anchore

CASE STUDY

ModuleQ reduces vulnerability management time by 80% while meeting the highest regulatory compliance standards

ModuleQ, an AI-powered enterprise knowledge solution, reduced vulnerability management time by 80% with Anchore Enterprise while meeting regulatory compliance for the financial services industry. Anchore Enterprise integrated seamlessly into ModuleQ's existing DevSecOps workflow supporting enterprise deployments and now automates previously manual vulnerability processes.

moduleQ

Cupertino, CA
www.moduleqcom

INDUSTRY
Software development

SEGMENT
Enterprise Knowledge AI Copilot

Challenges

- Identify, triage and analyze constant flood of new vulnerabilities with limited resources
- Ensure critical vulnerabilities never reach production without disrupting developer workflow
- Address regulatory compliance demands for strict container security requirements

Solutions

Anchore Enterprise secures the software supply chain with:

- Turnkey container vulnerability scanning, triage and analysis
- Cloud native integration enabling proactive vulnerability notification and remediation workflow
- Support for enterprise deployments to meet uncompromising compliance requirements

Results

- 80% reduction on time spent managing vulnerabilities
- 50% less time on security tasks for production deployments
- Built immediate trust with financial services customer base

Introduction

ModuleQ's enterprise AI software delivers timely, proactive customer insights by anticipating user needs, helping organizations streamline their decision-making processes. Operating in the highly regulated financial services industry, ModuleQ deploys its solutions directly within customer-controlled tenants, ensuring data security and compliance.
The software is built using a robust development stack that includes .NET and C#, with Azure DevOps Pipelines driving the build environment. The platform consists of a single application made up of dozens of microservices, utilizing a multi-stage pipeline to ensure stability and security. As code progresses from nightly builds to production, container scans are automatically run to identify vulnerabilities, ensuring secure and seamless deployments.

Challenge

» Managing constant flood of new vulnerabilities with limited resources

With a small but dedicated team, ModuleQ was straining under the weight of the constant flood of new vulnerabilities released. High-profile security incidents like the Log4j supply chain attack and Crowdstrike incident only served to highlight the importance of vigilant vulnerability management. The sheer volume of new vulnerabilities—25,000 in 2023 alone—was overwhelming ModuleQ's manual processes.
ModuleQ quickly recognized their current systems were no longer scaling with the resources on hand and started researching a turnkey vulnerability management solution that automated vulnerability scanning, management and analysis.

» Ensure crictial vulnerabilities never reach production without disrupting developer workflow

In the high-stakes threat environment that ModuleQ operates in they found that requiring engineers to break out of their workflow and manually review vulnerabilities didn't meet the security posture they needed. Each time their developers switched to a traditional, passive vulnerability management dashboard, they would lose context. This led to concerns around potentially missing critical vulnerabilities. With limited resources and the constant pressure to secure sensitive data, a natively integrated DevSecOps solution was needed to retain the high velocity of their software delivery and maintain the highest possible security guarantees.

This called for a vulnerability management platform that embedded into their existing DevSecOps ecosystem. By directly integrating vulnerability scanning and management into their existing automation tooling they could remove all manual intervention from vulnerability scanning, triage and reporting.

» Address regulatory compliance demands for strict container security requirements

ModuleQ specializes in deploying its enterprise AI software into customer environments operating in the highly regulated financial service sector. To meet the expectations of clients, ModuleQ needed a partner capable of supporting enterprise deployments while guaranteeing airtight security. These institutions operate in high-stakes environments where even a minor security lapse can have catastrophic consequences, especially with sensitive content like Microsoft 365 and Salesforce data.
Deployments are often conducted directly by the financial institutions themselves, meaning no data can leave the client's secure environment. This created the need for a security solution that could operate effectively without external network access, delivering bulletproof protection against sophisticated threats from state-sponsored actors and cybercriminals.

Anyone can push out code quickly. Can they push secure code with the highest confidence that it fits the risk profiles of critical national infrastructure like financial services?.

—Joseph Zuromski, VP of Engineering, ModuleQ

Solution

ModuleQ selected Anchore Enterprise as their container vulnerability solution to solve the challenges presented by their customer base:

» Turnkey container vulnerability scanning, triage and analysis

Anchore's container vulnerability scanning and analysis platform helped ModuleQ automate and streamline its security processes. Previously manual security reviews of software builds heavily taxed the engineering team. With Anchore Enterprise, ModuleQ now automatically scans all software builds nightly, stores the reports for reference and analyzes the identified vulnerabilities to determine prioritization in the development cycle.
Anchore Enterprise automates each step of this process and provides the analysis tooling to quickly derive actionable security insights. ModuleQ is now able to de-risk their software deliverables and free up their developer's time for new features rather than hunting down low-signal vulnerabilities.

Anchore was one of the first tools that we brought on. It was recommended by our CISO who has been deeply involved in the security community for decades.

—Joseph Zuromski, VP of Engineering, ModuleQ

» Cloud native integration enabling proactive vulnerability notification and remediation workflow

Anchore Enterprise was designed to be integrated directly into any modern, cloud native DevSecOps pipeline to help organizations shift security left from release time earlier into the development cycle. By embedding vulnerability scanning and reporting directly into their CI/CD pipeline, ModuleQ stops crucial vulnerabilities from slipping into production with the reliability guarantees of a fully automated system.
Anchore Enterprise automatically reports all HIGH and CRITICAL vulnerabilities directly to the build runner which immediately breaks to prevent these vulnerabilities from being promoted to production. This provides immediate feedback to the engineering team and initiates the remediation process. This proactive security posture prevents any potential disastrous vulnerabilities from being missed and reduces time wasted by developers context switching out of their existing workflow.

On top of this, Anchore's support for ModuleQ's existing developer toolchain—including Azure DevOps Pipelines, .NET, and C#—was paramount. The benefits that Anchore Enterprise brings to ModuleQ are possible because of Anchore's support for the Microsoft ecosystem of development tooling.
.

» Support for enterprise deployments to meet uncompromising compliance requirements

ModuleQ selected Anchore Enterprise for its support for on-prem deployments. Given that ModuleQ's customers expected on-prem deployments to safeguard their data, Anchore was able to reinforce ModuleQ's commitment to meeting and exceeding these security expectations.
Anchore's platform was designed from the ground up to operate in on-prem and even air-gapped environments, ensuring that no external connectivity is required. These design choices gave ModuleQ the confidence that Anchore was the trusted partner to support container security needs of their demanding customer base.

Results

The implementation of Anchore Enterprise transformed ModuleQ's security posture and business operations::

» 80% reduction on time spent managing vulnerabilities

By leveraging Anchore's automated scanning and reporting capabilities, ModuleQ reduced the time spent managing vulnerabilities. This unlocked efficiency gains allowing the team to focus on developing new features and improving customer satisfaction.

» 50% less time on security tasks for production deployments

Anchore Enterprise's cloud native integration and proactive vulnerability management system streamlined ModuleQ's production deployment process, cutting security task time in half. This allowed ModuleQ to maintain its rapid cadence of software delivery while maintaining the highest level of security.

» Sinificantly increased confidence that newly shipped customer releases will meet the highest security requirements

Anchore's experience with on-prem deployments gave ModuleQ the confidence that their software releases would meet the rigorous security standards of their financial services clients. This confidence translated into stronger customer relationships and trust in ModuleQ's security posture.

"I can't emphasize enough, there is a ton of scrutiny around security—especially around our containers. We deploy into large banks and financial institutions worldwide. You can imagine the security involved with these types of deployments. Anchore is a key component in making these deployments successful."

—Joseph Zuromski, VP of Engineering, ModuleQ

By leveraging Anchore Enterprise, ModuleQ has positioned itself as the trusted partner with the expertise to meet the highest levels of security and regulatory compliance.

Request a demo

anchore

sales@anchore.com
anchore.com