

Commerzbank Strengthened API Security with Akamai

Leading German bank secured 6B monthly API calls through proactive threat detection and enhanced API controls



Enhanced
API visibility



Detected threats in
6B monthly API calls



Improved API
governance

Driving secure innovation in digital banking

Commerzbank, one of Europe's largest financial institutions with a strong international presence, delivers value to customers through innovative, API-powered digital services. From the very beginning, the bank emphasized creating highly reusable solutions, starting with its CRUD (Create, Read, Update, Delete) operations. This approach laid the foundation for exceptional scalability and extensibility, making it easier to integrate internal and external APIs into its ecosystem over time.

But in an era accelerated by AI, Commerzbank recognized that traditional security-by-design measures weren't sufficient to maintain customer trust and meet growing expectations for secure, seamless access. The bank implemented a wide range of robust mechanisms, including adherence to OWASP principles, well-defined and clean interface definitions, strict policies, secure token concepts, and regular [penetration testing](#). Yet as threats and complexity grew, Commerzbank needed a solution that could adapt in real time.

To that end, the bank partnered with Akamai and Deloitte to deploy a dedicated API security layer that strengthened and extended its existing API management platform. The initiative helped the bank detect anomalies, uncover unmanaged [shadow APIs](#), and strengthen governance across departments — all while maintaining agility, compliance, and the ability to scale securely as its API ecosystem expands.

COMMERZBANK

Location

Frankfurt, Germany
commerzbank.de

Industry

[Financial Services](#)

Solution

[API Security](#)

Expanding visibility beyond the API gateway

Commerzbank processes over 6 billion [API calls](#) each month, supporting a vast digital ecosystem of customer, partner, and internal applications. Since 2017, it has relied on the Axway Amplify API Management Platform to manage both internal and internet-facing APIs. But as threats grew more sophisticated, Principal Software Engineer and Solutions Architect Volker Sulzbach recognized the need for strong API defense.

“Our API management platform does its job well,” Sulzbach said. “But we wanted a way to identify abnormal API behaviors and potential attacks before they caused problems.”

While the bank’s SOC handled broader network protection such as [firewalls](#), Sulzbach’s team wanted direct oversight of all business-related APIs to detect anomalies and shadow APIs early — without slowing innovation.

Introducing Akamai API Security

After evaluating multiple vendors, Commerzbank selected Akamai’s API Security solution, which continuously discovers, classifies, and protects APIs across environments. “Anomaly detection was our top priority,” Sulzbach said.

“We needed behavior-driven evaluation, not just call-by-call inspection. Akamai enables that,” he continued. Using [machine learning](#)-powered anomaly detection, API Security identifies abnormal API behavior, potential misuse, and shadow APIs, providing full visibility into both managed and unmanaged endpoints.

“We were impressed that API Security helps identify ‘rogue’ APIs and incorporate security during the development phase,” explained Sulzbach.

Scaling protection to thousands of APIs

The first phase of implementation began with Commerzbank’s sandbox gateway, used to simulate and test APIs before they go live. Once the team validated API Security’s accuracy and responsiveness, it initially secured about 25 production APIs.

“We first wanted to shape rules, reduce false positives, and ensure our teams can act on alerts. The next phase would expand the use of API Security,” Sulzbach explained.

That expansion will eventually cover thousands of APIs and endpoints, providing continuous visibility and security across both internal and external traffic.

“

API Security enables us to ensure better governance over and protection of the APIs driving our business.

— **Volker Sulzbach**
Principal Software Engineer and
Solutions Architect, Commerzbank





Strong API protection is essential to maintaining customer trust, and Akamai helps us uphold that promise.

— **Christoph Berentzen**

Manager, Business Connectivity Division, Commerzbank

Complementing governance and compliance goals

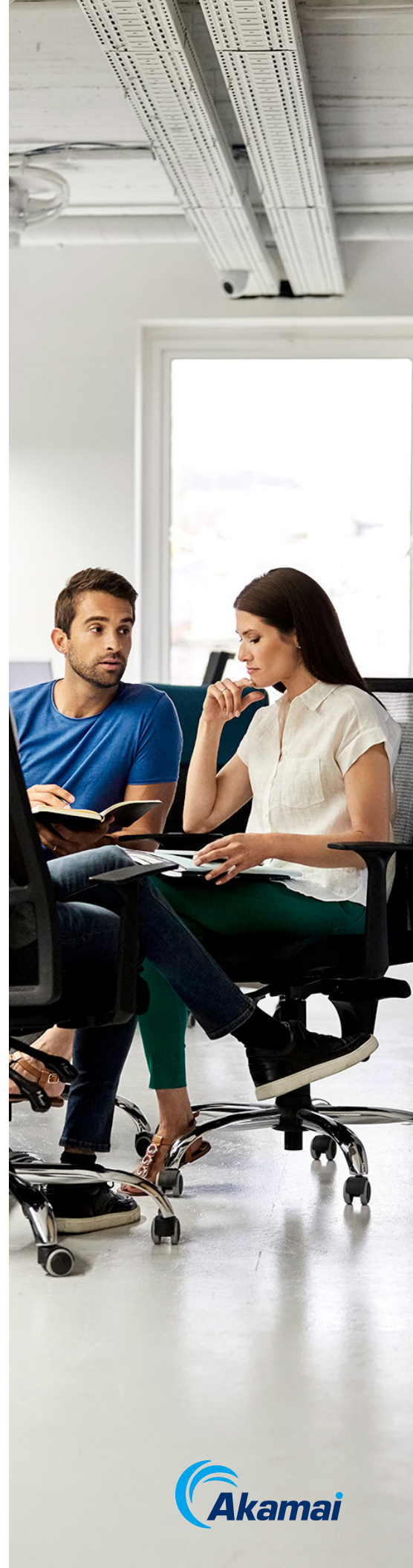
Beyond security, the solution advanced Commerzbank's [API governance](#) strategy. The bank enforces strict naming and formatting standards for APIs to ensure consistency and transparency. Yet some API owners had previously bypassed rules, such as avoiding abbreviations and German terms, to accelerate launches.

With [API Security](#), this no longer happens. "We are now aware of all business-related APIs, which means we can be sure they follow our governance rules," Sulzbach said. "That visibility gives us leverage with management and helps us prove to regulators, including the European Central Bank, that we're proactively securing our APIs."

On-premises first, with SaaS flexibility

Although Akamai offers [API Security](#) as SaaS, Commerzbank chose to begin with an on-premises deployment for greater control and faster onboarding. This phased approach allows the team to build confidence, refine policies, and eventually integrate with cloud native workflows as the security framework matures.

"It wasn't about rejecting the cloud. We wanted to start quickly, validate the solution, and keep our security data internal while still gaining all the detection benefits," explained Sulzbach.



Partnering with Deloitte for rapid rollout

To streamline deployment and configuration, Commerzbank partnered with Deloitte, which provided both technical and strategic support. The partnership helped accelerate setup, fine-tune rules, and prepare the bank's internal team to manage the platform long term.

"Deloitte knows our environment and Akamai's technology inside and out, providing clear guidance and expertise that streamlined deployment," said Sulzbach.

Continuous API protection at global scale

By adopting Akamai API Security, Commerzbank positioned itself to reduce risk, strengthen compliance, and innovate securely in an increasingly connected financial ecosystem. The bank's roadmap includes integrating API Security into every business-driven API, enabling continuous protection from design to runtime. Ultimately, it will alert API owners to potential misuse, empower teams to fix vulnerabilities early, and even automatically block threats.

"We want to protect our vast API landscape in the best way possible. API Security enables us to do just that by cataloging, scanning, and protecting every API that matters to our business," Sulzbach concluded.



With its two business segments — corporate clients and private and small-business customers — Commerzbank, as a full-service bank, offers a comprehensive portfolio of financial services. It is the leading bank for corporate clients in Germany and for the German Mittelstand, and it is a strong partner for about 24,000 corporate client groups. With more than €400 billion in assets under management, Commerzbank is also one of the leading banks for private and small-business customers in Germany. It offers a wide range of products and services with an omnichannel approach: online and mobile, via phone or video in the remote advisory center, and personally in its approximately 400 branches.