

# First Known Targeted OSS Supply Chain Attacks Against the Banking Sector

Archived: 2026-04-05 17:59:01 UTC

## Learn how Checkmarx and AWS have partnered to help your financial services firm adapt to the evolving landscape

The way we bank has changed beyond recognition. Where transactions once took place in person within the walls of impressive buildings, we now see mobile and online banking on the rise. Anywhere, anytime, palm-of-your-hand banking is the norm, and our expectations are shaped by the seamless, personalized app experiences that have become the default in the digital universe. At the same time, the global acceleration of digital banking licenses has created a new competitive landscape populated by fast-moving market entrants and born-in-the-cloud providers.

One thing that hasn't changed, though, is the position of trust at the cornerstone of the banking system. Indeed, in today's volatile economic and cybersecurity environment, building brand trust is more important than ever. Whether you are a legacy brand or a new market entrant, any lack of trust compromises your ability to succeed.

So financial services firms face a continuing challenge: how to innovate at the speed required without compromising customer safety and system security? Most are turning to the cloud for answers. Its flexibility and scalability are making it central to financial service organizations' efforts to embrace new trends and deliver innovative services at pace.

AWS has some intriguing solutions to meet the challenge. The cloud leader provides a full suite of services to help banks achieve the agility to thrive in the digital age, while certified partners such as Checkmarx ensure the security of the applications and services banks develop.

Recently, the team at AWS identified [seven key trends that are impacting the financial services industry](#). Here we take a deep dive into three areas where AppSec is highly relevant and explore what they mean for the sector.

### **Trend 1: Customer experience — speed and security must be dual priorities**

Today, the economic power is passing to a digital-native generation with little loyalty to legacy banking brands and great expectations of how personal and business financial services should perform. This means customer experience is the modern commercial battleground. Banking must be hyper-personalized and service-led. Increasingly, banking is integrated into consumers' day-to-day journeys through embedded financial services within trusted brands such as Starbucks and Uber.

Banks are leaning heavily on AI and machine learning to predict customer needs through analysis of internal and external datasets, while the omnichannel drive continues through solutions such as authentication based on voice

recognition, real-time sentiment analysis of customer service calls, chatbot support, and automated self-service options.

AWS supports these initiatives and many more through cloud-powered big data analysis that allows banks to leverage AI and machine learning on a massive scale. It also, in its own words, “helps compress time to innovation and, ultimately, time to value, by facilitating rapid development, testing, and deployment to produce new ideas and customer propositions.”

AWS allows banks to accelerate innovation through its cloud-native application development services, but they also need to ensure the code they create is secure and resilient. Achieving application security assurance without putting a brake on delivery speed is crucial. However, a recent Checkmarx survey of banking and insurance CISOs found that 84% of respondents undergoing digital transformation and implementing a cloud-native strategy were concerned about secure application development and deployment.

As an AWS accredited partner, Checkmarx understands that security must work at the speed of DevOps. The [Checkmarx One™ Application Security Platform](#) is designed for the cloud development generation and delivered from the cloud, bringing integrated one-click AppSec testing that allows financial services companies to deploy more secure code — fast.

#### **Trend 2: Ecosystem-based banking and banking-as-a-service — APIs take center stage**

The open banking era is unlocking the doors to greater innovation and collaboration. Providers can now seize new opportunities to develop products that blur the boundaries between different types of financial services. They are establishing solutions that offer their banking services, including fully managed banking propositions, to third parties securely via microservices and a common platform.

AWS identifies two key approaches to this trend. The “marketplace” approach sees banks providing “value-added and contextualized services to their customers such as ERP integrations or personal finance management.” The aim is to deepen the relationship with individual and business customers beyond basic service provision.

The “banking-as-a-service” approach sees banks offering a range of services — from standalone specific regulatory-driven services like Know Your Customer’s Customer (KYCC) to fully managed offerings that let any organization set up a branded banking service.

Center-stage in both approaches are the bank’s APIs, designed to allow banking products and services to be distributed to customers and third parties. Modernizing API architecture in the cloud accelerates the development and testing of APIs, making them easier to integrate as well as providing scalability.

[Checkmarx API security](#) offers banks and their customers and partners a crucial service that helps discover, control, and mitigate API security risk. It offers complete visibility into your API inventory and identifies vulnerabilities and misconfigurations. Controlling API risk is an essential component of developing financial marketplace ecosystems and banking-as-a-service solutions.

#### **Trend 3: Cyber event recovery — reducing the attack surface and responding to regulatory requirements**

Given its nature, it is not surprising that the financial services sector faces more cyberattacks than any other. On top of these external incursions comes the disruption of digital transformation, which can also create vulnerabilities including third-party and supply chain risk.

Banks are investing in a range of measures designed to manage and mitigate risk and accelerate recovery from any attack. Reducing the attack surface and minimizing vulnerabilities is an essential activity if the sector is to safeguard its reputation and maintain customer trust. Additionally, the growing library of regulations designed to ensure banks are meeting their security obligations means they need to adopt solutions that support compliance.

AWS offers a wealth of solutions to ensure client data is protected and banks can recover quickly from attacks. These include Amazon Simple Storage Service (Amazon S3), key management services, software-defined firewalls that facilitate network isolation, and geographic sovereignty solutions that meet compliance requirements.

These and many other offerings take care of Amazon's part of the shared security bargain, however, banks are also responsible for securing the workloads they deploy in AWS. This is where Checkmarx steps in, providing comprehensive AppSec solutions that integrate seamlessly with AWS SDLC tools to secure the entire process. Checkmarx addresses all types of application risk, from [custom code errors](#) to [open-source component vulnerabilities](#), [API risks](#), and [infrastructure as code misconfigurations](#).

These are dynamic times for financial services firms, and AWS with Checkmarx are helping them capitalize on opportunities while defending against threats — both malicious and competitive.

## Interested in learning more?

*We're exploring these trends in detail in our webinar on May 4, 2023, where AWS and Checkmarx will explain how you can turn AppSec into a competitive advantage as you continue your cloud transformation journey.*

[REGISTER FOR THE WEBINAR](#)

## Stay Ahead of Supply Chain Attacks: Secure Your Banking Sector Software

*Protect your banking sector software from targeted OSS supply chain attacks with Checkmarx's cutting-edge solutions. With Checkmarx SCA, effortlessly generate SBOMs for all your applications, enabling your developers and security teams to gain immediate insights into potential security risks. Our SBOM generation feature empowers organizations not only to identify vulnerabilities within their supply chains but also to maintain up-to-date information within constantly changing CI/CD workflows. Ready to fortify your software against threats? [Request a demo today](#) and take proactive steps towards securing your banking sector infrastructure.*

Tags:

AppSec

Banking Sector

Breaking News

Checkmarx Security Research Team

English

security research

Supply Chain Security

---

Source: <https://checkmarx.com/blog/first-known-targeted-oss-supply-chain-attacks-against-the-banking-sector/>