



# < Let's Talk

## 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 having an effective authentication strategy.

Providing strong authentication to the entire enterprise population is an essential component in protecting your organization. The budgetary and administrative challenges of widely deploying strong authenticators are causing organizations to look for more solutions that are not only flexible, but cost-effective.

Only a versatile authentication platform, which allows companies to choose different types of authenticators based on individual user requirements and associated costs, can effectively meet enterprise requirements.

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.

### Entrust IdentityGuard: Strong Authentication for Enterprises

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

The Entrust IdentityGuard versatile authentication platform allows organizations to match the authentication strength and mechanism to the amount of risk involved in the user's role, the usability requirements and cost considerations. This enables organizations to apply strong authentication across the enterprise, instead of just for 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 desktops or the extranet, which can be used for leading applications like Microsoft® Outlook® Web Access.

### Product Benefits

- Versatile authentication platform that can be deployed at a fraction of the cost of traditional authentication solutions
- Widest range of cost-effective authentication methods
- Core to consolidating security measures for physical and logical access
- Authenticates identities for multipurpose smartcard environments
- Protect leading applications like IP-SEC and SSL VPNs, Microsoft® Windows® desktops and enterprise Web applications like Microsoft® Outlook® Web Access
- Built on Entrust's FIPS140-2-validated cryptographic engine
- Broad platform support including Microsoft® Windows® Server 2003, Sun Solaris, AIX and Linux



The Entrust IdentityGuard versatile authentication platform is an SC Magazine "Best Buy" with a five-star overall rating.

## Entrust IdentityGuard Advantages

### Range of Strong Authentication Capabilities

Entrust IdentityGuard provides the widest range of authentication capabilities on the market today. The variety of authenticators 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 within an organization.

Unmatched in versatility, efficiency and affordability, Entrust IdentityGuard enables strong authentication without requiring client-side software, hardware or significant changes to the user experience.

Some authenticators require virtually no user interaction, such as device fingerprinting, digital certificates and IP-geolocation. Authentication techniques that don't require a second physical form factor include knowledge-based, username and password, SMS soft tokens, eGrids, and out-of-band, one-time passcodes (OTP) via SMS or voice.

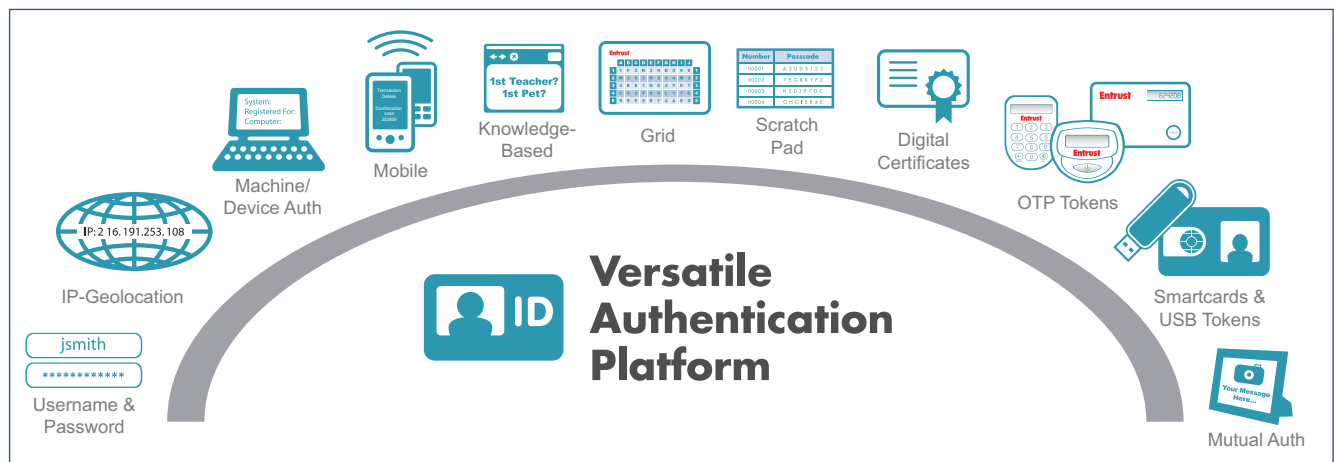
The platform also supports soft tokens and out-of-band OTPs via Entrust IdentityGuard Mobile. This is an innovative mobile identity application that helps organizations strongly authenticate users without requiring specialized security hardware.

Using the OATH standard for time-based, one-time passcodes, Entrust IdentityGuard Mobile supports the leading smartphone platforms on the market today, providing flexibility and security.

The Entrust IdentityGuard platform also supports authentication environments that require a form factor — this includes grid cards, time- and event-based OTP hardware tokens, and slim Display Card tokens. Entrust IdentityGuard affords a level of choice, flexibility and personalization to both end-users and enterprises.

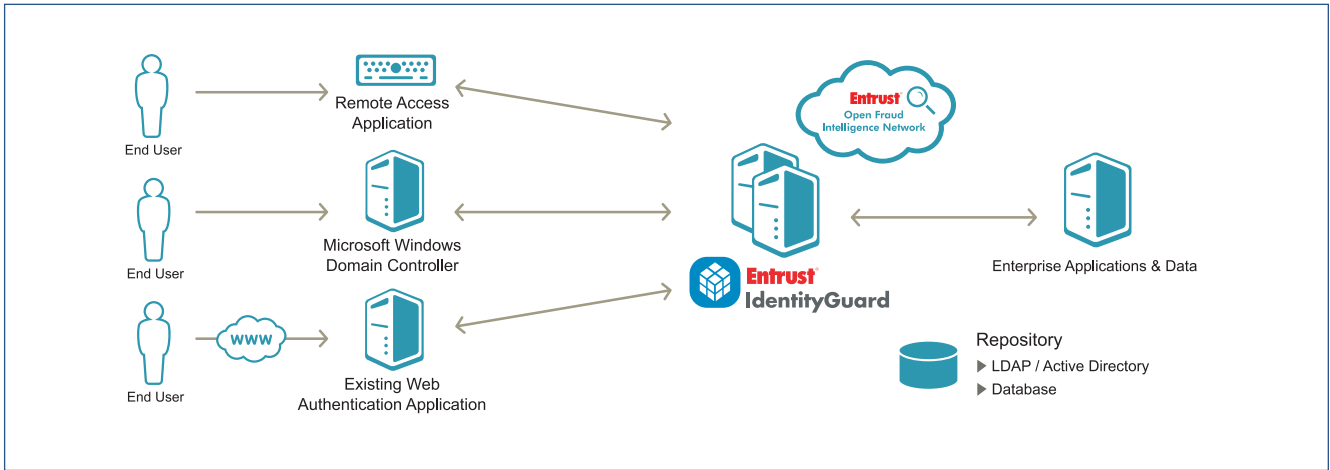
Organizations can choose how they want their users to authenticate depending on the type of user, risk assessment and the application being used (e.g., remote access, Microsoft Windows desktops and applications deployed on the extranet). The platform can be readily extended to other delivery channels, 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

# < Let's Talk



**Figure 2:** Entrust IdentityGuard Enterprise Architecture

**Physical, Logical Access**

Easy for the end-user and more efficient for organizations, the convergence of physical and logical access helps streamline the important security aspects of an organization. This often includes credentialing, secure access to facilities, strong authentication to desktops and network resources, and digital signature capabilities — all enabled via a single smartcard credential.

Entrust IdentityGuard helps organizations marry physical and logical access requirements to provide consolidated management, improved ROI and a total security view. And for organizations that prefer an end-to-end option, Entrust Credentialing Services provide the comprehensive steps for a full credentialing deployment.

**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.

Entrust IdentityGuard 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.

It does not require additional client or server software for VPN remote access, interoperating with various leading IP-SEC and SSL VPN applications from Cisco, Checkpoint, Juniper Networks, F5 and more. The solution even includes native 802.1x support.

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 uses 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.

**Easily Extends to Secure Customer Environments**

With its broad range of cost-effective authentication methods, Entrust IdentityGuard is unique in its ability to provide strong authentication to both enterprise and large-scale customer environments. Not only can it be used to properly secure enterprise applications, access and networks, it can provide highly usable, cost-effective strong authentication to multimillion-user customer deployments.

# < Let's Talk

## Entrust & You

More than ever, Entrust understands your organization's security pain points. Whether it's the protection of information, securing online customers, regulatory compliance or large-scale government projects, Entrust provides identity-based security solutions that are not only proven in real-world environments, but cost-effective in today's uncertain economic climate.

## 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](http://www.entrust.com/identityguard)**.

## Company Facts

Web Site: [www.entrust.com](http://www.entrust.com)  
Employees: 359  
Customers: 4,000  
Offices: 10 globally

## Headquarters

One Lincoln Centre  
5400 LBJ Freeway, Suite 1340  
Dallas, Texas 75240 USA

## Sales

North America: 1-888-690-2424  
EMEA: +44 (0) 118 953 3000  
E-mail: [entrust@entrust.com](mailto:entrust@entrust.com)



## About Entrust

Entrust provides identity-based security solutions that empower enterprises, consumers, citizens and Web sites in more than 4,000 organizations spanning 60 countries. Entrust's identity-based approach offers the right balance between affordability, expertise and service. For strong authentication, fraud detection, digital certificates, SSL and PKI, call 888-690-2424, e-mail [entrust@entrust.com](mailto:entrust@entrust.com) or visit [www.entrust.com](http://www.entrust.com).

**Entrust<sup>®</sup>** Securing Digital Identities & Information

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. In Canada, Entrust is a registered trademark of Entrust Limited. All other Entrust product names and service names are trademarks or registered trademarks of Entrust, Inc. or Entrust Limited in certain countries. All other company names, product names and logos are trademarks or registered trademarks of their respective owners. © Copyright 2011 Entrust. All rights reserved.