COALFIRE

CASE STUDY

Contrast Security leverages Coalfire-authored white paper to map powerful technology with compliance standards

AT A GLANCE

Contrast Security's software security platform transforms application security by making software self-protecting. Intelligent Contrast agents integrate into application code, equipping applications with smart, agile sensors that detect and correct vulnerabilities before software deployment and protect applications in operation. For Contrast, evaluating its products against security best practices and compliance standards is critical for doing business with payment entities.

CHALLENGE

Contrast developed and launched Contrast Assess and Contrast Protect to help customers identify and mitigate risks earlier in the software development lifecycle. The security suite from Contrast provides always-on and continuous detection and protection through interactive application security testing (IAST), runtime application self-protection (RASP), and software composition analysis (SCA).

To expand into the payment industry marketplace, Contrast needed to demonstrate how Contrast Assess and Contrast Protect could effectively address important Payment Card Industry Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and Payment Card Industry Software Security Framework (PCI SSF) requirements. Furthermore, they wanted to be able to share a third-party validation to support sales and marketing efforts.

After a vendor evaluation, Contrast engaged Coalfire to independently validate how security practitioners can use Contrast Assess and Contrast Protect as part of their compliance programs to identify and defend software vulnerabilities. Coalfire was ultimately chosen based on their compliance expertise and experience writing numerous objective product applicability guide white papers.

APPROACH

Using security best practices and customized testing methodologies, Coalfire assessed Contrast's products' capabilities against the standards for compliance. Coalfire reviewed documentation and interviewed subject matter experts, solution architects, developers, and other key stakeholders. “The Coalfire team was great at time management,” stated Erik Costlow, developer advocate for Contrast. “Everything was well-tuned at each meeting, from documentation to demo.”

The security technology solution was set up in a lab environment and integrated into an intentionally vulnerable web application. Using the lab environment, Coalfire independently tested Contrast’s capabilities of their IAST, RASP, and SCA features to identify vulnerabilities in code (custom code and open-source software libraries and frameworks), measure the exploitability of vulnerabilities based on use of the code, remediate vulnerabilities through developer guidance and virtual patching, and protect the application against attempted exploitation. Costlow expands on the methodology, “Coalfire never just took our word. We had to prove everything in the lab and explain how it worked for customers in the wild. This independence, expertise, and strong validation are among the reasons we selected Coalfire.”

After comparing the Contrast technology to many existing approaches, Coalfire formed the following opinion: “The capabilities of Contrast Protect allow the software to be protected with greater fidelity than what is offered by traditional software security approaches (for example, web application firewalls).” Coalfire further aligned the tested capabilities with security outcomes and requirements of PCI DSS for application protection, as well as PA-DSS and PCI SSF for supporting secure software lifecycle (SLC) requirements for developing secure payment applications.

RESULTS

In coordination with Contrast, Coalfire wrote and published a white paper on how Contrast Assess and Contrast Protect function within an organization and meet security best practices and multiple compliance standards, including PCI DSS, PA-DSS, and PCI SSF.

“The white paper is clear and includes a table that lists different parts of the standards alongside how they apply,” explains Costlow. “This table helps guide discussion with parties who know the standard.”

The report has assisted Contrast’s ability to grow within the PCI and provide more tailored content at industry events.

The full report is available from Contrast Security at https://www.contrastsecurity.com/pci-compliance.

COALFIRE.

About Coalfire

Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe. For more information, visit **Coalfire.com.**