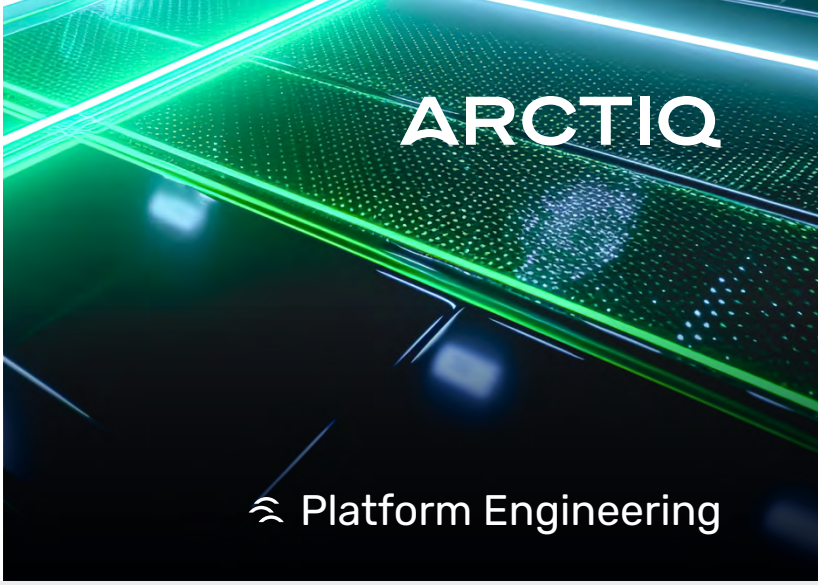
Architect Transformation

DevSecOps

Application Security Services



Build and maintain secure software applications in today's dynamic and evolving digital landscape

As technology continues to advance, so do the threats and vulnerabilities that can compromise the integrity and security of applications. At Arctiq, we understand the critical importance of robust application security in safeguarding sensitive data, maintaining customer trust, and ensuring regulatory compliance.

Traditional models often treat security as a bottleneck in the development process, leading to delays and rushed deployments. Additionally, a reactive posture towards security, with scans conducted post-development, often results in crucial vulnerabilities being addressed too late, escalating risks.

Arctiq's Approach to Security-Driven Software Development

Early Integration of Security into the SDLC

Arctiq embraces the "Shift-Left" methodology, embedding security considerations and checks at the outset of the development process to proactively identify and address risks. By conducting regular, automated security scans throughout the development cycle, continuous visibility is maintained and vulnerabilities are detected early.

Fostering Collaborative Security in DevOps

Arctiq champions a DevSecOps culture, where security is a collective responsibility integrated seamlessly into DevOps workflows. By establishing a continuous feedback loop, developers and security teams maintain open communication, swiftly resolving issues as they arise and sharing insights for mutual growth.

Efficiency through Automation

Arctiq deploys automated security scanning tools that evaluate code for vulnerabilities with each commit, merge, or build. This automation reduces manual effort, accelerates the identification of vulnerabilities, and employs AI/ML technologies for automated triage and prioritization. By focusing developers' attention where it's most needed, resources are optimized, and security remains robust.

Comprehensive Application Security & DevSecOps Solutions

We offer a complete range of services covering all aspects of application security, ensuring a holistic approach to safeguarding your applications throughout their lifecycle. Our solutions include proactive vulnerability scanning, secure deployment practices, real-time threat detection, and continuous monitoring.

Static Application Security Testing (SAST) and Software Composition Analysis (SCA)

Arctiq employs SAST as a proactive measure in our security strategy, while SCA is utilized to scrutinize and secure open-source components within your software, reducing the risk of vulnerabilities and ensuring their integrity.

Application Self-Protection

Through Runtime Application Self-Protection (RASP), Arctiq enables real-time threat detection and mitigation within your applications. By integrating RASP directly into your applications, we empower them to block malicious activities during runtime, bolstering their security posture.

Container and Kubernetes Security

We specialize in securing containerized applications within cloud-native environments. By effectively managing and securing Kubernetes deployments, we enhance the resilience of your infrastructure, protecting your applications and data from potential threats.

Comprehensive Security Monitoring

Arctiq implements comprehensive monitoring solutions to provide continuous visibility into your digital environment. These solutions deliver timely threat detection, enabling proactive responses to potential security incidents and minimizing overall risk.

Real-World Challenges. Solved.

CHALLENGE

Maintaining Software Integrity in the SDLC

Ensuring software integrity amid widespread use of open-source and third-party components is challenging. Issues like opaque component usage complicate vulnerability management and compliance. Challenges also include integrating SCA and automating SBOM generation effectively without overwhelming developers and refining shift-left strategies to enhance productivity.

SOLUTION

Arctiq automates vulnerability detection with SCA tool integration and SBOM updates for better visibility and control. We streamline notifications, align strategies with risk appetites, and foster continuous improvement with best practices.

CHALLENGE

Swift, Secure Application Delivery

CTOs face the dual challenge of quickly delivering secure applications while managing the disruptive potential of SAST tools that often generate excessive false positives.

SOLUTION

Arctiq optimizes cybersecurity in development practices, ensuring compliance and fostering a security-focused culture. We enhance SAST tool integration into workflows, minimize disruptions, and efficiently balance security with development speed.

CHALLENGE

Cloud-Native Security Management

Cloud-native applications bring unique security challenges, often exacerbated by traditional security tools that lack proper context and generate too many alerts.

SOLUTION

Arctiq provides tailored configurations of CNAPP and CSPM tools, focusing on critical vulnerabilities for more relevant alerts and deeper insights. We also ensure continuous monitoring and offer ongoing training to maximize security tool effectiveness.

Partner with Arctiq to build and maintain secure, resilient, and compliant software applications.

Book a consultation