VASCO
THE AUTHENTICATION COMPANY

Taking a Risk-Based Authentication Approach to Financial Fraud Protection

By David Strom

Table of Contents

Executive Summary

On the Internet, the bad guys are sadly winning the war against banks and other financial institutions. Cybercriminals are becoming more sophisticated, deploying blended threats against banking and payment networks, and using multiple access methods to steal money. Their market share is increasing too. This isn't good news for legitimate businesses that want to stop money laundering, e-commerce threats, account takeovers, pre-paid debit card abuse and other online banking exploits.

Two-factor exploits (such as Emmental*) have also grown, making three or more factor methods more important. And as more banking is done using mobile applications, institutions are faced with more challenging security requirements as customers can authenticate and conduct their business from anywhere and with any device.

This paper will describe these problems and how using a risk-based authentication approach can protect the entire lifecycle of banking activities as well as satisfy the needs of users for convenient and transparent access to their accounts.

www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-finding-holes-operation-emmental.pdf

Introduction to stronger authentication methods

The notion of using stronger authentication tools, such as multiple factors, has a long history, indeed predating the Web itself. Some of you probably remember the biometric whole-hand scanners that secured many a data center entry point as your first brush with these sorts of devices. This continues today with a variety of other biometric devices including voiceprints and fingerprints exploiting the latest smartphone-based sensors.

Today, there are dozens of vendors who offer one-time password tokens of various shapes and formats. This includes some very clever software-based tokens that run on smartphones, such as ones that recognize QR codes and send SMS texts. Numerous consumer companies such as Google, Apple, Twitter, Facebook and LinkedIn are using multifactor tools to help strengthen their users' logins.

That's a terrific start, but somewhat cumbersome, mainly because users don't always like to use these tokens, even if they are clever solutions. Tokens do get in the way of the actual transaction itself. IT staffs tolerate tokens but they do require a fair amount of programming effort to integrate into their existing systems. Tokens have their limitations and typically only address a single access threat vector. For example, some systems are great at protecting e-commerce connections but don't handle remote connections to in-house systems or pre-paid debit card exploits.

This is why multifactor methods are evolving to handle better security methods.
But before we talk about that, let's look at today's threat landscape.

Responses to today's threat landscape

Financial institutions are tremendous targets of opportunity; after all, they have lots of assets that are ripe for electronic thievery. There are four trends we've observed in how they respond to current threats:

The rise of non-traditional threat vectors

Blended threats, improvements to man-in-the-middle exploit kits, and other advances in malware have made threats more numerous and more available to less-skilled cybercriminals. It used to be that exploits that collected credit card data were common: now there are numerous threats that are entering the banking networks from other sources.

Regulations haven't kept up with exploits in some countries

As these exploits have blossomed, regulators have struggled to figure out best practice recommendations. Europe is better at this than the US here. For example, while the US Federal Financial Institutions Examination Council regulations require banks to use stronger, two-factor authentication mechanisms, it doesn't go far enough. According to Gartner, there are no standards specific to adaptive access control. However, there are relevant standards that would be used as the building blocks for an adaptive access control solution[1] . Payment Card Initiatives and other banking regulations are a great first start, they haven't kept up with the growing all-cash economies in the third world, the explosion of digital currencies such as Bitcoin that make tracking payments nearly impossible, and global gangs that effortlessly move money across continents within nanoseconds.

Too many security tools, too little integration

Banks have purchased different systems to manage the different risks. While this means they are great at consuming security tools, the result is they have too many different ones that don't necessarily integrate or work well with each other. For example, many of the early risk-based authentication methods are focused on cloud or Web-based services and don't work with Windows or local network logins. Banks typically have had different fraud prevention departments and used different tools for each type of exploit. So there are solutions for ecommerce prevention, but these don't work in any other context.

1 Gartner Technology Overview for Adaptive Access Control, Ant Allan, 29 May 2014

Responses to today's threat landscape

Limited analytics

Tracking the actual effects of all kinds of fraud has been almost non-existent. Network intrusion devices are woefully outdated or improperly deployed, and have focused on incoming attacks rather than outgoing ones. Few tools can provide a total coherent view to the satisfaction of an IT security manager, such as tracking unusual account activity or frequent withdrawals. Many tools have focused on end-user behavior, rather than monitoring criminal activities.

What are the risks?

Given all these threats, fraud continues to increase, even as payment volumes stay relatively level. Today's banks have three potential areas for exposure to these criminals:

Monetary losses

Once funds leave the customer's account, the bank usually has to make good on the fraudulent transaction. Given these losses, revenue preservation should be a top priority.

Regulatory costs

Increasingly, financial services regulators levy stiff fines for security breaches or leaking customer information. Once an institution becomes a target, there are additional lawsuits and counter-claims by the injured parties. With record fines being imposed by regulators and officers of the company in many jurisdictions being criminally culpable, enterprise security managers need better mechanisms to assure compliance.

Institutional reputation

How often has the Target Corp. been a go-to word in the past year as the poster child of security missteps? Having been the, ahem, target of such a well-known attack can take time to reclaim one's business reputation and competitive advantage.

Most people have more than 25 online accounts for shopping, storage, subscriptions, banking, gaming and social media.

Introducing risk-based authentication methods

These areas of exposure mean that financial institutions have to step up their security game. For example, “the best-practice approach is encapsulated in an architectural principle that Gartner calls ‘risk-appropriate authentication’. An organization must consider multiple use cases and, for each, evaluate minimum levels of assurance and accountability, commensurate with the level of risk.”[2]

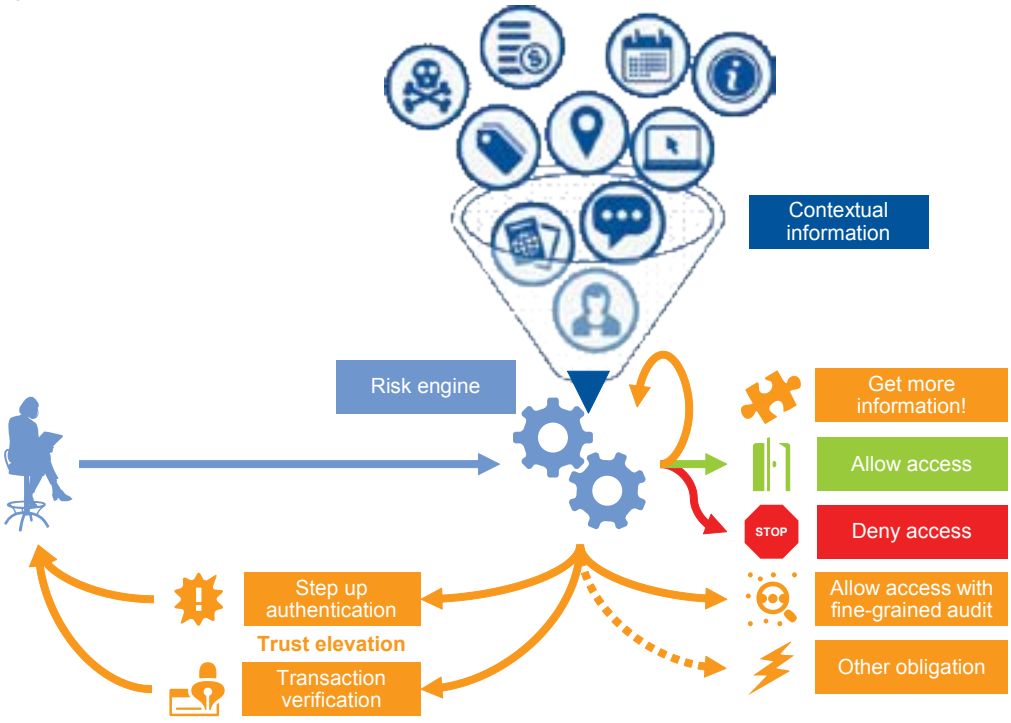
This means that stronger authentication methods are needed to stop attackers before they even enter your networks or get to a login page. This is variously called risk-based authentication, context-aware or adaptive access controls. For the purposes of this paper, we will use risk-based authentication (RBA) as the descriptor for the category of these products.

2 Computer Weekly http://www.computerweekly.com

Introducing risk-based authentication methods

What is RBA, exactly? The idea is to base any access decisions on a dynamic series of circumstances. These count as the additional authentication factor, rather than rely on a particular set of tokens or pieces of smartphone software. Access to a particular business application goes through a series of trust hurdles, with riskier applications requiring more security so that users don't necessarily even know that their logins are being vetted more carefully. Moreover, this all happens in real time, just like the typical multifactor methods.

Figure 1. Adaptive Access Control



Source: Gartner (May 2014)

Adaptive access control is an instance of context-aware access control consuming contextual information about the user, endpoint, transaction, asset and so on to make a dynamic risk-based access decision and acting to ensure a level of trust commensurate with the risk indicated by an analysis of current conditions at the moment of access[3] .

3 Gartner Technology Overview for Adaptive Access Control, Ant Allan, 29 May 2014

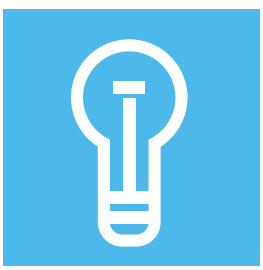
The risk-based tools work silently, in the background, to collect and score a login based on a series of quantifiable metrics (see diagram on next page). This is similar to how many of the next-generation firewalls operate with their own risk scoring tools of internal network packet behavior. RBA tools use elements such as:

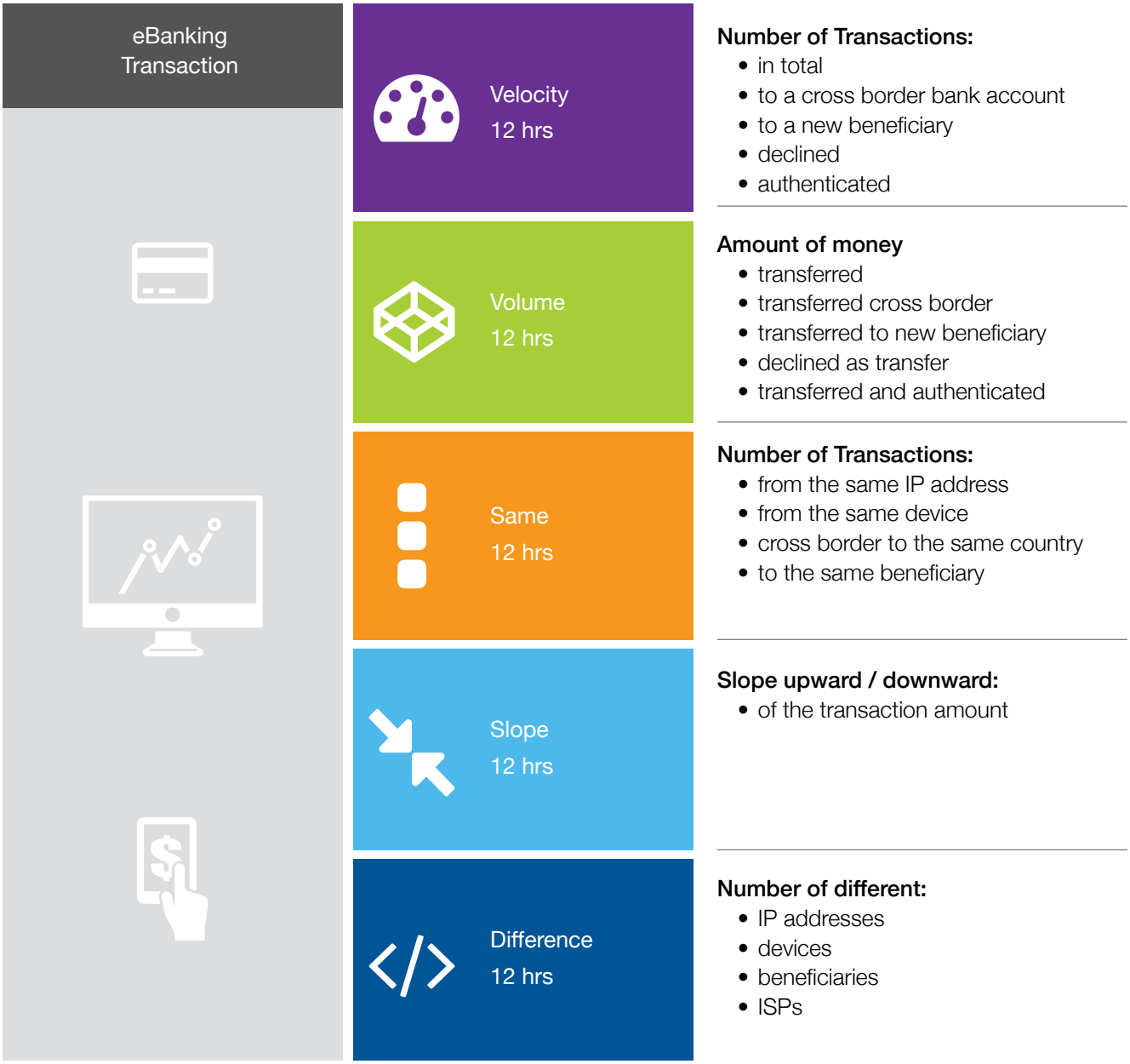
• **Role-based**. Is the user a member of any privileged class, such as network administrators or account supervisors? If so, they need to pass a more stringent authentication dialog.

• **Location-based,** either by detecting the physical endpoint or specific geographic location. For example, if the user logged in ten minutes ago from Canada and is now trying to log in from China, it's definitely considered a higher risk transaction. Other attributes can figure into the overall risk score too.

• **Activity-based,** such as large value account transfers have a higher risk associated than just a balance inquiry.

• **Changes in usual transaction patterns.** If a user is doing something that doesn't match his or her purchase history, that becomes a riskier transaction so that authentication requests and logins can be challenged with an additional authentication measure. There are various ways to measure these changes, as shown below, including the velocity of transactions, whether the rate is increasing or decreasing, and the monetary amounts that are covered with each transaction. The more sophisticated RBA tools can incorporate these different measurements. This means that challenging unusual spending patterns creates a barrier that a hacker or fraudster cannot easily circumvent, while not doing the customer the disservice of demanding such authentication in a blanket manner.





Like multifactor methods, these risk-based tools make use of out-of-band authentication methods to eliminate potential man-in-the-middle attacks and phishing exploits. But unlike multifactor methods, they make use of finer-grained authorization methods, again depending on the particular business application or use case.

The business benefits of RBA

By the end of 2016, 50% of large enterprises will employ adaptive access control, primarily in workforce and partner remote access use cases, up from less than 5% today[4]. That could be the case, given the velocity of exploits seen in the financial and retail sectors and the number of vendors who already have some kind of offering in the marketplace. Let's look at some of the real business benefits that RBA can bring to financial institutions.

Overall risk reduction

Because risk-based authentication adapts to particular circumstances, it can reduce overall fraudulent activities.

Better user experience and adoption

Using more flexible and escalating higher-trust authentication methods makes it easier for users to get their legitimate banking needs taken care of without onerous authentication dialogs. Users are prompted for higher-risk methods only when these are needed, such as for wiring funds.

Better mobile device support

Since mobile devices can be lost or stolen, having adaptive controls on authentication can be used to determine context and usage to provide better security here. Devices can be scored based on a particular combination of circumstances, so if a user is connecting from a different city or country, this increases risk and asks the user for a more secure login with a software-based two-factor token as an example.

Easier to use and deploy

Unlike older multifactor methods, there is little to no end-user software to deploy and less systems integration on the server-side as well. End-users don't have to mess around with hardware tokens and there can be fewer help-desk calls. This means faster time to market and a more nimble security solution too.

Improved compliance

Using risk-based authentication can keep an organization at higher compliance as standards are improved and are refined.

4 Gartner Technology Overview for Adaptive Access Control, Ant Allan, 29 May 2014

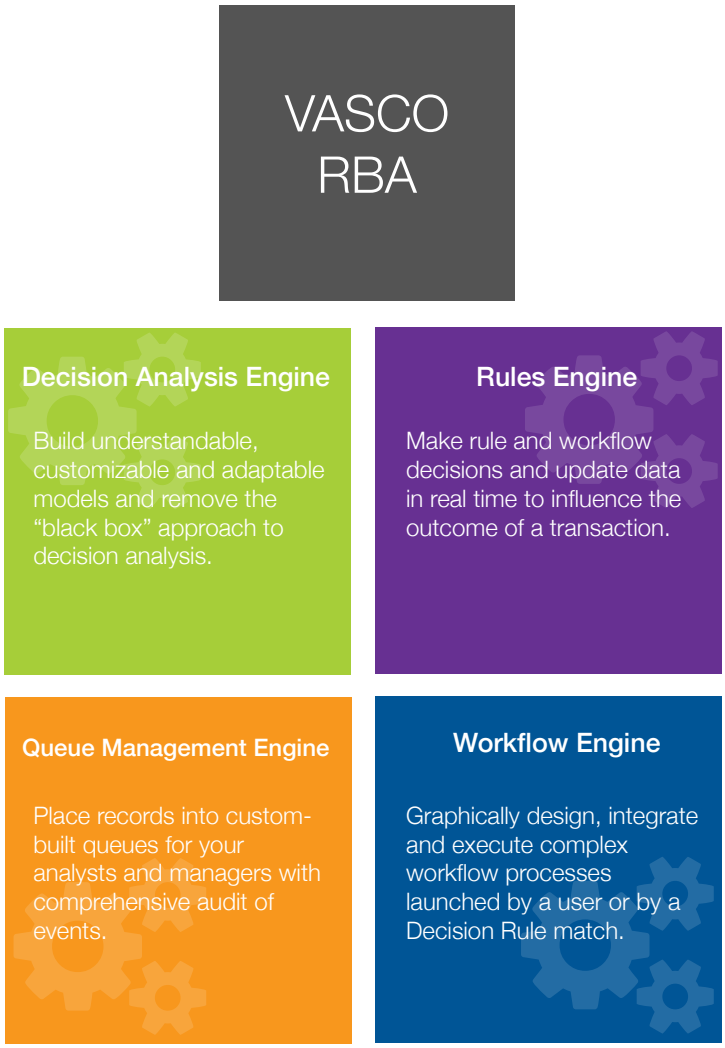
How VASCO's RBA solution stacks up

VASCO of course has its own RBA product that works to supplement its existing multifactor software DIGIPASS and IDENTIKEY with step-up authentication that matches the risk level of the potential login with a wide variety of assessment tools. Non-IT staffers can manage it with an intuitive interface. Administrators can easily create powerful security policy rules and quickly set up custom workflows, without an enterprise having to pay for a lot of custom support services or specialized programming. And it handles multiple threat vectors and authentication channels with ease as well as scoring the relative risk of particular transactions.

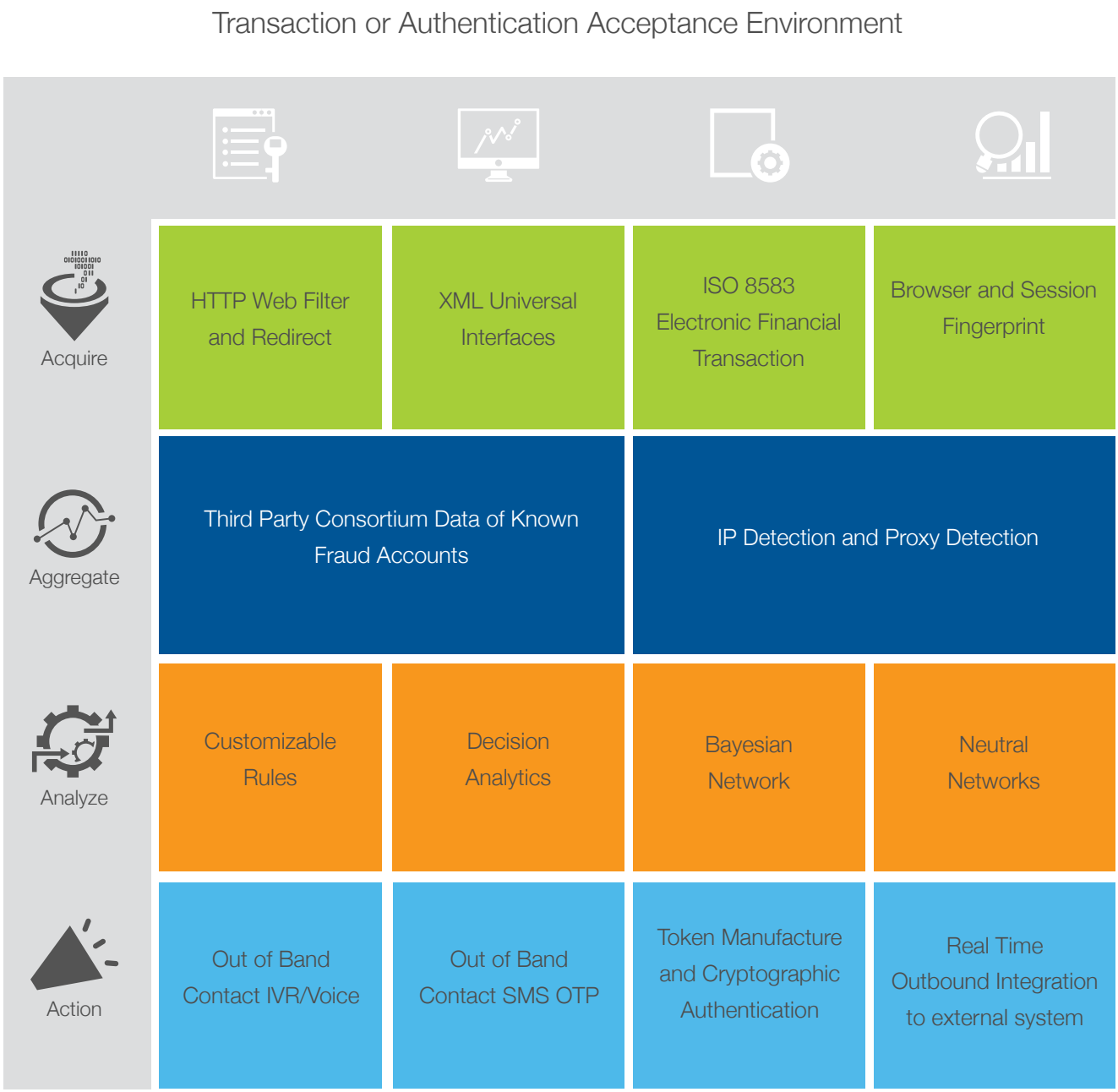
Its goal is to improve control over the entire customer lifecycle of Web and mobile applications, including customer onboarding, Web and mobile application login, Web and mobile financial transactions, and a broad variety of non-monetary events.

VASCO's RBA can be installed either on-premises or in a managed services cloud environment, thus providing tremendous flexibility.

VASCO's RBA comes with four different decision analysis engines to help score and analyze each authentication threat. (See diagram below.)



In addition to these four engines, there are a variety of analytical routines that produce the risk scores, including ones that aggregate information from a variety of sources, compare this information to known standards, and other efforts as shown in the diagram below. For example, VASCO's RBA can compare the geolocation information collected from various sources to determine if the user is authentic.



Conclusion

Financial organizations continue to experience sophisticated and complex cyber attacks from well-organized and well-funded criminal organizations, threatening both business opportunity and brand reputation. And as more of their customers prefer to do their banking via mobile-based transactions, banking applications are increasing at risk. Stay one step ahead of advanced threats while delivering a seamless user experience with VASCO's RBA. VASCO protects more than half of the Top 100 global banks and its RBA solution has the flexibility to work across multiple threat vectors and multiple authentication channels. For more information on VASCO solutions, please visit www.vasco.com.

About VASCO

VASCO is the world leader in providing two-factor authentication and digital signature solutions to financial institutions. More than half of the Top 100 global banks rely on VASCO solutions to enhance security, protect mobile applications and meet regulatory requirements. VASCO also secures access to data and applications in the cloud, and provides tools for application developers to easily integrate security functions into their web-based and mobile applications. VASCO enables more than 10,000 customers in 100 countries to secure access, manage identities, verify transactions, and protect assets across financial, enterprise, E-commerce, government and healthcare markets.

Learn more about VASCO at www.vasco.com or visit www.blog.vasco.com

About David Strom

David Strom (@dstrom, strominator.com) is one of the leading experts on network and Internet technologies and has written and spoken extensively on topics such as VOIP, convergence, email, cloud computing, network security, Internet applications, wireless and Web services for more than 25 years. He has had several editorial management positions for both print and online properties in the enthusiast, gaming, IT, network, channel, and electronics industries, including the editor-in-chief of Network Computing print, DigitalLanding.com, and Tom's Hardware.com. He began his career working in varying roles in end-user computing in the IT industry. He has a Masters of Science, Operations Research degree from Stanford University, and a BS from Union College.