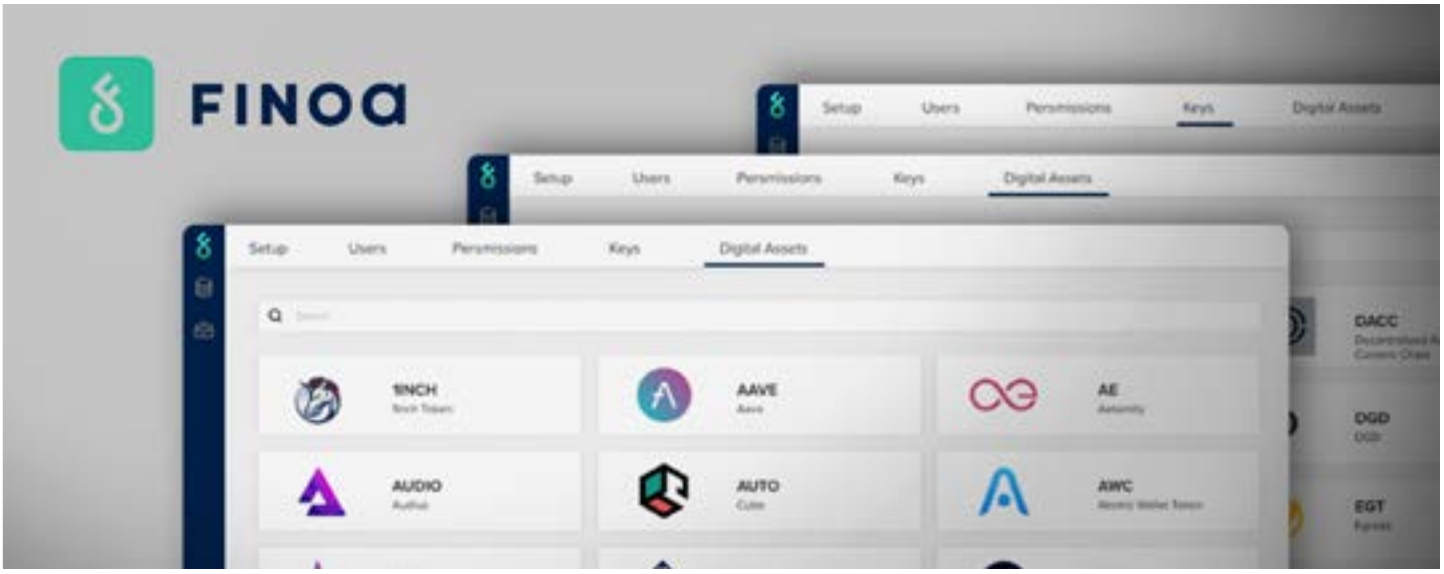
MYRA

CASE STUDY

IT security, BaFin compliance & smooth deployment from a single source

Case Study
Finoa

Solutions
DDoS Protection
Hyperscale WAF
Deep Bot Management
CDN



Crypto custodian Finoa relies on managed Security for a holistic protection concept

Executive Summary

Finoa operates as a financial institution for cryptocurrencies in a highly regulated sector. Founded in 2018, the fintech based in Berlin acts as a crypto custodian. Finoa offers its customers a custody solution for more than 185 crypto assets – from Bitcoin, Ethereum to new protocols such as MINA, NEAR and FLOW. For the technology used to store and manage of crypto assets requires the highest level of IT security and data protection. The accounts of Finoa customers must be protected from unauthorized access, sabotage and manipulation, as crypto assets are a sought-after prey for cybercriminals.

To expand the protection of its crypto platform, Finoa opted for Myra Security's managed services at the end of 2021. The German provider's security-as-a-service solutions protect Finoa's web applications from distributed denial-of-service (DDoS) attacks and malicious manipulation attempts. As a regulated company, it is crucial for Finoa to outsource cybersecurity services to a GDPR-compliant provider from Germany with extensive industry expertise. Myra fully meets these requirements. As a specialist provider, Myra also supports customers from the financial industry with ready-made contracts to eliminate administrative hurdles in advance - this saves resources for both contracting parties and ensures that the required protection services are provided quickly.

Technological support

When it comes to securing its crypto platform, Finoa relies on a holistic protection concept. Myra secures the fintech's services against cyberattacks at application level (layer 7). The implementation of the protection system does not require any additional hardware or software. Technical activation is possible in two ways: Either the DNS entry is adapted via the CNAME entry, or the authoritative DNS server is connected to MySQL by importing existing zones. As soon as the corresponding SSL certificates of the customer are provided to the Myra Dashboard via API or upload, the TLS connection can be terminated, and a deep packet inspection can be carried out. In close coordination with the customer, the Myra Network Operations Center Center (NOC) then configures the filter rules.

Customized filters allow granular traffic control to detect malicious or suspicious requests with the Myra Hyperscale WAF (Web Application Firewall) before they reach Finoa's systems. With this technology, Finoa can even respond to new types of threats such as the Log4Shell vulnerability in the shortest possible time to ensure the protection of customer accounts. The Deep Bot management offers additional options for targeted control of automatic access by both benign and malicious bots. Around half of all website accesses today are accounted for by autonomously acting bots, of which over 20 percent are classified as potentially dangerous – they scan web platforms for vulnerabilities or attempt to infiltrate user accounts.

Regulatory Challenges

Since Finoa has classified Myra's Security-as-a-Service as a significant service outsourced, this involves strict regulatory requirements. Such IT outsourcing must comply with the requirements of the KWG (German Banking Act), BAIT (banking supervisory requirements for IT), MaRisk (Minimum Requirements for Risk Management) and FISG (Financial Market Integrity Strengthening Act). In some cases, legislators and the German Federal Financial Supervisory Authority (BaFin) specify concrete measures for the technical and procedural organization of IT systems, information security requirements, emergency concepts, outsourcing contracts and exit management. These concern both Finoa itself and Myra as an affiliated service provider.

Industry expertise as a catalyst

Myra provides its clients from the financial sector with a prefabricated set of contracts for significant and not significant services outsourced as well as for other external outsourcing, which is drawn up by legal compliance experts and continuously adapted to the applicable financial regulations. These contracts together with comprehensive certification of technology and services form the basis for compliant IT outsourcing that also withstands the strict audits of BaFin. As a provider of new crypto products, Finoa is increasingly the focus of financial regulators, so there is no room for error. Myra's service allows Finoa to deploy protection services smoothly and quickly.

Summary

Since going live, Finoa has benefited from a comprehensive protection concept for its platform. This means that the company is setting new security standards for crypto custody. Myra secures the Finoa solutions fully automatically using DDoS protection at application level, hyperscale WAF and Deep Bot Management. The systems are hidden from attackers behind a three-layer filter system, which only allows valid access. High-performance content delivery is ensured by Myra's global content delivery network, which uses RAM caching for low latencies, short page load times and stable performance – even during unforeseen load peaks. All protection and performance services used have been audited and certified several times to meet the technical and procedural requirements from MaRisk, BAIT and KWG in full.

"In Myra, we have found a service provider that not only has the necessary technical expertise to secure our platform, but who also actively supports us in compliance issues. This support helps us enormously in complying with the increasingly strict regulatory requirements," is the assessment of Finoa's Chief Risk & Compliance Officer Michael Heinks. Ingo Lalla, Vice President Myra Security, emphasizes the importance of cyber security, especially for the financial sector in particular: "Banks are attacked up to 300 times more than other companies. As a BSI-certified service provider, Myra specializes in IT security in the highly regulated financial sector."

Benefits Overview

- Protection of the crypto plattform against syber incidents
- Compliance contracts and comprehensive certification (ISO 27001 based on IT baseline protection of the BSI, PCI DSS-certified, BSIG KRITIS-qualified, IDW PS 951 Type 2 (ISAE 3402) audited, BSI-C5 test certificate type 2)
- Marketing radiance: Finoa relies on the same high quality standards for security and compliance that are also improtant for its customers.
- Local/German-speaking 24/7 support via the Myra NOC at the headquarters in Munich
- Audit-proof compliance: Section 25 KWG, FISG, MaRisk AT9, BAIT
- Legal certainty: 100% GDPR-compliant

ISO 27001 BSI zertifiziert
auf der Basis von IT-Grundschutz
Zertifikat Nr.: BSI-IGZ-0479-2021

PCI DSS Certified

BSIG KRITIS-qualifiziert

BSI C5 TESTAT TYP 2

Trusted Cloud SERVICE 10043

CERTIFIED IDW PS 951 ISAE 3402

Certified by the German Federal Office for Information Security (BSI) in accordance with ISO 27001 on the basis of IT-Grundschutz | Certified in accordance with Payment Card Industry Data Security Standard | KRITIS-qualified according to §3 BSI law | Compliant with the (EU) 2016/679 General Data Protection Regulation | BSI-C5-Testat Type 2 | Certified Trusted Cloud Service | IDW PS 951 Type 2 (ISAE 3402) audited service provider