🟩 CASE STUDY

Enhancing Cybersecurity Operations at an Automotive Digital Marketplace Company Overview

This B2B automotive auction platform and provider operates throughout the United States. In addition to their wholesale digital vehicle marketplace, they also operate related lines of business offering value-added services such as vehicle finance, transportation, and data services for dealers. Data security is a significant organizational priority, and the company strives to ensure that information remains confidential, accurate information is presented during transactions, and financial transactions are secure.

The head of cybersecurity has been with the company for several years and leads multiple security programs including application security, endpoint detection and response (EDR), incident response (IR), product security, and security operations (SecOps) engineering, which includes cloud and infrastructure security.

Challenges

While exploring avenues for improving cybersecurity operations within the organization, the cybersecurity leader highlighted the challenges within their vulnerability management (VM) program, citing the difficulty in aggregating data from various tools like traditional vulnerability scanners, software composition analysis (SCA), static application security testing (SAST), dynamic application security testing (DAST), API security tools, and cloud security posture management (CSPM). The absence of a centralized platform made prioritizing vulnerabilities a daunting task.

PROFILE

Location
Northeastern U.S.

Industry
Automotive Ecommerce

Customer Size
2000+ employees

BACKGROUND

Zscaler Unified Vulnerability Management (UVM), provides continuous risk management, giving large enterprises contextual insights into their top security issues and automated workflows to reduce cyber risk. Built on the patented Data Fabric for Security, the platform curates and correlates data from 100s of sources, in any format and scale, to aggregate risk factors, mitigating controls, and business context.

Solution

After encountering limitations with first-generation vulnerability aggregators and experimenting with next-gen aggregators, the security leader learned about UVM from an advisor. The team was impressed by the immediate functionality of the platform, with actionable insights for prioritization and more efficient workflows, as well as the longer-term potential of the data fabric at the heart of the UVM platform.

Although they are still in the early stages of implementing Zscaler UVM, the team is pleased with the metrics obtained and the platform's ability to deliver critical information to the business. The team also has a lot of expertise and agility, so we were able to complete our evaluation quickly and see fast wins in improved vulnerability assessment and remediation verification.

Outcomes

Looking forward, the company plans to expand coverage for more applications and streamline workflows through automation, envisioning an ideal state where vulnerability management is seamlessly integrated into the development pipeline.

Summary of the company and Zscaler UVM

- **Aggregation of information from any data source**
  The UVM platform enables the company to consolidate data from disparate cybersecurity tools, providing a centralized view of vulnerabilities across the organization's tech stack.
- **Actionable insights and metrics**
  Zscaler UVM provides the company with actionable insights and metrics, empowering the cybersecurity team to make informed decisions about which fixes would be most effective and ways to communicate security posture to the business.

> "We're already saving a lot of hours each month, and we're building out more reports and dashboards to benchmark and see trending on remediation by different teams."
>
> —The Head of Cybersecurity

- **Accelerate response and remediation**
  The UVM automation capabilities streamline vulnerability management workflows, accelerating response times to security incidents. By identifying top security issues proactively, Zscaler helps the company minimize its exposure to cyber threats and enhance its overall cybersecurity resilience.

> "Like most companies, we had all our data coming from different systems, so our teams were stuck trying to use Excel to tie together related information."
>
> —The Head of Cybersecurity

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com