STACKHAWK

AWESOME CUSTOMER SUCCESS STORY

Growing Health Tech Leader Standardizes Security Across Five Business Units

BACKGROUND

A healthcare and data technology company comprised of five distinct business units faced significant security challenges stemming from rapid growth and decentralized operations. The company was grappling with the complexities of maintaining a robust security program across a diverse and rapidly expanding landscape. Each of these units operated with its own established workflows, development methodologies, and security protocols. This decentralized approach created a significant challenge for the central security team. The lack of standardized processes and tooling across the organization resulted in inconsistent security practices, leaving potential gaps and vulnerabilities exposed.

The rapid growth of the company also placed immense pressure on the small security team, who were tasked with safeguarding the development efforts of all five units. The sheer volume of applications and APIs, coupled with the absence of a centralized inventory, made it exceedingly difficult to maintain a comprehensive understanding of the organization's security posture. Manual spreadsheets, the primary tool for tracking testable applications, proved inadequate, prone to errors, and time-consuming.

HealthTech

Use Case

Standardizing and Scaling Security

Industry

Health Tech

Employees

+650

Location

USA

THE PROBLEM

Rapid growth and decentralized operations led to inconsistent security practices and a lack of centralized visibility, straining the small security team.

THE SOLUTION

The company implemented StackHawk for automated API discovery and CI/CD integrated security testing, providing centralized control.

THE RESULT

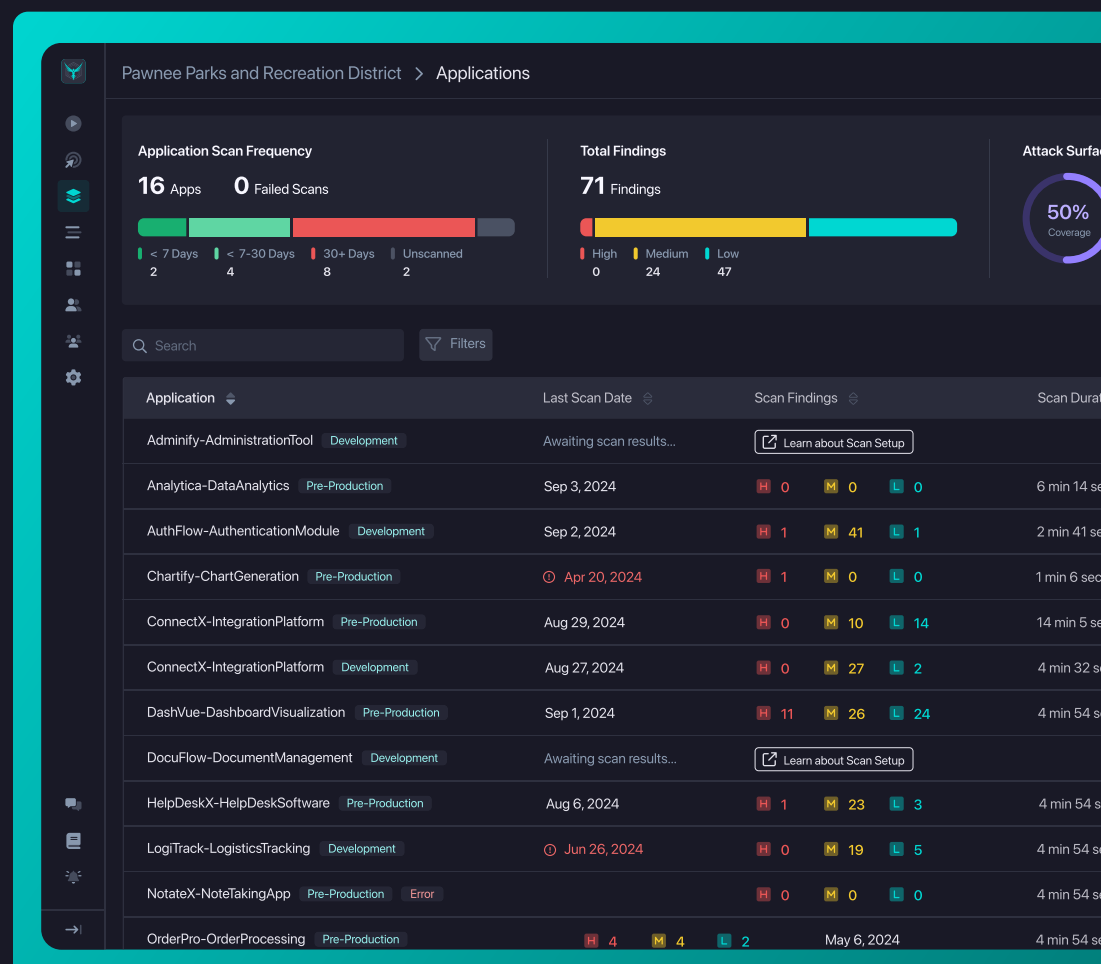
Improved visibility, efficiency, and standardized security practices, enabling proactive vulnerability management and reducing risk.

CHOOSING A SOLUTION

Recognizing the urgent need for a more efficient and scalable security solution, the company sought a solution that would provide centralized visibility and automated security testing. After evaluating several options, they chose StackHawk for its:

Automated Security Testing in the SDLC

Embedding security testing in the software development lifecycle was crucial for the company, as it would enable developers to identify and remediate vulnerabilities early in the development process, reducing the risk of costly and time-consuming fixes later on. StackHawk is designed to work where and how developers work, making security testing part of their normal development workflow.



Automated API Discovery

The company had a large attack surface with over 1,700 repositories, creating a significant backlog and headache for their security engineer to try to figure out what repositories are out there and which ones they need to be interested in. The vast number of repositories spanned across multiple Azure DevOps organizations had inconsistent groupings and manual tracking, making it impossible to prioritize which repositories needed to be scanned.

StackHawk's API Discovery enabled the company to gain a comprehensive view of its application security landscape by building an internal database of repositories and metadata to help identify and prioritize the most important repositories and streamline the process of correlating repositories to teams/projects. They have since been able to eliminate the reliance on manual spreadsheets and maintain an accurate view of the organization's attack surface in real-time.

> *Every element of the StackHawk experience has been amazing from the beginning. It's a sign of a strong partnership.*
>
> - Chief Security Information Officer

EXPERIENCE WITH STACKHAWK

Since rolling out StackHawk, the company has seen significant improvements in its overall security posture and operational efficiency, including:

Enhanced Visibility

StackHawk provides a clear and comprehensive view of all applications and APIs requiring security testing, eliminating the guesswork and manual tracking that previously hindered their efforts. This enhanced visibility has also improved their ability to coordinate between different teams to address application security issues when they arise.

Improved Efficiency and Scalability

Automating security testing empowered the company's small security team to effectively support the development teams across all five business units. This scalability was crucial for accommodating the company's continued growth.

Standardized Security Practices

By centralizing security testing with StackHawk, the company is starting to standardize security practices across its diverse business units, creating a more consistent and powerful security posture.

Proactive Vulnerability Management

By discovering and identifying vulnerabilities earlier in the SDLC, the company is able to remediate issues before they reach production, reducing risk and improving overall security.