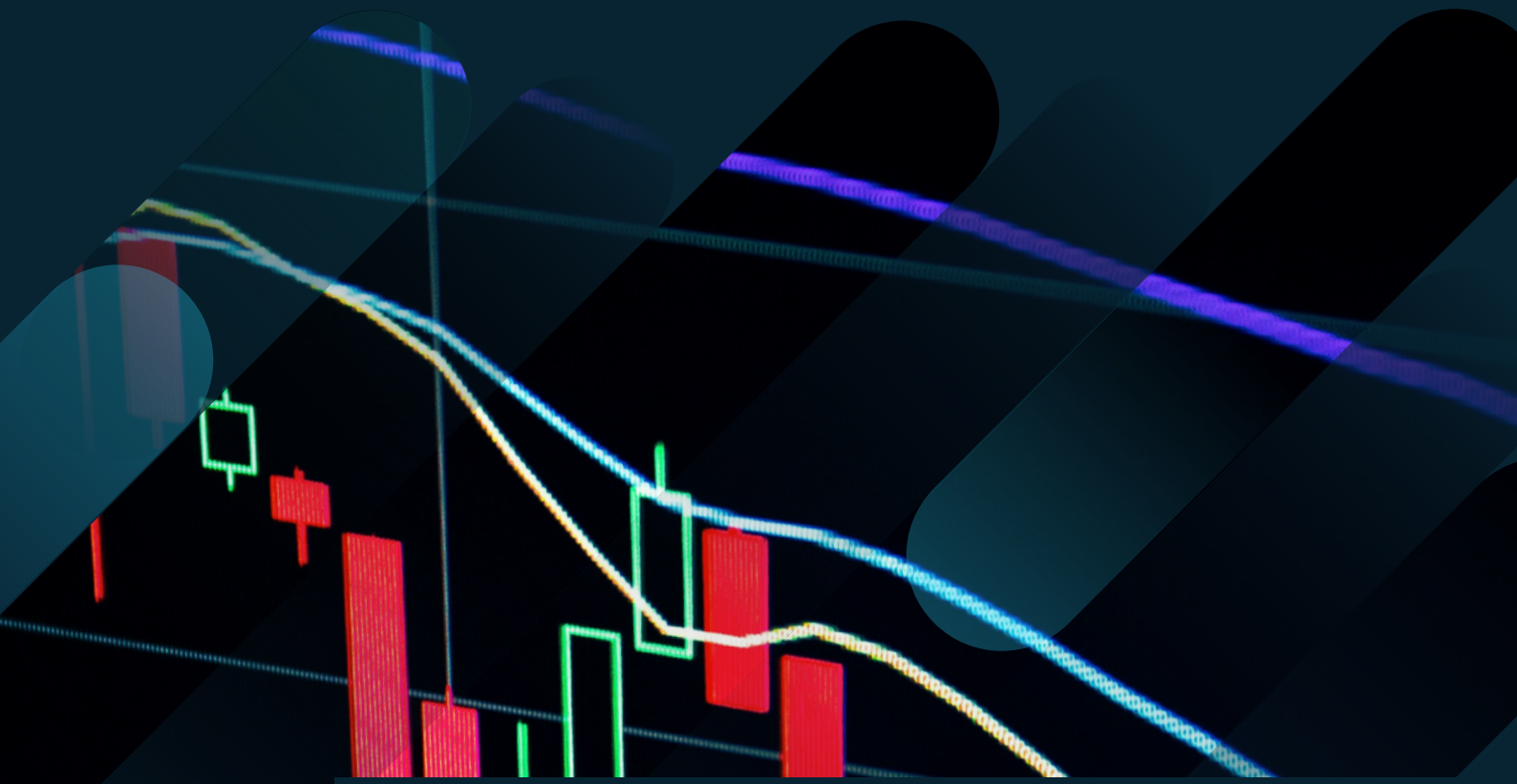


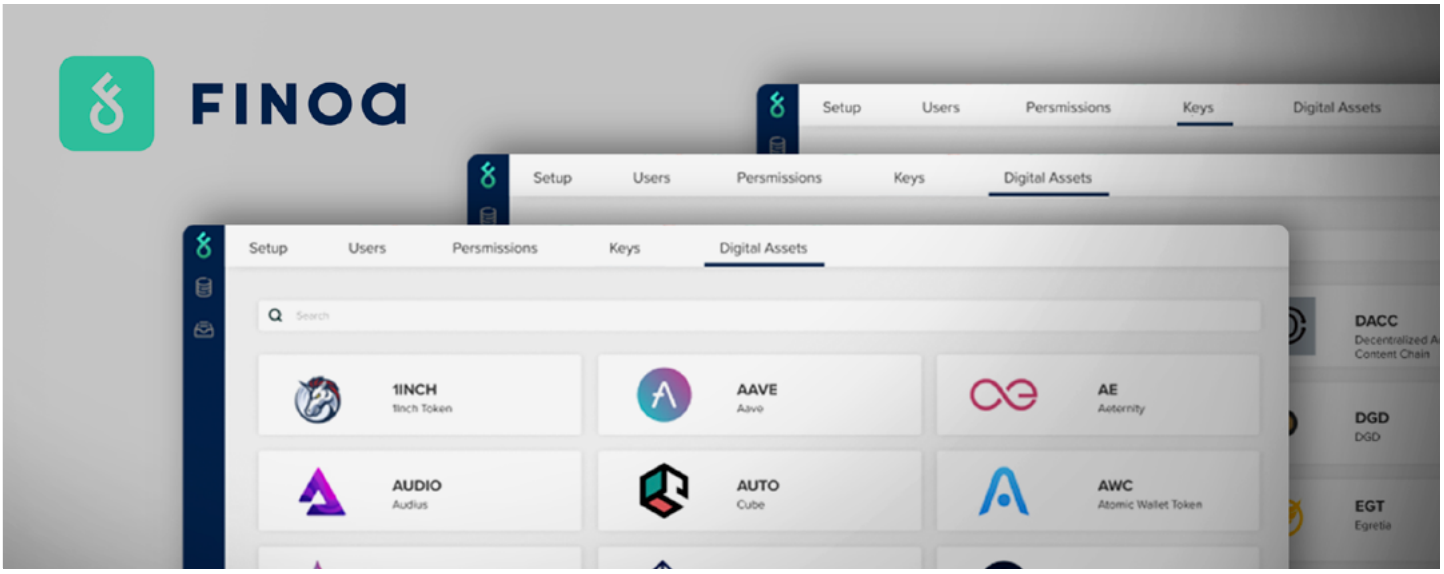
MYRA

CASE STUDY

IT-Sicherheit, BaFin-Compliance & reibungsloses Deployment aus einer Hand

Case Study
Finoa

Lösungen
DDoS Protection
Hyperscale WAF
Deep Bot Management
CDN



Krypto-Verwahrer Finoa setzt auf Managed Security für ein holistisches Schutzkonzept

Executive Summary

Finoa ist als Finanzinstitut für Kryptowährungen in einem hochregulierten Bereich tätig. Das 2018 gegründete Fintech mit Sitz in Berlin agiert als Krypto-Verwahrer. Ihren Kunden bietet Finoa eine Custody-Lösung für mehr als 185 Krypto-Assets – von Bitcoin, über Ethereum bis hin zu neuen Protokollen wie MINA, NEAR oder FLOW. Für die Technologie zur Verwahrung und Verwaltung von Krypto-Assets ist ein Höchstmaß an IT-Sicherheit und Datenschutz erforderlich. Die Konten der Finoa-Kunden müssen vor unzulässigen Zugriffen, Sabotage und Manipulation geschützt sein, da Krypto-Assets eine begehrte Beute für Cyberkriminelle darstellen.

Um den Schutz ihrer Krypto-Plattform auszubauen, entschied sich Finoa Ende 2021 für die Managed Services von Myra Security. Die Security-as-a-Service-Lösungen des deutschen Anbieters sichern die Finoa-Webanwendungen vor Distributed-Denial-of-Service-Angriffen (DDoS) und schadhaften Manipulationsversuchen. Als beaufsichtigtes Unternehmen ist es für Finoa entscheidend, bei der Auslagerung von Cybersicherheitsdiensten auf einen DSGVO-konformen Anbieter aus Deutschland mit umfangreicher Branchenexpertise zu setzen. Myra erfüllt diese Vorgaben vollumfänglich. Als Spezialanbieter unterstützt Myra zudem Kunden aus der Finanzindustrie mit vorgefertigtem Vertragswerk, um administrative Hürden im Vorfeld auszuschließen – das schont Ressourcen für beide Vertragsparteien und sichert eine schnelle Bereitstellung der erforderlichen Schutzservices.

Technologische Umsetzung

Bei der Absicherung ihrer Krypto-Plattform setzt Finoa auf ein ganzheitliches Schutzkonzept. Dabei sichert Myra die Services des Fintechs gegen Cyberattacken auf Anwendungsebene (Layer 7) ab. Die Implementierung des Schutzsystems erfordert keine zusätzliche Hard- oder Software.
Die technische Aufschaltung ist über zweierlei Wege möglich: Entweder erfolgt eine Anpassung des DNS-Eintrags über den CNAME-Eintrag oder der autorative DNS-Server wird mithilfe eines Imports bestehender Zonen an Myra übertragen. Sobald nun die entsprechenden SSL-Zertifikate des Kunden per API oder Upload im Myra Dashboard zur Verfügung gestellt wurden, kann die TLS-Verbindung terminiert und eine Deep Packet Inspection durchgeführt werden. In enger Abstimmung mit dem Kunden übernimmt das Myra Network Operations Center (NOC) abschließend die Konfiguration der Filterregeln.

Maßgeschneiderte Filter erlauben eine granulare Traffic-Steuerung, um schadhafte oder verdächtige Anfragen mit der Myra Hyperscale WAF (Web Application Firewall) abzufangen, noch bevor sie die Systeme von Finoa erreichen. Mit dieser Technologie kann Finoa selbst auf neuartige Bedrohungen wie etwa die Log4Shell-Sicherheitslücke in kürzester Zeit reagieren, um den Schutz der Kunden-konten sicherzustellen. Das darauf aufbauende Deep Bot Management bietet zusätzliche Möglichkeiten zur zielgenauen Steuerung automatischer Zugriffe von gutartigen wie auch bösartigen Bots. Rund die Hälfte aller Website-Zugriffe entfällt heute auf autonom agierende Bots, wovon über 20 Prozent als potenziell gefährlich einzuordnen sind – sie scannen Webplattformen nach Schwachstellen oder versuchen Nutzerkonten zu infiltrieren.

Regulatorische Herausforderungen

Da Finoa die Security-as-a-Service-Dienste von Myra als wesentliche Auslagerung klassifiziert hat, sind damit strenge regulatorische Auflagen verbunden. Ein solches IT-Outsourcing muss den Vorgaben aus dem KWG (Kreditwesengesetz), BAIT (Bankaufsichtliche Anforderungen an die IT), MaRisk (Mindestanforderungen an das Risikomanagement) und FISG (Finanzmarktintegritätsstärkungsgesetz) gerecht werden. Mitunter werden darin durch den Gesetzgeber und die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) konkrete Maßnahmen für die technische und prozessuale Organisation der IT-Systeme, für Anforderungen an die Informationssicherheit, Notfallkonzepte, Outsourcing-Verträge oder auch für das Exit-Management vorgegeben. Diese betreffen sowohl Finoa selbst als auch Myra als angeschlossenen Dienstleister.

Branchen-Expertise als Katalysator

Myra stellt seinen Kunden aus der Finanzbranche ein vorgefertigtes Vertragswerk für wesentliche und nicht wesentliche Auslagerungen sowie für sonstigen Fremdbezug zur Verfügung, das eigens von juristischen Compliance-Experten erstellt und laufend an die geltende Finanzregulatorik angepasst wird. Diese Verträge bilden im Zusammenspiel mit umfassender Zertifizierung von Technologie und Diensten die Basis für ein Compliance-konformes IT-Outsourcing, das auch den strengen Prüfungen der BaFin standhält. Als Anbieter von neuen Krypto-Produkten steht Finoa verstärkt im Fokus der Finanzaufseher, hier ist kein Raum für Fehler. Der Service von Myra erlaubt Finoa ein reibungsloses und schnelles Deployment der Schutzdienste.

Resümee

Seit der Aufschaltung profitiert Finoa von einem umfassenden Schutzkonzept für ihre Plattform. Damit setzt das Unternehmen neue Sicherheitsmaßstäbe für Krypto-Custody. Myra sichert vollautomatisch die Finoa-Lösungen mittels DDoS-Schutz auf Anwendungsebene, Hyperscale WAF und Deep Bot Management. Dabei werden die Systeme hinter einem dreischichtigen Filtersystem vor Angreifern verborgen, das nur valide Zugriffe zulässt. Für eine hochperformante Auslieferung der Inhalte sorgt wiederum das globale Content Delivery Network von Myra, welches durch RAM-Caching niedrige Latenzen, kurze Seitenladezeiten und stabile Performance realisiert – und das selbst bei unvorhergesehenen Lastspitzen. Alle eingesetzten Schutz- und Performance-Dienste sind mehrfach auditiert und zertifiziert, um die technischen und prozessualen Anforderungen aus MaRisk, BAIT und KWG vollständig zu erfüllen.

„Mit Myra haben wir einen Dienstleister gefunden, der nicht nur über die notwendige technische Expertise zur Absicherung unserer Plattform verfügt, sondern der uns auch in Compliance-Fragen aktiv unterstützt. Dieser Support hilft uns enorm bei der Einhaltung der zunehmend strengeren regulatorischen Auflagen“, so die Einschätzung von Finoas Chief Risk & Compliance Officer Michael Heinks. Ingo Lalla, Vice President Myra Security, unterstreicht die Bedeutung von Cybersicherheit insbesondere für die Finanzbranche: „Banken werden bis zu 300-mal häufiger angegriffen als andere Unternehmen. Als BSI-zertifizierter Dienstleister ist Myra auf IT-Sicherheit im hochregulierten Finanzbereich spezialisiert.“

Benefits Overview

- Absicherung der Krypto-Plattform gegen Cybervorfälle
- Compliance-gerechtes Vertragswerk und umfangreiche Zertifizierung (ISO 27001 auf Basis von IT-Grundschutz des BSI, PCI-DSS-zertifiziert, BSIG KRITIS-qualifiziert, IDW PS 951 Typ 2 (ISAE 3402) geprüft, BSI-C5-Testat Typ 2)
- Marketing-Strahlkraft: Finoa setzt auf dieselben hochqualitativen Standards bei Sicherheit und Compliance, die auch für ihre Kunden bedeutend sind.
- lokaler/deutschsprachiger 24/7-Support über das Myra-NOC am Hauptsitz in München
- revisionssichere Compliance: §25 KWG, FISG, MaRisk AT9, BAIT
- Rechtssicherheit: 100%ig DSGVO-konform

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

CERTIFIED IDW PS 951 ISAE 3402

DIN EN 50600 zertifiziert BETRIEBSSICHERES RECHENZENTRUM

Zertifiziert vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 auf Basis von IT-Grundschutz | Zertifiziert nach Payment Card Industry Data Security Standard (PCI DSS) | KRITIS-qualifiziert nach §3 BSI-Gesetz | BSI-C5-Testat Typ 2 | Geprüfter Trusted Cloud Service | IDW PS 951 Typ 2 (ISAE 3402) geprüfter Dienstleister | Zertifizierung von Rechenzentren nach DIN EN 50600