HOW TO LAUNCH SAAS WITH A DEFENSIBLE SECURITY STORY

leostream

LOCATION

Boston, MA

INDUSTRY

Software Development

EMPLOYEES

11-50

CUSTOMERS

Siemens Energy
Framestore
Portugal Telecom

Leostream Corporation is a growing enterprise software company that helps organizations securely manage remote access to critical systems. The company was expanding to include a new AWS-hosted SaaS offering designed for dynamic access use cases. With Software Secured, Leostream validated the security of its cloud infrastructure, operating system, and application layers.

Cloud Deployment Redefined the Security Model

Leostream's move to the cloud was not a routine modernization project. It was the introduction of an entirely new delivery model. For the first time, a product that had historically lived on customer-managed infrastructure would run in the cloud. That change fundamentally altered Leostream's threat model.

The new application introduced new attack surfaces. Cloud infrastructure, identity boundaries, and network exposure created risks the team had not previously needed to manage.

Timing added pressure. The product was in an MVP stage and scheduled for a beta release the following quarter. Security validation was required to support early customer conversations. Enterprise buyers were already asking questions about cloud security, and Leostream needed credible third-party proof.

The company also anticipated new compliance obligations. With a cloud-hosted service, SOC 2 was now on the roadmap. Leadership knew they needed deep testing, fast turnaround, and a partner who could help educate the team while validating real-world risk.

High-Touch Penetration Testing for Cloud SaaS

Leostream chose Software Secured to bring a fresh perspective to its penetration testing program. The goal was to secure the cloud deployment of an application by testing beyond the web layer and into the underlying operating system and infrastructure.

HOW TO LAUNCH SAAS WITH A DEFENSIBLE SECURITY STORY

ABOUT SOFTWARE SECURED

20%

of all vulnerabilities are critical or high

26

vulnerabilities on average per pentest

3X

more vulnerabilities found than the leading competitor

Software Secured conducted a comprehensive penetration test of the new AWS-hosted SaaS application, with a deep focus on the Linux-based gateway component, which was providing remote access into the customer's network. Testing went beyond standard checklists. The team analyzed custom business logic, cloud exposure, identity paths, and OS-level controls that had not been externally validated.

The engagement was collaborative and high-touch. Software Secured worked closely with Leostream's engineers, providing context, clarity, and education throughout the process. Light threat modeling was incorporated to ensure testing aligned with how the product would be deployed and used in real customer environments.

Findings were delivered through Software Secured's Portal, giving Leostream clear visibility into risk severity, remediation status, and compliance alignment. Vulnerabilities could be exported directly into CSV format to streamline ticket creation and sprint planning.

The remediation process was structured across three rounds. This allowed Leostream to prioritize fixes, align with development cycles, and prove progress over time. Flexible scoping and time-boxed testing ensured the assessment fit both technical and budget constraints.

With the Dashboard, I can assign different SLAs to each vulnerability to ensure and monitor that my development team is resolving critical and high issues within those SLAs. — ***Karen Gondoly, CEO, Leostream***

HOW TO LAUNCH SAAS WITH A DEFENSIBLE SECURITY STORY

Measurable Security Gains Across Cloud, OS, and Application Layers

The first round of testing immediately improved Leostream's security posture. High, medium, and low-risk issues were addressed quickly, bringing the product into what leadership described as "a good state" ahead of beta.

The operating system–level focus delivered new value. Leostream had confidence in the security of the Linux gateway that underpins both its new SaaS offering and existing products. The engagement also raised internal security maturity. Developers gained a clearer understanding of web security concepts, defensive coding, and the differences between cloud-hosted threats and on-premises deployments. The clarity around compliance mapping helped leadership confidently plan for SOC 2 Type I, with a clear runway toward Type II.

Operationally, the vulnerability management workflow saved time. CSV exports reduced administrative overhead. Clear remediation guidance reduced friction between security and engineering. Communication stayed efficient and focused.

A Confident SaaS Release Backed by Independent Security Proof

Leostream successfully prepared its first AWS-hosted application for beta release with independent, third-party validation. The company entered customer conversations with confidence and a defensible security story for its SaaS platform.

Most identified vulnerabilities were resolved within the initial remediation cycles. The gateway component is now externally validated and reusable across products, reducing future testing costs.

Security is enabling growth. Leostream is onboarding customers, supporting new Proofs of Concept tied to its marketplace strategy, and advancing toward SOC 2 certification with clarity and momentum.