



< Let's Talk

TRANSFORM YOUR TOKENS FOR FREE*
TokenTradeUp.Entrust.com



Entrust IdentityGuard for Consumers

Countering Online Identity Fraud

Organizations are faced with a dramatic rise in online identity fraud, and are also required to comply with mounting regulatory pressure to improve the security and privacy of online transactions and customer data.

Highly publicized identity breaches, combined with ongoing identity attacks like phishing, man-in-the-browser (MITB) and other malware, have frightened many consumers away from online banking and e-commerce — or have driven them to competing organizations who offer more secure approaches for online transactions.

When securing online transactions, organizations need to evolve beyond basic username and password and employ a range of strong authentication capabilities that enable the right authenticator to be applied based on the risk of the transaction. This enables organizations to secure online users without taking a one-size-fits-all approach to authentication.

While increasing security is critical, ensuring that it does not impact the user experience is a primary concern. Organizations need to ensure continued growth of online adoption while implementing an authentication strategy that offers a range of strong authentication capabilities that can reduce fraud and restore consumer confidence.

Entrust IdentityGuard: Strong Authentication for Consumer & Business Banking

Entrust's strong authentication platform can help organizations protect user identities and reduce the risk of fraudulent transactions. The Entrust IdentityGuard versatile authentication platform provides one of the widest ranges of strong authentication capabilities on the market today.

The solution affords organizations a level of choice, flexibility and personalization that is unmatched by traditional strong authentication offerings, delivering a wide variety of authentication capabilities in a single platform.

With Entrust IdentityGuard, organizations can authenticate users only when necessary — through non-invasive methods if appropriate — and thereby minimize the risk of abandoned transactions and increased support calls. Entrust IdentityGuard provides a broad range of strong authentication capabilities that is also cost-effective for large-scale deployments.

Product Benefits

- Wide range of user-authentication capabilities including:
 - IP-geolocation
 - Device
 - Knowledge-based
 - Grids and eGrids
 - Digital certificates
 - SMS and mobile soft tokens
 - Out-of-band OTP with transaction details and signatures
 - Event- and time-based tokens, including display card tokens
- Mutual authentication with picture and caption replay, grid serial number, with the added ability to layer in EV SSL certificates
- Proven protection against man-in-the-browser attacks
- Only vendor that offers three distinct methods for stopping man-in-the-browser malware
- Cost-effective for large deployments in consumer, enterprise or business-banking environments



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

The platform, combined with Entrust TransactionGuard's real-time, zero-touch fraud detection capabilities, provides a true integrated consumer authentication and fraud detection solution for financial institutions and organizations of all sizes.

It's also the only solution on the market that provides three distinct and highly proven methods of addressing man-in-the-browser attacks — effectively and without user inconvenience.

Entrust IdentityGuard Advantages

Range of Strong Authentication Capabilities

Entrust IdentityGuard's strong authentication capabilities provide an effective defense against a range of online attacks, including phishing and man-in-the-browser. With the ability to authenticate users at login, as well as at the transaction level, organizations can be more confident about the protection of their users from online identity fraud.

Unmatched in versatility, efficiency and affordability, 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. This includes the ability to identify individuals using one or more authenticators by leveraging non-intrusive options like IP-geolocation, device, knowledge-based, out-of-band one-time-passcode (OTP) authentication or digital certificates.

Physical second factors such as Entrust's patented grid-based authentication, a credit card-sized display card token, and cost-effective event- and timed-based OTP hardware tokens can be deployed for advanced authentication.

Non-physical second factors, including SMS and mobile soft tokens, and innovative eGrids, are just as secure but are appropriate for organizations that don't want to require users to carry a tangible authenticator.

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 (e.g., partners, employees) 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.

Entrust IdentityGuard also delivers mutual authentication capabilities, including picture and caption replay, which can add an important layer of security in the fight against online attacks. The platform supports strong username and password authentication, enabling organizations to manage all types of authentication through a single, proven security infrastructure.

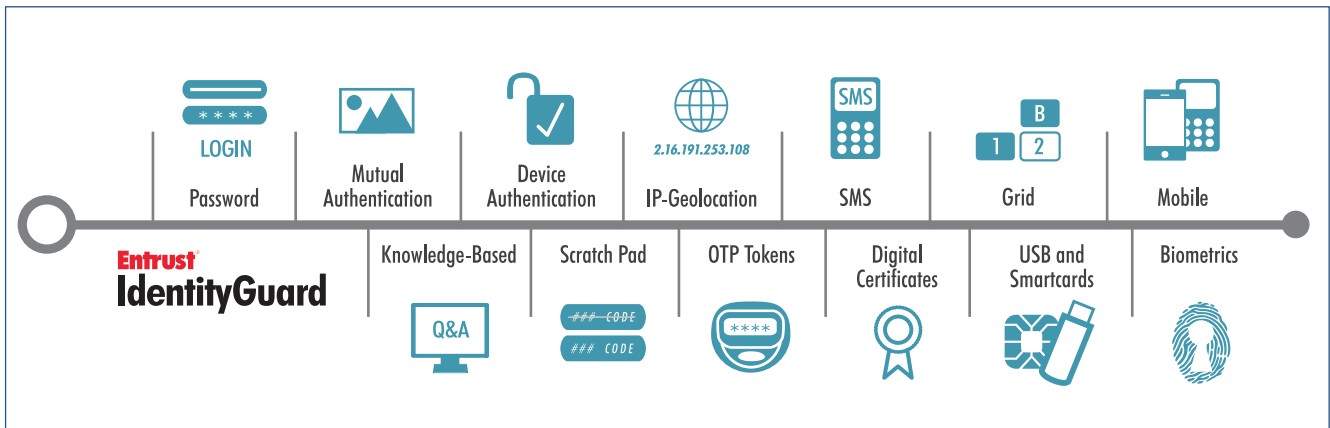


Figure 1: Entrust IdentityGuard provides one of the widest ranges of authentication capabilities on the market today

< Let's Talk

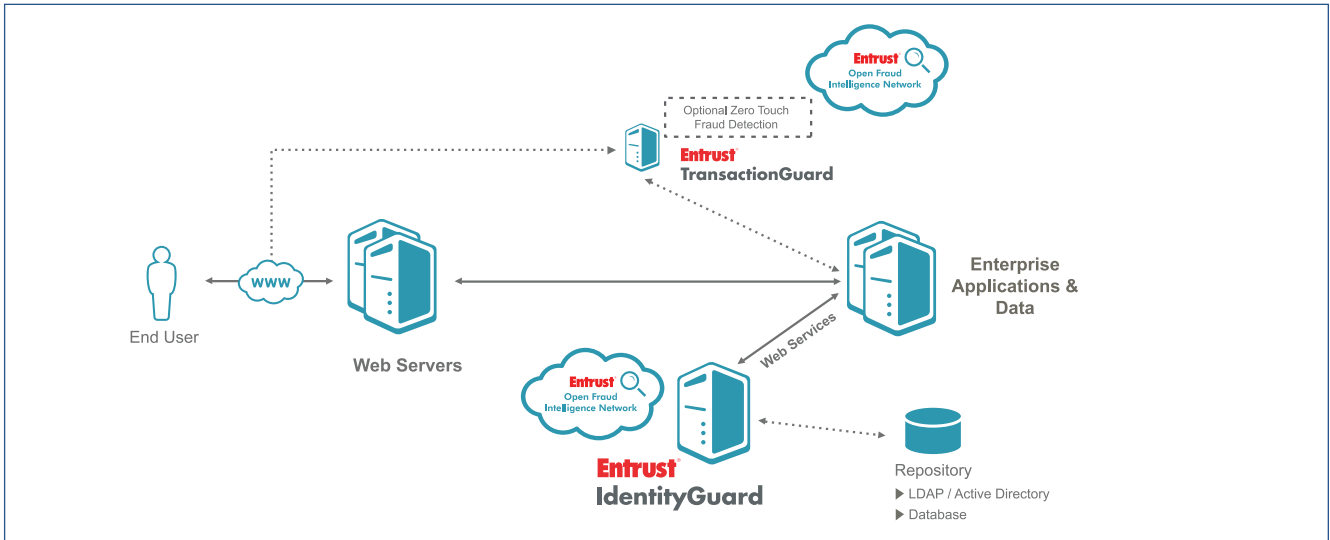


Figure 2: The Entrust IdentityGuard Versatile Authentication Platform

More Choices, Better Security

Entrust IdentityGuard can be extended to other delivery channels including interactive voice response (IVR), mobile and in-person transactions. Many authentication methods can be scaled across multiple platforms and used to conduct various types of transactions without typically requiring specialized hardware or direct hardware connections with the computer.

Entrust IdentityGuard also can use data delivered through the Entrust Open Fraud Intelligence Network (OFIN), which is an information-sharing service that combats online fraud by anonymously consolidating and sharing key fraud behavior patterns and data among network participants.

In addition, the platform enables organizations to easily accommodate accessibility requirements of a diverse consumer population, including the visually impaired.

Authenticators are supported by a single administrative layer that allows organizations to manage all users through one process while being able to tailor the specific authentication policy on a per-user or group basis. The platform is built on Entrust's FIPS 140-2-validated cryptographic engine.

Proven, Non-Invasive Platform

In addressing the requirement to strengthen authentication, perhaps the greatest consideration is minimizing any disruption to the user experience. Each authentication interaction with the user runs the risk of resulting in an abandoned transaction or support call.

Entrust IdentityGuard can help minimize the likelihood of these events by delivering non-invasive, easy-to-use authentication methods that are employed only when required based on the risk of the specific transaction.

By supporting methods such as device authentication and leveraging IP-geolocation data from the Entrust Open Fraud Intelligence Network, organizations can increase the confidence that the legitimate user is accessing their account, with minimal disruption to the online experience. If these initial methods suggest some risk in user identity (e.g., IP is not normal for the user or is on a black list), additional authentication can be layered to address an escalation of risk.

< Let's Talk

Proven to Stop MITB Attacks

Entrust's comprehensive identity-based approach leverages the Entrust IdentityGuard versatile authentication platform and the Entrust TransactionGuard fraud detection solution to deliver three proven methods for stopping man-in-the-browser attacks. Entrust IdentityGuard helps defeat man-in-the-browser attacks with out-of-band, one-time-passcode (OTP) authentication with transaction details, which can be delivered through SMS, voice or Entrust IdentityGuard Mobile.

Readily Deployed for the Masses

The Entrust IdentityGuard solution is designed to work in an organization's existing environment with little impact to the current infrastructure. This includes layering strong authentication over existing password applications, as opposed to replacing the way users authenticate today.

Entrust IdentityGuard leverages Web services standards for application integration and supports leading database and directory environments for user repositories. It is designed for highly scalable consumer deployments and takes into account the availability and service levels required in these environments.

To help manage the environment, Entrust provides enhanced reporting that allows Administrators to run system and user reports from the platform's console. This enables them to efficiently manage their Entrust IdentityGuard deployment and improve the user experience.

Easily Extended to Address Enterprise Security

The uniqueness of the Entrust IdentityGuard versatile authentication platform is demonstrated by its ability to provide strong authentication to both consumer and enterprise environments. Not only can it be used to provide security for Web applications services or transactions, but it can also be extended for strong authentication to remote access deployments as well as Microsoft® Windows® desktops.

Product Architecture

The Entrust IdentityGuard server can run as a standalone authentication server or can 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 about the Entrust IdentityGuard versatile authentication platform, contact the Entrust representative in your area at **888-690-2424** or visit **www.entrust.com/identityguard**.

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 or visit www.entrust.com.

Entrust® 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.

* Certain conditions apply. See full details of special offer.