Entrust Datacard™

Entrust IdentityGuard Adaptive Authentication

Transparent Authentication for Online and Mobile Channels

Digital Business has proven its value in both the workplace and the marketplace. Opportunities fueled by mobile and cloud offer great improvements. Digital services are becoming attractive targets to criminals as more and more services move online. Usernames and passwords are now insecure and frustrating to use, and strong authentication is necessary to keep information secure.

Traditional authentication methods, however, get in the way of business. The resulting challenge becomes discovering how to implement controls that delight customers with their ease-of-use, but disappoint hackers thanks to top-level security. The solution to the problem is transparent identity-based security that grants frictionless user access.

Delight Customers – Disappoint Hackers

Finding the right balance to secure online and mobile access can be challenging. Entrust IdentityGuard Adaptive Authentication provides an innovative approach to adding a new layer of security. Entrust IdentityGuard Adaptive Authentication can be added to either an existing username and password or a digital identity. Adaptive Authentication assesses a range of contextual attributes in real-time, and provides deep security and identity insights during login. Entrust IdentityGuard Adaptive Authentication is able to do this in a cost effective manner and without any involvement of the end user.

Utilizing Entrust IdentityGuard Adaptive Authentication leads to fewer step-up challenges, fewer help desk calls and reduces the number of fraudulent transactions typically seen online.

Deep Insight with Security Built Right Into Your Applications

Criminal attacks are becoming increasingly sophisticated and traditional device fingerprinting is no longer effective. Entrust IdentityGuard provides easy-to-deploy toolkits that provide an extensive device attribute collection, analysis and access context for both browser-based and mobile application based access.

Flexibility to Layer Additional Authentication As You Need It

Entrust IdentityGuard Adaptive Authentication can be augmented with rich capabilities to further secure mobile and online access. From mobile push authentication and user self-service—to out-of-band transaction verification and extending your identities' multiple channels and domains, Entrust IdentityGuard provides you a solution that will grow as your business needs evolve.

Entrust Datacard Local Partner

ELLIOTT DATA SYSTEMS, INC.

St. Louis, MO
17825 Edison Ave
Chesterfield, MO 63005
(636) 386-8400

Memphis, TN
5045 Covington Way
Memphis, TN 38134
(901) 372-4600

www.elliottdata.com

Solution Benefits

- Streamline the digital experience with transparent authentications
- Secure both mobile and online channels with single solution
- Reduce help desk calls by reducing when and how users are challenged with additional security verification
- Policy management that give you the control to tailor solution for individual applications
- Multi-dimensional analysis including device fingerprinting, time, geo-location and more
- Fully integrated to the Entrust IdentityGuard platform, providing you a turnkey authentication solutions
- Deploy at your pace – Adaptive Authentication can be added to your existing identity environment avoiding "rip and replace" scenarios

How It Works

Entrust has been providing Adaptive Authentication solutions for the past decade with Entrust IdentityGuard. A number of enhancements have been made to help realize a new, fully comprehensive Adaptive Authentication solution.

The diagram below illustrates the vision for the Entrust IdentityGuard Adaptive Authentication solution. The solution is equipped to handle a broad array of inputs: device fingerprint, device reputation, user behavior and others, from which, authentication decisions can be made based on granular customer defined policy settings.

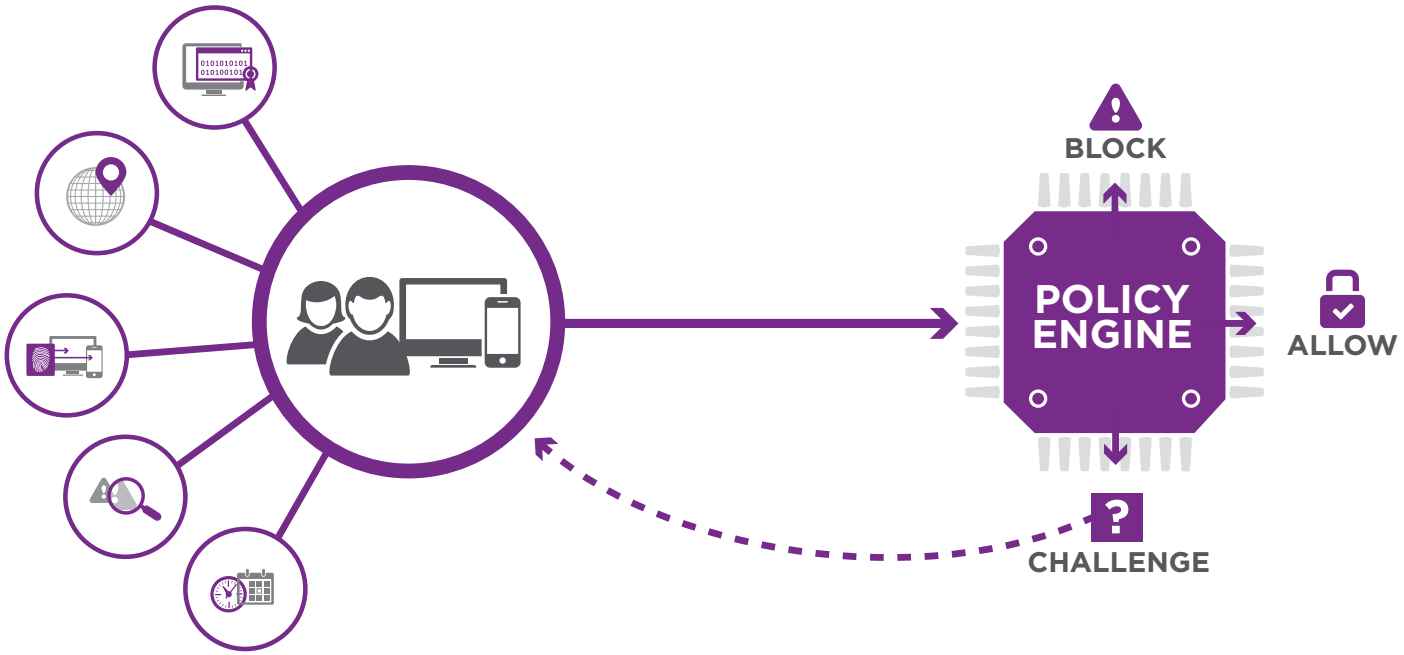
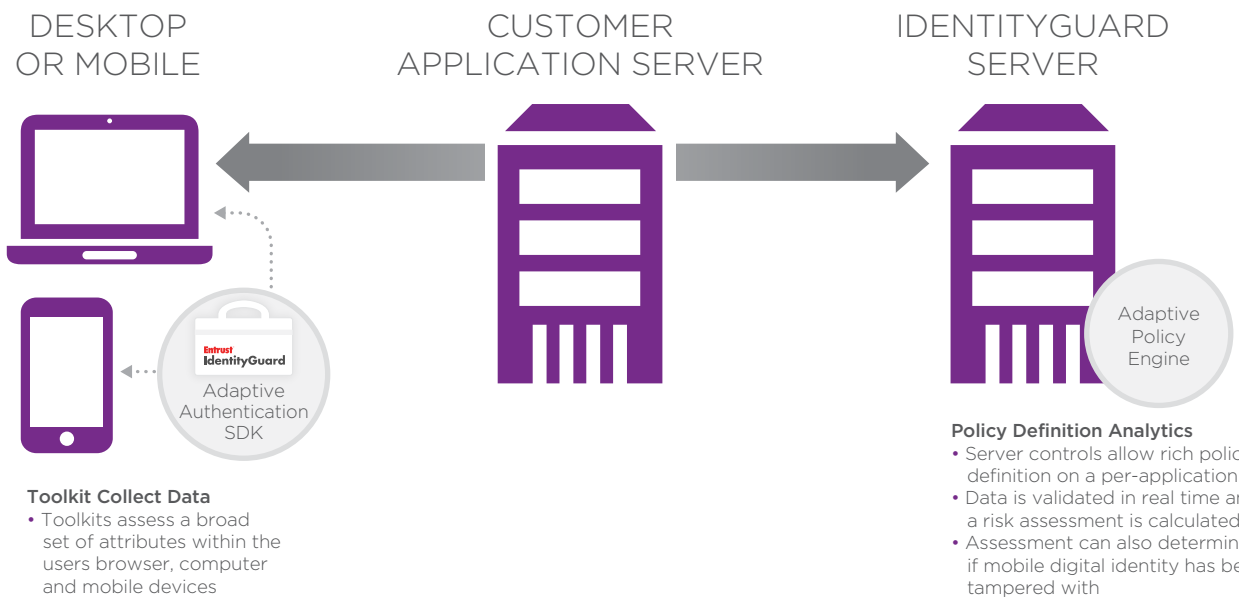


Figure 1 Adaptive Authentication can assess a range of contextual information including external risk scores to affirm the user identity. Once all attributes are assessed, the user will be allowed, blocked or issued an authentication challenge.

Entrust IdentityGuard Adaptive Authentication moves away from the persistent storage of session data in web browsers and simple device assessment. We provide two Device Fingerprinting Software Development Kits (SDKs), one for web access and one for mobile applications, both of which are required in today's world.

When a user accesses the website / application, the device and access context is assessed in real-time, validated if the contextual analysis passes and the user is logged in to the application. If the level of risk exceeds defined thresholds, the user can be challenged in a number of different ways



Toolkit Collect Data

- Toolkits assess a broad set of attributes within the users browser, computer and mobile devices

Policy Definition Analytics

- Server controls allow rich policy definition on a per-application basis
- Data is validated in real time and a risk assessment is calculated
- Assessment can also determine if mobile digital identity has been tampered with

On the server side, the solution provides rich policy controls that both define the device parameters which are to be collected and provide the flexibility to assign weighting to each parameter. The weighting allows you to design a finely tuned authentication methodology on a per application basis.

Geolocation parameters can be assessed and balanced against a number of checks including:

- IP Address - is the IP address black-listed?
- Expected Location – is the user expected to authenticate from this location?
- Location History – has the user authenticated from this location previously?
- Velocity – has the user authenticated from previous locations in a time frame that is inconsistent with the distance between the locations?
- External risk score - import user / session-risk score from external fraud detection / behavioural analysis.

Flexibility and Additional Layers of Security

Entrust IdentityGuard allows the customer to collect additional data through a modification to the Entrust IdentityGuard Device Fingerprinting SDKs.

The customer has the ability to weight aspects of device's digital fingerprint in computing the risk score. In mobile, OTP and PKI SDK can be used to augment security, and convenience can be improved with additional controls on the device side (i.e. using the user's fingerprint [TouchID]).

When it comes time to challenge the user, we offer the broadest choice of authentication methods so you can tailor your solution to meet your users' and line of business' specific needs.

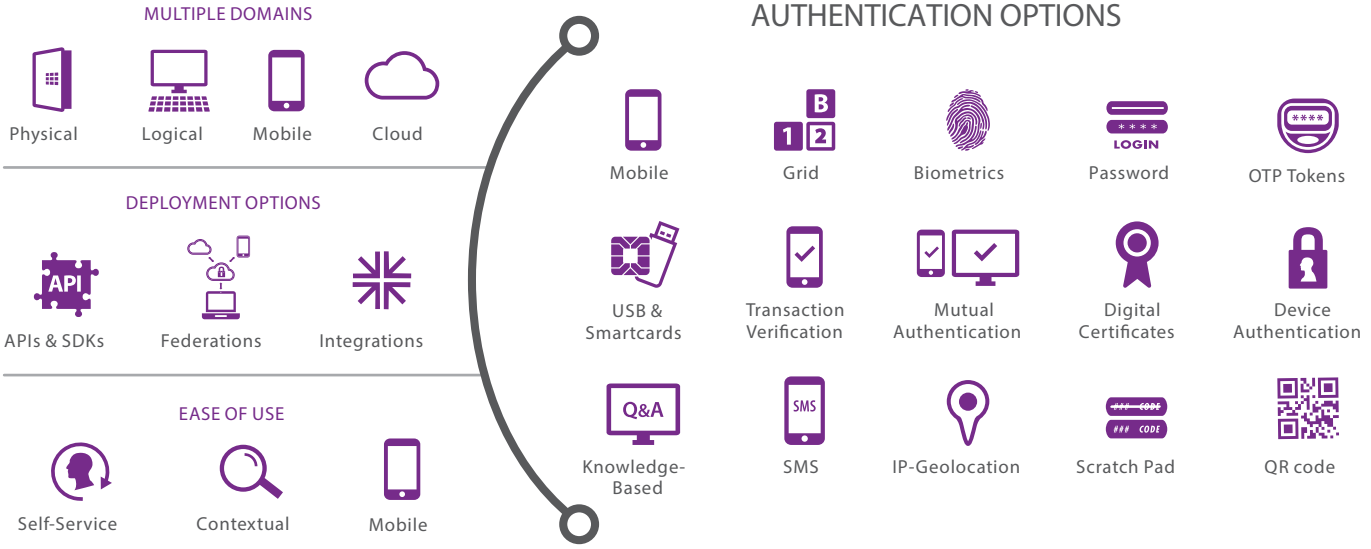
Entrust IdentityGuard Adaptive Authentication

Transparent Authentication for Online and Mobile Channels

Entrust IdentityGuard: The Flexible Authentication Platform

Entrust IdentityGuard is a next-generation identity-based security framework that serves as the foundation for your current and evolving digital identity needs. With rich, contextual policy management, security can automatically adapt according to access requirements or the risk in a given transaction, across diverse users and applications.

Entrust's software authentication platform does not impact normal user behavior or back-end applications, speeding deployment and helping to save money. Entrust IdentityGuard affords the flexibility for specific authenticators to be defined per application and/or group so you can tailor your security to the use case and risk situation. Simple policy change can seamlessly adjust the authentication behavior of all applications virtually instantly and without have to re-architect applications, giving you the flexibility to protect what matters most proactively.



Software Authentication Platform

Entrust's management framework is unique in the market and drives significant value for today's connected enterprise. The solution enables organizations to deploy strong, risk-based authentication to properly secure employee access, privileged user accounts and even customer and partner access to company portals.

- Deploys to a single server
- Co-deploy with existing authentication solutions for smooth migration
- Simple integration and easy-to-use APIs
- Mobile, physical and logical authentication
- Federate internal and cloud-based applications (e.g., Salesforce.com, Microsoft 365)
- Reduce cost and maximize staff efficiency with an intuitive self-service module

About Entrust Datacard

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

Entrust Datacard™

30116-1-1115