REPORT REPRINT

Cleafy fine-tunes anti-fraud portfolio as it seeks growth in North America

FEBRUARY 10 2020

By Fernando Montenegro, Matthew Utter

The broader trends around online attacks point to a future where these attacks will look more like fraud attempts than security exploitation. Cleafy is banking on its European experience as it pursues a North American growth strategy and a fine-tuning of its anti-fraud portfolio.

451 Research®

Introduction

One of the immutable laws of conflict – such as the perennial tug-of-war between attack and defense in cybersecurity – is that both attackers and defenders evolve. As attackers shift tactics to focus more on human elements of transactions and business logic abuse, organizations are looking to ensure their anti-fraud architecture is able to withstand these attacks. Cleafy has been steadily working on evolving its platform and fine-tuning its go-to-market strategy, and now looks to make a stronger push into the North American market.

451 TAKE

As the nature of attacks changes, we expect anti-fraud considerations to rise in importance for organizations. Understanding just how risky the inbound application traffic actually is will drive organizations to pay more attention to continuous monitoring and expedited response. This is the opportunity that Cleafy is pursuing, looking to capitalize on its European experience to drive more business there and, importantly, in North America. Moving into new markets will require a strong commitment in terms of building both go-to-market and customer-success motions. We expect the company will face significant competition from several well-established vendors, but its core approach should resonate with financial and online customers.

Context

Cleafy was founded in 2014 and is led by Matteo Bogana and Nicolò Pastore. The company is based in Milan and has North American operations in Boston. Cleafy has about 35 employees and has expanded its operations in Asia-Pacific, EMEA and Latin America.

The company is still led by its original founders. Before becoming CEO, Bogana held roles at Accenture and GE. He also worked as the coordinator for PoliHub, the innovation district and startup accelerator at the Polytechnic University of Milan. Additionally, CTO Pastore has experience in network security, and during his time working as Fractional CTO helped to launch numerous startups.

In 2015 Cleafy participated in a seed round led by EIT Digital Accelerator, but exact funding numbers were not disclosed. The company has been part of the Moviri Group since 2017.

Market

The fraud-prevention market offers different paths – from protection of online transactions and anti-bot management to back-end fraud analytics and protections for transaction security. Unlike other areas of security that may be more focused on security and IT teams, anti-fraud efforts usually feature a strong partnership between application/business owners, IT for technology platforms, security teams for domain knowledge about attacks, and a back-end anti-fraud team that processes cases. Among the key trends in online fraud prevention there's an increased focus on continuous authentication of users and deeper integration into the technology stack.

Strategy

Cleafy's main thesis is that detecting online fraud should move from hardcoded logic checks to deployments with continuous monitoring and risk assessments, while the response to fraudulent events should consist of orchestrated workflows. It targets primarily financial services – particularly online banks and payments services – and online retailers. The company indicates that it has approximately 40 customers and has seen significant growth over the past few years.

Given its roots, it's understandable that Cleafy has had a strong presence in Europe – particularly Italy, Switzerland, Eastern Europe and Spain, which also gives it some reach into Latin America – but the company is clear about expanding from its existing European base into North America, working in conjunction with parent company Moviri Group.

Cleafy has worked on alliances with more specialized value-added resellers and technology partners. Reseller/integrator partners include European VARs such as Botech, Solvit and Tempest, and the company recently announced a partnership with Accenture. Cleafy has also formed technology alliances with infrastructure vendors such as Citrix, Kong, Microsoft, Splunk and Elastic.

Moving forward, the company expects to provide more tailored services for its key verticals – financial services and online retail – via packaged portfolios and the evolution to a more orchestrated approach to response and a stronger focus on identity management. The company is also investing more heavily in its North American presence.

Technology

Cleafy offers a modular system for detecting malicious tampering of online applications. The product provides continuous risk assessments of the application traffic and can alert – or kick off responses – on a number of common fraud scenarios.

The key use case that Cleafy aims to address is management of application integrity for web and mobile apps. As it detects changes to the application, it aims to protect against transaction tampering, payment fraud, credential hijacking and a number of other scenarios. For mobile applications, scenarios such as SIM swapping, jailbroken devices or malicious applications are considered in-scope.

The Cleafy portfolio can be deployed on-premises or be consumed as SaaS. The on-premises approach seems favored by its current customers. The modules are deployed as virtual images or as Docker containers, and scale horizontally. There are separate detection modules for different detection techniques, plus a risk engine, rules engine, user interface, API endpoints, and connectors for inbound threat feeds and outbound integration to SIEM systems.

The detection module integrates with customer load balancers both for dynamically inserting instrumentation code and for collecting a copy of the traffic for analysis. For mobile use cases, Cleafy instrumentation is provided by an SDK that can be built into the applications.

The key detection mechanism is the Cleafy instrumentation code, which is delivered to the browser in an obfuscated manner and reports back details about the remote browser's current state. Once that is received in the central location, the platform analyzes the response for evidence of numerous possible attacks, such as form tampering, man-in-the-browser attacks and more. As the page is analyzed, different indicators contribute to calculating a risk score of 0-1000, with the possibility of tuning this calculation on a per-application basis. The detection module also extracts the malicious content for immediate analysis, and then adds relevant tags and the risk score to the session data to facilitate analysis and rule creation. Moreover, Cleafy complements this detection mechanism with behavioral and transactional analysis. The system comes with numerous prebuilt rules for detecting common attacks.

Once the attack is detected, the platform sends the alert via different methods, including SIEM integration, web hooks or API calls to orchestration systems. Users can also use the interface to perform queries using the Cleafy query language.

The company is now updating its portfolio by tailoring the different modules, services and threat intelligence for each specific market. Cleafy expects this will assist with simplifying deployments. The company is also making updates to its rules packages and looking for additional use cases; it plans an upgrade of the user interface in the near future. Cleafy is also working at extending its platform to become a data hub and centralized orchestration engine.

Competition

The company mentions both IBM and F5 as key competitors. When competing against IBM, Cleafy proposes that its approach is more effective than IBM's Trusteer, particularly around simplified instrumentation and lower false positives. For competition against F5, the typical scenario is against F5's WebSafe, which Cleafy claims to have displaced in some deals.

Cleafy also sees numerous other vendors in competitive tenders. These include, but are not limited to, BioCatch, SiftScience, EasySolutions, XTN, Buguroo, Distill Networks and Zimperium.

Beyond these vendors, the competitive landscape will also be dictated by the use cases. If protecting online transactions, vendors such as iovation, RSA, PerimeterX or ThreatMetrix may be relevant. If the use case drifts toward anti-bot, then offerings from Akamai, Cloudflare, Fastly, Radware and others may come into play.

SWOT Analysis

STRENGTHS

The combination of Cleafy's application integrity approach, insertion methods and low instrumentation requirements should help customers looking to efficiently address a variety of use cases and threat actors.

WEAKNESSES

The company's portfolio has been centered on on-premises deployments for its European customers, but may need to quickly ramp up to support more cloud-centric deployments in North America.

OPPORTUNITIES

The general trends in the evolution of security threats point toward more focus on application-layer and business-logic concerns, such as those that Cleafy has been addressing with its offering.

THREATS

Anti-fraud, bot management and online protection are markets that have attracted significant interest over the years, and now feature vendors that are much larger and better funded than Cleafy.