CONTRAST SECURITY

CASE STUDY | RETAIL / E-COMMERCE

TRANSFORMING AN APPLICATION SECURITY VISION INTO A REALITY AT A LARGE RETAIL AND E-COMMERCE COMPANY

"I wanted people to think of application security as a key ingredient of the application rather than as an afterthought."

CHRIS | APPSEC MANAGER

ORGANIZATION SNAPSHOT

Industry: Retail / E-commerce

Company Size: Over 25,000 employees; $5 billion in revenue in financial year 2015-16

Contrast Involvement: Protecting 6 major global brands with millions of customers

Application Security: Roadblock to Agile

As the company's retail / E-commerce platform became a leading sales channel, the company transitioned to an agile development process. With that change, this multi-specialty E-commerce company moved from 6-week release cycles to 3-week cycles in order to accelerate innovation. The more rapid release cycles demanded an intense focus on security to avoid brand damage and customer data loss. However, the company found that its existing application security products prevented it from attaining a highly agile process. Application security became a disruption to the release cycle schedule and forced all those involved in the SDLC to reprioritize their work. Chris, the Application Security manager at the company, found himself being in the critical path for every production deployment, as well as being outnumbered in the entire process.

Application Security Drivers

According to the 2016 Verizon Data Breach Investigations Report, web application attacks are the leading source of data breaches – a fact not lost on the company. So, while PCI is a regulatory mandate for the E-retailer, protecting its brand and customers from data breaches is equally important. To make application security a proactive and continuous process, Chris was looking for a product that could be automated like other agile tools, could eliminate delays, and could provide the visibility and context necessary to remediate vulnerabilities. With a small Application Security team and billions of dollars at stake, it was critical for Chris to change the perception of Application Security from being the gatekeeper to being the security enabler. "I wanted people to think of application security as a key ingredient of the application rather than as an afterthought," Chris stated.

Scanning Challenges

Traditionally, application security at the company was done at the integration testing phase, which was one step before the application was released to production. The company used leading commercial SAST and DAST products, but those took up to 24 hours to produce reports and were still prone to human error. The Application Security team would then go back to the engineers to get a fix for these issues, only to find out that the issues were either false positives or irrelevant. Moreover, because this was happening so close to the final release into production, the process either added significant "rework cost" (i.e., time stolen from other planned work) or postponed security fixes to a later application release. Chris noted that to work around the complexities of the existing application security products his team would reluctantly pressure developers to fix reported vulnerabilities before the weekend. That way, in an effort to be less disruptive, the Application Security team could re-run DAST scans over the weekend. However, this solution became difficult for the entire team to manage.

Strained Processes

The company's past application security processes were placing a strain on the organization in multiple ways. First, the entire process of vulnerability scanning and remediation added a delay of weeks to every release. As a result, only items designated as Critical and High got the development team's attention, and the issues marked as Medium and Low became just "nice-to-haves." The second impact was on the Application Security team, which had to handhold the DAST solution through its scanning process. The team's active involvement in every release cycle meant that as a small team it was unable to stay on schedule. Finally, it was difficult for the company to manage security at an application – or enterprise – level with the information the company had. Specifically, the Development team knew it had vulnerabilities to address, but it did not know the root causes. The team also needed more details to resolve the vulnerabilities, and there was no automated way to capture the necessary metrics.

DISCOVERING CONTRAST

In order to gain visibility, better allocate resources, and get rid of the delay in the application security step, Chris was actively looking for a product that would seamlessly integrate into the existing SDLC chain and improve security processes there. However, DAST products were slow and needed a lot of manual effort, which would make it impossible to scan the entire application using them. SAST products covered more of the application, but were highly inaccurate because they couldn't discover vulnerabilities in the running application.

While reading about various application security products in the Gartner Magic Quadrant, Chris came across Contrast. Contrast's vision instantly resonated with his own: continuous application security in real-time. When it came to testing the product, Chris was glad that Contrast delivered on what it promised. "I was very surprised by the ease of deployment as well. Simply running the application with the Contrast agent got things up and running. The agent can be turned on and off by a click of a button, and provide visibility to anybody in the chain," Chris said. He was also glad to see how easily he could integrate the agent into the list of tools that the company already used.

"I was very surprised by the ease of deployment as well. Simply running the application with the Contrast agent got things up and running. The agent can be turned on and off by a click of a button, and provide visibility to anybody in the chain."

CHRIS | APPSEC MANAGER

BECOMING AGILE

Since making the switch to Contrast, the Application Security team at the company is no longer the bottleneck. The team has been able to keep pace with the other teams involved in the application development and release cycles, while being more effective overall. "I am able to work along with my project teams, instead of working against them," Chris said.

"I am able to work along with my project teams, instead of working against them."

CHRIS | APPSEC MANAGER

With an automated application security process built on Contrast Assess, applications now report their vulnerabilities as they are tested. There is no longer a separate application security scanning step during the release cycle. This has helped the company eliminate the delays that were caused by the additional scanning step and become truly agile.

Contrast Assess has also given Chris and his team the ability to drill down to application-level detail and inform the engineering team exactly what vulnerabilities to fix, where to fix them and how to fix them – all in real-time – as issues are detected. His team also has quick and easy access to organization-level metrics, which it is able to share in order to keep everybody informed and involved. Chris also found it easy to work with the Contrast team. "We were able to ask for product enhancements that we thought would be helpful to us, and get those enhancements implemented."

CONTINUOUS APPLICATION SECURITY

The switch to Contrast helped this global E-commerce company reach its vision for security across all its applications and brands, and protect its customers. Chris is now able to inform and "security-enable" teams at every level. Contrast delivered the visibility, real-time vulnerability detection, and automation required to make security a core discipline of application development at the company.

CONTRAST SECURITY

240 3rd Street
Los Altos, CA 94022
888.371.1333

102416