REPORT REPRINT

ThreatMetrix rises above the DIN to tell you whom you're dealing with

ERIC OGREN, DAVID IMMERMAN

25 MAY 2016

The company is on a mission to help enterprises by stitching together various aspects of user interactions, including device, identity, location, and behavior, to better authenticate customers, employees and partners accessing the business through websites.

Gone are the days when website owners could reasonably count on endpoint security software to help secure transactions. According to ThreatMetrix, the use of mobile devices in conducting online banking transactions has increased 200%. While some applications can build security into custom apps for phones and tablets, the primary use cases are now browsers on iOS and Android devices. This places the burden of security squarely in the technology of websites and their security teams.

The ThreatMetrix Cybercrime Report released in April provides fresh emphasis on the problem of attacks launched against websites by organized and professional cybercriminals. Website owners see this attack influx in the form of automated bots operating with stolen and manufactured digital identities. The cloud-based ThreatMetrix service detected and blocked 311 million bots in Q1 alone, an increase of 35% over a busy Q4. Equally revealing is the 100 million fraud attacks that were thwarted, a staggering annual increase of 52% over the first quarter of 2015. This implies that cybercriminals are finding the path of least resistance, using stolen account credentials or zombie accounts (no live user) to walk into websites and generate fraudulent transactions. It is a very real problem that drives security teams to web behavior analytics products for relief.

THE 451 TAKE

The ThreatMetrix report highlights the popularity of using the business logic encoded into websites against the business, mostly in the form of creating phony accounts, taking over existing accounts, scraping valuable information and denying service to other users. Cybercriminals cash in by using seemingly legitimate accounts in seemingly legitimate ways. It is much easier than discovering a vulnerability, writing exploit code and deploying the attack before traditional defenses can be prepared. A behavioral approach correlating users, devices and personal characteristics is the only way of detecting fraudulent activity that follows approved business logic. We believe a cloud-based service to be the logical place for securing web activity – an enterprise cannot control all the devices connecting to the website, and the service can more efficiently apply its intelligence to all traffic and instances of enterprise websites. Web behavior analytics is a formative market, but ThreatMetrix has been able to channel its ability to identify users and devices into business benefits for website operations.

CONTEXT

ThreatMetrix is based in San Jose, with additional locations in New York, The Netherlands, UK, France, Australia, Japan and Hong Kong. The company was founded in 2005, and its headcount is now at 175. A $20m series D funding round came in March 2014, led by Adams Street Partners, August Capital, Technology Venture Partners, CM Capital Investments and U.S. Venture Partners, bringing total funding to more than $56m.

In 2012 ThreatMetrix acquired Australian anti-malware company TrustDefender, and its underlying technology is part of the current ThreatMetrix Digital Decision Platform. ThreatMetrix operates its Digital Identity Network out of datacenters in the US, Amsterdam and China. The technology represents a 95% recognition rate in distinguishing real users from imposters, and enterprise customers wishing to accurately identify their clients have added 600 million new devices to the DIN coming from 240 countries and territories around the world. The DIN supported more than 4,000 businesses, 30,000 websites and 20 billion transactions in 2015.

TECHNOLOGY

ThreatMetrix is tackling the challenge of fraud detection and identity authentication with its Digital Identity Network (DIN). The network is a repository of accumulated anonymized information from internally processed transactional data and collaboration with its partnership ecosystem. The ThreatMetrix platform is architected to analyze and model multiple sources of information for real-time decision-making.

The recently announced ThreatMetrix Open Intel capability allows businesses to incorporate third-party intelligence signals into the ThreatMetrix platform to orchestrate fraud prevention and authentication decisions. This provides the digital businesses with a framework to build customer integrations of external signals and third-party vendor data solutions onto the ThreatMetrix Digital Intelligence and Smart Analytics platform, thereby preserving existing technology investments while paving the way for future integrations.

This approach allows ThreatMetrix to drill down to individual transactions and interactions for internet users all over the world, creating digital identity profiles. For each digital identity, there is a digital identity graph. The graph measures the identity with numerous interactions and data points, including phones, tablets, computers and websites. Using behavior analytics based on predefined business rules and a policy engine, analyzing correlations and interactions between these device endpoints creates the digital identity graph and areas where potential fraudulent activities occur in real time.

ThreatMetrix's spring 16 release features ThreatMetrix Smart Analytics, which includes machine learning and user-behavior analytics. Also announced were new SDKs available for iOS and Microsoft Windows desktop and endpoint applications, and a state-of-the-art integration and orchestration hub that can enable value-added services like two-factor authentication and identity validation. In 2015 ThreatMetrix announced ThreatMetrix Connect, a new alliance program enabling technology providers to easily integrate services with the ThreatMetrix Digital Identity Network.

STRATEGY

Legacy authentication systems were designed to support local users, and can be challenging to scale to the needs of a connected world. Even unsophisticated attackers now use 'dark web' tools to barrage websites with automated sessions masquerading as legitimate users. Enterprise security teams are tasked with looking beyond traditional authentication methods to find a more holistic, layered approach to establishing a user's identity without hampering ease of use requirements for legitimate customers.

ThreatMetrix's strategy features a layered platform approach combining multiple coefficients in its directed graph algorithms. By that we mean a device fingerprint is important, but devices can be shared or lost; user transaction behavior is important, but not all changes in behavior indicate an attack; geolocation is a reliable indicator, but sometimes people travel, etc. A layered approach continuously correlating points of reference provides security for each and every interaction, which we believe is an improvement over point-in-time authentication products.

The cloud-based Digital Identity Network is central to the ThreatMetrix product strategy. The DIN provides access for vendors to contribute intelligence to the network at multiple layers, as seen in the recently announced Open Intel partnership agreements. We believe the ability to provide digital identity and anti-fraud services across enterprises to be a noteworthy capability. Most enterprises can only base digital identity decisions on their own experiences, but using the DIN helps organizations expand their visibility to identify users from neighbor organization experiences.

ThreatMetrix sees its offerings pertaining to e-commerce and financial services verticals because of the necessity of securing transactional processes and identifying fraudulent personas. Merely identifying whether a buyer is the person they claim to be for e-commerce is a major issue; ThreatMetrix detected 264 million botnet attacks for e-commerce alone in the first quarter of 2016.

COMPETITION

ThreatMetrix will see most of its competition in applied behavior analytics and identifying fraudulent personas. We feel the company's strategy, which aligns with business requirement and metrics, is one of the key differentiators from competitors. While others are talking about bots, ThreatMetrix is talking about fraudulent transactions and identifying returning customers with less hassle.

Having said that, ThreatMetrix has very serious competitors for budget allocations in the web behavior analytics market. While the products and technologies are differentiated – ThreatMetrix is taking a layered platform approach while others are more whole-product-oriented – the business problem WBA vendors confront is consistently similar. For some enterprises, a focus on anti-bot technology suffices, or integration with TIBCO, IBM or SAS analytic engines is critical. Most ThreatMetrix competitors now offer a cloud-based service, allowing them to quickly react to changes in attack methods.

Distil Networks protects against bot-driven attacks to websites and mobile APIs. F5, iovation, PerimeterX and Shape Security all offer code for the mobile device to secure transactions to protected websites from bot engines. Moving up the anti-fraud stack will bring vendors such as Kount, NuData Security and RSA Security into play. Finally, we see interest in anti-bot measures identifying fraudulent sources of traffic from service providers such as Akamai and CloudFlare.

SWOT ANALYSIS

STRENGTHS

ThreatMetrix provides enterprises a higher form of authentication for returning customers without requiring two-factor authentication, CAPTCHA or other ad hoc challenges.

WEAKNESSES

The platform approach may require customization, which can extend sales cycles into the 12-18 month range. Customer acquisition could be accelerated if ThreatMetrix had a low-end on-premises product.

OPPORTUNITIES

ThreatMetrix is at the size where it has an opportunity to derive significant revenue growth by aiming service packages at its installed base. These packages could be high-value anti-fraud analytics, features focused on specific vertical markets or integration with in-house IT systems. The company has large customers, and can start its verticalization in e-commerce and finance industries.

THREATS

Databases of device fingerprints and user profiles are sure to cause privacy concerns, even as the company assures international regulators the data is securely hashed and tokenized. ThreatMetrix may have to open datacenters to appease local governments and assure that citizen traffic does not flow through US controlled resources.