BLUE HILL
RESEARCH

ANATOMY OF A DECISION

Selection of Entrust IdentityGuard OnPremise as an Authentication Platform Solution

Published: November 2016 **Report Number:** A0259

Analyst: Dr. Alea Fairchild, Entrepreneur-in-Residence, Security Research

Share This Report

What You Need To Know

Authentication technologies not only provide the best way for organizations to protect themselves from attacks, but also give the ability for organizations to seamlessly enable digital business. IT departments are now shifting their focus to mobile and cloud capabilities, and are expected to provide a secure and efficient ecosystem for partners, networks, and personnel to both rapidly and accurately authenticate the identities of users and their devices without sacrificing user experience. But using only a simple identifier such as a password is too vulnerable of an approach, and compromised credentials are one of the primary causes of serious and costly security breaches.

On the other end of complexity, traditional two-factor authentication (2FA) has a significant total cost of ownership (TCO) and is known to frustrate users. The myriad of applications, combined with remote and mobile workers who bring mobile devices (BYOD) is accelerating the authentication problem.

Entrust Datacard offers a robust authentication platform that includes a breadth of capabilities, a range of assurance levels, mobile innovation, and a choice of deployment models such as on-premise, virtual appliance, and cloud.

In this Anatomy of a Decision, Blue Hill spoke with two enterprises who have chosen Entrust Datacard as an authentication solution to understand the need that was not being met by other authentication vendors, the selection process leading to EntrustDatacard or to upgrading to Entrust IdentityGuard 11, the value that Entrust Datacard was expected to provide, the value that has actually been realized to date, and next steps for each Entrust Datacard customer in facing future authentication challenges.

In order to assist organizations with this evaluation process, this report identifies key drivers, solution evaluation factors, and performance impact that drove two organizations to select Entrust's IdentityGuard platform to provide authentication management in a data-sensitive workspace.

AT A GLANCE

About This Report

This report examines the decision-making processes that led customers to choose Entrust Datacard's authentication solution.

Solution Selected

Entrust IdentityGuard –
On-Premise

Impact of the Solution

- Efficiency of customer support
- Reliability of platform solution

Investment Drivers

- Volume of users exponentially growing
- Multifactor authentication required for solutions supported

Core Investment Drivers

The need for an authentication platform that automates the process and provides the structure to better manage risk is driven by trends towards leaner IT staffing, an increasing number of people remotely accessing networks and applications with mobile devices, and a plethora of security and authentication alerts needing to be addressed in a rapid manner.

Key contributors to these challenges include:

- A need for flexibility in implementation, given the use of different devices and platforms at different levels of the organization
- Scalability, given the number of users involved and the ease of use for a user to be authenticated
- Quick responsiveness to authentication problems, as the users require rapid access to the applications involved

> “Entrust Datacard allowed us rapid recovery when there is an issue regardless of time of day. Certificate had expired and together with the team at Entrust Datacard, we identified the problem in off hours and sorted the user out so they could log back into the application.”
>
> *Security Administrator*
> *National Network of Local Health and Human Services Providers*

Another main driver was the need for reliable multi-factor authentication (MFA). Entrust IdentityGuard leverages multiple methods including one-time password tokens, grid cards, and digital certificates; knowledge-based authentication, including personal identification numbers; and adaptive authentication, which includes IP geolocation and device-based authentication.

One of the participants is developing and implementing the provincial Electronic Health Record (EHR) throughout a province in Canada. The EHR is a secure health information-sharing network used by healthcare providers to improve patient care. The participant had a two to three-month timeframe for their solution decision; the slowest part of the decision process was internal, as the Entrust Datacard implementation team was quite responsive. Their decision was made with their technical team and a quick demo from sales that had a strong impact. The rationale for the decision was the choice of platform options and the range of authentication choices. Two-factor authentication (2FA) was a major factor in their decision, as was the flexibility in choice for repository (own or external reporting).

Entrust IdentityGuard is so well-accepted in their organization on the patient/provider side that in future implementations, they will be replacing their corporate solution (RSA) with the Entrust Datacard authentication solution.

Overall, the profiled organizations shared a common concern with having a variety of authentication options (e.g. mobile token, 2FA) to choose from, and considering a stable platform with excellent customer support mandatory.

Solution Evaluation and Selection

Why implement an automated authentication platform? Blue Hill identified four factors used in the evaluation of these solutions, reported among participants:

- Choice of authentication technology solution (hardware, software, mobile-enabled, etc.)
- Ease of use for user authentication
- Responsiveness and quality of customer support
- Solution cost and ease of maintaining solution

Overall, the participants reported that that Entrust IdentityGuard was the only solution considered that provided the mix of functionality sought. The solution's identified ease of use also contributed a top factor in determining selection. The profiled organizations reported that the customer support was attractive both for the ability to rapidly assist users but also to save costs on internal helpdesk support resources.

Table 1: Evaluation of Entrust IdentityGuard

	Entrust IdentityGuard	Other Options Considered / Previous Solutions
Scope of Capabilities	• Provided "exactly" the mix of multi-factor authentication capabilities needed to support policy • Flexible on repository choices (own or external reporting such as Active Directory)	• Solutions did not provide future implementations such as mobile tokens • Other solutions were not fully implementable as needed now, lacked certain aspects such as two-factor authentication as an option
Ease of Use	• User interface found to be intuitive and easy to use • Users proved quick to accept it	• Opinions varied on existing solutions but participants felt that they were not as user-friendly as Entrust IdentityGuard • Previous solutions either not fully implemented or cost effective
Customer Support	• "Very good" • Highly responsive with demonstrated willingness to partner with clients	• No observations discussed
Solution Cost	• Pricing competitive with other options considered • Help-desk cost reduction with self-service module, reduction of burden on helpdesk resources	• Prices varied, with most options considered within acceptable ranges

Source: Blue Hill Research, November 2016

Solution Impact Reported

The two organizations participating in this research selected Entrust IdentityGuard to provide a flexible and multimodal use of authentication technologies. One of the participants selected Entrust IdentityGuard to improve the range of authentication choices (mobile token, one-time password, etc.). In each case, the primary benefits identified by the participants related to three major areas of value:

- Reduction of cost due to self-service module
- Speed of implementation and ease of maintenance
- Continuity and responsiveness of customer support team

> Entrust IdentityGuard is a 'rock-stable' solution. The only mistake to make with it is to ignore the solution for too long as it is so stable or to not take advantage of all the features and functions it provides.
>
> *Security Administrator*

While the participants identified various aspects of the solution as contributors to the value provided by Entrust IdentityGuard, these factors ultimately result from a fundamental shift in how flexible they were in both configuration and maintenance of the authentication solution.

Blue Hill thus advises organizations to pay particular attention to the commonality of multi-factor authentication approaches at each company regardless of overall deployment size and maturity level differences. Although authentication is critical in handling sensitive data and its utilization amongst users, authentication also needs to play a role in their networks delivering extraordinary end user experiences. Based on this analysis, organizations confronted with complex sets of users and networks should consider multi-factor authentication as a must for their authentication platform, and remember that the growth of mobile device usage will play an increasing role in authentication technologies.

Conclusions

We have examined in this Anatomy of a Decision the choices Entrust Datacard customers have made to define an ecosystem that uses today's state-of-the-art authentication technology by enhancing their technology option choices to provide a more robust security profile. The goal is to create authentication deployments that are rigorous, highly cost-efficient, and willingly used by network partners and service providers that protect the sensitive data of consumers.

As these participants are both healthcare business models with both sensitive information and strong regulatory compliance issues, it is evident that the resulting efficiency in authentication has improved user attitude towards using authentication technologies and improved trust in the respective networks.

Key Observations and Takeaways

Entrust's IdentityGuard platform represents an example of a robust authentication solution platform with an excellent reputation for customer support allowing participants to reduce cost and increase user trust and satisfaction. The more sensitive the data is, the higher the priority must be on the robustness and security of the solution. In these two cases, the participants were handling sensitive health care data across a network of multiple participants. Doctors, nurses, and administrators accessing EHR records have a regulatory need to utilize compliant 2FA software for electronic prescription of controlled substances, for example. Ease of use of authentication is vitally important as healthcare providers and facilitators can become increasingly frustrated by the need to use complicated passwords, tokens, cards or other cumbersome forms of authentication to log into their EHR system. Evolving business needs around these kinds of applications, use of the cloud and mobile devices, combined with rising threats, and the need to reduce costs, require multiple considerations for access control. Multi-factor authentication serves a vital function within any organization by securing access to corporate networks, which protects the identities of users and their sensitive data.

> “We use this in our consumer network, and we intend to replace our corporate authentication solution in future with IdentityGuard due to its 2FA implementation.”
>
> *Solution Architect*
> *Healthcare Service Provider*

With a wide variety of access control offerings available today, it is important for organizations to carefully evaluate the available solutions before making a decision on which solution to implement. When choosing a solution, organizations should take a number of factors into account, including: the cost of supporting the platform, the scalability of the solution, the number of authentication technologies it supports, and the reliability of the platform to make the users more confident and trusting in authentication as an activity.

Implementing Entrust IdentityGuard as an authentication platform, with its multi-factor authentication and excellent customer support is, in Blue Hill Research’s considered opinion, the best way to effectively enable superior network authentication in this rapidly-Smobilizing multi-enterprise world.

BLUE HILL
RESEARCH

ABOUT THE AUTHOR

Dr. Alea Fairchild

Entrepreneur-in-Residence

Dr. Alea Fairchild is an Entrepreneur-in-Residence at Blue Hill Research. Alea covers the convergence of technology in the cloud, mobile, and social spaces, and helps global enterprises understand the competitive marketplace and to profit from digital process redesign. She has expertise in the following industries: industrial automation, computer/networking, telecom, financial services, media, transport logistics, and manufacturing. Her clients are both commercial, government / public sector, NGO and trade associations. Dr. Fairchild received her Ph.D in Applied Economics from Limburgs Universitair Centrum (now Univ. Hasselt) in Belgium, in banking and technology. She has a Masters degree in International Management from Boston University/Vrije Universiteit Brussel, Brussels, Belgium, and a Bachelors degree in Business Management and Marketing from Cornell University. She is a masters Olympic weightlifter for Belgium, having won many international medals.

CONNECT ON SOCIAL MEDIA

@AFairch

linkedin.com/in/aleafairchild

bluehillresearch.com/author/alea-fairchild

For further information or questions, please contact us:

Phone: +1 (617) 624-3400
Fax: +1 (617) 367-4210

Twitter: @BlueHillBoston
LinkedIn: linkedin.com/company/blue-hill-research
Contact Research: research@bluehillresearch.com

Blue Hill Research offers independent research and advisory services for the enterprise technology market. Our domain expertise helps **end users** procure the right technologies to optimize business outcomes, **technology vendors** design product and marketing strategy to achieve greater client value, and **private investors** to conduct due diligence and make better informed investments.