CUSTOMER SUCCESS STORY

Securing AI software development without slowing down

How Synthesia's code-to-cloud approach combines AppSec precision with cloud context and runtime clarity

Overview

At Synthesia, speed isn't a nice-to-have, it's foundational to the product. The company's AI-powered video platform enables users to create studio-quality, multilingual videos in just minutes using only text; no cameras, actors, or audio equipment required. Thousands of companies rely on the platform for everything from training and internal comms to marketing and customer engagement.

At scale, that promise of simplicity depends on an engineering organization that can ship quickly and safely. But this velocity doesn't happen by accident. Behind the seamless UI and user experience is a fast-moving development engine with frequent deployments, complex machine learning pipelines, and a growing customer base with increasingly rigorous security expectations.

As Synthesia has scaled its AI video platform, AWS has provided the cloud infrastructure foundation to support compute-intensive AI workloads, model training, rendering performance, and reliable global delivery. Synthesia uses AWS infrastructure to help meet growing enterprise demand for AI video.

Keeping up with that level of innovation isn't just a technical challenge, it's a security one. For **Martin Tschammer, Head of Security at Synthesia**, who has led the security team for a few years, meeting that challenge means enabling product teams to move fast without compromising trust, safety, or delivery timelines.

Embedding application security into how teams build

Martin has led security at Synthesia for over three years. The team is lean but highly focused, split between Corporate Security (CorpSec), which oversees trust operations, cloud security, SIEM, EDR, CSPM, and broader SecOps and Application Security (AppSec), which partners closely with product and engineering to secure the software development lifecycle (SDLC) from the inside.

Synthesia's security mission is to build and maintain a constructive and solution-oriented security-positive culture while never standing in the way of innovation. AppSec plays a central role in that mission by building close-knit, proactive relationships with teams driving software development and maintaining deep familiarity with the codebase, workflows, and product-specific risks.

Synthesia formalized its collaborative security approach through an initiative called the **AppSec Partner Program,** which assigns a dedicated security engineer to each product engineering team, guiding threat modeling, defining security requirements, assisting with issues, and sharing best practices.

Rather than acting as an external reviewer, AppSec works shoulder to shoulder with engineers, engaging early to provide context, support secure development, and accelerate delivery without friction.

> "We built our AppSec Partner Program to make sure our engineers were in the room from the beginning, not showing up at the end," says Martin Tschammer. "AppSec at Synthesia focuses on enabling engineers to build secure applications quickly, prioritizing support over enforcement."

At Synthesia, Application Security isn't about enforcing rules from the sidelines, it's a trusted counterpart focused on helping teams move fast and stay secure. The emphasis is on enablement, not enforcement. But even the strongest security culture needs tools that reinforce that approach

That approach aligns well with the shared responsibility model of modern cloud security: AWS helps provide secure, scalable infrastructure, while Synthesia's security and engineering teams remain focused on securing the applications, code, dependencies, and development workflows built on top of that foundation. Semgrep strengthens that application-layer responsibility by helping teams find and fix code-level risk earlier in the SDLC.

Semgrep

CUSTOMER SUCCESS STORY

When legacy AppSec tools couldn't keep pace

As Synthesia's development velocity increased, their existing static analysis tools began to show their limits. Rule customization was inflexible, supply chain alerts were noisy, and false positives eroded developer trust.

Every time a new library or framework was introduced, especially in fast-moving Python, React, Node.js, and AI/ML libraries, security tooling lagged behind. Detection rules were slow to adapt, and AppSec spent valuable time triaging alerts instead of enabling teams to ship securely.

The team needed tooling that could move at the same speed as their engineers without sacrificing precision or credibility.

The Semgrep approach: Speed meets signal

The security team set out to find a tool that aligned with their development culture: fast, flexible, and developer-first. The search for a better fit led the team to Semgrep.

Semgrep stood out for its transparent static analysis, deep rule ecosystem and the ability to rapidly create context-specific detections tailored to Synthesia's codebase. Features like PR comments and AI-assisted triage further aligned security feedback with developer workflows delivering signal at the right moment without blocking development.

For a company building and scaling AI software on AWS, this matters: AWS helps power the infrastructure behind AI development, while Semgrep helps ensure the software moving through that environment is secure, actionable, and trusted by developers.

> "We discovered Semgrep through a mix of online research and peer feedback. We were immediately impressed by the transparency, the customization, and how quickly we could write new rules. But the real game-changer was reachability analysis. It helped us cut through the noise and focus on what actually mattered."
>
> **Máirtín O'Sullivan**
> Staff Product Security Engineer

Rapid time to value

With Semgrep's managed scans, onboarding was swift. Within weeks, Semgrep was live across numerous repositories. The development team quickly adopted Semgrep, incorporating its findings into their workflows. Engineers appreciated the low-touch and non-disruptive nature of the tool, something Synthesia had prioritized in their tool evaluations.

> "We try to be invisible as possible and only provide feedback to engineers when it's necessary" O'Sullivan says."Semgrep helped us strike that balance. It gives developers just enough signal at the right moment without overwhelming them."

From triage to trust

The impact was immediate. Triage queues shrank. Remediation times dropped. Engineers began resolving issues directly in pull requests, and AppSec could shift its focus to strategic security initiatives rather than chasing false alarms. The improvements were measurable: developer experience improved, remediation time decreased, and findings became more accurate, relevant and actionable — all without sacrificing speed.

But the gains weren't just operational, they were business-critical. Synthesia's enterprise sales cycles depend on trust and compliance.

As AWS supports the infrastructure scale required for Synthesia's AI platform, Semgrep helps provide the application security precision needed to keep that innovation moving safely. Together, they support a model where infrastructure scalability and application security work in parallel, rather than creating friction for developers.

With Semgrep, the security team could streamline audits, accelerate certifications (like SOC2 and ISO27001), and respond to customer risk assessments more efficiently.

> “Everyone — security, engineering, leadership cares about velocity,” says Tschammer. “But it has to be safe. Semgrep gives us the confidence to move fast without cutting corners.”

Adding cloud context: Semgrep & Wiz

To further sharpen prioritization, Synthesia layered Semgrep’s code insights with Wiz’s cloud context. The integration allows them to understand not just what vulnerabilities exist in the codebase, but whether those issues are reachable in the cloud production environment.

This “code-to-cloud” approach adds another layer of signal clarity. Vulnerabilities that were once high priority in isolation can now be downgraded or confidently ignored if Wiz confirms they’re not exploitable. Conversely, reachable risks get immediate attention.

This is especially important in cloud-native environments running on AWS, where teams need to connect application-level findings with cloud context to better understand real-world exposure and prioritize what matters most.

> “Pairing Wiz with Semgrep gave us critical context,” says Tschammer.“We’re no longer chasing noise. We can zero in on what’s actually reachable and prioritize what truly matters.”

This alignment has drastically reduced the volume of alerts the team needs to triage. By combining Semgrep’s precise static analysis with Wiz’s runtime visibility, the team now focuses only on the risks that matter most; saving time, increasing developer trust, and improving response time across the board.

What’s next: Scaling securely

Of course, there’s still more to do. Synthesia continues to expand its use of Semgrep, with plans to triple active contributors by year’s end. The team has submitted feature requests including uv.lock support, smarter policy controls, OSS risk indicators beyond CVEs, and enhanced GitHub Actions scanning to ensure Semgrep evolves alongside their needs. And at a company innovating at AI speed, that level of integration isn’t a nice-to-have, it’s essential.

As Synthesia continues scaling AI video innovation on AWS, Semgrep helps ensure that secure development scales with it, giving developers fast, trusted feedback while helping security teams focus on the risks that matter most.

> “Semgrep isn’t just another scanner. It’s part of how we build.”
>
> **Martin Tschammer**
> Head of Security at Synthesia

About Semgrep

Semgrep enables teams to use industry-leading AI-assisted static application security testing (SAST), supply chain dependency scanning (SCA), and secrets detection. The Semgrep AppSec Platform is built for teams that struggle with noise by helping development teams apply secure coding practices.