



CASE STUDY

IT Security, Compliance & Smooth Deployment from a Single Source



Case Study

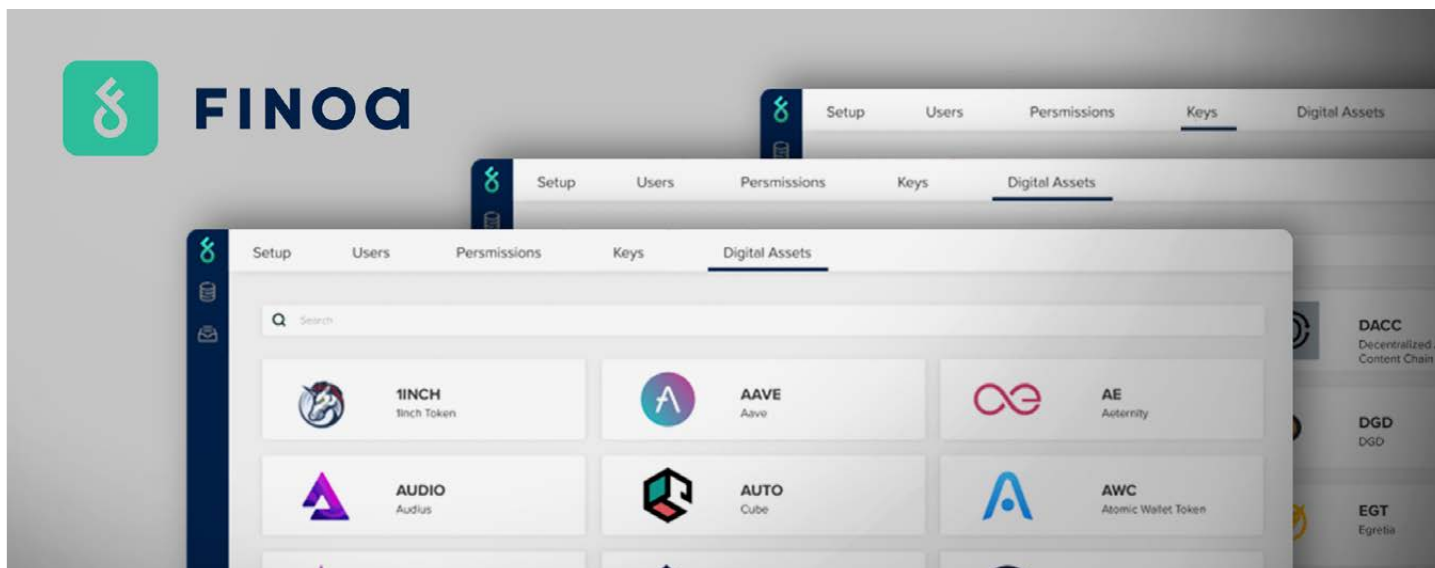
Finoa

Solutions

DDoS Protection
WAF
Bot Management
CDN



MYRA



Finoa Relies on a Holistic Protection Concept

Update: Since 2026, Finoa has been operating as a provider of institutional crypto infrastructure services – however, its activities as a regulated crypto custodian in Germany have been discontinued.

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. The technology used to store and manage crypto assets requires the highest level of IT security and data protection. Finoa customers' accounts must be protected from unauthorized access, sabotage, and manipulation, as crypto assets are coveted by cyber criminals.

To expand the security 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's critical for Finoa to partner with a GDPR-compliant provider from Germany with deep industry expertise when outsourcing cybersecurity services. 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 security services are provided quickly.

Technological Support

Finoa relies on a holistic security concept to protect its crypto platform. Myra protects the fintech's services against cyberattacks at application level (layer 7). No additional hardware or software is required to implement the security system. The technical implementation is possible in two ways: either the DNS entry is adapted via the CNAME entry or the authoritative DNS server is transferred to Myra using an import of existing zones. As soon as the customer's corresponding SSL certificates have been made available in the Myra dashboard via API or upload, the TLS connection can be terminated and a deep packet inspection carried out. In close coordination with the customer, the Myra Network Operations Center (NOC) then configures the filter rules.

Customized filters allow granular traffic control to stop malicious or suspicious requests with the Myra WAF before they reach Finoa's systems. With this technology, Finoa can respond to even novel threats such as the Log4Shell vulnerability in the shortest possible time to ensure the protection of customer accounts. Bot Management, which builds on this, offers additional options for the targeted control of automatic access by both good and bad bots. Around half of all website accesses today are accounted for by autonomously acting bots, over 20 percent of which can be classified as potentially dangerous – they scan web platforms for vulnerabilities or attempt to infiltrate user accounts.

Regulatory Challenges

As Finoa has classified Myra's Security-as-a-Service solutions as material outsourcing, they are subject to strict regulatory requirements. Such IT outsourcing must meet 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). The legislation and the German Federal Financial Supervisory Authority (BaFin) include specific 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.

network, which uses RAM caching to achieve low latency, 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 fully comply with the technical and procedural requirements of MaRisk, BAIT and KWG.

"In Myra, we have found a service provider that not only has the necessary technical expertise to secure our platform, but also actively supports us in compliance issues. This support helps us enormously in complying with the increasingly stringent regulatory requirements," says Finoa's Chief Risk & Compliance Officer Michael Heinks.

Industry Expertise as a Catalyst

Myra provides its customers from the financial sector with a ready-made set of contracts for material and non-material outsourcing as well as for other external procurement, which are drawn up by legal compliance experts and continuously adapted to the applicable financial regulations. Together with comprehensive certification of technology and services, these contracts form the basis for compliance-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 and there is no room for error. Myra's service allows Finoa to deploy the protection services smoothly and quickly.

Summary

Since going live, Finoa has benefited from a comprehensive protection concept for its platform. The company is thus setting new security standards for crypto custody. Myra secures Finoa solutions fully automatically using DDoS Protection at application level, WAF and Bot Management. The systems are hidden from attackers behind a three-layer filter system that only allows valid access. High-performance content delivery is ensured by Myra's global content delivery

Benefits Overview



- Securing the crypto platform against cyber incidents
- Compliance-approved contracts and comprehensive certification (BSI ISO 27001 based on IT-Grundschutz, PCI DSS certified (level 1), BSI KRITIS qualified DDoS Mitigation, IDW PS 951 Type 2 (ISAE 3402) audited, BSI C5 attestation Type 2)
- Marketing power: Finoa relies on the same high-quality standards of security and compliance that are important to 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
- Legally compliant with GDPR

ISO 27001 BSI zertifiziert
auf der Basis von IT-Grundschutz
Zertifikat Nr.: BSI-IGZ-0667-2024



KRITIS
Nachweis gemäß
§ 8a, Abs. 3 BSIG



Certified by the 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 (PCI DSS) | Qualified for critical infrastructure in accordance with §3 BSI Act | BSI C5 Type 2 | Certified Trusted Cloud Service | KRITIS operator in accordance with Section 8a (3) BSI Act | Quality management according to ISO 9001