invGUARD

Schutzsystem vor Cyberattacken

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 SCHLÜSSELVORTEILE

- Bestes Marktverhältnis „Preis-Funktionalität„;
- invGUARD AS kann als eine virtuelle Maschine funktionieren;
- Möglichkeit, invGUARD als eine zusätzliche Netzwerklösung zu nutzen (Schrittweise Einführung, es gibt keine Notwendigkeit, die vorhandene IuK-Infrastruktur neu zu konfigurieren);
- Sicherung der früheren Investitionen in die IuK-Infrastruktur bei der Systemeinführung von invGUARD;
- Vollautomatische Aufdeckung und Verhinderung von Cyberattacken;
- Programmierschnittstelle für das Verwaltungssystem von invGUARD;
- Die Managementplattform InoSphere Cloud Services wurde durch die Programmierschnittstelle invGUARD unterstützt und integriert;
- 100+ vorkonfigurierte Modelle für die Gleichrichtung und Verhinderung von Cyberattacken;
- Umfassende Möglichkeiten für die Systemanpassung nach Anforderungen der Kunden;
- Möglichkeit, dem Endverbraucher Dienstleistungen für den Schutz vor Cyberattacken zu attraktiven Preisen oder frei zu bieten;
- Verwaltungsmöglichkeit von invGUARD mit Zugang durch Mobilgeräte;
- 24/7 technischer Support, einschließlich der Vor-Ort-Unterstützung;

KAUFOPTIONEN VON invGUARD

Einmalige Zahlung

Monatszahlung

Einkommensteilung für die dem Endverbraucher tatsächlich erbrachte Dienstleistung (Schutz vor Cyberattacken)

Möglichkeit, das ganze System oder seine einzelne Subsysteмen zu erwerben (invGUARD AS, invGUARD AS & invGUARD CS)

Bis zum 5+ Tbit/s	die Geschwindigkeit der Datenverkehrs-analyse und der Verhinderung von Attacken im Netzwerk
100+	Router im einheitlichen Verwaltungsinterface
20 000+	Beobachtungsobjekte (Informations-systeme, Webseiten, Online-Shops, Internetdienstleister usw)
inhomogenes Medium	Netzwerktechnik: Juniper, HPE, H3C, Cisco, Huawei, Alcatel, Extreme usw.
250+	Berichtsformen von verschiedenen Datenverkehrs- und Objektarten
100+	Typen von aufgedeckten Cyberattacken
10 000+	Anomalien werden täglich mit der ständigen Aufbewahrung der Detaillierung gleichgerichtet
80-	Stunden für die Systemeinführung

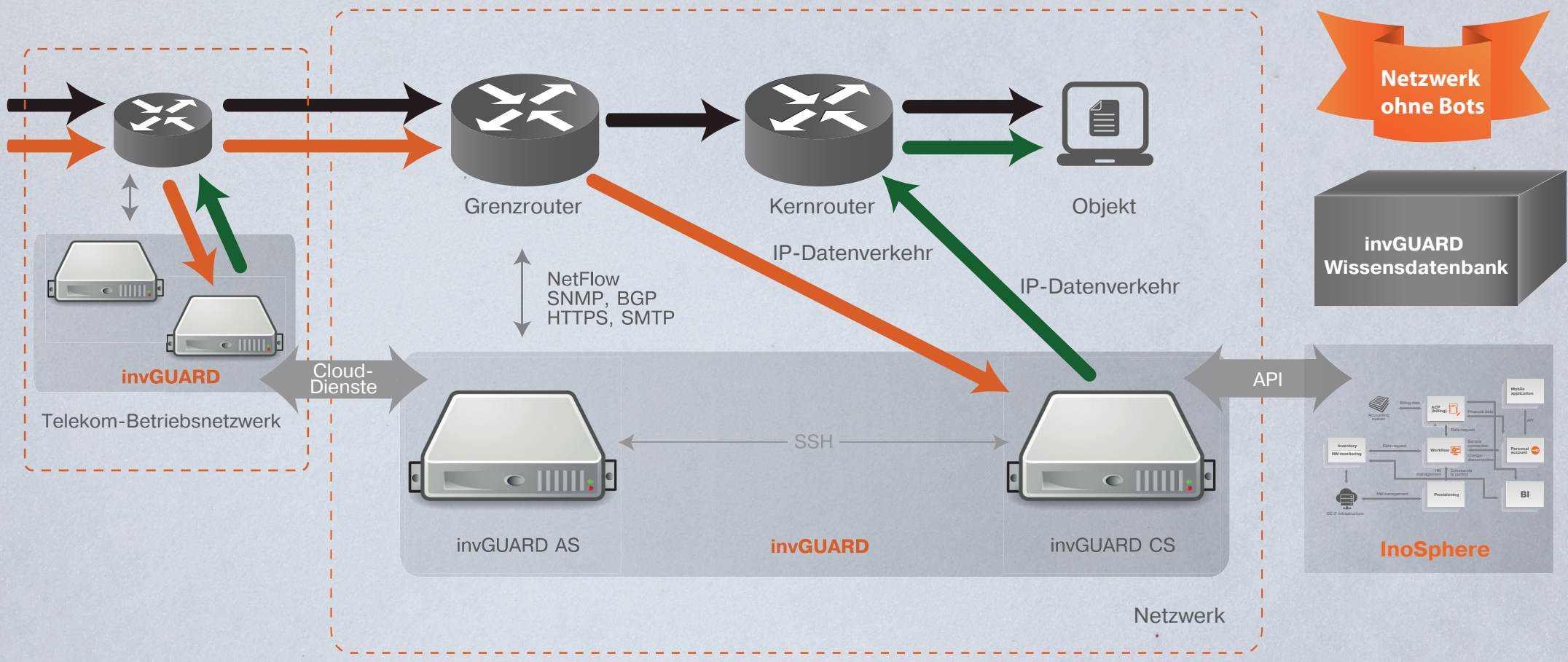
VERWENDUNGSBEREICH VON invGUARD

- Telekombetriebe
- Serviceanbieter
- Operatoren in Datenverarbeitungszentren
- Medienunternehmen (Massenmedien, Internet-Massenmedien)
- Banken und Finanzinstitute
- B2B und B2G mit einer eigenen entwickelten IuK-Infrastruktur
- Hosting-Unternehmen

EINFÜHRUNGSZIEL VON invGUARD

1. Eine kostengünstige Lösung für die Gleichrichtung und Verhinderung von Cyberattacken (DoS/DDoS-Angriffe und Attacke ohne deutliche Signaturen);
2. Senkung von DoS-Angriffen zu den Beobachtungsobjekten (Webseiten, Online-Shops, Massenmedien usw.);
3. Effektives Instrument für Datenverkehrsanalyse und Optimierung des IT-Systems;
4. Einfache Integration mit den vorhandenen Netzwerkmanagement-Plattformen durch SNMP (HP OV, IBM Tivoli, Zabbix, Nagios usw.);
5. Zusätzliche Sicherheit durch den mehrstufigen Schutz (Cloud Signaling);
6. SLA-Monitoring für den Zugang zu den Verwaltungsobjekten;
7. Effektives Instrument für die Kostenverwaltung von telco services;
8. Zusätzliche Einnahmenquelle von Dienstleistungen, die mit der Verhinderung von DoS/DDoS-Angriffen verbunden sind, für B2B/B2C-Kunden (Einfache Integration mit der Managementplattform InoSphere Cloud Services).

SYSTEMARCHITEKTUR



Subsysteme	Funktion	Anwendbare Technologien
invGUARD AS - Datenverkehrsanalyse bis zum 1 Tbit/s - Verarbeitung von bis zu 100.000 pakete/s	- Datenverkehrsanalyse; - Gleichrichtung von Anomalien und illegitimen Aktivitäten; - Gleichrichtung und Milderung der Angriffe; - Subsystemverwaltung von invGUARD CS/CS-01; - Persönliches Kunden- und Benutzerkonto; - Das zentralisierte Monitoring der Netzwerktechnik; - Die einstellbare automatische Verhinderung vor Cyberattacken; - Cloud-Dienste für mehrere Lösungen.	- Datenverkehrsanalyse im Netzwerk: NetFlow v5, v9 und IPFIX - Routerinformation: SNMP v2c - Router-Verwaltung: BGP v4 - Integration mit den Netzwerkmanagement-Plattformen (SNMP, syslog) - Benutzermitteilung: SMTP - Programmierschnittstelle invGUARD
invGUARD CS - Angriffsmilderung/ Datenverkehrsfilterung bis zum 20 Gbit/s, 30 Mio pakete/s	- Datenverkehrsfilterung, Prüfung der falschen Nutzung von Protokollen; - Angriffsmilderung (DDoS-Angriffe und Attacke ohne deutliche Signaturen)	Hochleistungsangiffsmilderung und Datenverkehrsfilterung durch speziellen Netzwerkkarten
invGUARD CS–01 - Angriffsmilderung/ Datenverkehrsfilterung bis zum 1 Gbit/s, 3 Mio pakete/s	- Datenverkehrsfilterung, Prüfung der falschen Nutzung von Protokollen; - Angriffsmilderung (DDoS-Angriffe und Attacke ohne deutliche Signaturen)	Angriffsmilderung und Datenverkehrsfilterung durch Netzwerkkarten mit Unterstützung von intel DPDK