

Document Logistix Combines SAST and DAST to Ensure Security of Sensitive Customer Data



Company overview

Since 1996, Document Logistix has supplied its uniquely affordable and scalable Document Manager software to a variety of SME and blue-chip clients around the globe. The company's U.K. and EMEA operations are headquartered in Milton Keynes, U.K., which is also its central point of product development, technical support, and training. The U.S. branch of the company is headquartered in Austin, Texas, and it has major contracts with the Texas Department of Public Safety, the Virginia State Police, and various agencies in other states. Document Logistix won Document Manager magazine's prestigious award for the 2018 Product of the Year for Workflow and BPM.

Summary

Document Logistix creates document management solutions that help eliminate the use of paper, improve records management, and automate business processes. Its software powers the operations of some of the world's most demanding, high-document-volume businesses, including major logistics companies like DHL and CEVA. These customers entrust Document Logistix with the handling of their information—much of which is highly sensitive or confidential—so security is a high priority.

Seeking a higher level of confidence in its application security testing, the company turned to Synopsys to secure its DevOps environment and automate its processes. Combining WhiteHat™ Dynamic for dynamic application security testing (DAST) with static application security testing (SAST), Document Logistix updated its application security program to better protect its customers' sensitive data. The company also relied on the security experts from WhiteHat Threat Research for added assurance in uncovering security vulnerabilities.

The challenge

Document Logistix's application Document Manager provides a flexible platform for paperless business processes and highly efficient archiving. Because it's not designed for a specific market, Document Manager is customizable for a large range of business processes, including those as straightforward as proof of delivery, where the risk of data loss is fairly minimal, and those involving more sensitive information like human resources records. This is especially important since the EU's General Data Protection Regulation (GDPR) went into effect, which has financial penalties for noncompliance.

Attorneys general in the U.S. also use Document Manager for disclosure purposes, publishing prosecution case material to defense attorneys. Failure to protect this information could lead to mistrial.

With such high stakes, Document Logistix has always been focused on protecting customer data, but the company lacked a true application security solution. Several of its clients performed their own penetration testing and submitted issues to Document Logistix to remediate. The company also had internal staff checking code manually for security vulnerabilities, but this proved to be time-intensive and costly. The company needed an in-house solution that was both cost-efficient and effective.

“With DAST, we have confidence in saying to our customers ‘this is what was done to make your information more secure,’ and they know that every time there’s a new build of the application, it gets a new test”

—Tim Cowell, Founder, Document Logistix

The solution

Document Logistix used SAST to scan code for errors and ensure secure product design. It then added WhiteHat Dynamic to detect and assess code changes in running applications, alert of new vulnerabilities, and provide reporting and intelligence metrics.

WhiteHat Threat Research provided Document Logistix with an added layer of protection against security vulnerabilities. At the end of each day, any new code was uploaded to Threat Research, checked by a Synopsys security expert, and sent back to Document Logistix in an automated report that identified anomalies to be addressed.

The results

The combination of SAST and DAST provided Document Logistix with a platform for testing its application and DevOps environment, automating the processes required to comply with the complex rules of paper and electronic document management. This included full auditability of its application, the ability to plan workflows, perform complex retention policy management, and define policies for certain classes of documents, including what documents should or shouldn’t be disclosed and to whom.

The Synopsys difference

Synopsys provides integrated solutions that transform the way you build and deliver software, accelerating innovation while addressing business risk. With Synopsys, your developers can secure code as fast as they write it. Your development and DevSecOps teams can automate testing within development pipelines without compromising velocity. And your security teams can proactively manage risk and focus remediation efforts on what matters most to your organization. Our unmatched expertise helps you plan and execute any security initiative. Only Synopsys offers everything you need to build trust in your software..

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com

©2023 Synopsys, Inc. All rights reserved. Synopsys is a trademark of Synopsys, Inc. in the United States and other countries. A list of Synopsys trademarks is available at www.synopsys.com/copyright.html. All other names mentioned herein are trademarks or registered trademarks of their respective owners. January 11, 2023 11:08 AM