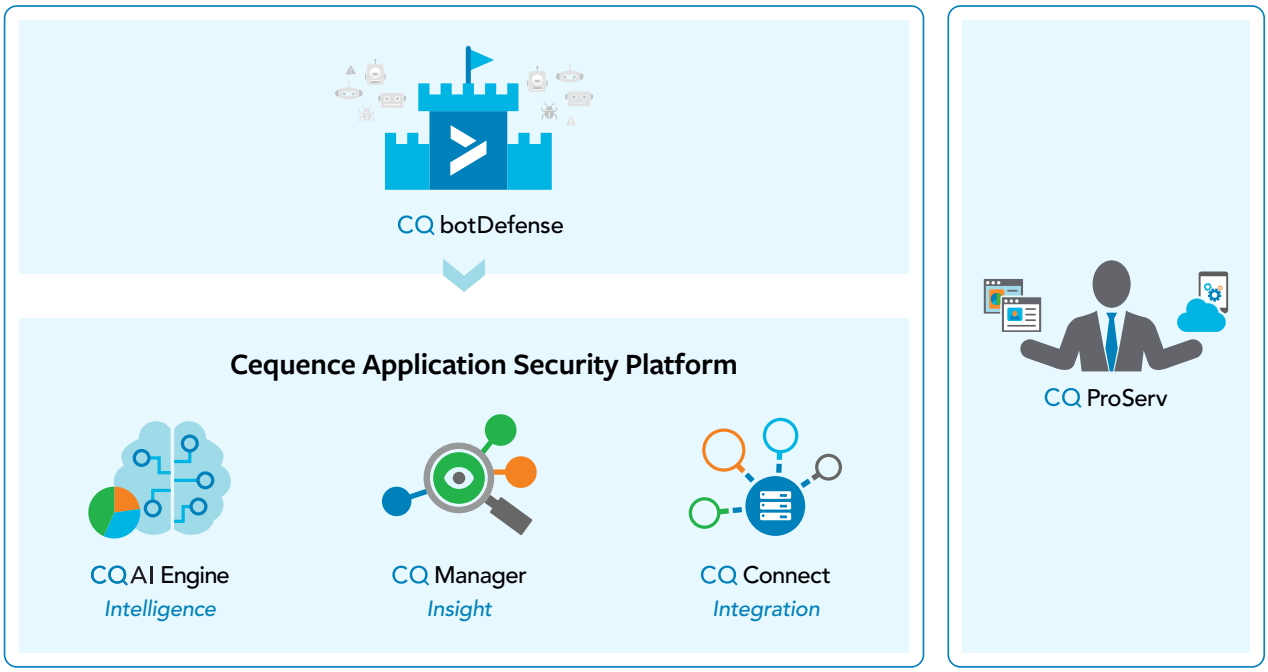
Cequence Security

Summary

Cequence Security is a venture-backed cybersecurity software company founded in 2014 and based in Sunnyvale, CA. Named a Gartner Cool Vendor in 2018, the company has developed the Cequence Application Security Platform (ASP), an open, distributed, and scalable software platform designed to protect customers' web, mobile, and API applications from the growing number of malicious bot attacks. Cequence Security will be delivering multiple security service modules for ASP, each designed to work together, simplify security architectures, and deliver strong protection for today's hyper-connected organizations. Cequence Security customers include F500 organizations across multiple vertical markets. The executive team is led by industry veterans that previously held leadership positions at Palo Alto Networks and Symantec.

Problem

Applications remain a primary target for attackers – and especially by bad bots – that want to exploit private customer data and intellectual property associated with these applications. The web application firewall (WAF) has been the traditional tool used by medium and large enterprises to detect and block application-level attacks. WAFs are typically deployed as in-line devices and rely on pre-defined signatures to detect and block behaviors and threats already known to be bad. In recent years, attack techniques have evolved significantly – increasingly employing armies of automated bots – to evade detection and gain access to internal resources. Point products for bot detection have tried to fill the gap, but they have proven to be complex to deploy and manage, and are limited in their ability to detect and stop attacks.



Solution

Cequence Security is focused on solving this problem by delivering Cequence ASP, an open software platform that is deployed anywhere including on-premises and cloud locations. The platform – in combination with the CQ botDefense security module – leverages a patent-pending analytics engine (CQAI), which combines applied artificial intelligence, machine learning, and behavioral analysis to deliver three key values to customers:

- **Discover** – The platform automatically discovers all web, mobile, and API applications deployed across the entire organization, providing insight into critical assets that must be protected.
- **Detect** – Metadata from client-server traffic flowing across the organization is continuously ingested, correlated, and analyzed in real time by the CQAI engine to automatically determine the source, target, and intent of potentially malicious traffic.
- **Defend** – Once an attack is confirmed, Cequence ASP with CQ botDefense can immediately and automatically end the attack by applying multiple policy-based mitigation techniques, including blocking, deception, rate limiting, and more.

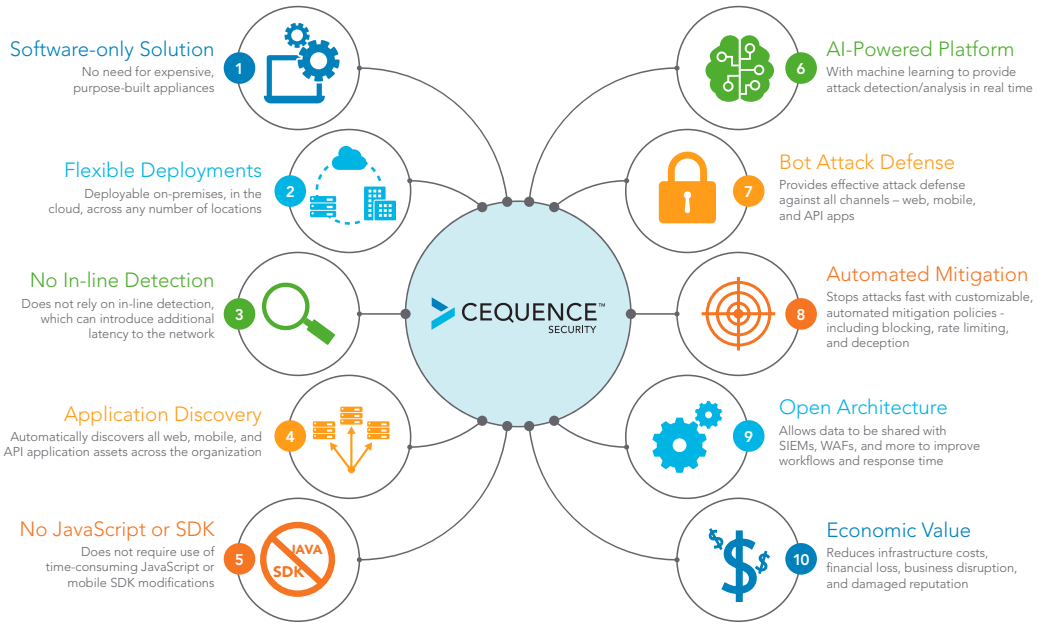
The open architecture of the Cequence platform allows all relevant information to be shared with other systems in the security architecture.

Deployment

Enterprises typically deploy application infrastructures both on-premises and in the cloud. For that reason, Cequence Security offers flexible and lightweight software deployment options that can be deployed rapidly on existing IT infrastructures, including on-premises data centers, private cloud infrastructures, and public cloud resources like AWS. Deployments are infinitely scalable across any number of locations, yet distributed deployments can still be managed as one integrated application security system.

Differentiation

Ten Ways Cequence Security Is Raising the Bar on Application Security:



Learn more or request a demo of Cequence ASP by visiting www.cequence.ai.

CEQUENCE SECURITY
100 Murphy Avenue, Suite 300, Sunnyvale, CA 94086 › 1-408-978-3258 › info@cequence.ai › www.cequence.ai