

Securing Digital Applications and Improving Compliance with Continuous Dynamic

Company overview

This financial services company—one of the largest financial firms in the U.S.—needed to

- Ensure stronger application security for all consumer-facing applications
- Reduce time and resources used on triaging false positives
- Improve risk and compliance

It chose Black Duck Continuous Dynamic to

- Provide automated and highly accurate results
- Improve compliance and risk management
- Accelerate time to remediation
- Gain instant insights into critical vulnerabilities and enhance decision-making
- Enable quick turnaround from the support team

“Application-level protection provides us with an invaluable layer of security for our platform and our customer data. Continuous Dynamic is extremely beneficial to us in reducing security vulnerabilities and risks.”

—Application Security Lead

Overview

This financial services firm’s partnership with Black Duck helped achieve effective and long-term risk and cost reduction. By protecting business-critical applications, Black Duck® Continuous Dynamic empowers this organization to secure its digital future.

The challenge

This financial organization is one of the largest online brokers in the U.S., so application security is a top priority. It needed to improve the security of its business-critical applications and identify vulnerabilities, such as those that would provide the ability to access other users’ account information, access other users’ message attachments, access admin functionality without admin-level access, and access authenticated functionality without a valid authenticated session. It also needed faster and more accurate remediation to ensure security assurance and risk compliance.

The solution

The organization chose Continuous Dynamic from Black Duck and have been using it for more than eight years to continuously analyze its most critical applications. Automation, easy integrations, accuracy of findings, and on-demand security testing expertise have helped mitigate issues in production. In addition, in-depth manual penetration testing of the application layer has been highly effective in finding complex business logic vulnerabilities that cannot be discovered by scanners alone.

Continuous Dynamic

- Delivers the highest level of accuracy with AI-enabled vulnerability verification and additional human verification to ensure near-zero false positives
- Provides continuous and concurrent, always-on risk assessments
- Is production-safe with no degradation in performance of production websites and applications
- Includes business logic assessments for vulnerabilities that scanners cannot discover
- Tracks real-time and historical data to measure risk exposure over time
- Helps meet requirements around application security in PCI DSS compliance
- Is scalable to fit any environment and match the pace of development

The results

Continuous Dynamic provides industry-proven web application security for modern and traditional websites, web applications, and frameworks.

Highly accurate findings

Continuous Dynamic enables the development team to assess applications in preproduction and production environments, so they can view vulnerabilities in a larger, more accurate context. Comprehensive and continuous scans find runtime

***“Continuous Dynamic—
it’s simple, it works.
Continuous Dynamic gets
me useful information
that I can transact on.”***

–Application Security Lead

***“Black Duck security
experts have been highly
responsive and provide us
with high-quality subject
matter expertise that
helps us remediate and
mitigate vulnerabilities
accurately and efficiently.”***

–Application Security Lead

***“Black Duck customer
service has been
outstanding, and support
staff is extremely helpful
to quickly schedule and
escalate business logic
assessments as needed.”***

–Application Security Lead

vulnerabilities that are tough to spot through source code analysis alone. And Black Duck security experts serve as an extension of the development and security teams by verifying results and eliminating false positives—over 9,500 since 2015.

Improved compliance and risk management

Business logic assessments (BLAs) are manual assessments performed by security engineers to look for application vulnerabilities that cannot be effectively found in an automated fashion. For development and security teams, BLAs complement the automated testing of Continuous Dynamic and help ensure regulatory compliance. These vulnerabilities include cross-site scripting, fingerprinting, content spoofing, cross-site request forgery, URL redirector abuse, brute force, and more.

More than 22% of the total vulnerabilities found were detected through the BLAs. Around 80% of the vulnerabilities found through BLAs had Critical to Medium rating.

Collaborating closely with Black Duck threat intelligence experts, the organization’s security team is able to identify real-time threats faster and share their findings with others in the organization.

Critical integration accelerates time to remediation

Integration with issue-tracking systems such as Jira enables the development team to deliver secure applications at the speed of development. As vulnerabilities are discovered in Continuous Dynamic, they are pulled into Jira to help ensure faster remediation. As vulnerabilities are retested, the integration allows developers to use Continuous Dynamic’s Ask A Question feature directly from the issue in Jira.

Valuable insights and reporting

The Continuous Dynamic dashboard and reports provide critical insights to the security team, enabling them to better understand security risks, prioritize remediation for critical vulnerabilities, and evaluate the results of the application security program. An overview of status, risks, and trends empowers managers, improves decision-making, and ensures that high-priority vulnerabilities are remediated. And expanded visibility across the entire application security program enables the security team to better manage risks and reduce exposure to data breaches.

Excellent customer service and support

The Black Duck support team helps align people, processes, and technology to achieve operational readiness. Working closely with the security and development teams in managing support services, vulnerabilities review, and more has ensured rapid problem resolution.

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.

©2024 Black Duck Software, Inc. All rights reserved. Black Duck is a trademark of Black Duck Software, Inc. in the United States and other countries. All other names mentioned herein are trademarks or registered trademarks of their respective owners. October 2024