

SUCCESS STORY



NetFoundry



Ominimo Builds Secure and Scalable Multi-Cloud Network for Insurtech with NetFoundry Cloud

Ominimo is an AI-powered digital insurer founded in Serbia, launched in Hungary with 300K+ policies sold in year one (~7% market share). With a proprietary low-code platform with AI-driven pricing across hundreds of variables, Ominimo is backed by Zurich Insurance Group & DA Direkt and is expanding into Poland, Sweden, Netherlands and 10+ EU markets.

- **Zero Trust networking foundation for Ominimo's insurtech architecture:** Within Ominimo's cloud-native insurtech architecture, NetFoundry Cloud provides a Zero Trust networking layer that enforces policy-driven, identity-bound connectivity between core insurance application services, data platforms, and operational control planes across multi-cloud regions and environments.
- **Launch Business Apps on micro services in record time:** Ominimo deployed a secure scalable private zero trust network overlay with NetFoundry for several containerized services including pricing engines, data pipelines, analytics, admin portals across Hetzner and AWS in under 72 hours.

- **Secure by design and compliant to standards & regulations:** Ominimo's infrastructure is architected to align with Cloud Regulatory Alignment (CRA), EU insurance directives, and regional data protection mandates. By combining Zero Trust identity-based access with microsegmented AppNets, the platform enforces least-privilege connectivity, ensures auditable compliance, and delivers military-grade security across all workloads and environments.
- **Network that enables container management and monitoring:** NetFoundry's overlay powers centralized monitoring via the ELK stack, while Portainer, secured by identity-based access policies, delivers DevOps with real-time visibility and lifecycle control over containerized services.



As CTO of an insurtech operating in several regions, I value solutions that reduce complexity without compromising security. NetFoundry delivered exactly that. Their product streamlined our environment setup across markets, and their support has consistently exceeded expectations.”

– Laslo Horvath, CTO

Requirements and Challenges

As Ominimo expanded rapidly across European markets, its infrastructure needed to balance agility, security, and control across diverse environments. Key challenges included:

- Core insurance workloads such as pricing engines and calculation services needed to communicate reliably with transactional data stores and downstream analytics components across [north-south] and within [east-west] cloud DCs without exposing services to the public internet or relying on flat network constructs.
- Container lifecycle management required Portainer to securely interact with container runtimes and application workloads across and within cloud environments.
- Traditional VPN-centric models introduced bottlenecks, expanded the attack surface through public IP exposure, and lacked the ability to enforce service-level isolation and least-privilege access, leaving gaps in compliance and security posture.
- Meeting EU insurance and data protection mandates demanded identity-aware, least-privilege access to internal services and developer tools.
- Unified orchestration, connectivity & centralized observability was essential for performance tuning, incident response, and continuous delivery across environments.



We moved beyond the perimeter with NetFoundry. It delivers a strictly 'least-privileged' access model that is incredibly easy to deploy. The management console turns what used to be a tangle of firewall rules into a streamlined, visual command center."

– Viktor Szabó, Deputy CTO

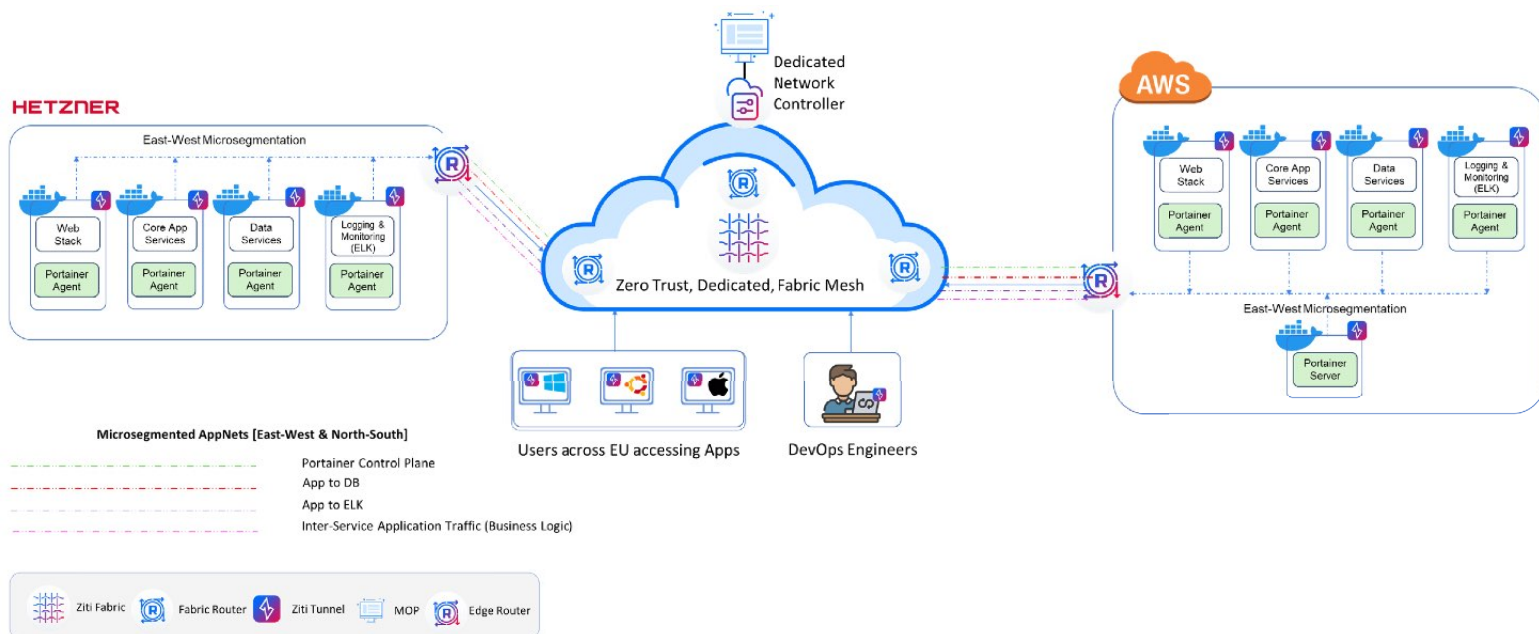
The NetFoundry Solution

Ominimo adopted NetFoundry Cloud as an application-centric Zero Trust networking layer for its cloud-native insurtech platform, enabling secure, identity-driven connectivity between core insurance services deployed across Hetzner and AWS.

Key capabilities included:

- Pricing engines, data services, analytics pipelines, & supporting platform services communicate through strong identity-bound AppNets, enforcing east-west & north-south microsegmentation.
- Portainer operates as a trusted platform service within the NetFoundry Zero Trust fabric, enabling secure, policy-driven container lifecycle management within & across clouds without VPNs or shared credentials.
- Log and telemetry data flows securely from application and platform services into centralized ELK environments over the same NetFoundry Zero Trust fabric, preserving visibility.
- Secure DevOps and production application access with Zero Trust micro-segmentation, eliminating VPN risks.
- Seamless Scalability & Resilience with NetFoundry Cloud's geo-scalable, self healing fabric supports quick onboarding of new regions (Poland, Sweden, Netherlands, and more)

NetFoundry Zero Trust “Secure By Design” Architecture



How Did Ominimo Benefit?

- 50% faster deployment and market launch timelines, accelerating entry into new EU markets.
- Seamless multi-cloud expansion, with secure connectivity across multi-cloud regions.
- 40% reduction in operational overhead through automation, APIs, and Zero Trust design (no VPNs, no inbound firewall rules, no IP clashes).
- Enhanced security and compliance, with identity-based, microsegmented access aligned to EU insurance regulations.
- Improved visibility and control, via centralized monitoring, analytics, and granular DevOps reporting.



As Ominimo expanded into new markets, NetFoundry enabled us to deploy a highly secure environment with remarkable ease. The low maintenance overhead and the team’s outstanding support made a significant difference for us.”

– Dušan Janković, Lead developer

Conclusion

Ominimo's journey from a disruptive insurtech startup to a multi-market leader demanded infrastructure that could match its pace, precision, and ambition. By adopting NetFoundry Cloud, Ominimo transformed its multi-cloud operations into a secure, scalable, and developer-friendly foundation for rapid European expansion, with every workload, user, and service protected by NetFoundry's Zero Trust - Identity-First Reachability™

About NetFoundry

NetFoundry helps businesses secure connectivity between components of their widely distributed workloads, across any set of networks. Founded by the inventors and maintainers of the world's most-used open source zero trust software, OpenZiti, NetFoundry's Identity-First Reachability™ enables zero trust connectivity with no VPNs, no open inbound ports, and no firewall changes.