



**KANOPY**

# From Blind Spots to Full Visibility:

How an NYSE-Listed Fintech Secures  
and Governs Hundreds of Agentic  
Automations with Kanopy Security



## Intro

NYSE-listed fintech is a global leader in online payment solutions, supporting more than 200,000 merchants worldwide with technology that streamlines transactions and reduces friction for businesses and consumers alike.

As the company grew, it turned to AI agentic automation on the UiPath platform to handle repetitive, business-critical processes at scale. While RPA boosted efficiency, the increasing number of bots interacting with sensitive financial and customer data created new security and compliance risks.

From managing back-office functions to automating customer workflows, agentic automation became a vital component of the company's operations. However, with hundreds of agents running across environments, many with access to sensitive customer and financial data, the company realized that the efficiencies gained also introduced new security and compliance challenges.

To address these challenges, NYSE-listed fintech partnered with Kanopy Security to establish an ongoing application security program that continuously monitors, detects, and remediates risks in its automation ecosystem.



**In three months, the NYSE-listed fintech resolved 99% of its security debt, and launched a security program that detects vulnerabilities and keeps production environments clean with continuous monitoring.**



## The Challenge

While AI agentic automation brought speed and scalability, it also created significant security blind spots. Traditional application security tools were not designed to scan or protect UiPath automations, leaving the security team with no efficient way to detect risks or enforce policies.

### The pain points soon became clear:

- **Limited visibility:** Hundreds of active agentic automations, but the security team had no real-time insight into whether they were configured securely.
- **Data exposure risks:** Automations routinely accessed sensitive information such as financial records and customer details, heightening the stakes of any misconfiguration.
- **Compliance concerns:** Without a way to apply governance across environments, regulatory requirements were at risk.
- **Resource constraints:** Security teams cannot review every agent or automation, while developers cannot identify all risks on their own.



**“We needed a way to implement security and governance controls to safeguard and ensure the success of our large-scale agentic automation initiative”**

– CISO, NYSE-listed fintech

# The Solution

Kanopy Security, the leading platform for securing employee-built apps and agentic automations, was the company's choice for enterprise-grade protection.

The decision was driven by Kanopy's agentless architecture, which allowed integration in minutes without disruption, and its ability to deliver actionable insights not just for security teams but also for platform owners and automation developers.

## Key elements of the solution included:

- **Seamless Deployment:** Kanopy's agentless architecture integrated in minutes.
- **Comprehensive Visibility:** Kanopy quickly mapped automations, users, environments, and data connectors, highlighting risks across governance, compliance, and security.
- **Actionable Guidance:** Clear, contextual remediation instructions empowered developers to fix issues themselves.
- **Developer-Friendly Guidance:** Instead of cryptic alerts, Kanopy provided clear, contextual instructions in employee language, enabling automation engineers to resolve problems independently.
- **Governance at Scale:** the NYSE-listed fintech implemented policies to automatically detect and block risky behaviors, from misconfigured permissions to outdated third-party components.

# Results: Measurable Business Impact

In the first three months, the NYSE-listed fintech was able to clean up existing security debt and launch a comprehensive application security program for its automations.

Kanopy's solution is integrated directly into the company's CI/CD pipeline, enabling inline security checks as automations are developed and deployed.

With Kanopy's continuous monitoring, the company keeps vulnerabilities out of production while scaling automation to new business areas.

**"We moved from reacting to risks to proactively keeping our environment clean. We can now expand agentic automation with confidence, knowing vulnerabilities are detected and fixed quickly. Kanopy didn't just flag issues, it helped us resolve them and build guardrails to prevent recurrence"**

- CISO, NYSE-listed fintech



Massive risk reduction:  
99% of uncovered issues remediated.



Compliance confidence: Agents auto-tagged data, boosting audit readiness and cutting compliance risk.



Operational efficiency: Citizen-Developers resolved issues without bottlenecking the security team.



Sustained governance: Policies kept new automations aligned with best practices.



# About Kanopy Security

Kanopy protects the fastest-growing attack surface in application security: apps, automations, and AI agents built by no-coders, outside traditional engineering.

As no-coders rapidly build tools across the enterprise, often resulting in thousands of assets, with 15% exposed externally, organizations face expanding blind spots, inconsistent governance, and elevated risk.

By giving security teams unified visibility and adaptive control, without slowing productivity, Kanopy turns non-developer-built software into a governed, secure, and trusted innovation.

Already trusted by Fortune 500 and public companies, Kanopy has quickly earned its place as the security foundation that keeps non-developer-built software into a governed, secure, and trusted innovation.

For more information, visit [kanopysecurity.com](https://kanopysecurity.com)

