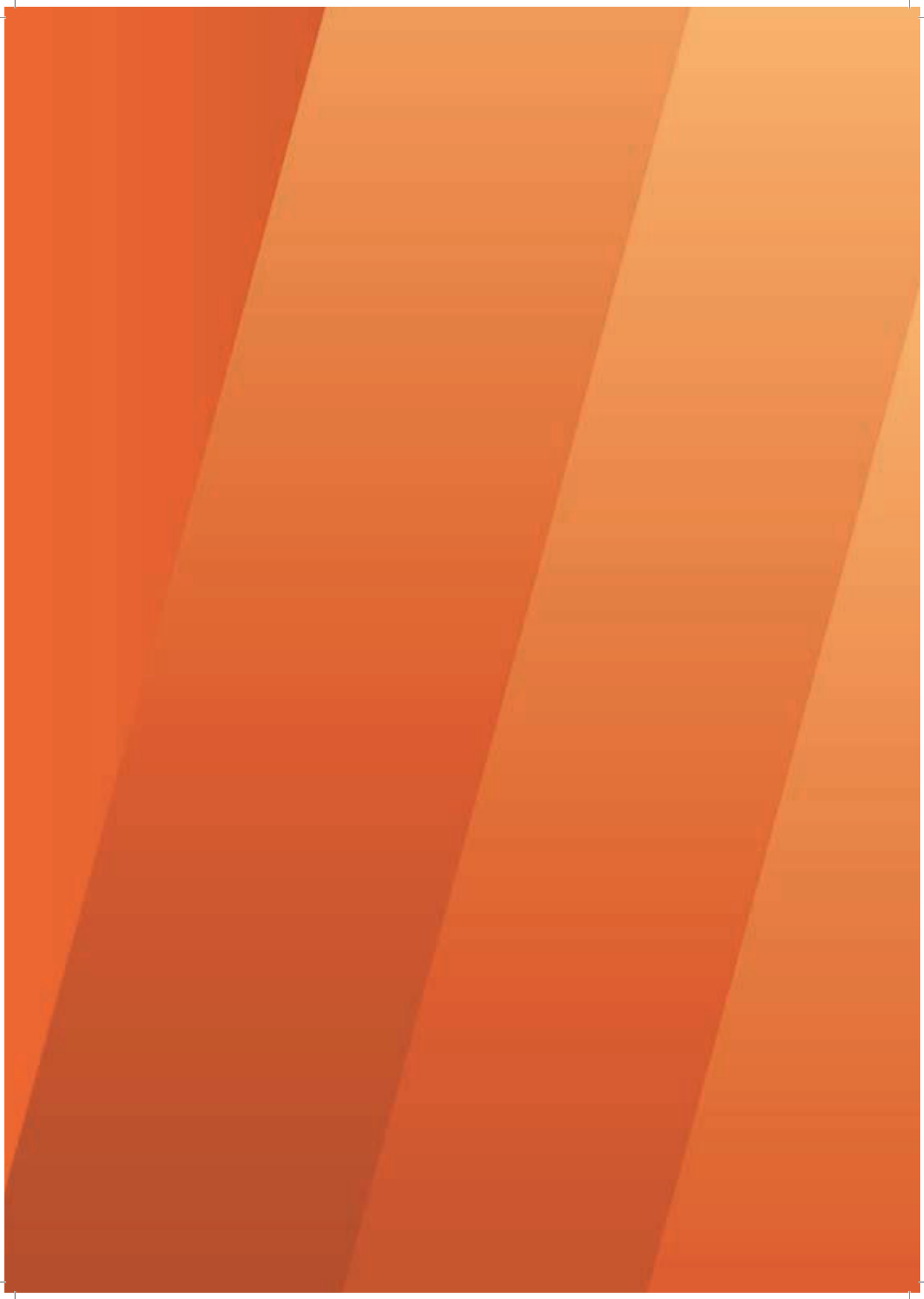

# invGUARD

Schutzsystem vor Cyberattacken

INOVENTICA TECHNOLOGIES



# INHALTSVERZEICHNIS

Was ist invGUARD? ..... 2
Funktionalität ..... 2
Systemarchitektur ..... 3
Technologien ..... 3
Verarbeitungsleistung ..... 3
invGUARD AS – Analysator ..... 4
invGUARD AS – Blockierung von Attacken auf Routern ..... 5
Instrument für Entscheidungsfindung ..... 6
Sicherheit ..... 7
Spezifikation von invGUARD AS (auf das Gerät) ..... 8
invGUARD CS – Reiniger ..... 8
invGUARD CS – Verhinderung von Attacken ..... 9
Spezifikation von invGUARD CS (auf das Gerät) ..... 9
Vorteile von invGUARD ..... 10
Verwendungsbereiche von invGUARD ..... 11
Technische Spezifikation ..... 15
Berichte ..... 18
Die Programmierschnittstelle invGUARD API ..... 19
invGUARD + inoSphere ..... 19
Integration von invGUARD mit den äußeren Monitoringssystemen nach SNMP-Protokoll ..... 19
invGUARD Cloud Signaling ..... 20
Projektplan von invGUARD ..... 21
Technischer Support ..... 21
Systemeinführung ..... 21

# invGUARD

Schutzsystem vor Cyberattacken

## WAS IST invGUARD?

**invGUARD** führt das Monitoring des Netzverkehrs in der Echtzeit durch, richtet DdoS-Attacke gleich und verhindert diese Attacke, um die schädigende Einwirkung auf das Netzwerk, die Datenverarbeitungszentren, Kunden oder Dienstleistungen zu verringern.

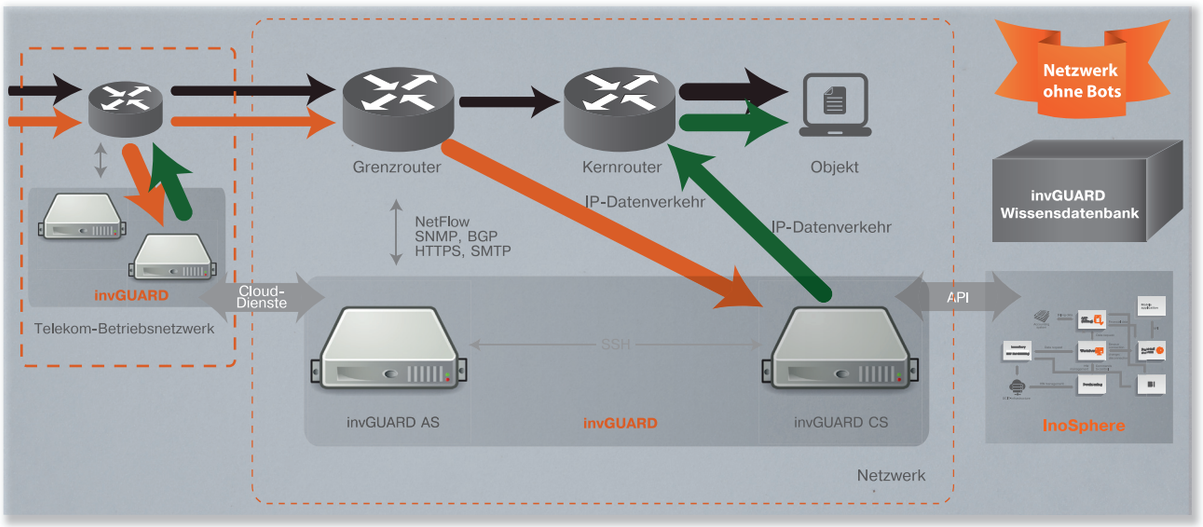
**invGUARD bietet:**

- Datenverkehrsanalyse bis zum 5 Tbit/s im Netzwerk von Dutzenden und Hunderten Routern
- Gleichrichtung und Verhinderung der Cyberattacken in der Echtzeit
- Hochleistungsfiltrierung und Reinigung des Datenverkehrs bis zum 200 Gbit/s
- Qualitätskontrolle des Datenverkehrs bei den Ressourcen, Kunden und Serviceanbietern
- Möglichkeit, den Kunden Schutz vor Cyberattacken zu bieten
- Niedriger Kaufpreis

## FUNKTIONALITÄT

- Sammelt und setzt NetFlow und SNMP-Daten, BGP-Upgrade zusammen
- Legt Berichte über verschiedene Schnitte der Protokolle TCP/IP und die Routing-Information von BGP vor
- richtet Anomalien der Objekte und Einwirkungen ohne deutliche Signaturen gleich
- richtet DDoS-Attacke – ICMP flood, TCP SYN flood, TCP Connection flood, UDP flood und mehr als 100 andere Arten von Attacken gleich
- Stellt mehr als 250 verschiedene Berichte zusammen
- Verhindert Attacke durch BGP-Berichte: Blackhole und FlowSpec
- Einwirkungen durch verwendet verschiedene Gegenmaßnahmen für Datenverkehrsfilterung, um schädigende Einwirkungen zu verhindern: TCP-Authentisierung, Transaktionsanzahlen und Verbindungen,
- Umfang der übertragenen Daten u.a.
- Wird in die Monitoringssysteme durch SNMP integriert
- Unterstützt Router verschiedener Hersteller: Juniper, Cisco, Huawei, HPE, H3C, Extreme u.a.
- Mehrsprachiges Interface

## SYSTEMARCHITEKTUR




## TECHNOLOGIEN

- Datenverkehrsanalyse: NetFlow v5, v9 und IPFIX, NetStream v5 und v9, sFlow
- Routerinformation: SNMP v2c und v3
- Routingtabelle und Router-Konfiguration: BGP v4
- Betriebssystem: Linux (Red Hat, CentOS oder ähnliche)
- Wird durch die Architektur x86 unterstützt
- Unterstützung von virtuellen Maschinen KVM für das invGUARD AS-System
- Steuerungssystem von Datenbanken MySQL Database
- Server der Web-Publikationen Apache
- Hochleistungsreinigung des Datenverkehrs wird durch spezielle oder intel DPDK passende Netzwerkkarten gewährleistet

## VERARBEITUNGSLEISTUNG

- Datenverkehrsanalyse bis zum 5 Tbit/s für den Schutz vor Cyberattacken
- 100+ Router in einem Interface
- 20000+ Beobachtungsobjekte
- Unterstützung von der heterogenen Infrastruktur: Juniper, HPE, H3C, Cisco, Huawei, Alcatel, Exterme u.a.
- 250+ verschieden Berichte über den Datenverkehr und Objekten
- 100+ Typen von gleichrichteten Cyberattacken
- 10000+ täglich gleichrichtete Ereignisse

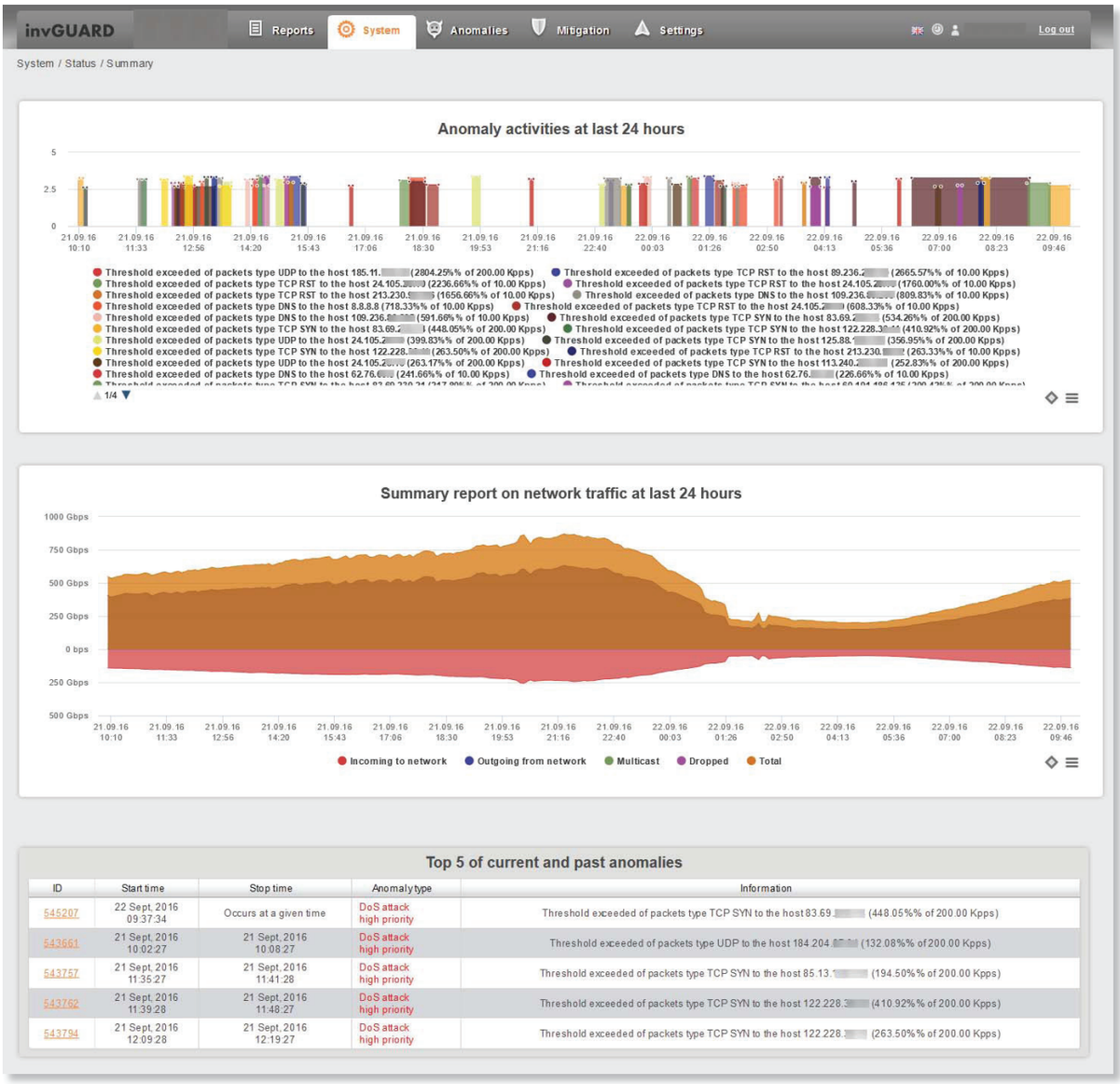
# invGUARD

Schutzsystem vor Cyberattacken

## invGUARD AS – ANALYSATOR

**invGUARD AS – Hauptkomponent des invGUARD-Systems:**

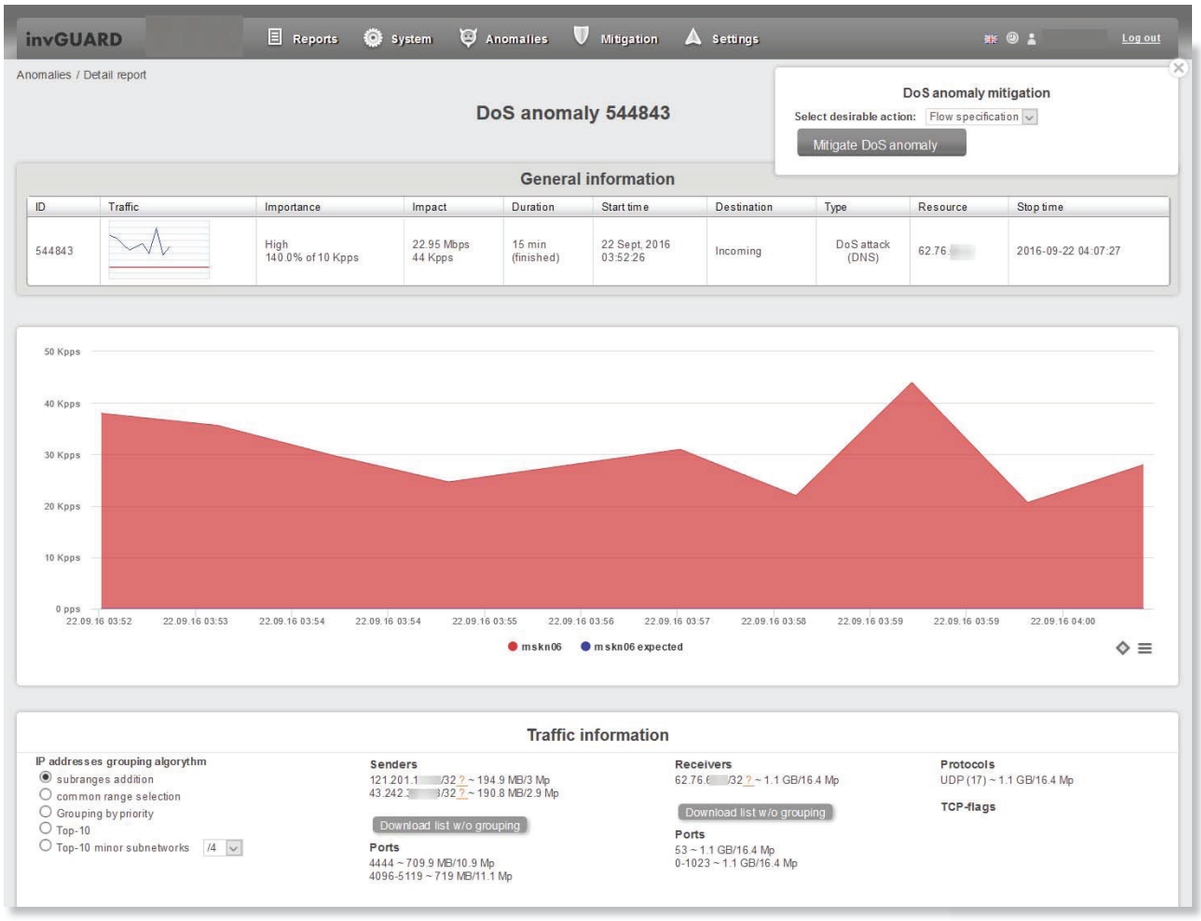
- sammelt, zusammensetzt, analysiert und speichert die Daten über den Netzverkehr von Routern durch Protokolle NetFlow, SNMP und BGP;
- richtet Anomalien im Netzverkehr, DDoS-Attacke und andere Arten von Cyberattacken gleich;
- legt ausführliche Berichte über Netzverkehr vor.




*Gesamtbericht des Systems*

# invGUARD AS – BLOCKIERUNG VON ATTACKEN AUF ROUTERN

- Blockierung des Datenverkehrs: BGP Blackhole
- Dynamische Filterung auf Routern (BGP FlowSpec): IP-Adresse der Quelle und des Empfängers von dem Datenverkehr, Protokolle, Porte, Flage, Umfang von Paketen, Fragmentierung
- Filterung durch ACL: IP-Adresse der Quelle und des Empfängers, Porte, Flage, Protokolle
- Optimierung des Datenverkehrs durch BGP FlowSpec




*Gleichrichtung der Anomalien (Attacken)*

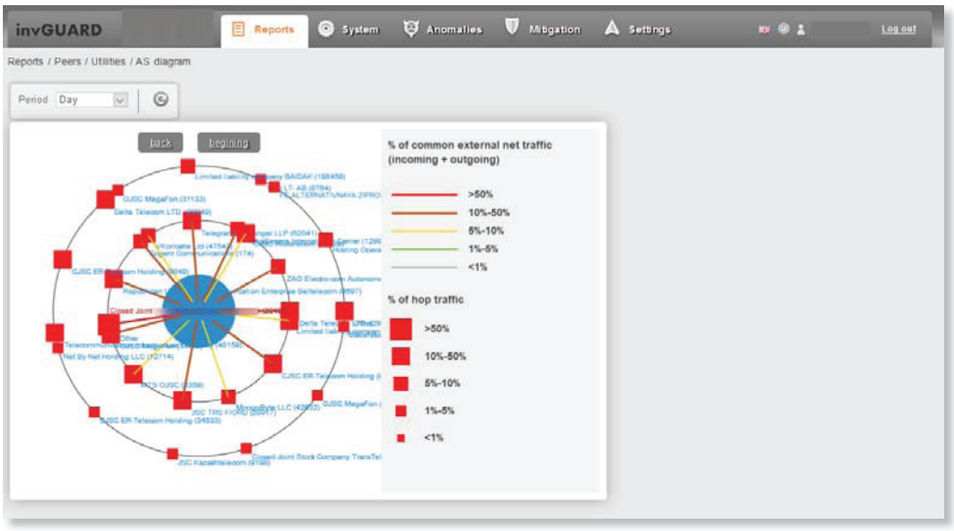
# invGUARD

Schutzsystem vor Cyberattacken

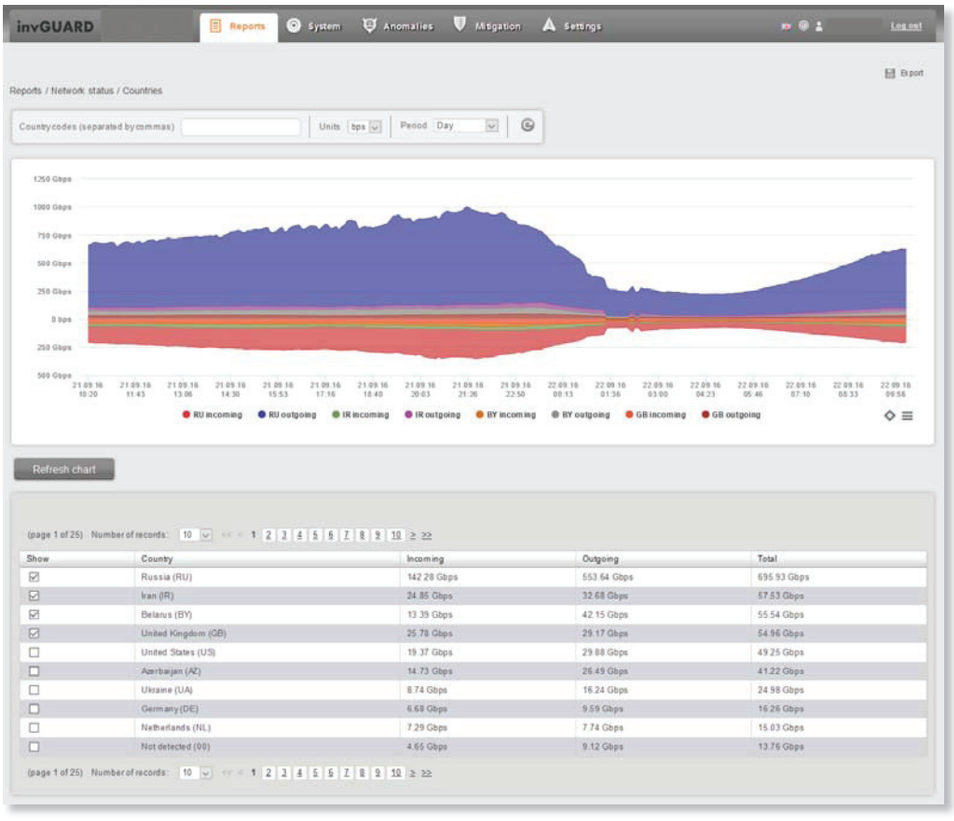
## INSTRUMENT FÜR ENTSCHEIDUNGSFINDUNG

**invGUARD AS – Instrument, das Antworten auf solche Fragen gibt:**

- Welcher Datenverkehr kommt ins Netzwerk und aus dem Netzwerk;
- Welcher Datenverkehrsweg hat der Datenverkehr;
- Welche Interfaces und Router sind eingesetzt und wie sind sie ausgelastet;
- Welche Adressen verwenden mehr Datenverkehr.




*Nachbar und Serviceanbieter*

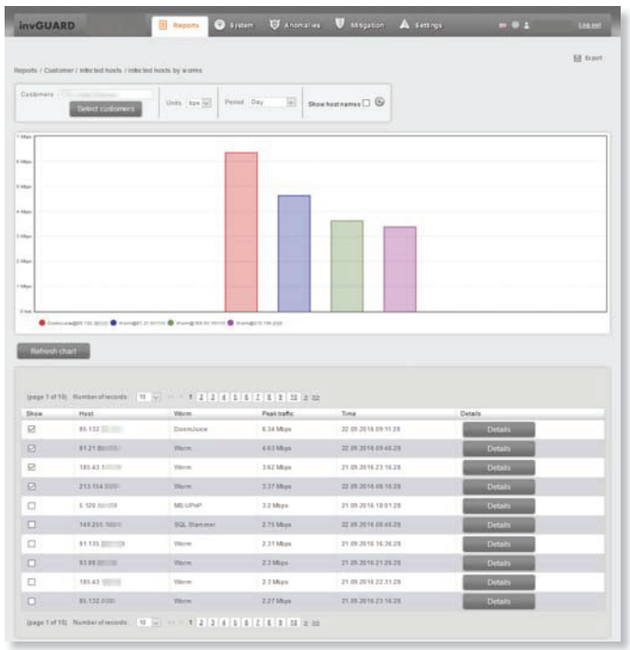



*landesweite Berichte*

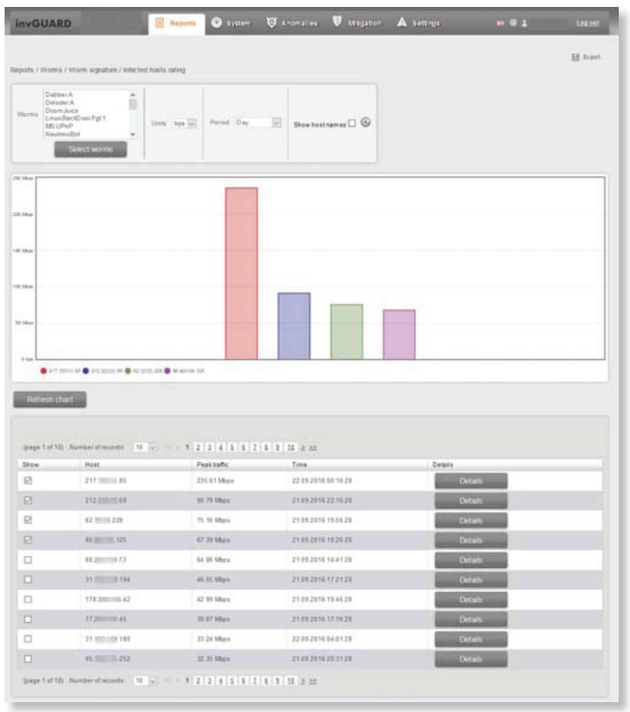
# SICHERHEIT

**invGUARD AS richtet Folgendes gleich:**

- Überschreitung des dynamisch ausgerechneten Datenverkehrsprofil;
- DDoS-Attacke: verschiedene flood-Arten, falsche Verwendung der Protokolle;
- Verseuchte Objekte im Netzwerk («Würmer»);
- Objekte, die mögliche Ziele für Attacke sind;
- Bots im Netzwerk und ihr Umgang mit Verwaltungszentren.




*Verseuchte Objekte*




*Bots im Netzwerk*

# invGUARD

Schutzsystem vor Cyberattacken

## SPEZIFIKATION VON invGUARD AS (AUF DAS GERÄT):

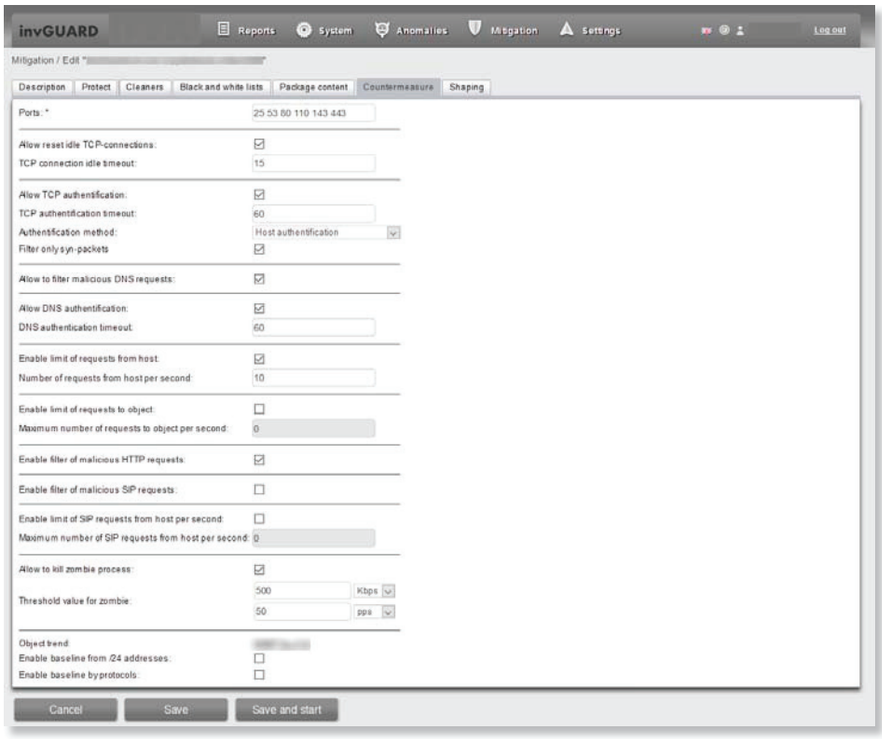
- Datenverkehrsanalyse bis zum 5 Tbit/s;
- NetFlow bis zum 100.000 Pakete/s;
- BGP: bis zum 100 Router;
- BGP: bis zu 6. 000. 000 Berichten in der Routingtabelle;
- API für Verwaltung der Beobachtungsobjekte, der Parameter für Gleichrichtung und Verhinderung von Attacken und API für Berichte;
- Mitteilungen: Berichte über SMTP, SNMP-trap und syslog;
- Webinterface für Management (Webseite-Manager, Sicherheitsingenieur);
- Webinterface für Kunden (persönliches Kundenkonto).

## invGUARD CS – REINIGER

**invGUARD CS reinigt sauber den Datenverkehr.**
Für die Umlenkung des Datenverkehrs vom normalen Verkehr zum Reiniger richtet InvGUARD AS einen BGP Next Hop Bericht auf die Router und dann wird der verseuchte Datenverkehr zum invGUARD CS gesendet, wo er analysiert und verhindert wird.

**invGUARD CS ermöglicht:**

- Sessionen des Datenverkehrs für Aufdeckung und Beseitigung der schädigenden Einwirkungen zu sammeln;
- Einstellungen der Gegenmaßnahmen für die Markierung der Datenverkehrspakete als «unrechtmäßige
- innerhalb des Systems» zu verwenden;
- unrechtmäßige Pakete zu löschen (den verseuchten Datenverkehr vom geschützten Objekt abhalten)
  Den gereinigten Datenverkehr zum geschützten Objekt durchzulassen.




*invGUARD CS Einstellungen der Gegenmaßnahmen*

## invGUARD CS – VERHINDERUNG VON ATTACKEN

- SYN-Authorisierung: Authorisierung der TCP-Verbindungen, Authorisierung der Verbindungen, Host-Authorisierung
- DNS-Authorisierung: Blockierung der Pakete mit falschen Adressen
- Schwarze und weiße Listen
- Globale Abstimmungen der Filterung (für alle Aufgaben im Bereich der Verhinderung von Attacken)
- Aufdeckung von Zombies: Filterung nach Verbindungs- und Transaktionsanzahlen und nach Umfang des Datenverkehrs
- Verhinderung der «hängenden» TCP-Verbindungen
- Aufbau der TCP-Verbindungen: eine richtige Reihenfolge der TCP-Fragmente von der Quelle zum Empfänger
- Automatische Verhinderung von Attacken: Aktivierung der Filterung nach Angaben von invGUARD AS
- Optimierung: Reduzierung des Datenverkehrs bis zu einem bestimmten Niveau
- Ermittlung der ausführlichen statistischen Daten
- Die Übernahme des Rohdatenverkehrs kann vom Kunden im Rahmen der Aufgabe aktiviert werden

## SPEZIFIKATION VON INVGUARD CS (AUF DAS GERÄT):

- Datenverkehrsfilterung und Reinigung des Datenverkehrs bis zum 20 Gbit/s (invGUARD CS)
- Datenverkehrsfilterung und Reinigung des Datenverkehrs bis zum 1 Gbit/s (invGUARD CS-01)
- Verhinderung von Attacken innerhalb der Anwendungen (HTTP, DNS, SIP,...)
- Automatische, teilautomatische und manuelle Verhinderung von Attacken
- Unterstützung der Feinabstimmungen der Filterung

# VORTEILE VON invGUARD

## 1. Lösungen, die für die Gleichrichtung und Verhinderung von Cyberattacken (DoS/DDoS-Attacken und Einwirkungen ohne deutliche Signaturen) kosteneffektiv sind

**invGUARD** bewahrt Investitionen auf – es wird keine Erneuerung der Netzwerktechnik gefordert, da das System offene Formate für Statistik des Datenverkehrs verwendet: SNMP und NetFlow.

Die beste Praxis für den Schutz vor Attacken besteht in der Nutzung des BGP-Protokolles für die Verwaltung der Datenverkehrsströme: Blackhole, FlowSpec und die Umlenkung des Datenverkehrs durch Next Hop. Alle diese Mechanismen werden von invGUARD unterstützt.

invGUARD richtet Anomalien und Einwirkungen wie das Datenverkehrsverhalten der (geschützten) Beobachtungsobjekte gleich. Für die vollfunktionelle Arbeit des Systems ist eine regelmäßige Erneuerung der Datenbanken der Signaturen nicht erforderlich.

## 2. Die Risikominderung von den Einwirkungen der DoS-Attacken auf die (geschützten) Beobachtungsobjekte, solche wie Webseiten, Online-Shops, Medienportale u.a.

**invGUARD** richtet Anomalien des Datenverkehrs, DoS/DDoS-Attacke und schädigende Einwirkungen ohne deutliche Signaturen gleich. Außerdem informiert invGUARD die Mitarbeiter in der Echtzeit, um die Einwirkung von Angriffen auf die geschützten Objekte zu reduzieren. invGUARD hilft auch den Objekten, immer zugänglich zu sein.

invGUARD reinigt den Datenverkehr nach schwarzen/weißen Listen, einer falschen Verwendung der Protokolle und schädigenden Einwirkungen, um DoS/DDoS-Attacke auf die (geschützten) Beobachtungsobjekte zu verhindern.

## 3. Ein passendes Instrument für die Datenverkehrsanalyse und Optimierung der Netzinfrastruktur

**invGUARD** gibt die Gelegenheit, den Datenverkehr im Netz bis zum 5 Tbit/s zu analysieren, der aus Hunderten Routern besteht: mehr als 250 einstellbare Berichte über Protokolle, Anwendungen, BGP-Attributen, Beobachtungsobjekten, Interfaces, QoS-Parameter, Routing Information Protocol und Länder.

invGUARD hilft, begründete Entscheidungen über die Optimierung der Netzverkehrsströme, den Datenverkehrsweg und die Netzinfrastruktur zu treffen.

## 4. Eine einfache Integration mit den existierenden Monitoringssystemen und Netzmanagementplatfformen nach SNMP-Protokoll (HP OV, IBM Tivoli, Zabbix, Nagios u.a.)

**invGUARD** integriert einfach mit den Monitoringssystemen und Netzmanagementplatfformen nach SNMP-Protokoll. Bei der Aufdeckung von Anomalien und Cyberattacken sendet das System SNMP-Traps unter Verwendung der registrierten Kennzeichnung enterprise.44937.1.1 OID.

Zusätzlich dazu verwendet invGUARD den Mechanismus SYSLOG für den Import und Export von Sicherheitsereignissen in die äußere Systeme.

## 5. Ein gestaffelter Schutz vor Cyberattacken für ein gehobenes Sicherheitsniveau (Cloud Signaling)

**invGUARD** hilft, einen gestaffelten Schutz der Informationsressourcen und Netzwerke durch Cloud Signaling zu errichten, um hochfrequente und umfangreiche DoS/DDoS-Attacke auf Netzwerkanbieter des geschützten Netzwerks zu verhindern.

invGUARD ist ein Instrument für einen effektiven mehrstufigen Schutz und für verschiedene Sicherheitsniveaus.

## 6. Durchführungskontrolle von SLA nach Zugriff zu den Informationsressourcen

**InvGUARD** legt mehr als 250 verschiedene Berichte vor, die ermöglichen, die Kontrollmechanismen SLA nach Zugriff zu den Beobachtungsobjekten (Informationsressourcen, Netzwerksegmente usw.) aufzubauen und Mitteilungen über SLA-Störungen zu senden. Die Berichte enthalten Information über Datenverkehrsprofil, Aufdeckungsschwelle, Perioden ohne Zugriff und mit dem Service.

### 7. Ein effektives Instrument für die Kostenverwaltung der Telekommunikationsdienstleistungen

**invGUARD** legt Berichte über Serviceanbieter/Nachbar vor und ermöglicht, die gefährlichsten (Quelle der Angriffe) und sicherste (ohne Quelle der Angriffe) Anschlüsse zu den äußeren Systemen zu bestimmen. Noch dazu bietet invGUARD Instrumente für die Nutzungskontrolle und Ressourcenverwaltung der Netzwerktechnik.

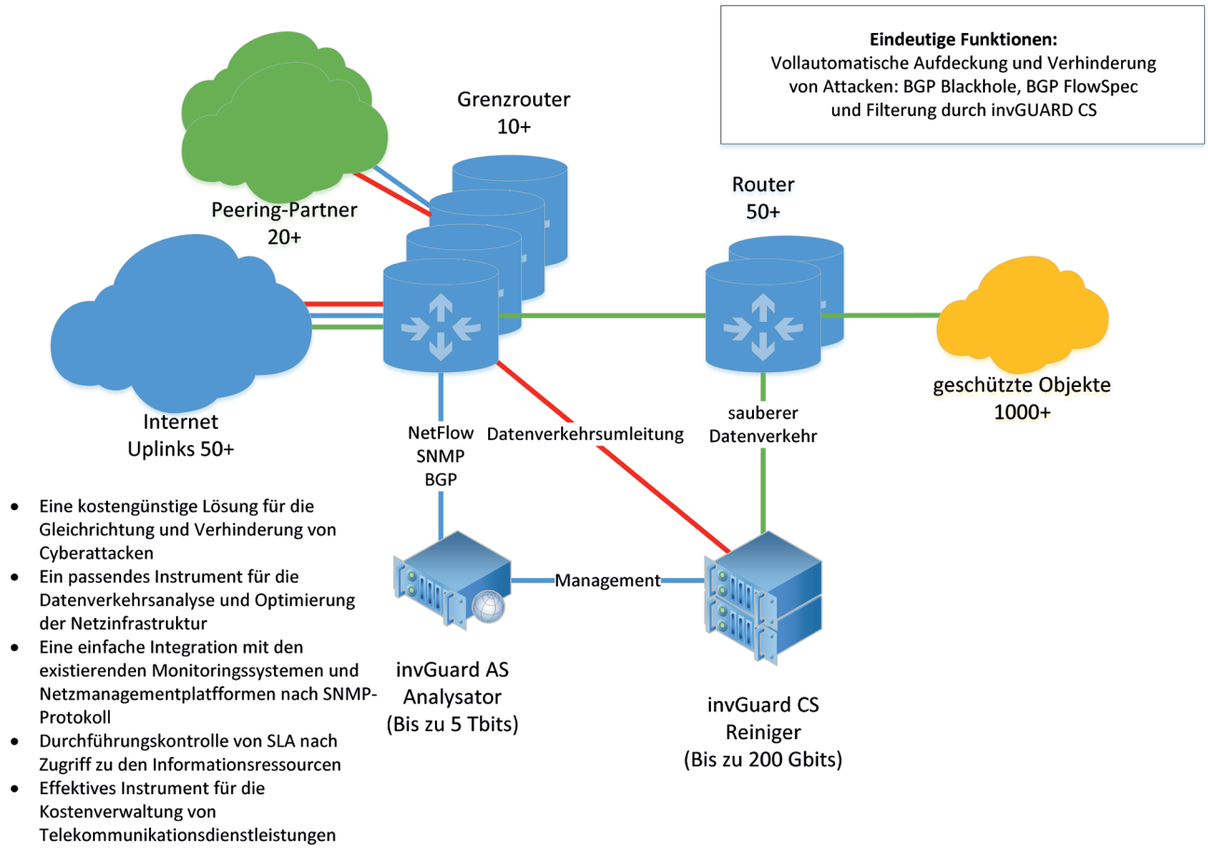
### 8. Eine zusätzliche Einnahmequelle für den Schutz vor DoS/DDoS-Attacken für B2B/B2C-Kunden (eine einfache Integration mit dem Netzmanagementplattform der Cloud-Dienste InoSphere)

**invGUARD** verfügt über ein offenes API für die Integration mit den äußeren Steuerungssystemen und wird mit der vorläufig eingestellten Konfiguration für den Schutz vor DoS/DDoS-Attacken geliefert. Dies erlaubt den invGUARD-Kunden die Erbringung von Dienstleistungen kurzfristig zu organisieren und zusätzliches Einkommen zu bekommen.

InoSphere ist eine Plattform für Cloud-Dienste für B2B/B2C-Kunden im automatischen Betrieb. InoSphere wird mit der eingebauten Unterstützung des Anschließens zu invGUARD geliefert und bietet den Schutz vor DoS/DDoS-Attacken mit der Möglichkeit, gebührenpflichtige Dienstleistungen zu erbringen.

## VERWENDUNGSBEREICHE VON invGUARD

### Telekombetriebe




- Eine kostengünstige Lösung für die Gleichrichtung und Verhinderung von Cyberattacken
- Ein passendes Instrument für die Datenverkehrsanalyse und Optimierung der Netzinfrastruktur
- Eine einfache Integration mit den existierenden Monitoringssystemen und Netzmanagementplattformen nach SNMP-Protokoll
- Durchführungskontrolle von SLA nach Zugriff zu den Informationsressourcen
- Effektives Instrument für die Kostenverwaltung von Telekommunikationsdienstleistungen

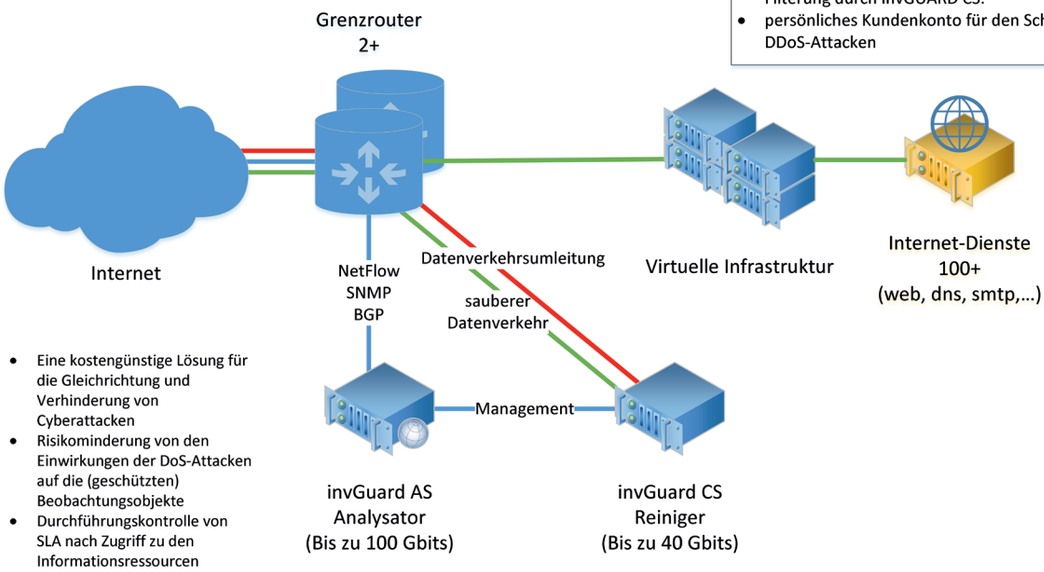
# invGUARD

Schutzsystem vor Cyberattacken

## Serviceanbieter

**Eindeutige Funktionen:**

- Vollautomatische Aufdeckung und Verhinderung von Attacken: BGP Blackhole, BGP FlowSpec und Filterung durch invGUARD CS.
- persönliches Kundenkonto für den Schutz vor DDoS-Attacken

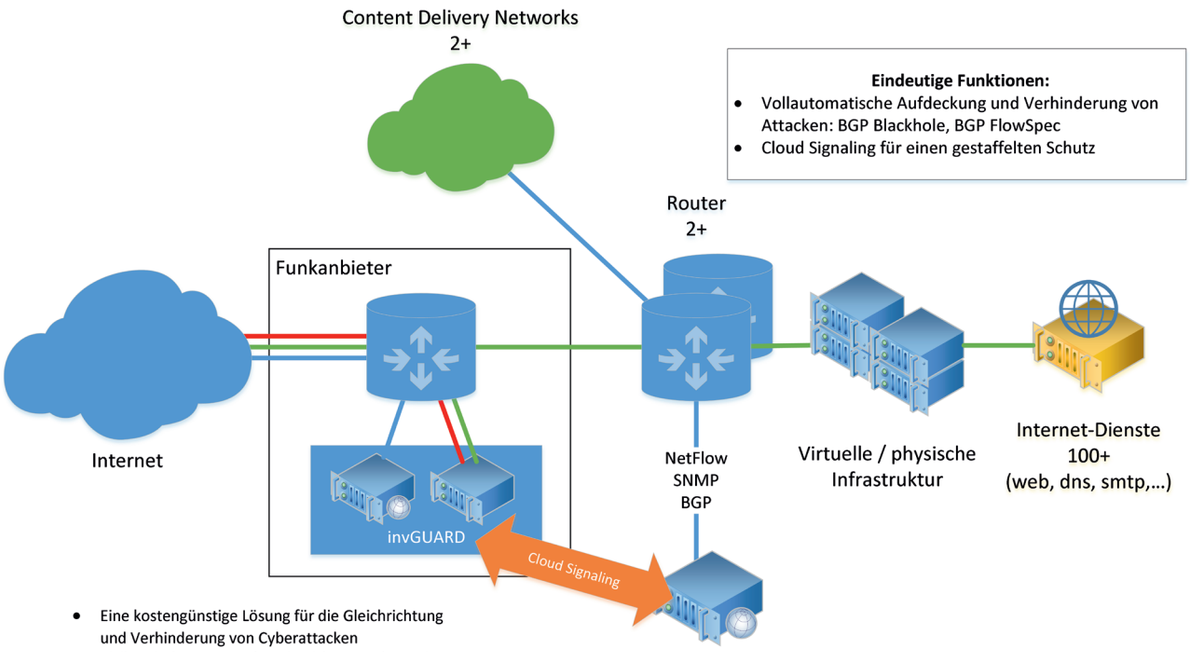



- Eine kostengünstige Lösung für die Gleichrichtung und Verhinderung von Cyberattacken
- Risikominderung von den Einwirkungen der DoS-Attacken auf die (geschützten) Beobachtungsobjekte
- Durchführungskontrolle von SLA nach Zugriff zu den Informationsressourcen
- Effektives Instrument für die Kostenverwaltung von Telekommunikationsdienstleist ungen

## Operatoren in Datenverarbeitungszentren

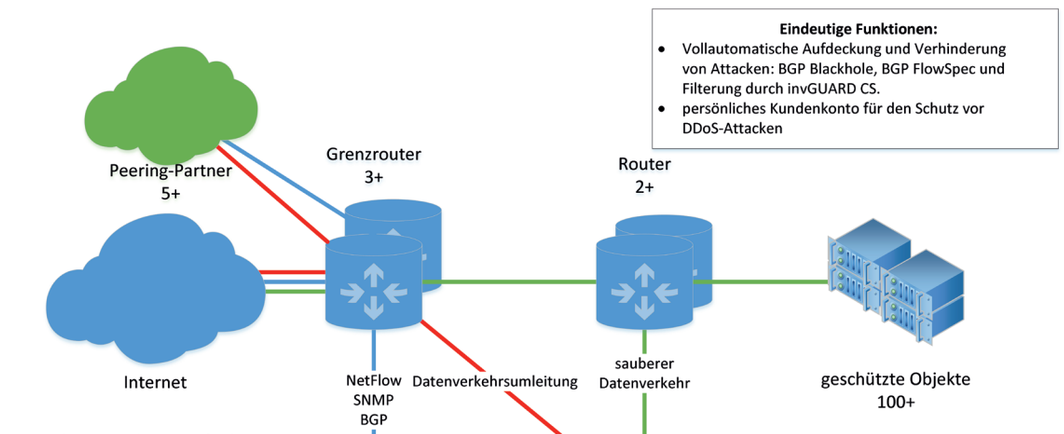
**Eindeutige Funktionen:**

- Vollautomatische Aufdeckung und Verhinderung von Attacken: BGP Blackhole, BGP FlowSpec
- Cloud Signaling für einen gestaffelten Schutz



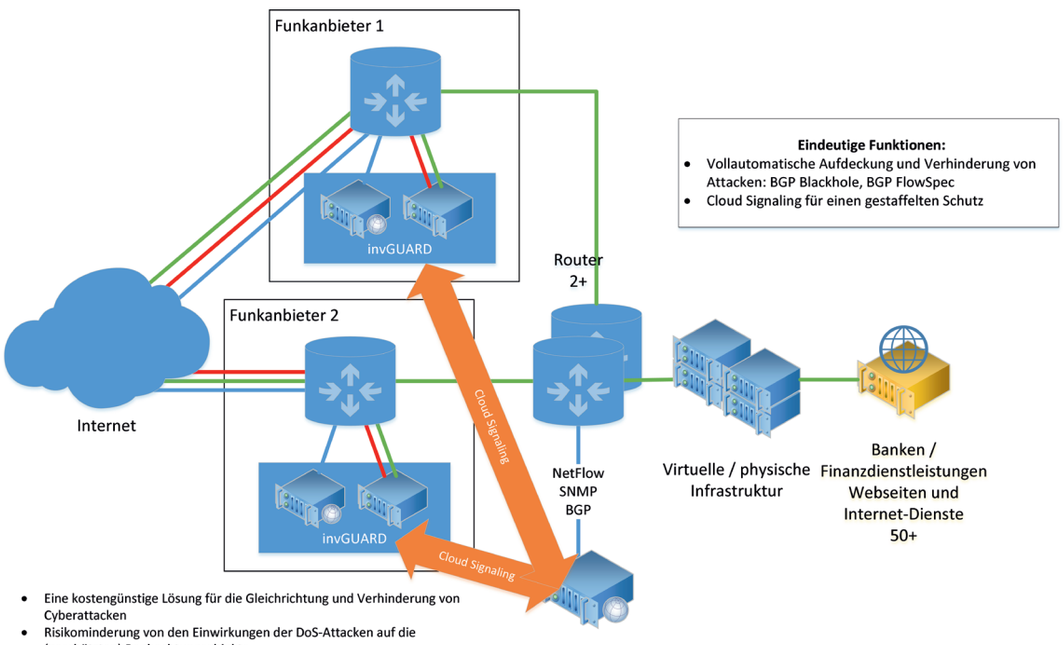

- Eine kostengünstige Lösung für die Gleichrichtung und Verhinderung von Cyberattacken
- Risikominderung von den Einwirkungen der DoS-Attacken auf die (geschützten) Beobachtungsobjekte
- Ein gestaffelter Schutz vor Cyberattacken für ein gehobenes Sicherheitsniveau
- Durchführungskontrolle von SLA nach Zugriff zu den Informationsressourcen
- Effektives Instrument für die Kostenverwaltung von Telekommunikationsdienstleistungen

## Medienunternehmen




- Eine kostengünstige Lösung für die Gleichrichtung und Verhinderung von Cyberattacken
- Ein passendes Instrument für die Datenverkehrsanalyse und Optimierung der Netzinfrastruktur
- Eine einfache Integration mit den existierenden Monitoringssystemen und Netzmanagementplatfformen nach SNMP-Protokoll
- Durchführungskontrolle von SLA nach Zugriff zu den Informationsressourcen
- Effektives Instrument für die Kostenverwaltung von Telekommunikationsdienstleistungen

## Banken und Finanzinstitute




- Eine kostengünstige Lösung für die Gleichrichtung und Verhinderung von Cyberattacken
- Risikominderung von den Einwirkungen der DoS-Attacken auf die (geschützten) Beobachtungsobjekte
- Ein passendes Instrument für die Datenverkehrsanalyse und Optimierung der Netzinfrastruktur
- Eine einfache Integration mit den existierenden Monitoringssystemen und Netzmanagementplatfformen nach SNMP-Protokoll
- Ein gestaffelter Schutz vor Cyberattacken für ein gehobenes Sicherheitsniveau
- Durchführungskontrolle von SLA nach Zugriff zu den Informationsressourcen
- Effektives Instrument für die Kostenverwaltung von Telekommunikationsdienstleistungen

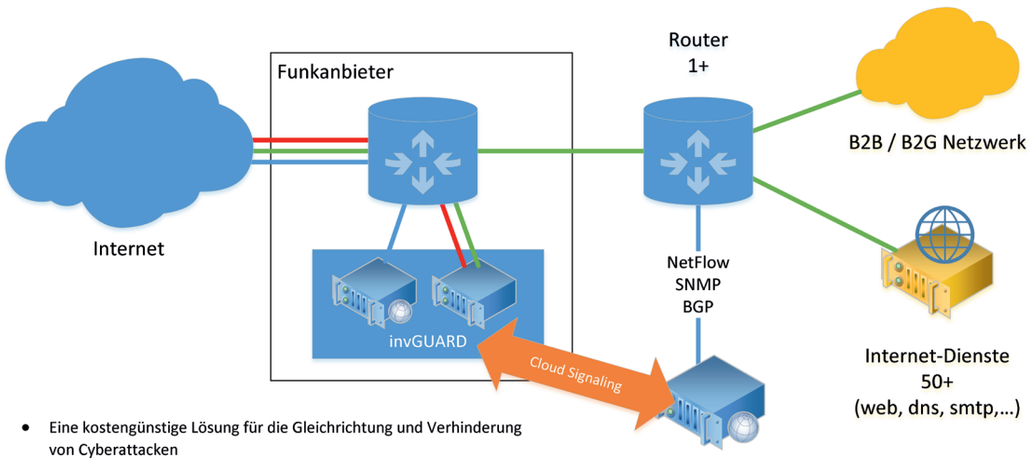
# invGUARD

Schutzsystem vor Cyberattacken

## B2B und B2G mit eigenen IuK-Infrastruktur

**Eindeutige Funktionen:**

- Vollautomatische Aufdeckung und Verhinderung von Attacken: BGP Blackhole, BGP FlowSpec
- Cloud Signaling für einen gestaffelten Schutz

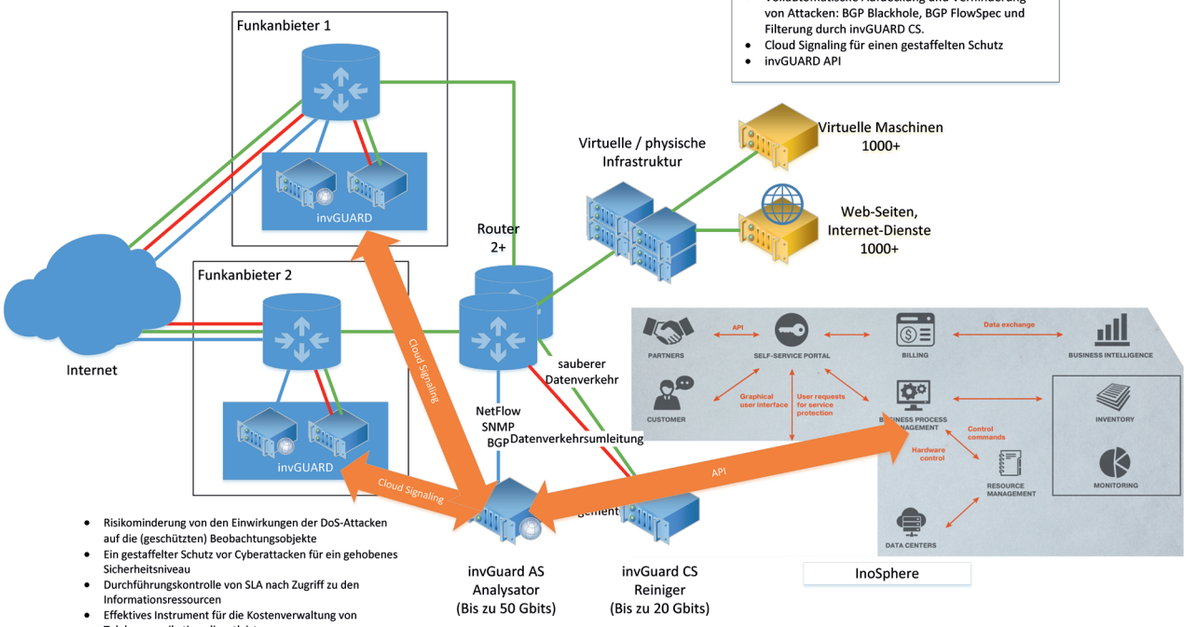



- Eine kostengünstige Lösung für die Gleichrichtung und Verhinderung von Cyberattacken
- Risikominderung von den Einwirkungen der DoS-Attacken auf die (geschützten) Beobachtungsobjekte
- Eine einfache Integration mit den existierenden Monitoringssystemen und Netzmanagementplatfformen nach SNMP-Protokoll
- Ein gestaffelter Schutz vor Cyberattacken für ein gehobenes Sicherheitsniveau
- Durchführungskontrolle von SLA nach Zugriff zu den Informationsressourcen
- Effektives Instrument für die Kostenverwaltung von Telekommunikationsdienstleistungen

## Schutz vor Attacken für Serviceanbieter der Cloud-Dienste und Hosting-Unternehmen

**Eindeutige Funktionen:**

- Vollautomatische Aufdeckung und Verhinderung von Attacken: BGP Blackhole, BGP FlowSpec und Filterung durch invGUARD CS.
- Cloud Signaling für einen gestaffelten Schutz
- invGUARD API




- Risikominderung von den Einwirkungen der DoS-Attacken auf die (geschützten) Beobachtungsobjekte
- Ein gestaffelter Schutz vor Cyberattacken für ein gehobenes Sicherheitsniveau
- Durchführungskontrolle von SLA nach Zugriff zu den Informationsressourcen
- Effektives Instrument für die Kostenverwaltung von Telekommunikationsdienstleistungen
- Eine zusätzliche Einnahmequelle für den Schutz vor DoS/ DDoS-Attacken für B2B/B2C-Kunden (eine einfache Integration mit dem Netzmanagementplattform der Cloud-Dienste InoSphere)

# TECHNISCHE SPEZIFIKATION

## DATENERFASSUNG DURCH NETFLOW

**invGUARD sammelt die Datenverkehrsstatistik durch Protokolle:**

- NetFlow v5
- NetFlow v9
- NetFlow v10
- NetStream v5 und v9 für Router Huawei mit der SNMP-Tabelle Umgestaltung der Interfaces
- IPFIX
- sFlow

**NetFlow-Parameter:** IP-Adresse der Quelle, Port, Abtastniveau

## EINWIRKUNG NACH SNMP-PROTOKOLL

**invGUARD sammelt Information über Interfaces unter Verwendung von SNMP-Protokoll:**

- Router-Interfaces: ifIndex, Beschreibung, Geschwindigkeit, IP-Adresse
- Statistik nach Datenverkehr (nach Zählern)
- Auslastung des Routerprozessors
- Verwendung des Arbeitsspeichers des Routers

**SNMP-traps für äußere Monitoringssysteme und Netzmanagementplattformen:**

- invGUARD wurde für die Integration mit den äußeren Monitoringssystemen entworfen, um die Ereignisse der Gleichrichtung von Cyberattacken durch SNMP-Trap zu steuern.
- Äußere Monitoringssysteme können invGUARD nach SNMP v2c –Protokoll mit einer bestimmten Kennzeichnung enterprise.44937.1.1 OID. abrufen, um die ausführliche Information über die Attacken
- zu bekommen.
  invGUARD integriert mit solchen Monitoringssystemen wie Zabbix, Nagios u.a. problemlos.

**SNMP-Parameter:** Version, IP-Adresse, community (für v2/v2c), Benutzername/Kennwort (für v3)

## VERKEHRSROUTING

- BGP-Update für die Änderung des Datenverkehrswegs:
  - Blackhole
  - NextHop
  - FlowSpec
- Dynamisches Routing unter Verwendung von GRE-Tunnels im invGUARD CS-System

**BGP-Parameter:** IP-Adresse des Routers, ID des Routers, lokale und entfernte Nummern der autonomen Systeme, md5-Schlüssel

## BGP-PEERING

- iBGP
- iBGP mit Routern – Route-Reflektor
- iBGP mit den Routingservern
- Verwendung von BGP-Routingtabellen anderer Router
- eBGP

## GLEICHRICHTUNG DER ANOMALIEN

- BGP-Fallen
- BGP-Instabilität
- Fälschung des BGP
- Verlust des BGP
- Übersprung des NetFlow
- Fehlen des SNMP
- DoS- und DDoS-Attacken
- Bereichsgrenzen nach Verkehrsumfang
- Bereichsgrenzen nach Festlegung von Interfaces
- Bereichsgrenzen nach Datenverkehr der Beobachtungsobjekte
- Datenverkehr der „dunklen“ IP-Adressen

## GLEICHRICHTUNG DER BOTS

- Gleichrichtung der Bot-Aktivität
- Bereichsgrenzen nach Datenverkehr der Bot-Aktivität

## GLEICHRICHTUNG DER CYBERATTACKEN

- TCP SYN Flood
- TCP RST Flood
- TCP Flood
- HTTP Flood
- DNS Request Flood
- DNS Amplification
- NTP Amplification
- SSDP Amplification
- FTP Flood
- Falscher SIP-Datenverkehr
- UDP Flood (Dienste auf Basis des UDP-Protokolls: SNMP, Radius, NTP, IPSec über UDP u.a.)
- ICMP Echo Request/Reply Flood

## FINGERABDRÜCKE

**invGUARD** verfügt über einstellbare Fingerabdrücke der Cyberattacken, die vom Kunden eingetragen oder aus der zentralen Paketquelle erhalten werden können:

- Kunden können die Fingerabdrücke durch Interface von invGUARD erzeugen und ändern.
- Fingerabdrücke können sich aus der zentralen Datenbank von Inoventica erneuert werden.

## KONFIGURATION DER INTERFACES

- Liste von Interfaces auf den Routern (Index, Bezeichnung, Beschreibung und Geschwindigkeit)
- Klassifikationsverwaltung von Interfaces
- Bereichsgrenzen des Datenverkehrs nach Interfaces

## AUTOMATISCHE KONFIGURATION DER INTERFACES

- Regelmanagement der automatischen Konfiguration von Interfaces: jede Änderung des Interfaces auf dem Router wird duch das System gleichgerichtet und invGUARD bestimmt den Typ des Interfaces nach den angegebenen Regeln.
- Die Regeln werden durch den regulären Ausdruck (regexp) nach Interface-Beschreibung für die Bestimmung des Types des Interfaces festgelegt.
- Die Regeln bestimmen den Typ des Interfaces (innerer, äußerer, unangesehene usw.)

## BEOBACHTUNGSOBJEKTE

- Arten: Kunde, Profil, Nachbar, Wurm
- Bestimmung des Datenverkehrs des Beobachtungsobjektes:
  - Binärer Ausdruck
  - Regulärer Ausdruck von AS Path regexp
  - CIDR-Blöcke
  - CIDR-Gruppen
  - BGP community
  - Interfaces
  - Angrenzende ASN
  - Lokale ASN oder SubAS
- Bereichsgrenze nach Datenverkehr des Objektes, nach Detektoren oder Datenverkehrsverhalten
- Parameter für die Gleichrichtung und Mitteilung
- Parameter für die Unterdrückung von Attacken: automatisch/manuell, Aufgabenschablonen und Methoden für die Verhinderung von Attacken

## EIGENE SICHERHEIT

- Die geschützten Anschließen zwischen den Komponenten von invGUARD
- Die Zugriffskontrolle und das Logging-System
- Management der Anwenderidentifikation und Benutzerautorisation
- Historische Berichte über den Zugriff zum System und zur Funktionsnutzung
- Gleichrichtung des Phishings durch NetFlow

# BERICHTE

Jeder im invGUARD vorgestellte Bericht kann für die Durchsicht der notwendigen Periode (Tag, Woche, Monat, Jahr u.a.) und für den Export der Berichte im Format: Text, XML, PDF (einfach die Schaltfläche „Export“ im Bericht drücken) eingestellt werden.

1. **Gesamtbericht über den Datenverkehr**
2. **Gesamtbericht mit aktiven Anomalien**
3. **Aktuelle und vergangene Anomalien mit einem einstellbaren Filter (Wichtigkeit, Beobachtungsobjekt, Router, Bereichsgrenze u.a.)**
4. **Systemstatus von invGUARD**
5. **Gesamtbericht über Router**
6. **Kontrollpanel des Routers**
7. **Gesamtbericht über Interfaces**
8. **Ein ausführlicher Gesamtbericht über BGP (Routingtabelle, Upgrades)**
9. **Vergleich zwischen NetFlow/SNMP**
10. **Berichte über Beobachtungsobjekte:**
    - a. Gesamtbericht
    - b. Nach Protokollen: ICMP, TCP, UDP
    - c. Nach BGP-Attributen: alle ASN, Origin ASN, Peer ASN, AS path, ASxAS, communities, Next hop, Präfixe
    - d. Nach Routern
    - e. Nach Interfaces
    - f. Nach anderen Beobachtungsobjekten (Kunden, Nachbar, Profil)
    - g. Multicast-Verkehr
    - h. QoS
        - i. ToS
        - ii. DTRM
        - iii. IP Precedence
    - i. Nach Paketengrößen
    - j. Nach Ländern
11. **Berichte über „Würmer“ und Bots:**
    - a. Aktivität nach Objekten oder IP-Adressen
    - b. Verseuchte Hosts (Ressourcen) innerhalb oder außerhalb des Netzwerkes
12. **Berichte über invGUARD CS**
    - a. Datenverkehrsfilterung
    - b. Statistik:
    - i. Nach Protokollen
    - ii. Nach HTTP: URL-Liste
    - iii. Nach DNS: Domains
    - iv. Nach SIP: Kundennummer
13. **Berichte über Anomalien:**
    - a. Aktuelle (aktive) Anomalien
    - b. Detaillierung über Anomalien:
    - i. Einfluss
    - ii. Ausführliche IP-Adressen: Absender und Empfänger
    - iii. Porte
    - iv. Länder
    - v. Nummer der autonomen Systeme
    - vi. Paketgröße
    - vii. Router und Interfaces
    - c. Vergangene (geschlossene) Anomalien

# DIE PROGRAMMIERSCHNITTSTELLE INVGUARD API

Die Programmierschnittstelle **invGUARD API** kann durch HTTPS-Protokoll mit der Unterstützung des JSON-Formats verwendet werden, das mit Hilfe des Mechanismus MessagePack eingepackt ist.

Die Programmierschnittstelle invGUARD API kann für die Automatisierung der Steuerungsaufgaben durch invGUARD-System aus den äußeren Systemen verwendet werden:

- Errichtung, Änderung und Dursicht der Beobachtungsobjekte
- Verwaltung von Parametern für die Gleichrichtung von Cyberattacken
- Ermittlung einer Liste von gleichgerichteten Cyberattacken nach den aktuellen und historischen Ereignissen
- Verwaltung von Parametern für die Verhinderung von Attacken
- Ermittlung von einer Aufgabenliste für die Verhinderung von Attacken
- Ermittlung von Berichtsdaten über den Datenverkehr der Beobachtungsobjekte

# invGUARD + inoSphere

**invGUARD** ist für eine schnelle und einfache Integration mit der Netzmanagementplattform der Cloud-Dienste InoSphere vorbereitet, um den Benutzern (den Kunden) von InoSphere den Schutz vor Cyberattacken zu bieten.

Die Benutzer von InoSphere bekommen einen kostenlosen Zugriff zur Datenverkehrsstatistik für jede IP-Adresse, die durch InoSphere-Dienste bestellt wird.

Die Schutzdienste vor Cyberattacken enthalten die Gleichrichtigung und Unterdrückung (Verhinderung) vor Cyberattacken. InoSphere leitet das invGUARD-System durch die Programmierschnittstelle invGUARD API, um die Parameter der Beobachtungsobjekte, die Parameter der Gleichrichtung und Methoden für die Verhinderung von Attacken einzustellen.

InoSphere bietet die Möglichkeit für die Tarifbildung und das Billing für den Schutz vor Cyberattacken: monatlich nach verschiedenen Tarifen und stundenweise.

Die Benutzer von InoSphere können ganz einfach die durch invGUARD-System dargestellte Schutzdienste vor Cyberattacken verwalten und den notwendigen Tarif durch persönliches Kundenkonto von InoSphere auswählen.

# INTEGRATION VON invGUARD MIT DEN ÄSßEREN MONITORINGSSYSTEMEN NACH SNMP-PROTOKOLL

**invGUARD** wurde für die Integration mit den äußeren Monitoringssystemen entworfen, um die Ereignisse der Gleichrichtung von Cyberattacken durch SNMP-Trap zu steuern.

Äußere Monitoringssysteme können invGUARD nach SNMP v2c –Protokoll mit einer bestimmten Kennzeichnung enterprise.44937.1.1 OID. abrufen, um die ausführliche Information über die Attacken zu bekommen.

invGUARD integriert mit solchen Monitoringssystemen wie Zabbix, Nagios u.a. problemlos.

# invGUARD CLOUD SIGNALING

**invGUARD Cloud Signaling** bietet Funktionen für «Cloud»-Datenverkehrsreinigung vor Cyberattacken, Filterung nach schwarzen/weißen Listen, Optimierung und falsche Verwendung von Protokollen.
invGUARD Cloud Signaling kann im System invGUARD AS für das Anschließen zum “Cloud” verwendet werden, das durch Telekommunikationsdiensteanbieter mit Hilfe des invGUARD-Systems und durch aktive Funktionen von invGUARD Cloud Signaling gewährt wird. Wenn der Benutzer über kein Reinigungssystem invGUARD CS verfügt, kann er zur “Cloud”-Datenverkehrsreinigung vom Serviceanbieter mit Funktionen von invGUARD Cloud Signaling anschließen und die Filterung und Datenverkehrsreinigung beim Serviceanbieter durchführen.
Das invGUARD-System verwendet ein Standardprotokoll von invGUARD Cloud Signaling für den Aufgabenaustausch im Bereich der Vehinderung vor Attacken und den Austausch von Statistik ohne Speicherung jeglicher kommerziellen Information auf den Systemen des Serviceanbieters.
invGUARD Cloud Signaling mit der “Kunden”-Funktion kann jedem invGUARD AS-System für zusätzliche Möglichkeiten der Verhinderung von Attacken mit Funktion der Datenverkehrsfilterung in Systemen mit der “Serviceanbieter”-Funktion ohne die Notwendigkeit, das invGUARD CS-System einzustellen, zugeordnet werden.
invGUARD Cloud Signaling mit der “Serviceanbieter”-Funktion kann den invGUARD-Systemen, bestehend aus dem System der Datenverkehrsanalyse invGUARD AS und dem System der Datenverkehrsreinigung invGUARD CS (mindestens ein davon) für das Anschließen der “Kunden” und für Erbringung der folgenden Dienstleistungen im “Serviceanbieter”-System zugeordnet werden:

- Filterung nach schwarzen/weißen Listen
- TCP-Authorisierung
- Verwaltung der TCP-Verbindungen und Beschränkungen der Verbindungsanzahlen
- Prüfung der Protokolle HTTP, DNS, SIP auf die Übereinstimmung mit den Standards (RFC)
- Beschränkungen der gleichzeitigen Anfragen zu/von dem Objekt oder Host
- Inhaltsprüfung der Datenverkehrspakete nach regulären Ausdrücken
- Datenverkehrskontrolle
- Gleichrichtung und Verhinderung der Aktivität von «Zombies»
- Optimierung des Datenverkehr

# PROJEKTPLAN VON invGUARD

| Die zweite Jahreshälfte 2017 | Die erste Jahreshälfte 2018 | Die zweite Jahreshälfte 2018 |
|---|---|---|
| • Analyseinstrumente für die Gleichrichtung und Verhinderung von<br>• Cyberattacken<br>• IPv6: Analyse durch NetFlow<br>• IPv6: Gleichrichtung von Attacken<br>• IPv6: Berichte über verschiedene Schnitte des Datenverkehrs<br>• BGP mit IPv6<br>BGP mit IPv6 Support für Blackhole und FlowSpec<br>• Partnerschaft mit Antivirenunternehmen | • IPv6: Datenverkehrsfilterung und Reinigung des Datenverkehrs<br>• Neue Methoden für Mitigation von Attacken über 100 Gbit/s<br>• Programmierschnittstelle (API) für Integration mit den fremden Sicherheitssystemen | • Bildung und Entwicklung der neuronalen Netze für die genaue Gleichrichtung und Verhinderung von Attacken<br>• Vollautomatische Gleichrichtung und Verhinderung von Attacken |

# TECHNISCHER SUPPORT

- Kostenlose Upgrades nach dem globalen Programm der Kunden-Updates
- 24/7 oder 8/5 technischer Support
- Entwicklung von neuen Berichten auf den Anforderungen des Kunden – von 2 Wochen
- Integration mit den Monitoringssystemen– von einem Tag

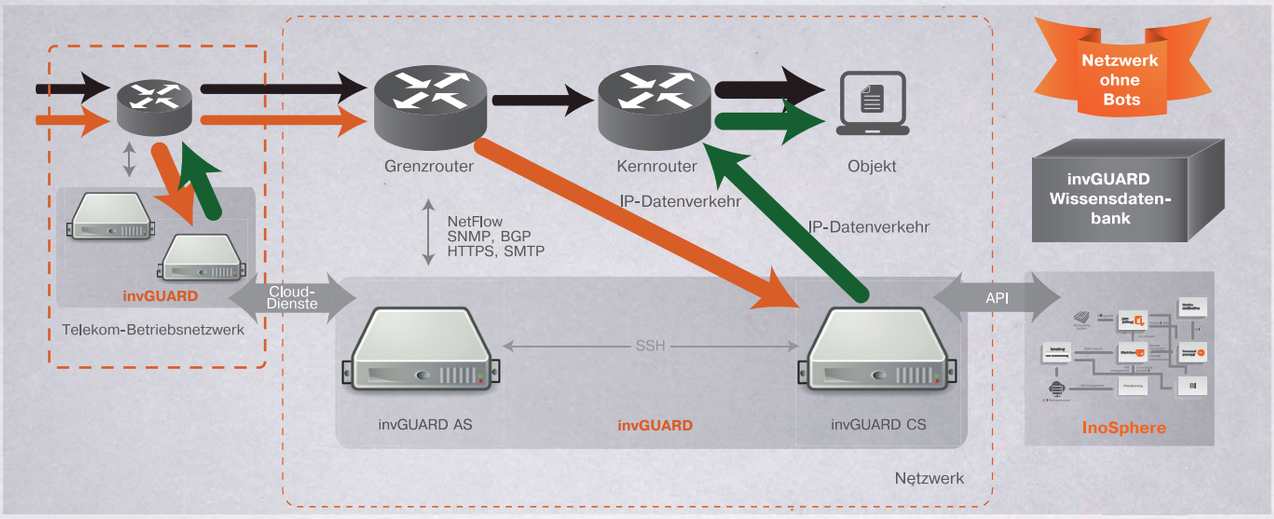
# SYSTEMEINFÜHRUNG

Die Systemeinführung für das typische Netzwerk dauert 2 Wochen: von 3 bis 5 Router, Datenverkehr im Netzwerk bis zum 100 Gbit/s.

Eine entfernte Systemeinführung oder eine Einführung beim Besteller sind auch möglich

Eine Ausbildung für Experten des Bestellers bei den invGUARD-Experten

## SYSTEM ARCHITEKTUR

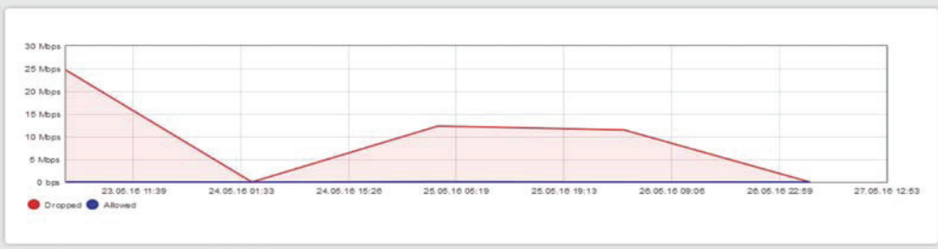



## ERKENNUNG VON DoS-ATTACKEN UND ANOMALIEN

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 521446 | | High<br>104.7% of 6 Gbps | 13.4 Gbps<br>1.27 Mpps | 16 min<br>(finished) | 28 July 2016<br>16:15:38 | Incoming | DoS attack<br>(Amount of traffic, bits per second) |
| 521445 | | High<br>83.4% of 700 Kpps | 13.39 Gbps<br>1.24 Mpps | 16 min<br>(finished) | 28 July 2016<br>16:15:37 | Incoming | DoS attack<br>(UDP flood) |
| 521451 | | Medium<br>85.0% of 361.82 Mbps | 668.48 Mbps<br>136.33 Kpps | 6 min<br>(finished) | 28 July 2016<br>16:16:36 | Incoming | DoS attack<br>(Excess traffic to profile) |
| 520928 | | Medium<br>83.8% of 78.6 Kpps | 1.07 Gbps<br>187.15 Kpps | 2 h 24 min<br>(finished) | 28 July 2016<br>13:34:35 | Incoming | DoS attack<br>(Excess traffic to profile) |
| 521161 | | High<br>3000.0% of 200 Kbps | 48 Mbps<br>4 Kpps | 18 min<br>(finished) | 28 July 2016<br>14:47:35 | Incoming | DoS attack<br>(Excess traffic to profile) |
| 521142 | | High<br>58.8% of 150 Kpps | 146.22 Mbps<br>281.15 Kpps | 17 min<br>(finished) | 28 July 2016<br>14:41:35 | Outgoing | DoS attack<br>(DNS) |
| 521110 | | Medium<br>88.8% of 10.88 Kpps | 55.67 Mbps<br>24.17 Kpps | 7 min<br>(finished) | 28 July 2016<br>14:31:35 | Incoming | DoS attack<br>(Excess traffic to profile) |

## REINIGUNG DES DATENVERKEHRS

| | |
|---|---|
| Name | |
| Task ID | 2 |
| Cleaner | Cleaner 1 |
| Prefixes | 143.35/32 |
| Start time | 27 May 2016 12:53:08 |
| Duration | min |
| Status | Stopped |




Traffic

| Period | Incoming | Allowed | Dropped | % Allowed |
|---|---|---|---|---|
| Last minute | 0 bps/0 pps | 0 bps/0 pps | 0 bps/0 pps | 0% |
| All time | 6.98 Mbps/7.93 Kpps | 4.04 Mbps/4.38 Kpps | 3.64 Mbps/5.02 Kpps | 58% |

Global exception list

| | Period | Allowed | % Allowed | Dropped | % Dropped |
|---|---|---|---|---|---|
| | Last minute | 0 bps/0 pps | 0% | 0 bps/0 pps | 0% |
| ⊞ | All time | 5.99 Mbps/6.87 Kpps | 86% | 987.65 Kbps/1.05 Kpps | 14% |

**inoventica.eu**

facebook.com/inoventica vk.com/inoventica twitter.com/inoventica instagram.com/inoventica