Solving Security and Identity Management for Today's Demanding Fintech Apps

Security for cloud applications is crucial today. This is even more true when it comes to fintech, which goes far beyond mainstream banking institutions and disruptive challenger banks to encompass an ever-expanding range of use cases: cryptocurrency exchanges, payment apps, investment, wealth management, and real estate.

Although these apps leverage a massive range of technologies, they all have one thing in common: They're operating in one of the most challenging areas when it comes to security.

With new software supply chain threats emerging all the time, developers have less control than ever over what goes into their apps. As the U.S. National Security Agency recently stated, "The developer holds a critical responsibility to the security of our software." That's a heavy responsibility, especially given that the way we develop software is changing—incorporating SDKs, open-source software, APIs, and so many other resources.

To stay competitive in this very crowded arena, fintech companies need to offer the ultimate in seamless modern UX while keeping a tight grip on security from day one of development. But that's not always simple.

Why?

- Fintech applications must meet tight regulatory standards that vary around the world, including PCI-DSS and AML/KYC, and entail steep fines for non-compliance.
- Fintech is one of the most tempting areas for attackers due to its potential for massive payoffs, as in the recent string of attacks on DeFi platforms.

Solvo is the first adaptive solution to automatically manage cloud security so you can keep all your apps safe. It's easy to use and perfect for keeping up with the cybersecurity requirements of fintech.

Let's explore some of the unique challenges involved in securing fintech apps and peek behind the scenes at how Solvo gives your developers the speed and agility they need while letting you keep a tight grip on security from day one.

The Challenges of Securing Fintech Development

First, it goes without saying that fintech developers face the same problems any digital provider must handle when it comes to security, including misconfigurations—which are responsible for two-thirds of cloud attacks—along with human error and identity management.

But beyond those "ordinary" challenges, fintech faces its own set of hurdles, including:

Data Security

This includes controlling, encrypting, backing up, and safeguarding sensitive assets from malware of all kinds, including ransomware, trojans, and spyware. Customers trust you to guard their most precious information, but that information is also very tempting to attackers.

Cloud Security

Fintech demands you ensure visibility, reliability, and correct configuration. Cloud is undoubtedly a positive development, making new types of apps possible and existing apps work better than ever, but it also creates new opportunities for misunderstanding and human error and expands potential attack surfaces.

Third-Party Services

In today's software development world, interoperability is essential, but it also leaves you vulnerable. Fintech developers must remain constantly alert for potential software supply chain issues, and possible vulnerabilities created by compromised APIs or vendors.

Compliance

This includes meeting tight local and global regulatory requirements and handling any necessary audits. Operating in the financial realm means providing a higher level of accountability to customers and across the industry; not only do you need to be ready for an audit, you also need to avoid the steep fines that come with non-compliance.

Migration & Scale

Whether it's moving a legacy app to a new and better cloud-based architecture or expanding your existing capabilities, the only constant in this industry is change. Any type of change leaves you vulnerable, and at cloud scale, it can be very difficult to even know what assets you have in play, let alone secure them all.

Obviously, the prime directive needs to be keeping user data and funds secure at all times, but you have to achieve that level of security without compromising on cloud benefits such as speed, scalability, and always-on availability.

To meet these challenges, security needs to be a baked-in component of your entire DevOps and/or CI/CD practice. Yet this often creates friction, particularly between dev and security teams, even sometimes delaying a product launch.

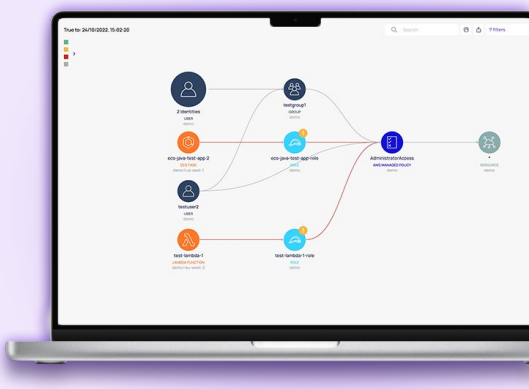
What's the source of this friction? It turns out to be rather simple.

Developers want to develop.
They're looking to the next cool feature and have little interest in wasting time going back, finding problems, and then fixing them.

Developers don't have a strong security awareness.
Often, it's not part of their professional training, or they don't have time to deal with this aspect (so they think). Some also believe it's simply not part of their job, though as we'll see, with the right tools, you can help them to start thinking differently.

Security professionals are cautious by nature.
Because of this, they may be seen as impeding fast delivery times with endless requirements. Of course, they're also legitimately busy and can't drop high-priority security crises to handle routine provisioning and configuration.

The biggest challenge is introducing security that won't slow down development and won't add more work for your teams. To solve this disconnect, many companies turn to platforms that provide some degree of infrastructure security and identity and access management (IAM).



However, many products that promise to help with secure development aren't up to the task, often because they're not designed to work in a real-world DevOps environment or because they end up generating more work for both developers and security.

Many platforms focus on detection in production, which is often too late. Some rely on heuristics, preconfigured rules that don't adapt to each application, or use logs to detect anomalies, which are hard to work with, generate a ton of noise, and present lots of blind spots. And most put much of the work of remediation back on the development team.

Solvo takes a different approach, giving you...

- Automated security infrastructure from the early pre-production environment all the way to production
- A granular, accurate, and dynamic security platform—updating at the same velocity that developers can deploy
- A developer- and DevOps-friendly environment, helping you ensure a secure product from day 1
- Actionable, enforceable insights into your development, QA, staging, and production environments, giving you an accurate and up-to-date picture of your security posture

Instead of logging and chasing down problems, Solvo automates the creation of new security configurations, based on an analysis of the permissions your app actually needs. So over-permissioned accounts—one of today's greatest security risks, along with one of the most ubiquitous, as we've seen from Twitter's recent security nightmares—become almost a non-issue.

Adding Automation to Cut Effort

Solvo's unique platform gets to work right away in three distinct stages:

1. ### Discovery.
   Analyzing the current cloud environment with an eye to best practices

2. ### Policy implementation.
   Creating new security policies based on discovered access, accounts, identities, and entitlements

3. ### Enforcement.
   Monitoring application changes and updating access policies in real time; automatically creating new policies when new code or resources are added

Right out of the starting gate, you'll have total visibility into your cloud infrastructure inventory along with a graphic representation of excessive accesses granted. Plus, Solvo includes a range of developer-friendly tools so fintech developers have the assurance that every development and operations environment is covered from end to end:

SecurityGenie™

SecurityGenie™ is a unique tool to assess the health of your cloud and get you up and running fast.

Policy Manager™

Policy Manager generates least-privileged security policies based on always-up-to-date asset profiles and app behavior.

IAMagnifier™

IAMagnifier provides a visualization and query tool for your infrastructure and security config, automatically triggering alerts if configurations change.

Compliance Manager

Compliance Manager helps you meet compliance benchmarks, displaying the current status and helping remediate violations of popular or customized frameworks.

Since Solvo works with developers and DevSecOps instead of against them, it's minimally intrusive and readily adopted, mainly because it lets them get back on-task fast. Most importantly, Solvo immediately begins delivering positive results.

Cutting Identity and Access Management Risk

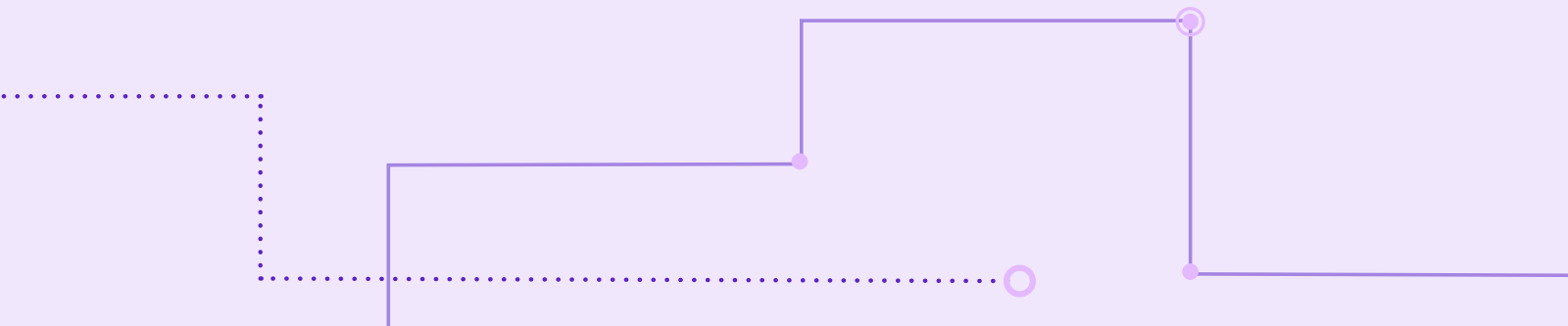
You've probably heard that over-permissioning is a growing threat. According to IBM, this is one of the most serious "cracked doors" that businesses are leaving open to cybercriminals; in IBM Security X-Force testing, penetration testers were able to gain access to 99% of client cloud environments through excess privileges and permissions. Once inside that door, attackers can move laterally through the organization and cause even greater damage.

Solvo uses data collected during development and staging to ensure that all applications receive only the necessary roles and privileges to carry out their tasks. Since ensuring least privilege (part of CISA's Zero Trust Maturity Model) is the leading security recommendation today, this alone will take a massive load off your security team.

Solvo also delivers a number of additional benefits to help secure your entire environment:

- Limits permissions to individuals and cloud assets that need them
- Leverages AWS IAM to improve network security and key management
- Improves secret management through IAM roles
- Restricts access to sensitive data per deep and dynamic granularity-based need
- Gives you total visibility into your cloud infrastructure inventory

Solvo lets your business achieve its cybersecurity vision, meet regulatory compliance and audit requirements without the headache, and replaces friction between developers and security teams with a culture of constant improvement. And it provides all the most crucial capabilities for fintech, including visibility (with IAMagnifier), control of your data and access (with Policy Manager), and automation for the most seamless possible journey.



Getting All Your Teams on the Same Page

Security threats are just part of doing business today—but that doesn't mean you can be complacent. The fintech community needs to remain aware and prepared for cyber threats by establishing a proactive security posture, getting out ahead of the complexity and scale of today's cybersecurity challenges.

Customers from the fintech industry have found that Solvo is truly capable of de-siloing teams and getting them working together more productively via a shared security mindset. Read our full case study to see one actual example of how Solvo accomplishes this while meeting all the other challenges of fintech development.

Making Solvo part of your development process means your teams can get up to speed in lightning time, building a secure product with the highest possible levels of consumer and retailer acceptance. So you can grow and scale without concerns, implement incredible new features, and rest assured that your app is secure every step of the way.

Solvo helps you do this, making it simple to meet all of the security and identity management needs of today's demanding fintech apps.

Sign up today for an up-close demo of what Solvo can do to help you take care of cloud security—and start getting all your teams on the same page.

{ } Solvo