Powered By
ATOMNIA
Connection Protection Detection

INTEGRATED SASE – Brief Technical Specification

INTEGRATED SASE in OMNIA is the unified security layer that wraps SD-WAN and cloud access in a full SASE/SSE stack: ZTNA, SWG, CASB and FWaaS. It is built on best-of-breed Check Point technology, with in-country cloud gateways for data sovereignty and 99.9%+ threat blocking effectiveness.

Area	Technical specification
Platform	Cloud-native SASE platform that unifies Zero Trust, Secure Web Gateway, CASB and cloud firewall in one integrated security layer for OMNIA.
Coverage	Protects users, devices, applications and data on-site, remote, mobile and across multi-cloud environments through a single policy framework.
Service options	Supports full SASE (SD-WAN + SSE) and pure SSE, depending on network architecture and use case.
Security framework	ZTNA, CASB, SWG, DLP and FWaaS provide multi-layered protection against current threats and zero-days.
Zero Trust	Enforces “never trust, always verify” across users, devices and applications, with least-privilege access to cloud and private applications.
Web security	Cloud or on-premises SWG filters user-initiated internet traffic, including URL and content filtering, malware and threat detection/prevention, DLP, and SIEM, SOAR and EDR integration.
Cloud security	CASB enforces enterprise security policies between users and SaaS, IaaS and PaaS services, providing compliance, visibility, threat protection and data protection.

Area	Technical specification
Firewall security	Cloud-delivered next-generation firewall capabilities, including web filtering, advanced threat protection, IPS and DNS security, centrally managed as a service.
Data sovereignty	Purpose-built in-country OMNIA gateways and data centres keep traffic and logs within required jurisdictions for sovereignty and compliance.
Architecture	Cloud-native design with regional PoPs for low-latency inspection and policy enforcement close to users and applications.
Management	Centralised console for policy creation, monitoring and reporting across SASE components.
Operations	Distributed architecture designed for always-on security and high availability; scales for new users, locations and applications without additional hardware roll-outs. The cloud service is continuously updated with threat intelligence and features.
Threat prevention	Check Point-backed security with 99.9% malware block rate and 100% phishing/malicious URL prevention, based on Check Point independent tests.

Deployment Models

- Cloud-based SASE/SSE via ATOMIUS Cloud gateways.
- On-premise security on VENA/VECTA SD-WAN appliances at the edge.
- Hybrid models combining centralised gateways, edge security and cloud enforcement.
- Centralised firewall architectures for legacy scenarios.
- Edge security on VENA/VECTA uCPE with SD-WAN and security.
- Cloud-based security through SD-WAN integration with cloud security providers.

Security Assurance

Check Point follows security-by-design principles using STRIDE-based design reviews, separate development, test and production environments, and continuous vulnerability tracking. Product hardening includes static code analysis, manual review, red-team testing and penetration testing. Supporting Check Point products comply with SOC 2, ISO/IEC 27000, Common Criteria, FIPS 140-2, NSS Labs, ICSA Labs, NIAP and CSfC, among other standards and schemes.