About this paper
A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

About 451 Research
451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

© 2016 451 Research, LLC and/or its Affiliates. All Rights Reserved. Reproduction and distribution of this publication, in whole or in part, in any form without prior written permission is forbidden. The terms of use regarding distribution, both internally and externally, shall be governed by the terms laid out in your Service Agreement with 451 Research and/or its Affiliates. The information contained herein has been obtained from sources believed to be reliable. 451 Research disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although 451 Research may discuss legal issues related to the information technology business, 451 Research does not provide legal advice or services and their research should not be construed or used as such. 451 Research shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.
Executive Summary

“We’re a retailer. We are not a security company.”¹ This is the crux of the problem for website anti-fraud and security teams – protecting the business without intruding on the business.

Chief security officers commonly lament that reducing fraud in the enterprise would be a whole lot more effective if only the products could understand the business just a little bit. This is especially true with websites, the primary interface of the business with its computing world of customers, partners and employees. Fortunately, the web behavior analytics (WBA) market is rapidly emerging to ensure both authenticated users and anonymous guests are interacting with the website in the expected ways. WBA products evaluate website sessions to prevent financial losses from automated attacks and fraudulent transactions – exactly the alignment with the business that CSOs crave.

Cyber criminals find that it is much easier to leverage compromised website accounts to profitably abuse business logic than it is to write custom software exploiting vulnerabilities. Websites by design allow users to log into their accounts, complete transactions and access important data. Unfortunately, this also allows fraudsters the opportunity to take advantage of the very same access paths for nefarious purposes. Web behavior analytics, including products such as RSA Security Web Threat Detection, is surging because of its ability to interpret the navigation and intent of each visitor to the website. It is one of the best ways to protect the business against the skyrocketing rates of website fraud.

Legacy tools such as web application firewalls (WAFs), which are architected to look at inbound traffic for attacks that take advantage of software defects, can’t prevent damage from account takeover, fraudulent transactions or the scraping of private data off ‘protected’ web pages. Attacks using cross-site scripting and SQL injection are more effectively corrected in the code than in any WAF rules. Security teams typically place WAF devices in passive mode off the data path to check the box for compliance mandates while turning to WBA devices to effectively deliver anti-fraud protection to website interactions.

This Pathfinder Report summarizes the key technical and use-case attributes of web behavior analytics before making recommendations on how to evaluate the capability. This report is sponsored by the RSA Security Web Threat Detection team.

¹A ‘multibillion dollar per year’ retail company. 451 Research, Voice of The Enterprise, 2015.
Important anti-fraud characteristics

Anti-fraud products are all about reducing financial losses while preserving positive user experiences; web application firewalls are all about preventing significant infrastructure damage from attacks. Web behavior analytics products observe everything in the clickstream and focus their anti-fraud features on users and devices, starting with assaults against the login page. Abuses of business logic after the website allows entry to the user are generally the most damaging to the enterprise because that is when attackers test stolen account credentials, order goods and services without any intent of payment, and steal proprietary data. WBA products have many security benefits, the most visible of which include:

- **Control access from bots.** Bots are software engines that impersonate real people for the purpose of cybercrime against websites. We have seen automated bots represent as much as 90% of the total traffic to a website. One retailer reported detecting a single IP address generating 21,221 clicks per hour against the login page trying to break into 20,775 user accounts. WBA recognizes bots by identifying unusual access patterns such as multiple connections from a common IP address, link click rates that exceed human capacity, and sessions dropping immediately after login.

- **Thwart username- and password-guessing attacks.** Tools including SentryMBA make it simple to purchase username/password credential off the dark web to be launched against a website looking for accepted combinations. For example, a leading global merchant found a password-guessing attack against 200,000 accounts produced 10,000 successful logins into customer accounts. A 5% hit rate such as that is typical and produces an acceptable yield of useful credentials to a cybercriminal.

- **Detect account takeover activity.** Attackers can either go through the work of setting up their own accounts with fake identities or simply use credentials they have acquired maliciously. The result is that attackers enter the website with all of the privileges of the users they are impersonating and are free to purchase goods, view content and consume website resources without fear of detection by security products that are not designed for detecting modern web fraud threats.

- **Prevent the loss of data by web-scraping threats.** The process of moving through a website extracting large amounts of data is called web scraping. This is a beautiful example of business logic abuse because the sensitive information is meant to be shared. However, scrapers plan to use the data for purposes detrimental to the business such as displaying it on their own websites to steal customers or undercut prices in competitive practices. Many sites require a customer or partner relationship, but if a trusted account is taken over, then sensitive data can be copied and resold or used as intelligence by competitors. Web scraping is a difficult problem to solve because search engines, which are desirable to attract new customers, also crawl through websites collecting content to compile ratings and indices.

**Most Important Features of Security Products**

Q. What makes a good security product?

- Ease of deployment
- Training / resources availability
- Out of the box functionality / ROI
- Support mission critical processes
- Usability
- Offers prevention
- Works in the background
- Centralized (and actionable) reporting
- Ability to integrate with other products

Source: 451 Research
Throttle application-level distributed denial of service (DDoS) attacks. DDoS attacks can be as simple as bots continually executing searches within the website. The searches consume valuable compute cycles that effectively deny service to legitimate visitors.

Catch cross-site scripting and SQL injection attacks. Although these are the mainstays of traditional security products, WBA products monitoring every user click and web page delivery also effectively catch these attacks.

Effectively secure transactions from mobile and tablet devices. Such devices likely utilize mobile APIs and alternate paths into the website. Because the enterprise cannot force use of a dedicated mobile app, the burden of anti-fraud security falls onto the website. WBA products can track device and user activity to ensure the integrity of the growing volume of website transactions from mobile devices.

Detect abuses of the business rules. This requires custom rules understanding the semantics of the business to ensure criminals are not taking advantage of the business. The challenge for WBA products is to keep up with the constant change in fraudster techniques across websites. This is easily the broadest category of important security characteristics with the greatest need to align security with business requirements.

Customer satisfaction suffers greatly as a direct result of successful attacks, especially those involving stolen credentials. No business wants its customers or partners calling the service desk complaining that its website anti-fraud mechanisms failed to catch attacks launched from their accounts. The business certainly does not want to help push many of those customers to find happier experiences with competitors. There are very distinct and compelling problems that drive enterprise anti-fraud and security teams to embrace web behavior analytics.

Selected examples of web behavior analytics in action
Attacks against e-commerce sites are the easiest of the web threats to visualize. One scenario is that attackers validate a stolen credit card by making a small donation to a local charity that likely has little security. When the donation is accepted, the cybercriminal then rushes to a commercial site and buys easily transferable goods such as gift cards, consumer electronics, and valuable travel and entertainment tickets. Given that users frequently reuse the same password across multiple sites, the attacker has a high likelihood of logging in and repeating the process at the next business. Thus, websites without WBA can succumb to fraudulent transactions even as they deliver the required business logic.

We believe the problem is only going to get worse as enterprises drive more business through websites. In fact, research data consistently shows criminals shifting attention to ‘card not present’ (CNP) fraud through websites, particularly as the introduction of EMV chip cards makes production of fake credit cards significantly more difficult. The UK has experienced this phenomenon, and we expect to see a similar trajectory in CNP fraud in the US.
The customer successes of RSA Web Threat Detection are indicative of the broad market appeal of the WBA approach:

- **A leading international retailer drives significant consumer business through its e-commerce site.** The organization had a problem where phishing attacks would obtain customer credentials that were then used to take over the account in making fraudulent purchases. WBA allowed the retailer to detect logins originating from phishing sites, act on a high number of login requests, catch simultaneous access from multiple IP addresses, and alert anti-fraud teams to unusual shopping patterns with discount coupons. WBA, with increased visibility into the entire transaction session, started reducing fraud in days, not weeks or months as with other approaches.

Credit Card Fraud Rates in the U.K., 2001–2012


- **A service bureau handles claims for product returns, with many of the anti-fraud processing demands shifting from telephone to website interactions due to enhanced identity proofing in the call center.** The organization needs to quickly take action on claim requests and is finding visibility into the history of the entire web session accelerates the fraud-checking process. We were impressed with the real-time integration with back-end analytic engines to make hold/allow decisions, an alignment of anti-fraud security with the business infrastructure that others should look to duplicate.

- **A large financial services organization is concerned about protecting its brand reputation and not letting web threats linger unresolved.** Keeping the company name off the front page is a high priority for the organization. The enterprise is finding that the visibility of website traffic, especially from mobile interfaces, is reducing the expenses of incident-response processes. The company has caught unauthorized API use by a third-party mobile app, seen surprisingly high traffic volume to password reset pages, and detected SQL injection and ShellShock attack attempts. We see this as a noteworthy combination of securing the business against fraud while also enhancing the entire incident-response process.

### Important technical characteristics

Interacting with customers, partners and employees through websites is a critical fundamental of every modern business. No enterprise can function for long without offering services through websites, which places unique technical requirements on anti-fraud products. For many organizations, website transactions are the lifeline of the business and must remain open for business at all costs. It has been our experience that products must adhere to important technical characteristics to ensure successful deployment:

- **Fit into existing infrastructure.** Website protection must have minimal impact on the existing technical architecture because website owners resist performance risks associated with configuration changes to accommodate anti-fraud protection. It is important to deploy software on the website to communicate with the WBA device and potentially handle exceptions, to sort out organizational responsibilities to process web security incidents, to have no impact on the network infrastructure such as firewalls, load balancers and switches, to secure virtual websites because they are dynamically provisioned to meet increasing demand, and it is vitally important to place no demands on user browser configurations.
• **Stay off the data path.** It is essential that websites stay open for business 24/7. As an anti-fraud executive, the last thing you want is a product on the data path that interrupts service delivery. The only reason to be a bump on the wire is to be able to block traffic at the transaction or user level, but it is far better to implement granular actions in the web server or at the firewall. Consider placing the WBA device off the SPAN port or network tap where it receives a copy of all of the clickstream traffic and can still communicate directly with the website as required without impacting performance.

• **Follow the rules.** Expressing anti-fraud protection as a set of rules is essential in providing businesses with the flexibility to effectively customize their web protection and stay aligned with business requirements. Web security has to understand the business context of interactions, and that context must be defined as a set of easy-to-understand rules. For example, transactions from business partners could require the browser to be located in specified locations, or anti-fraud mechanisms may differ according to the value of the transaction. In any event, web behavior analytics can never be a one-size-fits-all proposition. Rules are almost always required to custom fit WBA to the business logic of the website.

• **Let the business make informed go/no-go decisions with risk scores.** No two businesses or websites are alike when it comes to recognizing and prioritizing fraud incidents. Risk scores, the numerical result of analyzing activity against behavioral norms and business rules, allow the business to determine the best course of action when detecting elevated suspicious activity. In some cases, the business may assume the risk; in others, the business may redirect the user to a higher level of authentication, request management review and approval, or in severe cases, drop the session entirely. It all starts with the scoring engine to help the website execute the best decision, such as redirecting the user to customer service pages.

**Enterprise recommendations**

Your websites are too important to leave to legacy security products. We find that while compliance suggests WAFs, these devices tend to be deployed in passive audit mode to detect vulnerabilities that are more effectively fixed in the code. Web behavior analytics operates by observing business conversations to help make real-time determinations of suspicious activity. This is the one place where anti-fraud security enables business outreach and remains aligned with the needs of the organization.

Our recommendations for enterprise executives evaluating web behavior analytics start with comparisons between WBA-protected websites and those that rely on traditional approaches. We suggest you customize these approaches for your specific business environment:

• **Controlling automated traffic from bot engines reduces the risks of account takeover, web scraping and large-scale data theft, and it increases performance capacity of the website.** Measure the differences in invalid login requests, unauthorized web scraping attacks, fraudulent transactions and redirections to customer service pages.

• **Compromised account credentials can drain money from the business through fraudulent transactions, such as the bulk ordering of gift cards, consumer electronics or other liquid goods and services.** Enable WBA rules for every other user conducting transactions and compare metrics after one month. Contrast the level of users completing transactions with detected fraudulent activity, and calculate the cost savings from anti-fraud rules.

• **WBA tightly integrates anti-fraud supervision with application owners and IT operations.** We recommend collaborating before evaluating web behavior analytics to agree on measureable success criteria, metrics for fraud allowances and business intelligence, fraud investigation cost savings associated with enhanced visibility, and organizational communications reporting. Evaluate writing custom rules to test organizational responsibilities and the ability to stay aligned with the business.

**Conclusion**

Web behavior analytics by its very nature lends itself to quantifiable intelligence on website security. We believe the ability to guide anti-fraud capabilities with business rules, compute risk scores to automate decision-making, and measure the bottom-line effectiveness of anti-fraud mechanisms make a compelling case for organizations to enhance their website protection. WBA delivers a risk-based approach to anti-fraud security with built-in flexibility so it can shift with best business practices. We recommend that all website owners evaluate web behavior analytics capabilities as a strategic priority.