Success Story

Microsoft Trusts Rapid7 AppSpider

Building a World-Class Web Application Security Program

When Microsoft undertook an extensive evaluation of Web Application Vulnerability scanning solutions on the market, the company's Cloud and Enterprise Security Services team knew it would be no small task. Microsoft wanted to build a world class, scalable Web App Vulnerability scanning service that would serve all of their different service teams in building secure applications.

Microsoft's Application Security Program

With the technology landscape rapidly evolving, Microsoft foresaw that the homegrown solution it had previously relied upon for application security would soon struggle to keep pace with modern applications with rich, dynamic clients and numerous APIs on the back-end. So the team undertook an extensive, thorough evaluation that spanned several months and settled on AppSpider as one of its Web App Vulnerability Scanners, based in large part on the product's roadmap towards being able to handle complex application ecosystems that have rich clients and RESTful APIs.

"Due to the fact that Microsoft online services are extremely diverse, we started searching for a solution that had a great deal of flexibility and extensibility," said the Principal Security PM Manager at Microsoft. "We also wanted to work with a company that would be an agile partner in ongoing engineering efforts, so they'd need to be receptive to feedback and constantly seeking to innovate and improve. During the proof of concept, we looked at all the industry leaders – AppSpider had the right mix of what we were looking for."

Embarking on the proof of concept, the team knew they'd be looking at a range of products that all had the same basic functionality – in other words, their decision would ultimately boil down to a few key differentiators. The question was, which one would stand out from the rest as the best fit for their environment?

Decision Criteria

A slew of in-depth questions would go into making the decision, such as:

- Given a baseline model, how effective is the scanner in discovering vulnerabilities?
- Are scan results available in a centralized data store that can be easily queried for later analysis and reporting?
- Can built-in reports be easily modified?
- How easily can new vulnerability tests be created and added?
- Can new authentication models be added to the scanner?
- Does the product meet regulatory compliance requirements, such as FedRAMP?
- How easily can built-in documentation be modified?
- Can custom checks specific to Microsoft be supported?

> Top on the list of technical aspects was whether the Web App Vuln Scanning solution could handle the general scale of a company as large as Microsoft.

Another important element was having the ability to develop custom attacks on their own, via API. "We wanted to develop an API with a common interface, with an engine in the background doing the legwork," the PMmanager added. "AppSpider had a good mix of what we needed, and the team particularly liked that the solution had extensibility and a

"False positive rates are extremely important; that's practically a given. So of course our team wants to minimize false positives as much as possible. Coverage was also a key consideration – we don't want to have to get tons of partners to achieve the necessary results."

strong API. That tipped the scale in their favor." Another key consideration involved the fact that AppSpider would be focused on scanning Microsoft applications, so much was at stake: "We use AppSpider but it's our API that we put in front of customers; our reputation is on the line. The fact that AppSpider has a rich API makes our lives a heck of a lot easier."

A strong API and extensibility weren't the only must-have features. The product needed to handle complex authentication schemes with high accuracy: "False positive rates are extremely important; that's practically a given. So of course our team wants to minimize false positives as much as possible. Coverage was also a key consideration – we don't want to have to get tons of partners to achieve the necessary results."

AppSpider's ability to leverage and work with internal tools, was key. However, in addition to specific product features, Microsoft also wanted a vendor with high marks for customer satisfaction. This did not just mean having a responsive support team – the team wanted a vendor who would relish the challenge of working with a large, sophisticated enterprise customer that had particular requirements. "The folks behind AppSpider have very been strong partners. They're nimble and helpful in addressing our needs; whenever we come to them with feedback or future requests, they've made it happen."