Entrust® Securing Digital Identities & Information

Securing Your Digital Life

Security Beyond Today

Layered security for addressing fraud today … and adapting to tomorrow

March 2007

Table of Contents

1 Introduction

Across the globe, online criminals have focused dedicated funds, time and resources to perpetrate fraud — and they are very adept at this process. The result has been a dramatic increase in online fraud that specifically targets consumers, enterprises and citizens. Every data breach or costly identity-theft case reported in the media erodes the public's confidence in the security of online financial transactions. This loss of confidence could jeopardize the ability of organizations to conduct transactions online.

Today, a wide variety of organizations offering online services face increasing pressure to defend against phishing, man-in-the-middle attacks and other criminal activities that are ultimately focused on defrauding individuals and businesses. In addition, global regulations such as the US-based Federal Financial Institutions Examination Council guidance, the UK-based Faster Payments Initiative and others are focused on providing specific guidelines in response to online fraud, with many others, like the Red Flag initiative, on the near-term horizon.

A myriad of security vendors have stepped to the forefront in attempts to ease these concerns. While some are trusted sources of online security expertise, there are many newer players that lack the experience and know-how that larger organizations require.

While the intent of online security is clear — to better protect individuals and businesses from online crime — the implementation details are often far from transparent. And today, many organizations around the globe are struggling with the question, "Where should we begin?" Importantly, these same organizations are concerned with the next critical question as well, "What do we do next?"

Protecting the corporate brand, safeguarding customers and meeting the appropriate regulations are now primary security concerns. To properly implement a strong, layered security strategy that fulfils those goals, organizations need to thoroughly review their online activities and conduct risk assessments to determine the level of authentication and fraud detection required. Institutions must strategically develop and deploy additional online safeguards, including versatile authentication infrastructures, as identified by the assessment. Security threats will continue to evolve and organizations must develop solutions that can adapt to future challenges and protect consumers for the long term.

This document presents an overview of available security options that can help thwart fraud today and into the future, including versatile authentication and fraud detection solutions. With a clear understanding of the tools available and ways to effectively begin and evolve, organizations can take the essential steps toward protecting consumers, enterprises and citizens over the long term.

2 Risk Assessment and Security Options

Developing a strategic vision for securing online transactions means making security choices that will address today's requirements and can adapt to help meet tomorrow's challenges.

To realize this goal, it is necessary to carefully assess an organization's online activity and the level of risk presented by each type of transaction. Organizations need to consider which types of customers they are securing; the capability of their current transaction methods; information sensitivity and existing security; the ease of use and impact on the customer experience; and the overall volume of transactions completed.

Examples of these considerations include:

- ***Customer Type*** Retail, private banking, commercial, brokerage, insurance
- ***Transaction Capability*** Bill payment, transfers, stock purchase, loan origination
- ***Information Sensitivity*** Customer information and privacy regulations
- ***Ease of Use*** Relative importance and impact on customer experience
- ***Transaction Volume*** Number of transactions and impact on security choices
- ***Transaction Value*** The value of the transaction and the ultimate destination

As the majority of transactions that are performed online are actually legitimate, it is important to consider how you will deploy a layered security strategy for your online presence. Organizations should consider how different types of security can be layered across various points in any given transaction to achieve improved online security. In addition, when evaluating potential security solutions and vendor claims to realize this layered approach, carefully consider the following criteria:

Invasiveness No matter which security method or deployment plan is selected, it may not be appropriate for the new security safeguards to fundamentally change the way some or all customers are accustomed to banking. Choose a system that is flexible and can follow existing user-interaction models, or provide new options for securing the online experience.

Cost-effectiveness Future authentication and fraud detection requirements are an unknown. Choose a platform and vendor that can help meet needs now and can grow and change over time with new user populations and innovative challenges.

Adaptability As business demands change and innovative services are offered online, new security methods may be needed. Choose a full-featured security platform that uses a risk-based approach and is able to adapt to the requirement for securing multichannel application access. In addition, look for a platform that can be applied across the enterprise, both externally and internally, to reduce cost and increase efficiency

Integration Security solutions are just one part of a complex and multifaceted online system. Choose a platform that is integrated with other leading vendors, as well as compatible and usable with other systems.

Security Expertise Choose a company that is a security leader with a trusted reputation and focused dedication on security expertise.

Speed of Deployment Regulations often demand an aggressive timetable. Choose a platform that can help meet current and long-term goals, and can be implemented quickly from a proven vendor with deployment experience.

Openness of Solution Look for solutions that are open and adaptable to change that will inevitably happen in the future. Ideally, the vendor will approach the problem from a standards-based viewpoint versus a closed-proprietary perspective. This is especially important in the area of fraud, where it is proven to be more effective to share information broadly to defend against criminal activities.

Selecting the appropriate technology vendor to provide any security method can be daunting, especially if each one is evaluated individually as a stand-alone system. One key to assessing and selecting appropriate solutions is to examine security holistically — looking at all layers of security requirements as a single system with a variety of capabilities for different services. Select a platform that will deliver a range of versatile authentication and fraud detection capabilities that can respond and adapt to future changes. In addition, seek a platform that can plug into already-deployed solutions and still add significant value without mandating a complete switch-out.

3 Authentication Overview

Security threats will evolve and opportunities to strengthen the online relationship should continue to develop. Regulators have been clear: it is not enough to protect against current online account fraud and identity attacks. Regulated today or not, organizations must implement versatile methods that can address today's security needs and adapt to online crime in the future as well. A short review of authentication factors is helpful to understanding the implications of this position.

Authentication factors are independent ways to establish identity and privileges. Factors simply ask and answer, "How do we know you are who you say you are"? Existing authentication methods can involve up to three factors:

- ***Knowledge*** something the user knows (username & password, PIN)
- ***Possession*** something the user has (ATM card, smart card, OTP card/token)
- ***Attribute*** something the user is (biometric such as fingerprint, retinal scan)

Unfortunately, many organizations are specifically relying on usernames and passwords. In many cases, online customers possess a custom username and password to enter on a site, which serves as the only identity verification asset required to conduct any type of transaction online.

Adding factors of authentication can increase security and help limit vulnerability to identity attacks. Properly designed and implemented versatile authentication methods are more reliable, are stronger fraud deterrents and can have varying levels of user impact. With the advent of a new class of authentication strategy, coined a versatile authentication server (VAS) by Gartner, organizations have the ability to access a range of different authentication options through the deployment of a single security infrastructure.

Why don't all businesses use versatile authentication today? Based on most financial organization's innate ability to manage risk through business means, most have considered it unnecessary given the cost and resources required to manage and deploy multifactor solutions. Often, worries that users will find the process of authenticating with multiple factors complicated or intimidating have inhibited the use of multifactor solutions. But as risks increase, phishing attacks continue to grow and brands are impacted by fraud incidents, the true importance and necessity of versatile authentication becomes clear.

> "A versatile authentication server (VAS) is a common enterprise infrastructure supporting multiple open and proprietary authentication methods. This approach enables an enterprise to use different forms of authentication depending on who is logging in, where the login is taking place and for what purpose. A VAS also gives an enterprise a simple means of migrating to new authentication methods as its needs change and new methods emerge."
>
> *— Gartner*
> *"Token Price Obscures the True Value of Entrust Offering"*
> *Ant Allan & Ray Wagner*
> *February 2, 2007*

3.1 Authentication Methods

There are many diverse authentication methods that may be included in a versatile authentication platform, ranging from simple single-factor authentication in the form of user names and passwords to sophisticated mechanisms. In addition, mutual authentication options (identifying the site back to the end user) are key components of authenticating each party in an online transaction. Each method delivers a different balance point between increased security and user complexity.

User Authentication Options	Description	Key Aspects
Device Authentication & IP Geolocation	• User's machine, including local attributes (e.g., color depth, screen resolution), plus IP address to assess domain, location and historical login patterns	• Non-invasive way of strengthening user authentication • Store and validate the location or IP address of a registered machine • Ability to assess speed of login (velocity) from known locations can help to address risk of fraud
Knowledge-based Authentication/Shared Secrets	• Queries that require specific knowledge to answer	• Intuitive way of enhancing authentication without deploying anything physical to the end-user • May be used to bootstrap enrollment for other methods
Out-of-Band One-Time Password (OTP)	• Telephone call • E-mail message • SMS text message	• Delivers out-of-band, two-factor authentication via one-time passcode • Can help to address some forms of man-in-the-middle attacks
Non-Hardware-Based, One-Time Password	• Grid card with coordinate lookup • Scratch card	• Delivers strong second-factor security • Inexpensive to produce and deploy • Easy to use and support
Tokens	• Password-generating token (time synchronous or event-based) • Multiple form factors (challenge-response, response only)	• High security • Convenient, portable • Typically costly; new cost-effective alternatives now available • Traditionally proprietary algorithms, new generations focused on standards like OATH
Smart Card/USB Token	• Small devices/cards that allow physical and/or logical access to networks, servers or facilities	• Convenient, portable, multipurpose (physical/logical access) • EMV support with OTP for Point-of-Sale security can be combined for online use
Biometrics	• Finger prints • Iris configuration • Facial configuration • Voice patterns	• Costly & potentially inconvenient • Can be viewed as personally intrusive or invasive • Examples like voice biometrics can be effective layered security options for enrollment & recovery operations

Mutual Authentication Options	Description	Key Aspects
Picture & Caption Replay	• Authenticating Web site to consumer via shared secret or image	• Replay of something known to user (Image, message, or serial number) • Personalized for the user • Resistant to phishing and brute-force attacks
Extended Validation (EV) SSL Certificates	• Authenticating Web site to consumer via EV SSL certificate	• Easy-to-use mechanisms for customers to recognize they are on the correct site (e.g., green address bar, padlock, etc.) • Industry-standard vetting process • Requires user decision-making

4 Fraud Detection Overview

Online criminals repeatedly attempt to circumvent traditional authentication safeguards through sophisticated attacks including phishing and man-in-the-middle attacks. Fraud detection can add a much-needed layer of security for organizations and is an important element in any online user protection strategy focused on thwarting online attacks today and into the future.

Because fraud tactics rapidly evolve, a fraud detection solution should analyze patterns of behavior, rather than just individual transactions. While specific high-risk transactions should be identified according to pre-defined business procedures and flagged for closer evaluation, an advanced fraud detection solution will be able to evaluate patterns of transactions as well. Evaluating these patterns can help uncover fraudulent activity that might otherwise be missed by evaluating individual transactions alone. Solutions should be able to work in real-time or in batch mode to evaluate transactions, and should have the ability to analyze complete transaction patterns, not just small subsets of a transaction flow.

A fraud detection solution should also provide monitoring and forensic tools to help institutions evaluate access patterns and study potential new patterns of fraudulent behavior. Accordingly, a fraud detection solution must posses a powerful analytics engine to rapidly process the massive transaction volumes generated online. An effective fraud detection solution should have the capability to detect geolocation data, evaluate device information and analyze this data to detect transaction anomalies.

In addition, a fraud detection solution should offer the ability to share relevant information as part of an online fraud network between participating organizations. It is important to share more than typical fraud information (e.g., bad IP addresses, domains). The most effective way to address fraud today, and in the future, is to understand and share fraud behavior patterns. With an online fraud network, participating organizations should be able to seamlessly share fraud behaviors around the world in order to uncover fraud more rapidly. This collaboration through information sharing can help quickly identify emerging fraud tactics and help block their successful deployment on a global, rather than individual, basis.

Data masking, in which a customer's identity is protected by literally obscuring sensitive personal information such as account numbers on printed correspondence, is another key component in fraud prevention. While data masking is a decidedly low-tech element in a fraud prevention strategy, when used in conjunction with more advanced technologies such as fraud detection and multifactor authentication, it can play an important role in providing a layered defense against online fraud. And a layered approach to safeguarding customer information is the most effective strategy.

4.1 Fraud Detection Options

Although proven through many years of deployment for transactions like credit card payments, fraud detection systems for the online channel are relatively new. Based on these new systems, there are some key options for choosing a solution to effectively detect, defend and adapt to the ever-changing world of fraud. It is important that organizations consider each element carefully and choose a solution that can not only address today's concearns, but also tomorrow's potential needs.

Fraud Detection Elements	Description	Key Aspects
Architecture		
Onsite Software	• Physical deployment of fraud detection software on organization premise	• Requires deployment of software into enterprise environment • Typically J2EE or .NET based • Enables complete control over environment and maintains all data within enterprise boundary
Service Offering	• Fraud detection software remotely hosted	• No requirement to implement new software into enterprise • Requires that all data sent outside of the enterprise, which may have security and privacy implications
Deployment Options		
Non-Real Time	• Manual or automated reviewing of log files	• May provide rapid deployment option for post-transaction analysis with longer clearance periods • Even with log modification (change to application) may only cover a subset of all possible transactions • Non-real time removes ability to stop transactions at point of completion
Real-Time Online Monitoring External to Application • TAP/SPAN • Web Server Plug-in • Application Filter	• Ability to monitor all HTTP Web transactions in real time via external application	• Zero touch — no application changes required to see any real-time transaction data • No impact to application for sniffer and Web filter approaches • Application filter is inline to application, which may introduce risk to application reliability
Real-Time Online Monitoring Internal to Application • Direct call-outs	• Ability to monitor HTTP Web transactions in real time via internal application integration	• Extensive application modification to monitor specific transaction points • Cost and time intensive to deploy and maintain
Multichannel • Web • IVR/Voice • ATM	• Ability to monitor and incorporate transaction data from other channels beyond web into fraud detection process	• Data from voice, call center and ATM channels are natural considerations • Ideally suited for deployed software solutions (more difficult for service-based solutions)

Detection & Monitoring		
Pre-defined Rule Library • Categorized lists to address known fraud	• Included/available proven rules for addressing fraud	• Typically includes a range of proven rules for deployment • Tools should be included to easily create/modify new rules • May include ability to share rules with vendor and/or other organizations
Management Tools • Case management • Alerting	• Interface for day-to-day administration and management	• Typically a role-based tool available through the Web supporting case assignment and workflow • Includes user-specific views, such as known fraud incident status, current activities and new flagged items • Configurable alerting mechanisms, including e-mail and Web services notifications
Behavior Profiling	• Ability to characterize normal user behavior with goal of reducing false-positive alerting	• Typically associates transactions with behavior profiles for all users • More sophisticated systems track behavior for individual users • Should enable risk decisions based on deviation from normal behavior
Post-Transaction Analysis • Historical tracing of new types of fraud	• Capture and storage of all data elements for future analysis	• Primarily available via TAP/SPAN and Web filter integration due to comprehensive nature of data capture • Requires sophisticated capture and formatting of data for real-time storage and rapid retrieval and evaluation • Reporting tools should be included

5 Authentication and Fraud Detection: Better Together

Even now, advanced attacks are being mounted that can defeat many single-purpose security methods. As attackers adapt, organizations must stay one step ahead in order to maintain consumer trust in the online channel. This requires implementing additional safeguards to maintain the security of customer identities in the event an attack breaches one security layer.

In addition, regulations have given direction on how to safeguard consumers online. In the United States, for example, the FFIEC noted that single-factor authentication methods — notably simple usernames and passwords — did not offer enough protection for typical Internet-banking transactions. The result was the highly publicized guidance, requiring financial institutions under the jurisdiction of the FFIEC to implement enhanced safeguards for online banking customers by the end of 2006.

Beyond today, new mandates are expected to follow that will speak to concerns not currently addressed by legislation, such as guidelines from the SEC that will encompass, for example, brokerage houses, mutual fund companies and others. In addition, new types of legislation on the

horizon, including the "Red Flag[1]" identity theft regulations and the UK Faster Payment Initiative, represent the next security mandates for organizations to address.

A layered approach to safeguarding customer information can be the most effective strategy for protecting consumers and meeting past and future compliance mandates. With this approach, an integrated solution can be implemented to address security concerns today, with the ability to evolve and adapt to new realities in the future.

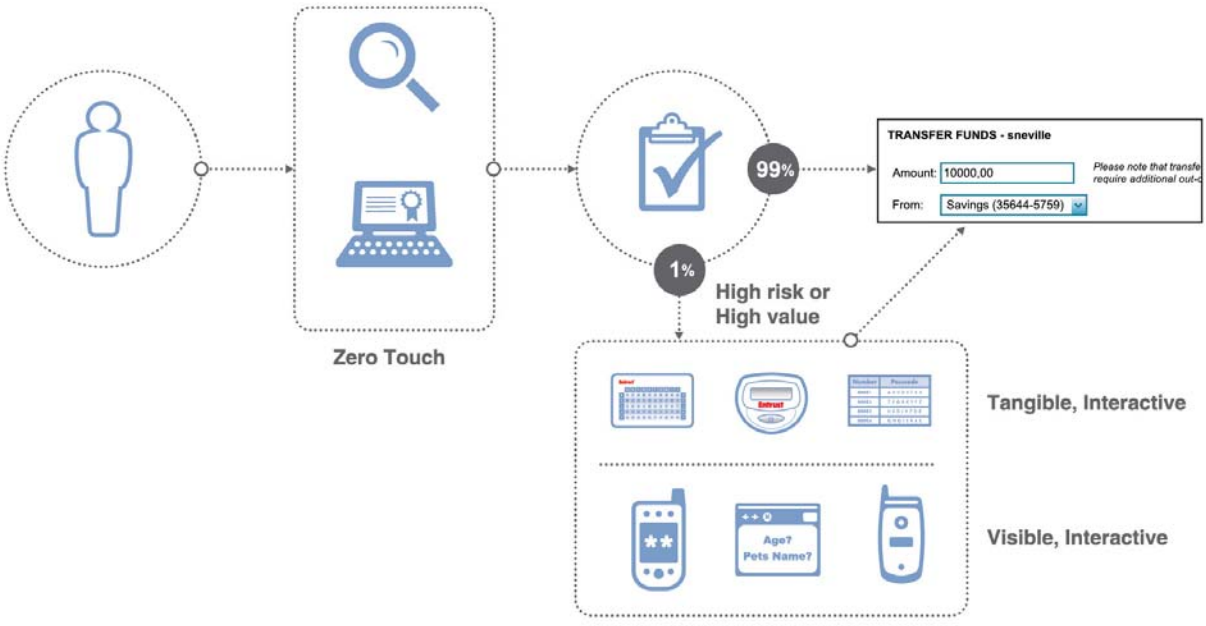
With an integrated approach, organizations have the flexibility to implement varying levels of security for a given application (as opposed to a one-size-fits-all approach) dependent on the type of risk (e.g., high-volume transaction, sensitive account information) involved.

As illustrated in Figure 1 below, there are multiple points where the risk of a user session should be assessed, as well as a range of options for layering versatile authentication onto the session to mitigate any risks that have been found.

Layered Security Examples:

- An Internet-banking application for viewing account balances may not require the use of stronger authentication if sensitive data has been appropriately masked. But, monitoring the behavior of users accessing this application could flag fraudulent behavior that can be dealt with post-transaction by a fraud analyst.
- Similarly, a brokerage or cash management application that allows transfers of large sums of money may require varying degrees of stronger authentication triggered by the value of the actual transaction. When combined with fraud detection capabilities, the ability to trigger stronger authentication based on risk can provide increased security without unnecessarily impacting users.

Figure 1: Layered security can help mitigate risk without being invasive



[1] A copy of the proposed Red Flag regulations can be found online at: http://www.entrust.com/legal/IdentityTheftRedFlagsJointNoticeProposedRulemakingNotice.pdf

It is important to note that the online channel is only one of the ways that organizations are interacting with customers today. Call centers (driven by interactive voice response (IVR) systems), ATMs and point-of-sale terminals all allow the end-user to interact in some way without physically being known. In many ways this is analogous to the online world and can benefit from a multichannel approach to layering security.

So, when examining options for fraud detection and authentication, organizations should look beyond the online channel to other interfaces. Telephone banking, typically driven by IVR systems, has been identified as a potential security vulnerability. Accordingly, authentication and fraud detection with IVR systems represent the next challenge for many organizations.

The key takeaway from the analysis is that organizations need to add security in layers and offer versatile authentication options, which will provide seamless security benefits that will deploy security factors based on types of activities, risk and fraud behaviors. The solution should have the ability to safeguard multiple channels, including telephone banking, and is architected in such a way that it can be adapted and applied in the future to protect additional channels such as voice or ATMs.

6 Solution Blueprint: Entrust Can Help

Entrust offers layered security through the Entrust Risk Based Authentication Solution, composed of real-time fraud detection provided by Entrust TransactionGuard, and strong authentication through Entrust IdentityGuard, an open, versatile authentication platform.

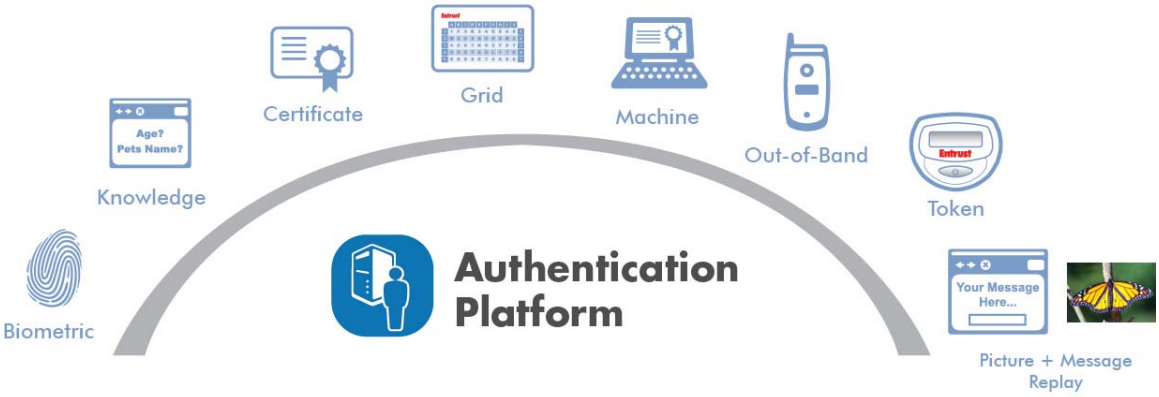
Complementing Entrust TransactionGuard, the Entrust Open Fraud Intelligence Network provides the ability to receive the latest fraud behavior information and best-of-breed IP data through a secure online network of participating organizations. Entrust TransactionGuard is modular and designed to be implemented rapidly with minimal adverse effects on the back-end application or end-user experience. This approach helps provide a smooth, hassle-free experience for organizations who seek to rapidly provide enhanced security to citizens, enterprise users or consumers.

Providing fraud detection, versatile authentication and an open fraud intelligence network enables a layered security strategy for better protecting consumers, enterprises and citizens. As a versatile authentication platform, Entrust IdentityGuard supports a variety of authentication methods including machine, knowledge-based, out-of-band one-time passcode, grid-based and time-synchronous tokens, along with mutual authentication to authenticate the Web site to the user. As an open authentication platform, it can be expanded and adapted to help security needs today and in the future. Entrust TransactionGuard provides real-time monitoring of transactions, passive detection of fraudulent activities, behavioral understanding of transaction patterns and non-invasive, user-notification methods.

6.1 Versatile Authentication Platform: Entrust® IdentityGuard

Entrust IdentityGuard is the authentication solution of choice for some of the world's leading financial institutions. Serving as a versatile authentication platform, it provides a range of strong authentication capabilities for improved confidence for both parties in an online transaction. These capabilities provide organizations the flexibility to help match the risk associated with the given transaction to the proper strength of authentication.

Figure 2: Versatile Authentication Options



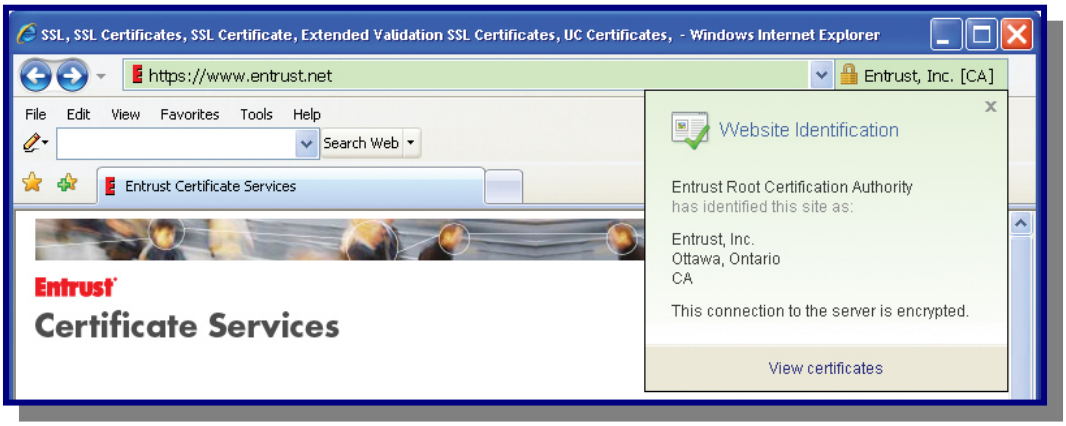
Entrust IdentityGuard offers a single point of administration regardless of the authentication option being used and can give organizations the ability to evolve and change authentication methods over time as risks and the operating environment change. This single point of administration also allows easy implementation into existing processes. Entrust IdentityGuard can layer on top of existing password infrastructures and can leverage current fraud detection capabilities, helping provide a low-risk deployment that can be completed in situations involving tight timelines. Integrated with leading enterprise-class applications, Entrust IdentityGuard leverages its standards-based approach to deployment to easily fit into any enterprise infrastructure.

Entrust IdentityGuard's range of easy-to-understand authentication methods have minimal impact on the user experience. Personalized and mutual authentication accelerates user acceptance and can help increase deployment success. For higher-value transactions, Entrust delivers intuitive and cost-effective options for second-factor authentication, including Entrust's patented grid authentication, as well as an extremely aggressively priced OATH one-time-passcode token — quantity one $5.

> "Enterprises that want one infrastructure for all types of users (whether or not they actually plan to deploy OTP tokens): Look for a VAS solution that supports and manages multiple authentication methods, provides dynamic policy-setting capabilities and can handle different authentication methods for the same user under different scenarios."
>
> *Gartner*
> *"Token Price Obscures the True Value of Entrust Offering"*
> *Ant Allan & Ray Wagner*
> *February 2, 2007*

A natural complement to Entrust IdentityGuard and a key component of a layered security strategy, Entrust Extended Validation SSL Certificates — commonly known as “EV” certificates — contain safeguards to help prevent fraud attacks (See Figure 3). When consumers use an EV SSL-aware, next-generation browser, the technology will help users make smarter decisions of trust, such as the ability to verify the identity information of the owner of an EV certificate-protected Web site.

Figure 3: Extended Validation (EV) Certificates provide a next-generation approach to addressing online attacks



6.2 Zero Touch Fraud Detection: Entrust® TransactionGuard

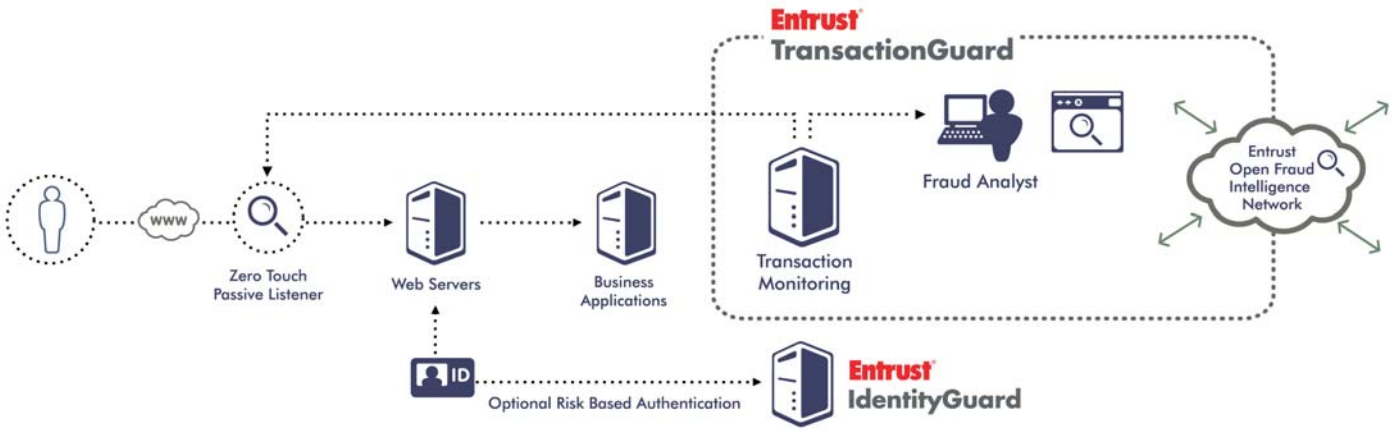
Entrust TransactionGuard can help protect online businesses with real-time transaction monitoring, passive detection of fraudulent activities, behavioral understanding of transaction patterns and non-invasive, user-notification methods.

Entrust TransactionGuard provides real-time fraud detection and comprehensive fraud analytics. This proven solution is ready for rapid deployment, requires no invasive integration with existing applications and does not impact the customer experience.

Entrust TransactionGuard transparently monitors user behavior to identify anomalies, then calculates the risk associated with a particular transaction — all seamlessly and in real-time. Unlike competitive offerings, Entrust TransactionGuard can analyze all points of interaction with the user on the Web site, allowing organizations to get a complete picture of potentially fraudulent behavior. Using customizable, pre-built fraud rules and business signatures, the solution can help identify anomalies such as: a user login from an unknown machine; a login from a risky IP address or location; a transfer of unusually large amounts to unknown accounts; or a change of personal information. The solution can also rapidly download and implement the latest defense against new behaviors from the Entrust Open Fraud Intelligence Network.

All analysis is done transparently, rapidly and does not require the application to be changed in any way or cause extra burden on the user. Reporting tools mine rich data sets and can help deliver key information to the right users in a timely manner. Importantly, Entrust TransactionGuard can be deployed in conjunction with not only Entrust solutions, but also additional third-party fraud offerings, delivering significant value to organizations looking to evaluate and understand all aspects of their online channel. This makes Entrust TransactionGuard complementary even to other fraud detection solutions on the market today, and provides a powerful tool to financial services organizations in the fight against fraud.

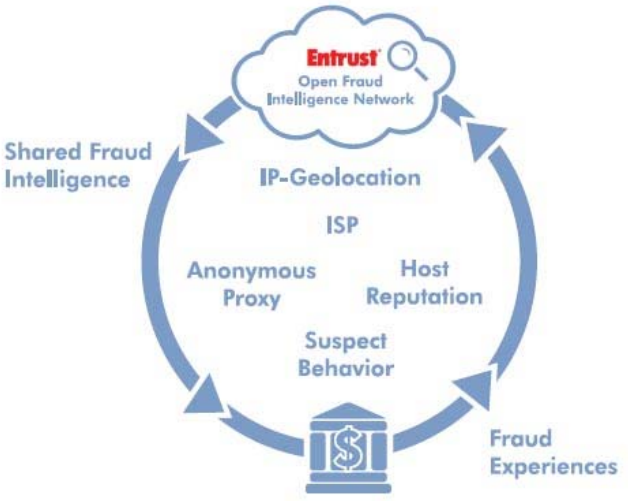
Figure 4: Entrust TransactionGuard — Zero Touch Fraud Detection & Analysis



Complementary to Entrust TransactionGuard, the Entrust Open Fraud Intelligence Network is an information-sharing service designed to help combat online fraud by consolidating and sharing key fraud behavior patterns and data among network participants. It is designed to provide participating members the latest fraud behaviors and tactics as well as key data for helping detect and combat fraud as it evolves.

The Entrust Open Fraud Intelligence Network is designed to provide rapid dissemination of data (e.g., IP-geolocation, anonymous and open proxy data, IP reputation) to help address impending fraud attacks as they evolve in real-time. Armed with this data, organizations will be more able to implement and respond to known and new types of fraud including man-in-the-middle and phishing attacks.

Unlike competitive offerings that provide a limited set of behavioral profiles and restricted ability to rapidly react to new fraud patterns, the Entrust Open Fraud Intelligence Network will help enable organizations understand new fraud patterns and implement solutions. Injecting the latest data and fraud behaviors into leading fraud detection products, including Entrust TransactionGuard, can help to more effectively address fraud. In addition, Entrust does not require participants to deploy proprietary software to be eligible to participate in and benefit from the network, and is working to bring a standardized sharing methodology to the industry through the IETF today.



7 Security Beyond Today

As the criminal element continues to evolve and adapt, the security measures that organizations implement need to include sophisticated, forward-thinking solutions to secure the online channel and protect consumers, enterprises and end-users. Entrust can help.

When addressing vital security requirements and regulatory compliance, organizations conducting online transactions need to consider a strong, layered security approach consisting of not only versatile authentication, but also real-time fraud detection coupled with an open fraud intelligence network. Following a layered approach can help provide a successful long-term strategy for protecting consumers, enterprise users and citizens. Deploying this tactic with the help of a single, experienced vendor will instill a synergy that embraces interoperability, efficiency and cost-effectiveness.

This close integration is part of Entrust's commitment to serving as a single security provider for best-of-breed tools in the fight against online criminals — both today and into the future.

Entrust's three security platforms — authentication, fraud monitoring and information protection — provide a diverse range of solutions to meet the needs of any security-conscious corporation, online retailer, enterprise or government agency. Whether it's a versatile authentication platform, fraud detection solutions or the support of an open fraud intelligence network, Entrust is the trusted, reliable vendor to implement security solutions for the challenges of today and tomorrow.

8 About Entrust

Entrust, Inc. [NASDAQ: ENTU] is a world leader in securing digital identities and information. More than 1,550 enterprises and government agencies in more than 60 countries rely on Entrust solutions to help secure the digital lives of their citizens, customers, employees and partners. Our proven software and services help customers achieve regulatory and corporate compliance, while turning security challenges such as identity theft and e-mail security into business opportunities.