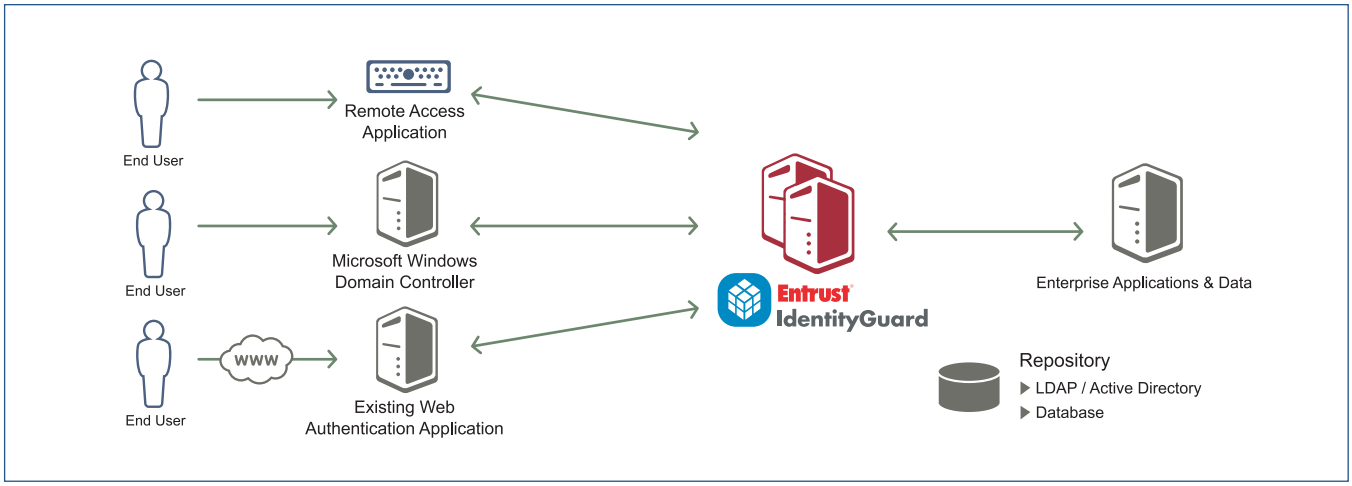

Figure 2: Entrust IdentityGuard Enterprise Architecture

Entrust IdentityGuard for Enterprise

Product Architecture

The Entrust IdentityGuard solution delivers its range of authentication options to multiple enterprise applications by virtue of its design as a dedicated versatile authentication platform. It leverages standards, including SOAP and Radius, to rapidly integrate with J2EE, .NET or legacy applications. In addition, Entrust IdentityGuard works with existing user records in current repositories, including leading LDAP directories such as Microsoft Active Directory, and databases from Oracle, IBM and Microsoft. Finally, in addition to a built-in Web-based management console, administrative actions can be integrated into current processes via a broad set of APIs.

Entrust IdentityGuard is developed for large-scale enterprise deployments, addressing both high scale and redundancy. The architecture has been designed and tested to support transaction rates associated with large-scale user deployments. To ensure availability, multiple Entrust IdentityGuard servers can be readily deployed in a load-balanced environment. Performance can scale and easily be enhanced by simply adding additional servers.

Entrust IdentityGuard is supported across a number of leading platforms including Microsoft Windows Server 2003, Sun Solaris, AIX and Linux. In addition, for organizations that have made significant investments in their application server environments, Entrust IdentityGuard supports leveraging both BEA Weblogic and IBM WebSphere as its application server.

Entrust IdentityGuard is a key component in a strong, layered security approach aimed at protecting today's enterprise online. Addressing the security challenges of today and tomorrow requires a layered approach that protects identities and information at multiple points to defend against ever-changing fraud threats in the online channel.

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 governments, enterprises and consumers in 1,650 organizations spanning 60 countries. Entrust leverages a layered security approach to address the growing risks to governments and enterprises worldwide. Our layered solutions help secure the most common digital identity and information protection pain points in an organization. These solutions include SSL, authentication, fraud detection, digital certificate management, 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