invGUARD

Cyberattack prevention system

INOVENTICA TECHNOLOGIES

Phone: +421 949 29 99 24
info@inoventica.com
inoventica.eu

facebook.com/inoventicagroup

twitter.com/Inoventica_eu

www.linkedin.com/inoventica-services

instagram.com/inoventica

INOVENTICA TECHNOLOGIES

invGUARD KEY ADVANTAGES

- Best market price-to-functionality ratio
- invGUARD AS maybe shipped as a VM
- Ability to utilize invGuard as an supplementary network solution (Step-by-step implementation, no need to reconfigure existing ICT infrastructure)
- Protection of investments into the ICT infrastructure
- Fully automatic cyberattack detection and prevention
- API for invGUARD system management
- InoSphere Cloud Services management platform supported and integrated via invGUARD API
- 100+ templates for cyberattack detection and prevention
- Easy customization to fit customer needs
- End-user cyberattack protection services at attractive prices or free
- invGUARD management interface optimized for mobile
- 24/7 technical support, including on-site support

invGUARD PURCHASE OPTION

One-time payment

Monthly payments

Revenue sharing for end-user cyberattack prevention services

As a whole or in subsystems (invGUARD AS; invGUARD AS & invGUARD CS)

Up to 5 Tbits	traffic analysis for cyberattack prevention
100+	routers in single management interface
20 000+	managed objects (information systems, sites, e-shops, internet-services, etc.)
Multi-vendors enviroment	Juniper, HPE, H3C, Cisco, Huawei, Alcatel, Extreme, etc.
250+	customized views of traffic and objects
100+	types of detectable cyberattacks
10 000+	threats per day performance
80-	hours for on-site deployment

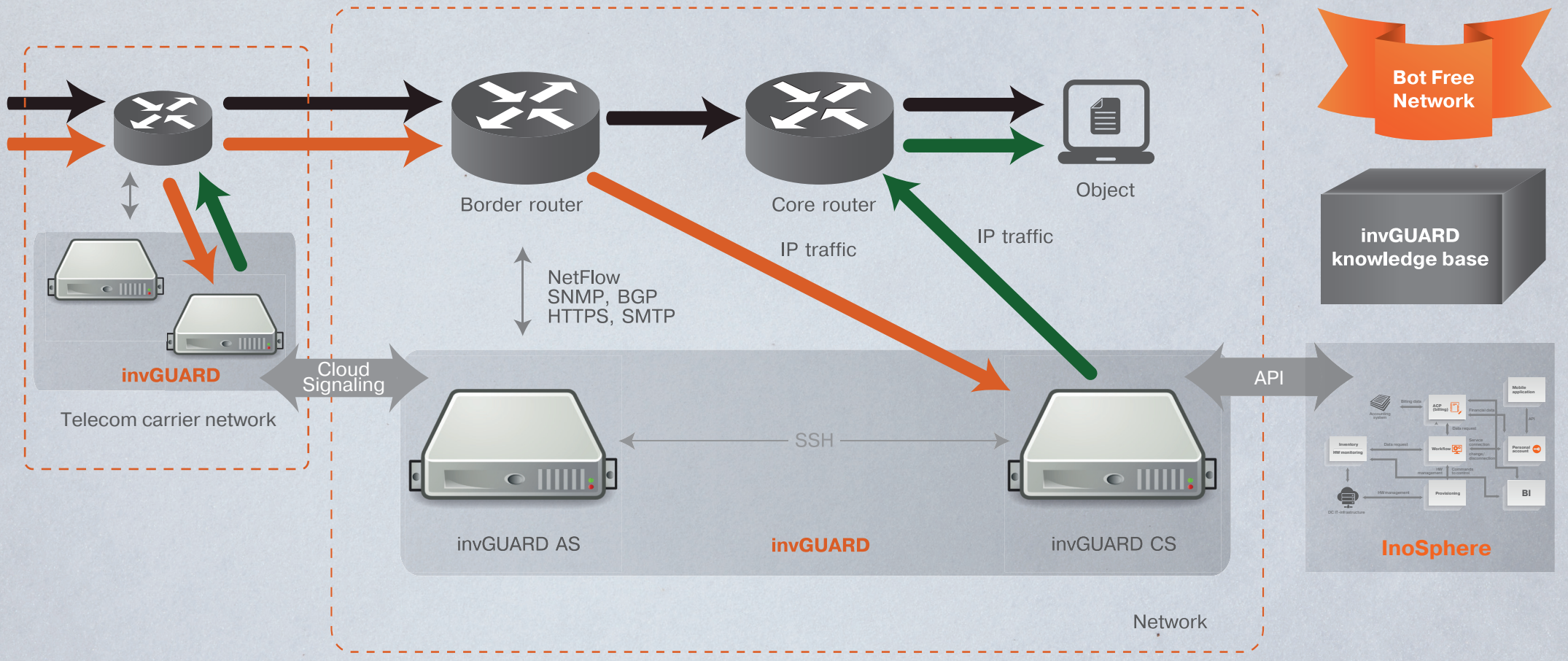
invGUARD MARKETPLACE

- Telecom carriers
- Service providers
- DC carriers
- Media companies
- Banks and financial institutes
- B2B and B2G with substantial own IT infrastructure
- Hosting companies

invGUARD IMPLEMENTATION VALUES

1. Cost effective solution for cyberattack detection and prevention (DoS/DDoS attacks, signature-less malicious impacts)
2. Risk reduction of denial-of-service attack to managed objects (web sites, e-shops, media, etc.)
3. Effective tool for traffic analysis and network infrastructure optimization
4. Easy integration with existing network management platforms via SNMP (HP OV, IBM Tivoli, Zabbix, Nagios, etc.)
5. Extra security via multi-level protection (Cloud Signaling)
6. SLA monitoring for managed objects access
7. Effective tool for manage of telco services expenses
8. Extra revenue source from DoS/DDoS prevention services for B2B/B2C (easy integration with InoSphere Cloud Services management platform)

SYSTEM ARCHITECTURE



Subsystem	Functionality	Applicable technologies
invGUARD AS - traffic analysis up to 1 Tbit/sec - processing up to 100000 flow/sec	- Traffic analysis - Detection of anomalies and illegitimate activity - Detection and attack mitigation - invGUARD CS/CS-01 subsystems management - Personal Account for users or customers - Centralized management of network equipment - Customizable automated cyberattack prevention - Cloud Signaling for multi-node solutions	Traffic analysis: NetFlow v5, v9 and IPFIX Routers info: SNMP v2c Routing management: BGP v4 Integration with network management platforms (SNMP, syslog) User notification: SMTP invGUARD API
invGUARD CS - Attack mitigation / traffic filtering up to 20 Gbit/s, 30 Mpackets/s	- Traffic filtering, protocols misuse checking - Attack mitigation (DDoS attack and signature-less malicious impacts)	High-speed attack mitigation and traffic filtering with special network cards
invGUARD CS–01 - Attack mitigation / traffic filtering up to 1 Gbit/s, 3 Mpackets/s	- Traffic filtering, protocols misuse checking - Attack mitigation (DDoS attack and signature-less malicious impacts)	Attack mitigation and traffic filtering with intel DPDK supported chipset network cards