snappi

Secure Access with SASE & Zero-Trust Protection

Zero-Trust remote access with unified protection.

Zero trust from the first login. No exceptions.

Snappi, Greece's first ECB-licensed neobank, operates without a traditional perimeter. Every employee, every device, every connection is remote by design.

Performance Technologies implemented a full SASE architecture — combined with NAC and ZTNA — giving Snappi continuous, identity-driven security across its entire workforce, fully aligned with DORA and ECB requirements.

The 1 Thing

Snappi does not have a network perimeter. So Performance built security that does not need one.

In a 100% digital financial institution, trust cannot be assumed based on network location. It must be continuously verified — per user, per device, per session. That is what SASE with zero trust delivers.

Industry: Financial Services — Neobanking • **Challenge:** A 100% digital neobank with distributed workforce, cloud and physical infrastructure, and ECB/DORA compliance obligations — no legacy perimeter, no margin for security gaps. • **Outcome:** One of the most complete SASE + NAC + ZTNA implementations in Greece, providing zero-trust protection for every user and device, regardless of location. • **Vendors:** Fortinet

Situation & Complication

As Greece's first neobank to hold a full ECB banking licence, it operates entirely digitally — no branches, no legacy estate, no traditional IT perimeter.

Its workforce is distributed across physical and cloud environments, and its customers are served entirely through digital channels. This is a competitive advantage. It is also a distinct security challenge.

In a conventional bank, the network perimeter provides a first line of defence. Snappi does not have one. Every employee accesses systems remotely. Every device is potentially outside corporate control. Every connection must be assumed untrusted until verified.

In a regulated financial environment — subject to DORA, ECB guidelines, and European data protection requirements — this is not a theoretical concern. It is a compliance and operational risk that requires a structural answer.

The gap was architecture, not just tooling.

Snappi needed a security model built around identity and device posture, not network location. It needed to verify continuously — not just at login — that every user and every device met security requirements before accessing sensitive financial systems. It needed this to scale as the company grew rapidly, without adding operational overhead. And it needed it to be auditable, with centralized logging and automated incident response.

A collection of point solutions would not meet this bar.

Resolution

Performance Technologies designed a unified SASE architecture — one of the most complete implementations of its kind in Greece

Snappi needed a security architecture that matched its operating model — not just a set of tools bolted onto a conventional framework.

The framework combines FortiSASE, FortiNAC, ZTNA, and virtualised FortiGate in a single coherent security model. What makes it notable is not any single component, but the integration: every layer — endpoint, ZTNA, SASE, NAC, SD-WAN — feeds into a unified operational picture.

FortiSASE is the core of the architecture: cloud-delivered security that covers advanced threat prevention, web and SaaS application protection, and unified access management via ZTNA. Every Snappi employee gets a consistent, secure access experience regardless of device or location. Latency is low, user experience is smooth — critical for a digital-only organisation where speed and availability are competitive differentiators.

FortiNAC adds continuous endpoint oversight: every device attempting network access — whether on-site or remote — is dynamically categorised, assessed for compliance, and subject to policy enforcement. A non-compliant, unpatched, or suspicious device is automatically isolated or restricted before it can reach sensitive systems. Virtualised FortiGate firewalls handle secure access to private corporate and cloud systems via SD-WAN connectors integrated with the FortiSASE cloud.

FortiAnalyzer ties the architecture together: centralised logging, advanced analytics, security rule correlation, and automated threat response. It collects data from every layer and produces a genuine 360° view of the organisation's security posture — the foundation for both operational response and regulatory audit trails.

How Performance Made It Possible.

Snappi needed a security architecture that matched its operating model — not a set of tools bolted onto a conventional framework.

Performance designed the engagement from first principles: what does zero trust mean for a digital-only bank? The answer shaped every component choice and integration decision. The result is not a standard deployment — it is a custom architecture that reflects Snappi's specific regulatory weight, operational model, and growth trajectory.

Impact

Snappi operates with a security posture that most banks reach only after years of incremental hardening. It achieved this before scale created complexity.

For compliance, the architecture is directly aligned with DORA's operational resilience requirements and ECB guidelines for information security in financial institutions. The unified logging and automated incident response capabilities support continuous compliance monitoring rather than point-in-time audits.

Operationally, the cloud-native foundation means Snappi can scale its workforce and infrastructure without new on-premises security investments. As the company grows into the European neobanking market, its security model scales with it — same policies, same visibility, same protection regardless of where employees are or what systems they access.

> Snappi needed an architecture that matched its operating model — distributed workforce, full cloud infrastructure, ECB-level compliance.

Zero trust is not a setting. It is an architecture.

- Every user access is identity-verified and device-posture-checked before reaching any system.
- Non-compliant devices are automatically isolated. Security events are centrally logged, correlated, and available for audit.
- The attack surface — the set of ways an adversary could reach sensitive systems — is substantially reduced compared to any perimeter-dependent model.

snappi

Secure Access with SASE & Zero-Trust Protection

Zero-Trust remote access with unified protection.

Contact us to discuss how you can implement SASE with Zero-Trust Protection

210 99 47 100

info@performance.gr

Pillars: GUARD | Solution Areas: Network Security & SASE, Zero Trust & Identity, Endpoint & Device Security

Powered by FORTINET Engineered by performance