CAYUGA
NETWORKS

BUSINESS CASE

Closing the Application Security Gap.

Inadequate Web Application Security Exposes Enterprises to Existential Risks

Organizations have traditionally focused security efforts on protecting the network perimeter with firewalls and IDS. However, many of the most damaging high-profile data breaches that have made headlines in recent years started at the application layer. For example, 52% of 2015 Financial Industry breaches targeted web applications, according to Verizon.

Soft Targets

The build-out of the web began over 23 years ago by developers using a variety of languages, antiquated tools, and obsolete server stacks. Security was a low priority for web apps developers. In many cases, the people who developed the web apps have left and are unable to fix vulnerabilities, making updates risky. Accordingly, 40% of banks and 47% of healthcare sites are vulnerable to severe attacks. To make matters worse, resources-constrained IT teams means these vulnerabilities remain exposed for 180 days on average.

Today's hackers can use a variety of free penetration tools, hacking services, and open source data to map weak points. For example, free Google Dorks website hacking searches were used by Iran to hack a New York dam.

Blind Defenses

Historically, most web applications have run naked: unmonitored and without any runtime protection. Where there are security controls in place, they are woefully inadequate because they rely on rules and signatures. For example, organizations have mainly attempted to protect web-based applications by deploying web application firewalls (WAFs) and runtime application self-protection (RASP). However, WAFs often fail to stop simple attacks and are prone to false positives, and because they rely on signatures, they fail to catch zero-day attacks. They also require cumbersome rule management, and their "moment in time" behavior models cannot keep pace with the continuously changing threat landscape.

> **"The gap between application security needs and available technology is huge.**
>
> This AppSec Gap creates a major blind spot, exposing enterprises to very real and present cyber dangers."
>
> — Maurice Stebila, CISO of Harman International

Current RASP solutions are limited by a lack of scope, a shortage of library support, and the need for programmers to change application code. Consequently, they do not offer the capability to protect complex commercial websites, which often include legacy applications.

Since WAFs and RASP have significant shortcomings, enterprises need to augment these defenses with specialized tools and expertise to achieve complete visibility and line-rate analytics. However, until now, even with unlimited budgets, this type of defense has not been feasible. First, the technology was not available to detect anomalies at line rates. Secondly, given the pressures on staffing, even the largest organization would find it almost impossible to investigate every potential attack.

> **"It would be impossible for even the largest security teams to research every security alert.**
>
> Our small team gets tens of thousands of alerts daily. Cayuga Networks provides us with highly actionable reports that are validated and provide full context so we can request the fix without doing any additional work."
>
> — Security Officer, Large University

Too Many Issues, Too Few Security Analysts

Technology shortcomings aside, one of the most pervasive problems is a shortage of security experts, with estimates running as high as a shortage of 1 million professionals. Consequently, alert overload is a real problem: security teams can typically respond to only 5% of alerts.

Finding Needles in Rapidly Moving Haystacks

Cayuga Networks was founded to protect enterprises from the huge deluge of attacks hitting today's web application attack surfaces. Its Decisis™ Next-Generation Web App Attack Detection not only spots indicators of attacks that otherwise go unnoticed in the web request stream, but also intelligently assesses the potential severity of threats and delivers early warnings of the most credible ones.

Only Alerts that Matter

This 100% actionable intelligence provides huge benefits to today's busy, resource-constrained security teams, such as eliminating false alarms. The fused machine/human managed service only warns customers when it determines that bad actors on the Internet know an app vulnerability exists and are actively probing or attacking it. Additionally, when the service does issue an alert, it provides a highly contextual report that enables security teams and owners of the app to quickly remediate the vulnerability.

CAYUGA
NETWORKS

317 N. Aurora St., Ithaca, NY 14850   607.216.9636
info@cayuganetworks.com cayuganetworks.com