WhiteHat SECURITY

Customer Case Study

wiredrive

Managing and Mitigating Risk at a Lower Cost

Project Background

The Wiredrive story begins in 1999 with Bill Sewell, Taylor Tyng, and Mitch Bassett creating a design agency which grew to serve the nation's top ad agencies and production companies. To better share large images and large files with customers, they built what became Wiredrive – a system that would flawlessly share large files and serve as a single spot to collaborate and collect all reviews for a project.

Wiredrive's capability of transferring large files, while also being highly adaptable, makes it the premiere file sharing platform for editing videos, sharing files, and collaborating with your team and clients. With a focus on rich media sharing, Wiredrive maintains the ability to retain HD quality of videos, images, and audio throughout large file transfers.

Wiredrive uses the latest cryptography methods in separate databases with expiration rules enforced in all environments. Additionally, it boasts an A+ security rating and is constantly monitored for vulnerabilities through consistent penetration testing. Wiredrive chose WhiteHat to reduce the time to it takes to fix their vulnerabilities, with a commensurate low false positive ratio, to reduce cost of remediation and maintain that high level of security.

As they evaluated various vendors for AppSec solutions, Wiredrive started doing Source Code (SAST) scanning with a pure-play SAST vendor. So why switch to WhiteHat Security? Daniel Bondurant, Chief Technology Officer, refers to total cost and ease of use. "As we grew our codebase, the other SAST tool was becoming price prohibitive."

The Use Case

Wiredrive embeds security through all phases of the Software Development Lifecycle. They used Source code scanning to review during the Development and QA testing. Daniel Bondurant, Wiredrive's Chief Technology Officer, says, "Static code scans have found problems before they go to production." Wiredrive uses Sentinel Source to scan the master branch in their code repository, although they also use Jenkins to build and deploy.

Their previous configuration with the alternative SAST vendor required running an on-premise dedicated server, which Bondurant says was challenging to set up. "With Whitehat, we use a very lightweight VM. Setup was very fast and straightforward."

WHITEHAT SENTINEL DYNAMIC KEY BENEFITS

- Easy to manage, SaaS based platform
- Run scheduled assessments daily or on demand
- Near zero false positives
- Advanced analytic capabilities to monitor trends and key statistics like remediation rate, time to fix vulnerabilities, and age of vulnerabilities
- Built-in PCI DSS reports
- Executive Dashboard
- WhiteHat Security Index
- Peer Benchmarking

WHITEHAT SENTINEL SOURCE KEY BENEFITS

- Assess code at any point in the development cycle – even partial code
- Run scheduled assessments daily or on demand
- Scan source code from any repository on premises
- Rule Packs identify and verify vulnerability defects
- Backed by Threat Research Center consultation

Bondurant indicates that with Checkmarx, it was very hard to track down the exact problem and there were many unfiltered inputs. Their legacy SAST tool interface would list hundreds of attack vectors, but when drilling down it was only one. Getting to the single problem was very time consuming. With Sentinel the results are filtered, so getting to the single problem was extremely easy. Sentinel identifies specific attack vectors which were easy for Wiredrive to reproduce, then build a test to make sure it doesn't happen again.

But a source code look isn't always the whole picture, and sometimes there are changes introduced by other teams which can challenge any DevSecOps team. Bondurant needed Dynamic scanning to track their entire web application portfolio across all their customers. Dynamic scanning and subsequent scoring via the WhiteHat Security Index allowed Daniel Bondurant, Wiredrive's Chief Technology Officer, to identify and then prioritize problems wherever they crop up.

"Using our old tool, the explanations for the vulnerabilities were always generalized. WhiteHat provides specific attack vectors, so we can easily reproduce, and build a test to make sure it doesn't happen again," Bondurant says.

But there can still be a gap between a vulnerability found and a vulnerability patched, and this is where a low risk tolerance demanded additional measures. Wiredrive chose to enable a Runtime Application Self-Protection (RASP) solution, with full product level integration with WhiteHat Sentinel Dynamic, against their critical assets. With RASP, Bondurant can mitigate Sentinel Dynamic-detected vulnerabilities automatically.

THE WHITEHAT DIFFERENCE

- 24x7 Access to Threat Research Center for Q&A on vulnerabilities as well as remediation advice
- WhiteHat Sentinel PE, SE and BE services exceed requirements of PCI DSS by providing ongoing, verified vulnerability assessments for both internal and public websites
- Open API integration with bug tracking systems, SIEMs, GRC, and WAF products

The Result

Bondurant finds WhiteHat Security results to be the most valuable in reducing Wiredrive's time to fix through virtually no false positives, and detailed descriptions of vulnerabilities with advice on how to fix them. This has reduced the total cost of remediation, as 24x7 access to the Threat Research Center for advice has effectively extended the Wiredrive DevSecOps team. They've minimized their window of exposure due to always-on risk assessment, combined with RASP blocking and notification.

For all of this, they've simplified their application security portfolio through one, easy-to-use platform in Sentinel, where all the results are displayed and available for reporting. Bondurant says they have reduced their time to remediate vulnerabilities between 10% to 24% since starting with Sentinel.

Additionally, the performance, reliability, and scalability are all best in class. "The reporting capabilities provide an easy compliance report to give to board and clients," says Bondurant.

Risk lower, cost lower, mitigation achieved. Wiredrive's AppSec Mission accomplished!

RUNTIME APPLICATION SELF-PROTECTION BENEFITS

- Immediate protection against attacks
- Simultaneously detect and mitigate vulnerabilities, lowering exposure time
- View both detected and mitigated vulnerabilities in the Sentinel interface
- Allow time for development teams to remediate critical vulnerabilities
- Reduce risk through lowered vulnerability exposure

WHITEHAT SECURITY, INC. 3970 Freedom Circle Santa Clara, CA 95054 • 1.408.343.8300 • www.whitehatsec.com