REPORT REPRINT

Cleafy takes to the cloud to reduce fraud for online businesses

ERIC OGREN

10 AUG 2018

Since the cloud is the source of increased fraud risks for web-facing application product lines, it's natural that website security and antifraud protection also be located in the cloud. Cleafy SaaS 1.0 is a cloud-based security service that merges customer and application intelligence to reduce fraud rates associated with online financial transactions.

Traditional approaches to protecting web-facing applications from attack often fail because of the friction resulting from attempting to control the customer side by deploying software in the critical application delivery infrastructure and the business side by embedding code in the business logic of the website. Placing the website security service in the cloud simplifies the inspection of the interactions between the customer and application, as well as the remote assessment of the customer browsing environment, and avoids complicating website operations processes. Cleafy offers a cloud-based security service that merges customer and application intelligence to reduce fraud rates associated with online financial transactions.

THE 451 TAKE

Cleafy SaaS 1.0 brings all of the major threat-detection features from the on-premises Cleafy Detect product to the cloud as a Cleafy-hosted subscription service. The offering's key features include continuous monitoring of customer interactions to deterministically detect attacks inserting themselves into the middle of an authenticated session, and injecting into the web application code or overlaying mobile apps on the endpoints. Providing these features without modifying applications and development operations processes differentiates the company from other web behavior analytics (WBA) specialists. Cleafy SaaS 1.0 supports integration with application delivery controllers (ADCs) and content delivery networks (CDNs).

CONTEXT

Cleafy maintains headquarters and development operations in Milan, Italy, with a North American office in Boston. The company was founded in 2014 and now has worldwide operations in other EMEA markets, the US, Latin America and Asia-Pacific.

Its products are deployed in larger financial institutions, and Cleafy claims to protect over five million consumers. The company has forged technology partnerships with major security vendors such as Citrix, Microsoft, SAS and Splunk.

Cleafy is an emerging player in the WBA market for protecting web and mobile transactions. WBA technology has to provide security insights into both consumer devices and websites without imperiling legitimate business transactions. Cleafy SaaS 1.0 responds to two key constraints for web security products:

- There is little appetite among line-of-business (LOB) decision-makers to lessen user experiences by requiring the use of a client-side app. Cleafy's challenge is to preserve transactional integrity against attack techniques such as man-in-the-browser or remote access trojans while remaining transparent to consumers.
- The company must be careful not to impact website operations by placing requirements on how websites are built and deployed as websites themselves are continuously modified with new content, cache requirements for performance, and the introduction of new features for mobile consumers.

PRODUCTS

Cleafy Detect provides the foundational features for cloud-based Cleafy SaaS 1.0. The technology examines the application traffic between the consumer and website for any anomalies indicative of a cyberattack or attempted fraud. By capturing both outbound and inbound traffic in the browsing session, the vendor can compare actual HTML Document Object Model content against what would normally be expected, and then identify threats arising from deviations. The product also retains the threat evidence (e.g., the code injected by the malware) to help security and antifraud teams repel the threat. Cleafy SaaS 1.0 relieves customers from the need to administer on-premises software.

The offering can monitor the inbound and outbound traffic directly from the ADC or CDN. There is no requirement for consumers to install any on-premises software and no requirement for protected applications to insert hooks for security software, although some customers may choose to insert small amounts of Cleafy JavaScript in the web code. Coordinating with the ADC or CDN allows Cleafy to protect both website transactions and mobile application gateways over a broad range of consumer devices. The company offers several integrations with ADC technologies such as F5 BIG-IP and Citrix NetScaler.

Cleafy SaaS 1.0 collects information from consumer devices, cyberattack behaviors and attempted fraud activity that can help manage transaction risks and respond to threats in real time. The company's dashboards can be directly accessed by users over the cloud. Cleafy also supports integrations with security information and event management (SIEM) systems. Cleafy App for Splunk feeds intelligence of detected threats – including insights into the consumer device – into the SIEM for further analysis, consolidated reporting and integration with security operations remediation workflows.

Shifting Cleafy Detect features into the cloud as Cleafy SaaS 1.0 also gives the vendor opportunities to introduce new products and services without having to distribute software to customers or consumers. Cleafy is now in a position where customers can utilize services such as remediation assistance, notification and workflow integration, as well as the sharing of fraudulent transaction behaviors.

COMPETITION

The web behavior analytics market has been stubbornly slow to evolve. Part of the reason is that WBA has three main decision-makers with different requirements that must be satisfied. Security teams traditionally prioritize integrity and availability, antifraud teams focus on managing fraud rates, and LOB caretakers drive consumer adoption and service availability. All must buy into a purchase decision that can stretch out sales cycles and test the messaging of every WBA provider.

Competitive forces have focused on two primary benefits of WBA: it protects against the takeover of consumer accounts, and it detects fraudulent transactions as early as possible. For protecting accounts, rivals to Cleafy SaaS 1.0 would include Distil Networks, PerimeterX, Shape Security and Unbotify. Akamai Bot Manage Premier and F5 WebSafe/MobileSafe work with CDNs, but do not generally include antifraud capabilities.

SWOT ANALYSIS

STRENGTHS

Cleafy SaaS 1.0 collects evidence of fraud activity by leveraging patented application integrity-detection technology and presents the information to security, antifraud and customer support teams without side effects on websites or consumer devices.

WEAKNESSES

The company's latest offering is in the early stages and it could use more ADC and CDN partnerships to drive sales.

OPPORTUNITIES

Cleafy SaaS 1.0 provides the vendor with a clear path from the cloud to introduce new security and antifraud products and services. It is aiming to extend its target markets beyond financial services.

THREATS

CDNs that have been using WBA to protect bandwidth by removing undesirable bot traffic may leverage their largest financial customers by offering antifraud services.