ON THE RADAR

Publication date
16 Dec 2020

Author
Rik Turner
Principal Analyst

Cequence extends runtime app security

Offering multiple elements of runtime app security on a Machine Learning-driven common platform

Brought to you by Informa Tech

Summary

Catalyst

The need for greater application security is not going away. Traditional application measures such as static and dynamic (SAST and DAST) application security testing approaches have been used for some time to test during the development pipeline. However, increased use of web services and APIs to rapidly build applications means that understanding and protection of what is happening during application runtime, becomes even more important. This involves several different facets which as the need becomes more widely recognized, are increasingly being offered together by vendors as a complete next generation application security platform.

Omdia View

Cequence's Application Security Platform (ASP) is designed to address the multiple threats to API and Web security through improved API visibility and controls, defense against malicious bot activities and a web application firewall (WAF) to protect against web vulnerabilities.

The Cequence ASP is based on its patented analytics engine, CQAI, which gives it machine learning capabilities which should make anomalies in API usage easier to spot. Around this core it provides Bot Defense for business logic abuse protection, an app firewall to block API-based exploits and API Sentinel for API visibility, all using a common policy engine.

While it addresses software development issues around the use of APIs, it will be security buyers that will benefit from its ability to dynamically create an inventory of all APIs in use at runtime and apply continuous risk-scoring based on non-conformance to set policies. Its approach should ease the process of bringing development and security closer together, especially in rapid development and multiple release practices such as DevOps.

Why put Cequence on your radar?

Organizations need to better understand what is happening in their software, particularly given the increasing reliance on open source and functionality that is developed under external control. In the rapid cycles of contemporary software development, rigor may sometimes be lacking or difficult to apply, or vulnerabilities unnoticed. The ability of the Cequence ASP to detect, manage and defend API and Web application risk using machine learning to support policy allows application estates to be continuously monitored and rigorous safety controls to be automated.

Market Context

The software development environment has changed. Development cycles have shortened, partly due to pressure for business evolution, and partly to user expectations raised by the way web and mobile applications have rapidly emerged, updated and evolved. Attitudes, processes and tooling within software development itself have also changed. Cumbersome, linear development processes have been replaced by Agile and DevOps, where multi-disciplinary teams collaborate and use continuous cyclical processes to refine and improve (a.k.a. continuous integration and continuous delivery, or CI/CD). Functionality has become fine-grained with microservices and containers, and is aggregated from a variety of sources, internal and third party.

Universal connectivity and the use of resources drawn from open-source software, services in the cloud and multiple third-party APIs has massively opened the attack surface and expanded the risk. There is a need for much closer attention to security and reliability, not just in the development pipeline, but also at runtime, as applications and services are deployed and used.

Individual legacy approaches to testing and validation cannot cope with the pace, diversity or scarcity of resources. This increases the need for automation and integration of multiple types of checking, testing and protection, all through the development, deployment and production lifecycle.

Security thinking and teams are already merging into DevOps, as DevSecOps starts to become a reality, but increasingly security protection and testing for software quality and reliability are merging, both in the development pipeline and at runtime. This can be seen as vendors from both spheres are developing or acquiring new functionality and services to provide a more comprehensive offering, to deliver next-generation application security (NGAS).

More integration, both technically in products and platforms, and also commercially through acquisitions and partnerships, is inevitable, but the pipeline and runtime elements are likely to progress at different paces. For some it will be sufficient to automate and merge static, dynamic, and interactive code analysis tools and test procedures, as well as software composition analysis (SCA), during the development process; others will keep their focus to runtime and the behaviors and responses of applications and APIs to network activities, automated threats and runtime errors. In each element, however, there is already significant M&A, development and integration activity, and this will continue, causing a re-alignment of the application security market.

Product/Service Overview

Cequence addresses multiple API security elements with a set of products that are part of its Application Security Platform. This offers

- automated API security at runtime,
- bot defense against business logic abuse,
- an app firewall to block threats and
- API usage tracking, visibility and risk assessment.

At the core of the platform is Cequence's patented CQAI analytical engine. This uses machine learning with over 150 automation indicators to automatically and continuously assess public-facing Web applications. By assessing every interaction from a user, client, network and application perspective it builds a behavioral blueprint to distinguish between malicious and benign activities to help determine policies. A combination of predefined system rules and custom rules enforce the policies specifically required by the organization and connect to the three main elements of functionality within the platform:

- Bot Defense. Attacks that have been unearthed based on CQAI intelligence can be mitigated by complete blocking, geofencing or rate limiting. Findings can also be exported to external systems for enforcement or added analysis. Deceptions to mislead attackers, such as serving up old content to price scraper bots, can also be employed.
- App Firewall. This uses CQAI to extend and simplify the implementation of Web Application Firewall (WAF) capabilities, typically focused on the OWASP Top 10 and PCI DSS 6.6 compliance, with predefined application profiles and policy templates. The machine learning and blueprinting provides insights to aid the creation and adjustment of policies, to better fit the operational environment.
- API Sentinel. This uses live monitoring of public-facing APIs to provide a complete runtime API inventory. Its real-time visibility ensures that deprecated, hidden or 'shadow' APIs, can be detected and continuous risk scoring identifies potentially rogue actions. These could be based on access control abuse, sensitivity of data being collected, the use of encryption and conformance to OpenAPI specifications. API usage can be analyzed in real-time with predefined filters to identify and act upon unusual activities or patterns.

The consolidation of API, web and mobile protection into a unified platform improves transparency of API activities, aids governance and ensures that security is embedded into the application development framework. It also offers more security automation, which will reduce the amount of time spent in development and in investigating or defending against vulnerabilities hidden in APIs or automated bot attacks. Using machine learning to identify patterns of misuse can help distinguish fake account creation and account takeovers, or credential stuffing, from valid actions in real time to avoid reputation manipulation and potential harm to a business and its users.

Cequence ASP is open and extensible, with a REST API to integrate and share information with backend security incident and event management (SIEM) and security operations center (SOC) systems and its distributed, container-based architecture means it can be used as a service or on a customer's premises, or public or private cloud deployment.

Company Information

Background

Cequence was founded in 2014 by Ameya Talwalkar, Shreyans Mehta and Michael Barrett. It has raised a total of $29.5m in funding from a seed round in October 2016, followed by Series A and B rounds in February 2018 and 2019. The lead investor for the $17m raised in 2019 was the VC arm of Dell Technologies.

Current President and CEO is Larry Link, former EVP of worldwide sales at Palo Alto Networks and SVP of sales for Silver Peak Systems. Co-founders Ameya Talwalkar, Chief Product Officer and Shreyans Mehta, Chief Technology Officer, both came from senior network security roles at Symantec. Ameya was a Director of Engineering and Shreyans was an Architect and Technical Director.

Current Position

Cequence ASP is designed to be a complete approach for API and application security, underpinned by a machine learning analytics engine. It can be deployed as a SaaS offering and its container-based nature means it can also be deployed in a customer-managed public cloud, data center or hybrid environment.

It was launched in November 2018 as an automated and analytics-led approach to deal with the tedious and time-consuming tasks of securing web and mobile applications, with a focus on "discover, detect and defend" with Bot Defense. It had flexible deployment options from the outset, but was managed as whole application security platform, including its management dashboard Open APIs for ease of integration and data sharing were also key to the intended goals of rapid configuration and time to value.

Its App Firewall was added in June 2019, designed to overcome the inherent security limitations of traditional WAFs and eliminate unwanted application network traffic.

The addition of API Sentinel in June 2020 extends API protection further to include discovery of API risks introduced by shadow publication, coding or non-conformance errors or flaws. The software is licensed via one- or three-year subscription tiers, based on the daily volume of transactions analyzed.

Future Plans

The current subscription model fits those with significant need and suitable budgets but does not scale down. Cequence is investigating additional licensing approaches based around usage models and numbers of APIs being protected.

Key facts

Table 1: Data sheet: Cequence

Product name	Cequence Application Security Platform (ASP)	**Product classification**	Application Security Platform
Version number		**Release date**	ASP, November 2018, App Firewall, June 2019 API Sentinel, June 2020
Industries covered	Any org that is moving towards API-based dev. Examples include retail, hospitality, FSI, social media, relationship apps)	**Geographies covered**	Americas, EMEA
Relevant company sizes	Mid to large enterprises	**Licensing options**	One- or three-year subscription tiers, based on the daily volume of transactions analyzed
URL	www.cequence.ai	**Routes to market**	Direct sales and channel
Company headquarters	Sunnyvale, California, US	**Number of employees**	~50

Source: Omdia

Analyst Comment

Cequence's end-to-end approach to application security means API risk will be clearly understood and better managed across the diverse groups involved in development, security, operations, and compliance. This will help address issues often seen in DevOps teams, where automation and continuous monitoring will also be seen as important benefits. The wider, but integrated approach including WAF and bot management will help Cequence to target security buyers, who already recognize the need to tackle the multiplicity of security challenges they face, but also to simplify, automate, consolidate and integrate what tools they require.

Cequence offers an extensive range of deployment options – datacenter, cloud, hybrid or SaaS - which includes an integration with content delivery networks (CDN) from Akamai and Fastly. Both of these vendors offer their own services for application security, Fastly through the recent acquisition of SignalSciences, and in both cases there is DDoS protection in addition to WAF, bot and API security. Cequence's integration with these providers might be a good demonstration of its deployment flexibility, but there are risks to this approach.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments or strategy could prove disruptive and of interest to tech buyers and users.

Author

Rik Turner, Principal Analyst, Cybersecurity

Rom Bamforth, Associate Analyst

Citation Policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials”) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) and represent data, research, opinions or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees and agents, disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial or other decisions based on or made in reliance of the Omdia Materials.

Contact Us

omdia.com

askananalyst@omdia.com