Wie DDoS-Schutz ihre Geschäftskontinuität sicherstellt

25. Oktober 2022

Agenda

- Was sind DDoS-Angriffe?
- Neue Arten von DDoS-Angriffen
- Wie kann man sich gegen DDoS-Angriffe schützen?
- Worauf ist bei der Auswahl einer Lösung zu achten?
- Live-Demo
- Fragen?

Was sind DDoS-Angriffe?

„Denial of Service“ und „Distributed Denial of Service“

Denial of Service (**DoS**; englisch für „Verweigerung des Dienstes“) bezeichnet in der Informationstechnik die Nichtverfügbarkeit eines Internetdienstes, der eigentlich verfügbar sein sollte. Häufigster Grund ist die Überlastung des Datennetzes. Das kann unbeabsichtigt verursacht werden oder durch einen konzertierten Angriff auf die Server oder sonstige Komponenten des Datennetzes erfolgen.

Aus „WIKIPEDIA“

Im Fall einer durch eine Vielzahl von gezielten Anfragen verursachten, mutwilligen Dienstblockade spricht man von einer *Denial-of-Service-Attacke* und, wenn die Anfragen von einer großen Zahl an Rechnern aus durchgeführt werden, von einer **Distributed-Denial-of-Service attack** (**DDoS-Angriff**, deutsch wörtlich *verteilter Dienstverweigerungsangriff*). Da beim DDoS-Angriff die Anfragen von einer Vielzahl von Quellen ausgehen, ist es nicht möglich, den Angreifer zu blockieren, ohne die Kommunikation mit dem Netzwerk komplett einzustellen.

DDoS-Angriffe in den Nachrichten – Heise Ticker

Angebliche Hacktivisten von russischem Geheimdienst gelenkt

Die Gruppen haben im Wesentlichen **DDoS**-Angriffe, Webseiten-Defacements und Einbrüche zum Datendiebstahl ausgeführt, erläutert Mandiant in der Analyse ....

27.09.2022 | heise Security

Cybersecurity-Spiel: Sich auf den Ernstfall vorbereiten

Die Zahl der Ransomware- und **DDoS**-Angriffe steigt stetig an und insbesondere kleinere Unternehmen und Organisationen sind häufig schlecht darauf vorbereitet....

01.07.2022 | iX Magazin

Markt + Trends | World Wide Web

Google hat nach eigenen Angaben den bisher größten Layer-7-**DDoS**-Angriff abgewehrt. Ein Botnetz schickte demnach in der Spitze 46 Millionen HTTPS-Anfragen pro Sekunde an einen Google-Cloud-Kunden....

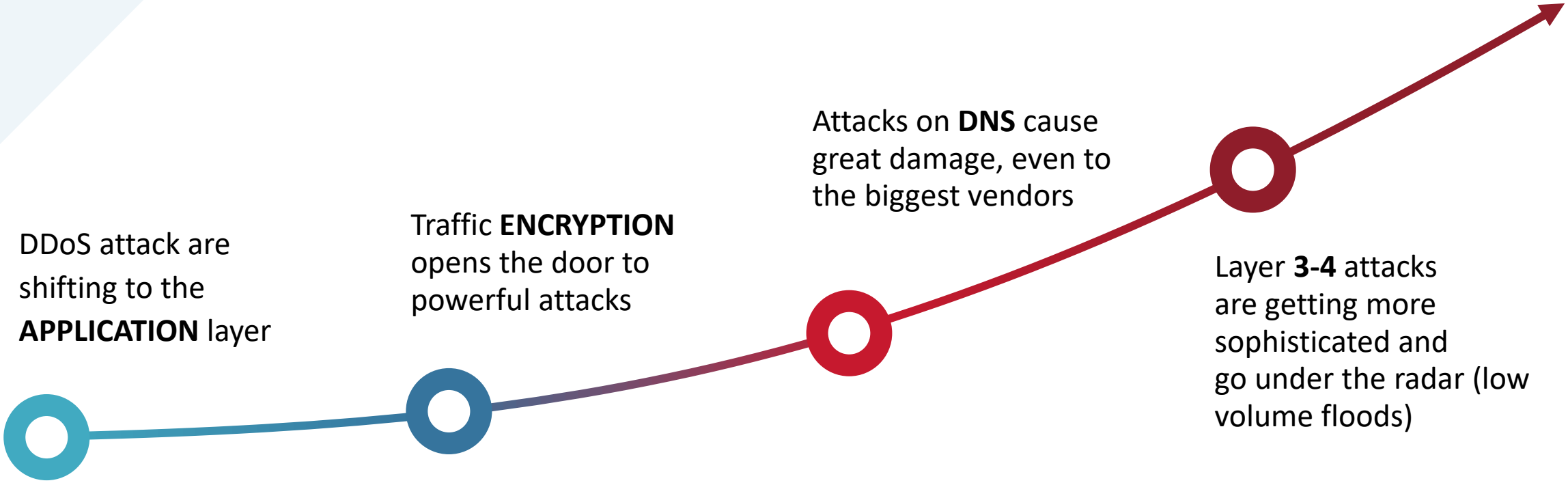
21.09.2022 | iX 10/2022, Seite 15

Ransomware: Nach Verschlüsseln kommt jetzt Kopieren & Zerstören

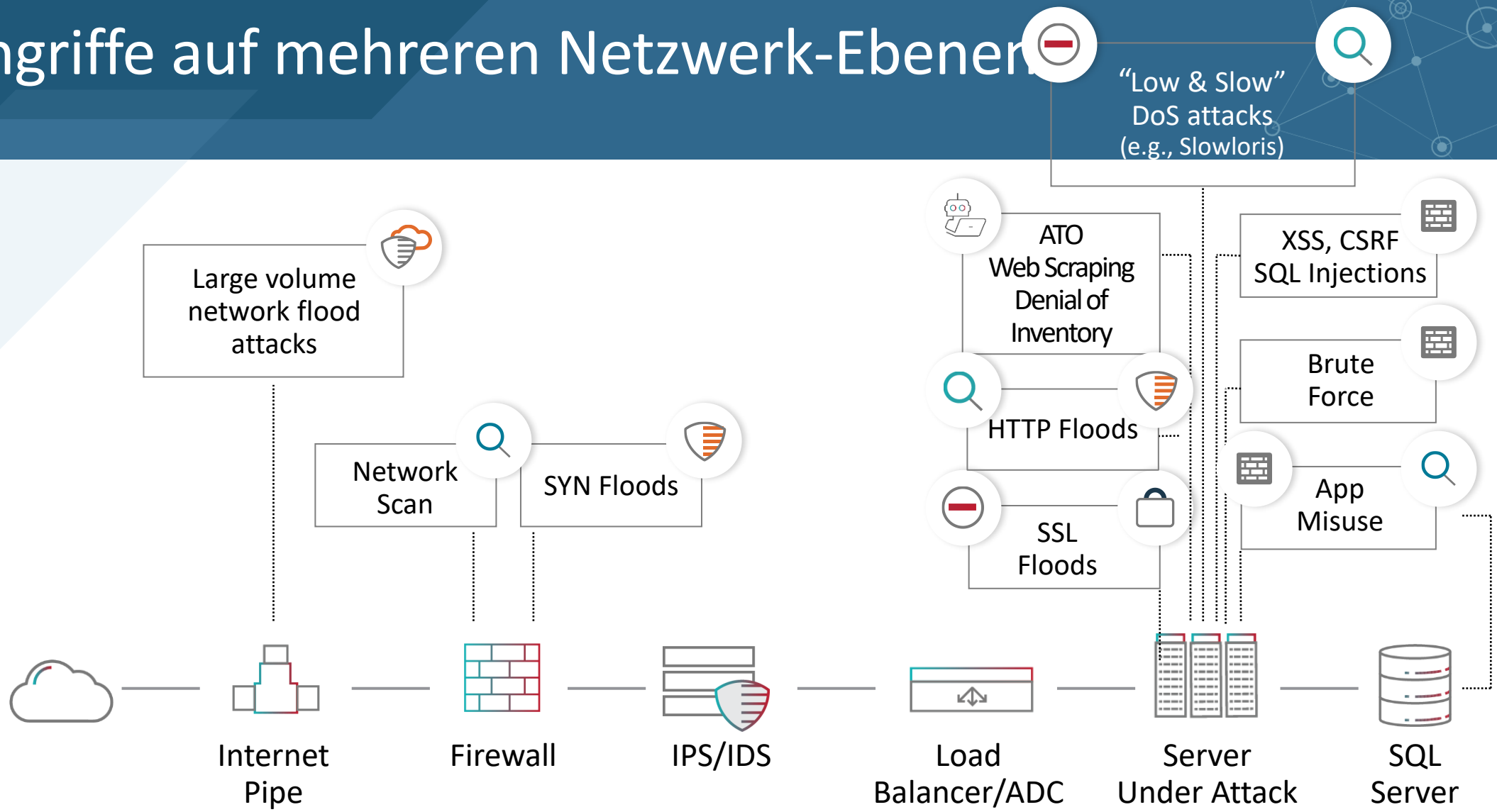
sich bei Cybercrime-Vorfällen die sogenannte Dreifach-Erpressung etabliert: Die Opfer zahlen für den Schlüssel, der ihre Daten wieder lesbar macht, für die Versicherung, dass interne Dokumente nicht veröffentlicht werden – und wenn das nicht reicht, hagelt es **DDoS**-Angriffe...

26.09.2022 | heise Security

Trends bei DDoS-Angriffen



Angriffe auf mehreren Netzwerk-Ebenen



Cloud DDoS Protection | DoS protection | Behavioral analysis | IPS | SSL protection | WAF | Anti-Bot

Ansteigender Trend bei DDoS Angriffen

Blocked Malicious Events

+203%

H1 YoY

Number of Events Blocked Monthly

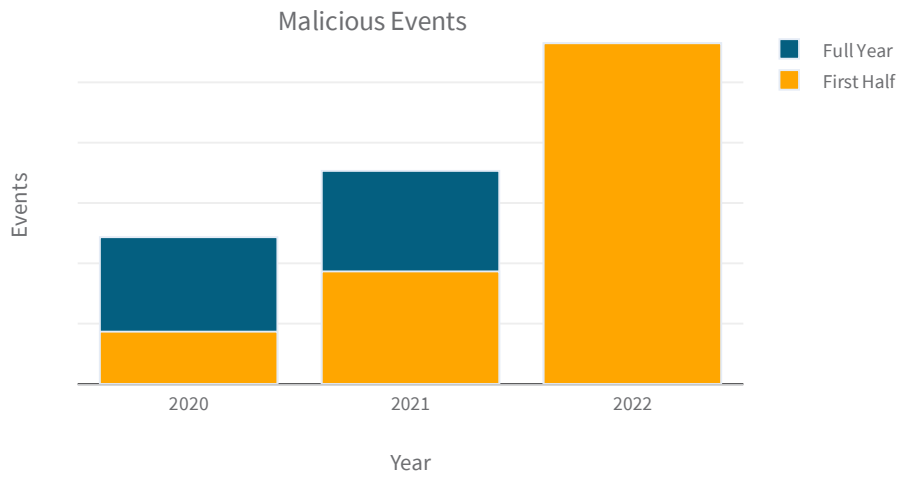
X2.5

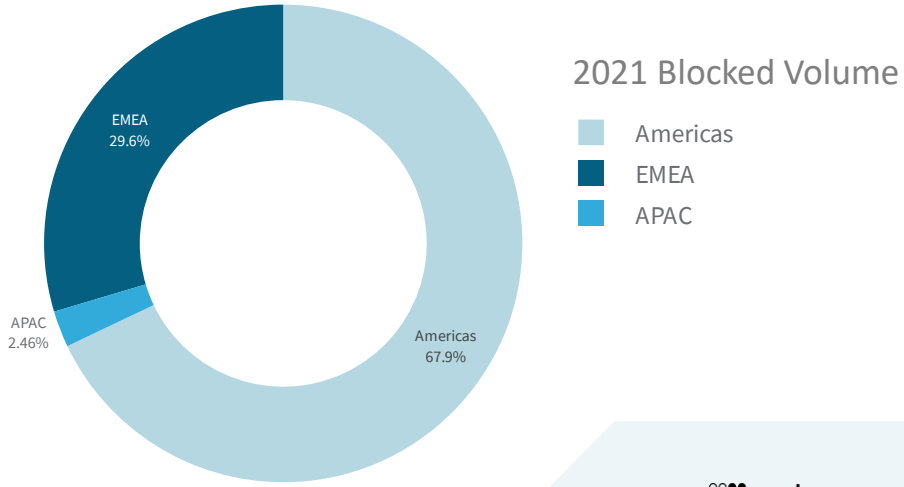
H1 YoY

Average volume Blocked Monthly

3.39TB

H1 2022



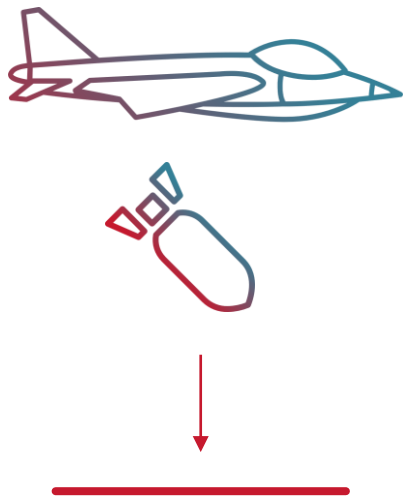


** Per customer*

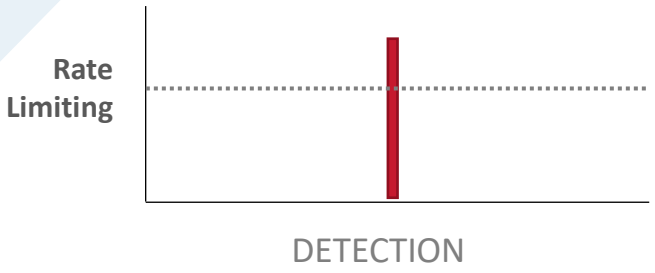
Neue Arten von DDoS-Angriffen

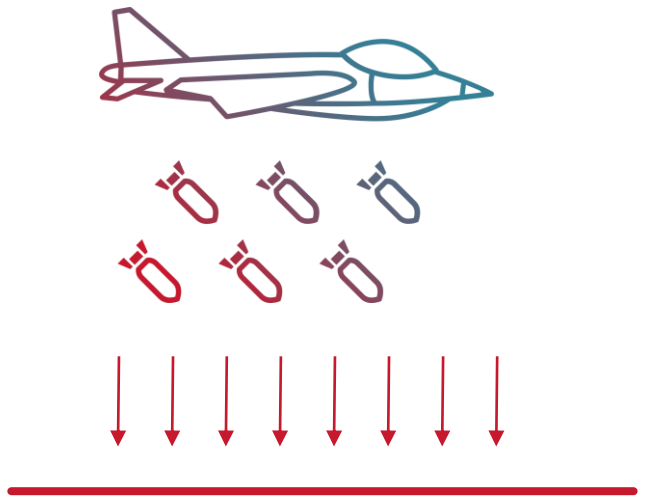
‘Carpet-Bombing’ Evasion Technique

Detection systems usually focus on destination IPS, not subnets or CIDR blocks, often resulting in the attack not being detected until too late

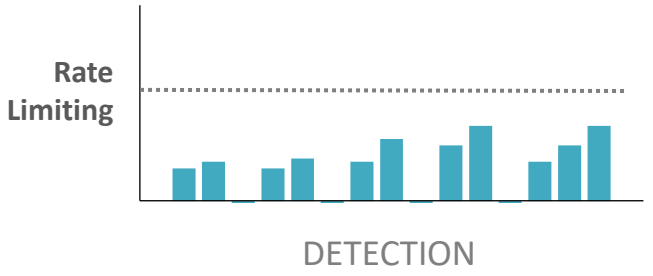


VICTIM IP





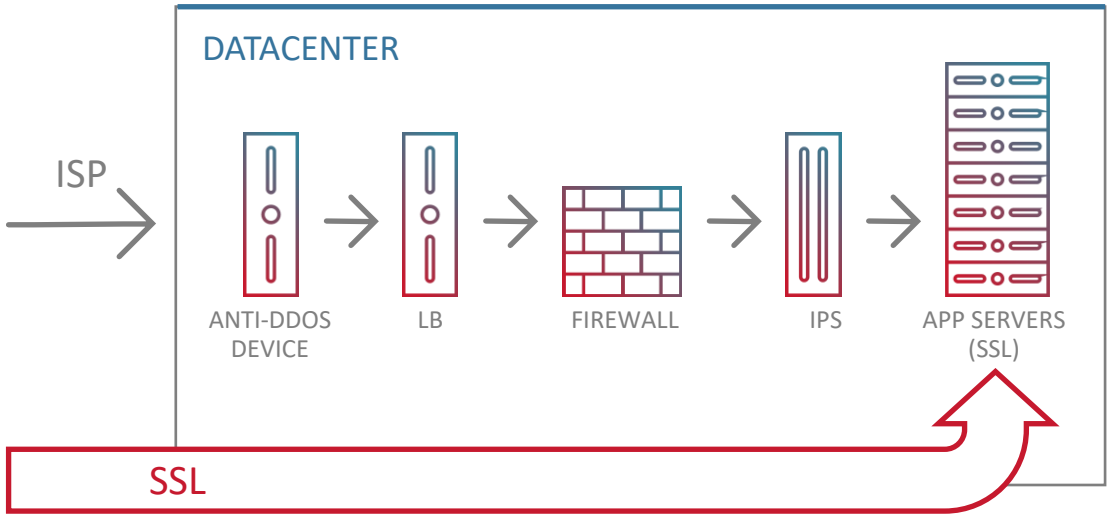
VICTIM CIDR



Verschlüsselte DDoS Angriffe

Zunehmender SSL-Verkehr bietet eine gute Gelegenheit für Angreifer

Angriffe auf die Applikations-Ebene über HTTPS sind mit herkömmlichen Mitteln schwer zu erkennen und abzuwehren.



Burst-Angriffe:

Burst-Angriffe schicken hohe Datenvolumen über eine sehr kurze Zeit.

Sie stellen eine Herausforderung bei Erkennung und Mitigation dar

High-volume Attack Bursts

~15 SEC TO 1 MIN

Random Intervals Between Bursts

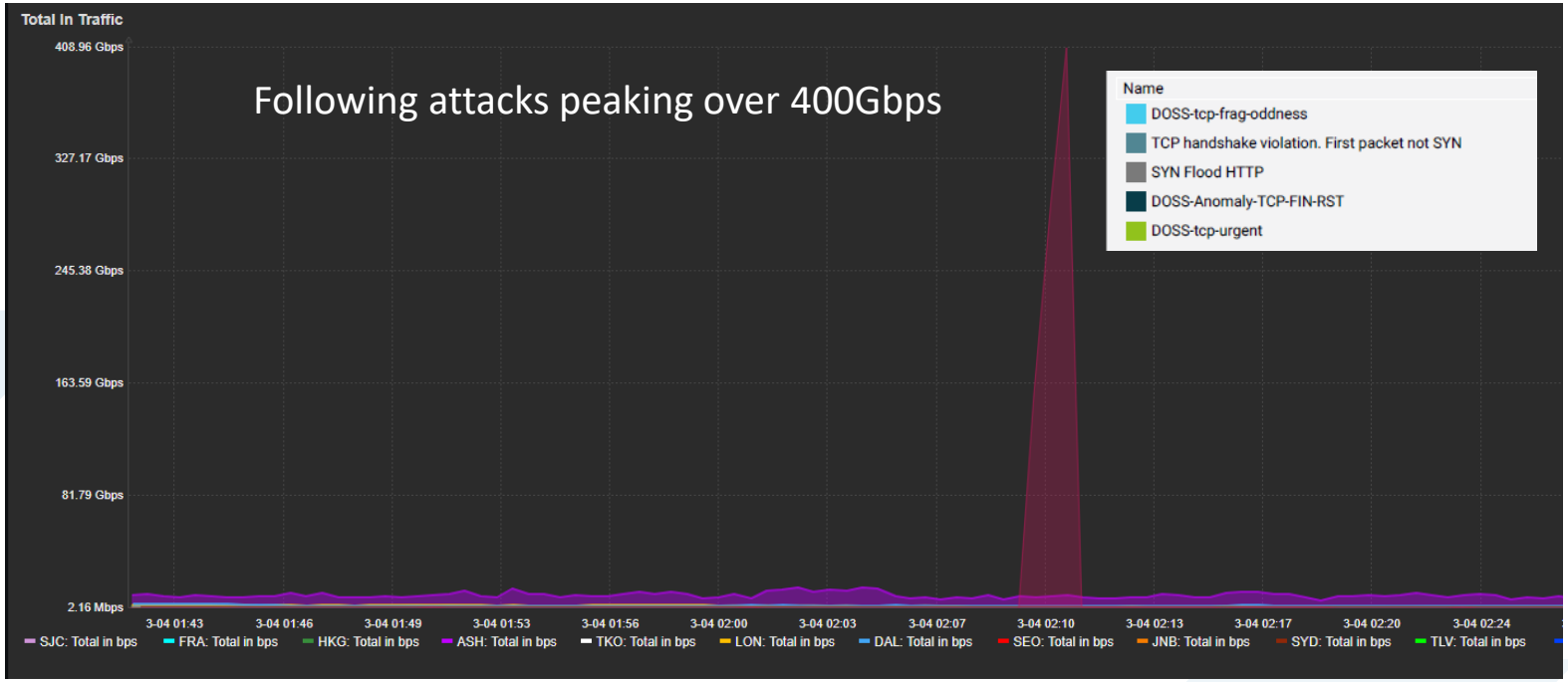
~ SECONDS TO MINUTES

Usually changing attack vectors

AND GEOGRAPHICALLY DISTRIBUTED

Angriffsbeispiel: Europäische Regierung

Februar, 2022



Angriffsbeispiel: Europäische Regierung

Februar, 2022

Full list of attack vectors:

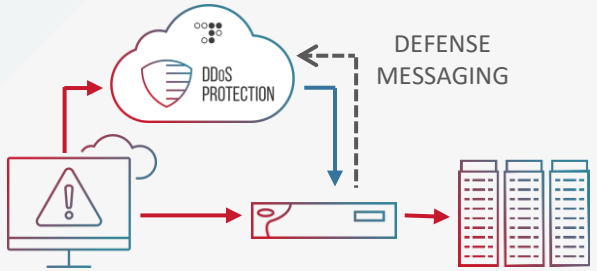
DOSS-UDP-flood-80-Req
HTTP-MISC-DosTool-ExAttack
ICMP-BlackNurse-Attack
Log4-p33-ert
Log4-p44-ert
Log4-p77-ert
Log4-p88-ert
network flood IPv4 ICMP
network flood IPv4 TCP-RST
network flood IPv4 TCP-SYN
network flood IPv4 UDP
network flood IPv4 UDP-FRAG
SYN Flood HTTP
SYN Flood HTTPS
TCP handshake violation. First packet not SYN
Routers ACLs

BO-Apache-HTTPD-log-Cookie
CPS - 665_CON_HTTP
CPS - 665_CON_HTTPS
DDOS-Mirai-GENUDP-flood
DDoS-UDP-MEMCACHED-AMP
DOS-LOIC-TCP-80-dun
DOS-LOIC-UDP-80-cat
DOS-LOIC-UDP-80-dun
DOSS-Anomaly-TCP-FIN-RST
DOSS-NTP-reflected-monlist
DOSS-NULL-UDP
DOSS-SSL-ClearText
DOSS-tcp-ack-zero-ack-num
DOSS-tcp-frag-oddness
DOSS-tcp-urgent
DOSS-tcp-zero-seq

Wie kann man sich gegen DDoS-Angriffe schützen?

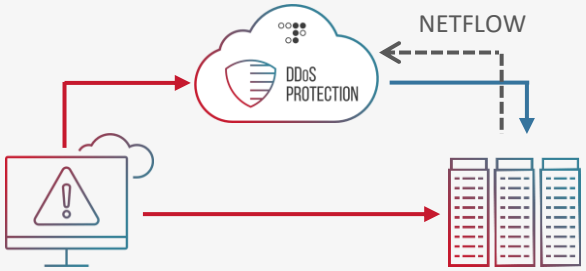
Dedizierte Schutzmodelle für unterschiedliche Zielgruppen

Hybrid



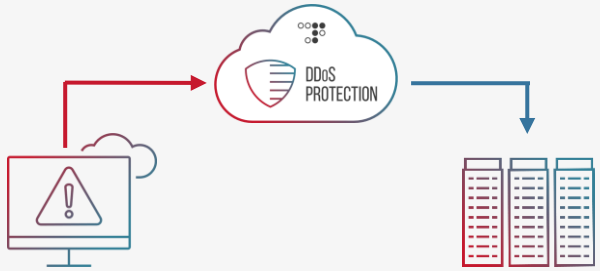
- Kombination aus lokalem Schutz und einer Cloud-Komponente
- Schnelle Erkennung und Mitigation von Angriffen durch die locale Appliance
- Einfache Möglichkeit Verschlüsselten Traffic zu untersuchen
- Wenn ein Angriff für die Internet-Anbindung zu gross wird, erfolgt eine automatische Umleitung in die Cloud

On-demand



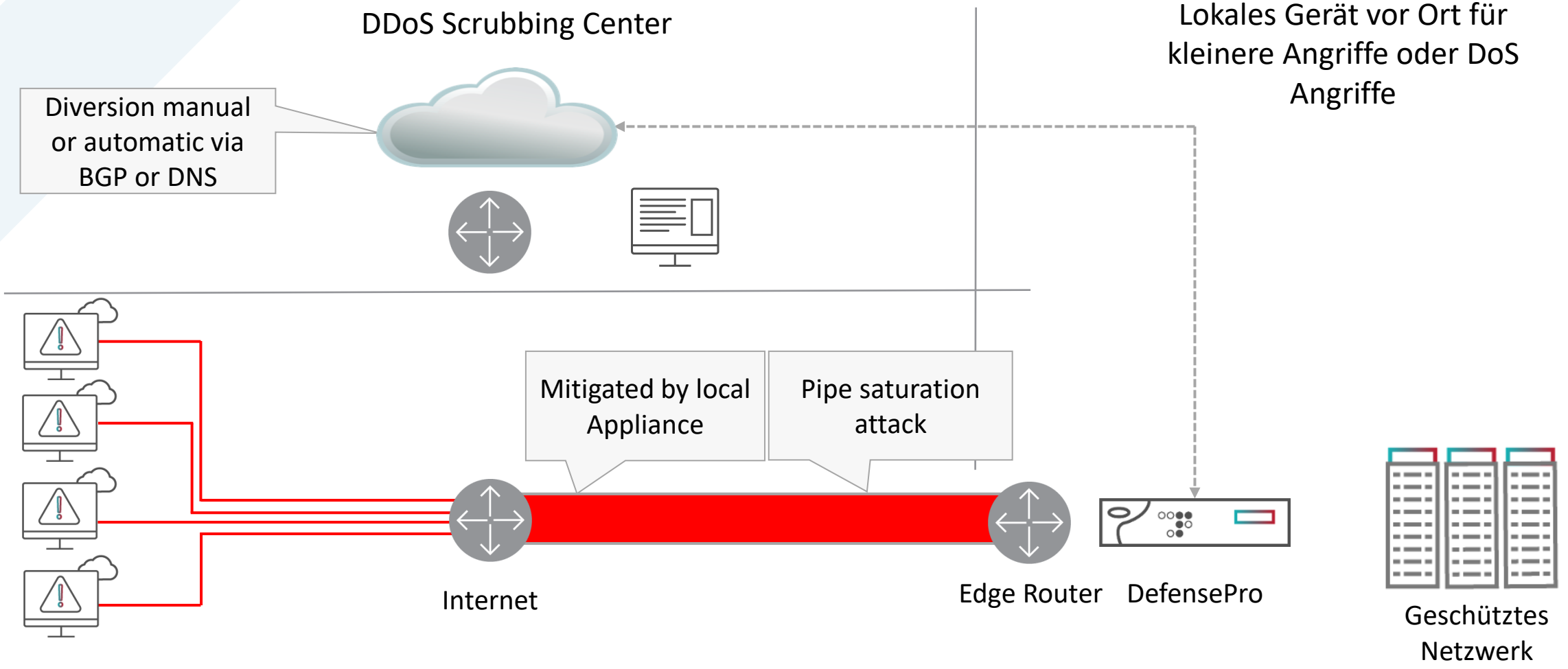
- Keine lokale Komponente, im Normalfall wird der Traffic auch nicht durch die Cloud umgeleitet
- Erkennung eines Angriffs durch Analyse von Netflow-Daten
- Eignet sich besser zur Erkennung von volumetrischen Angriffen
- Bei einem Angriff wird der Traffic in das nächste Scrubbing Center Umgeleitet
- BGP wird bei diesem Scenario empfohlen

Always-on

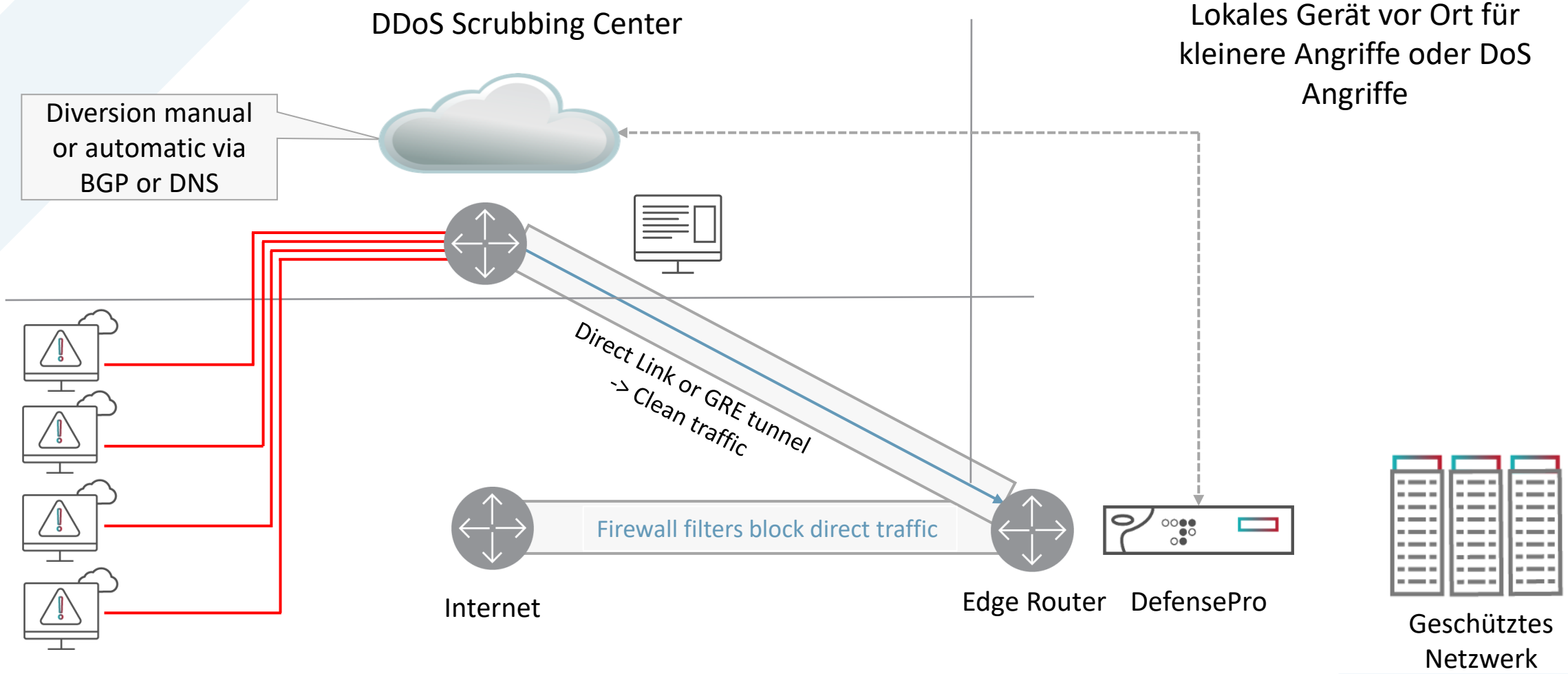


- Der Traffic wird immer durch ein Scrubbing-Center geleitet
- Sofortige Erkennung von Angriffen durch das Scrubbing-Center
- Benötigt wenig Betreuung durch das lokale Team
- Guter Ansatz wenn der Kunde kein eigenes ASN hat und der Traffic über DNS umgeleitet wird

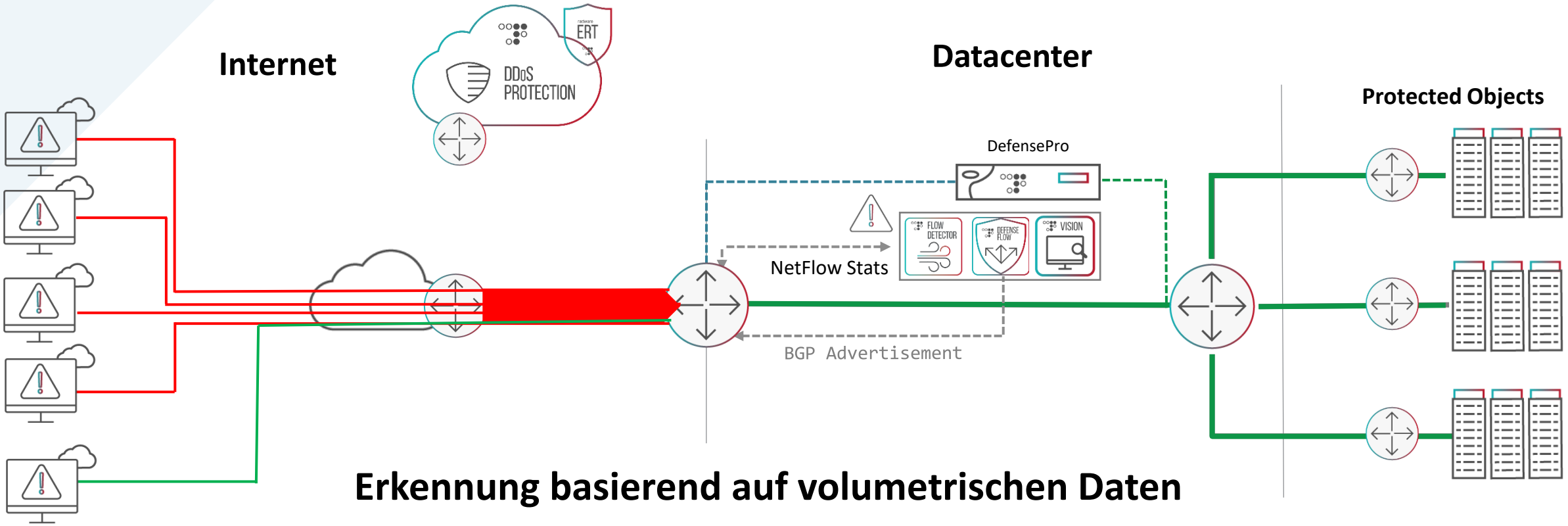
Demo Scenario: Hybrid DDoS Mitigation (1/2)



Demo Scenario: Hybrid DDoS Mitigation (2/2)

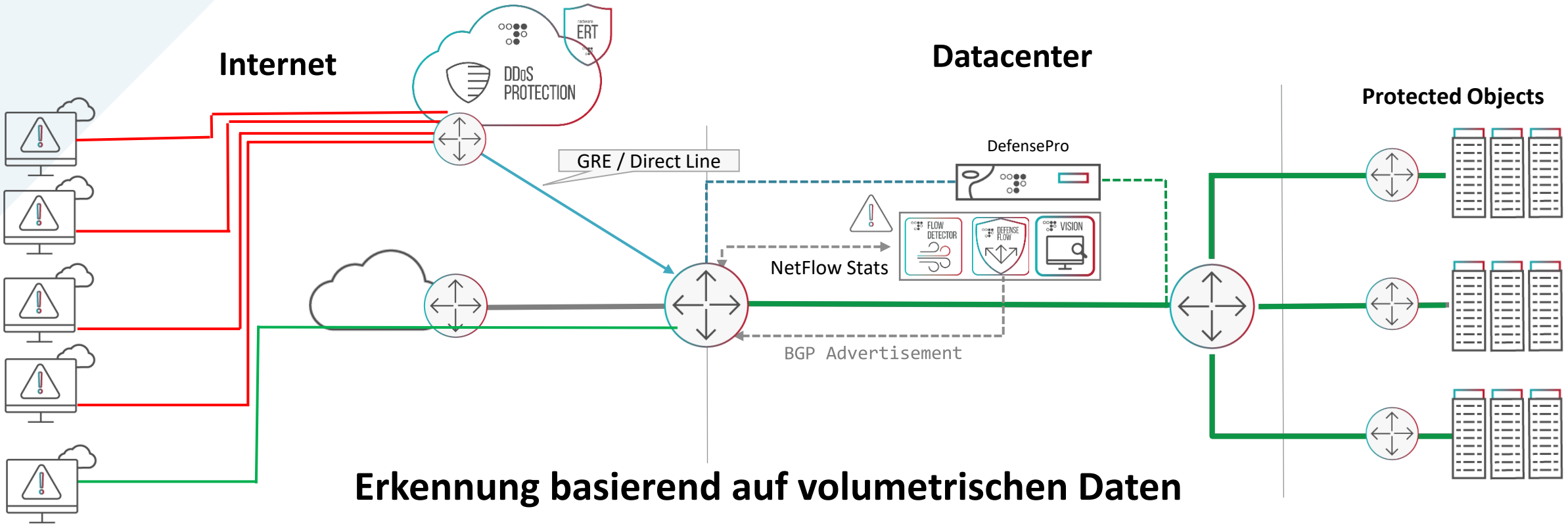


DDoS-Schutz für Service Provider



Erkennung basierend auf volumetrischen Daten

DDoS-Schutz für Service Provider

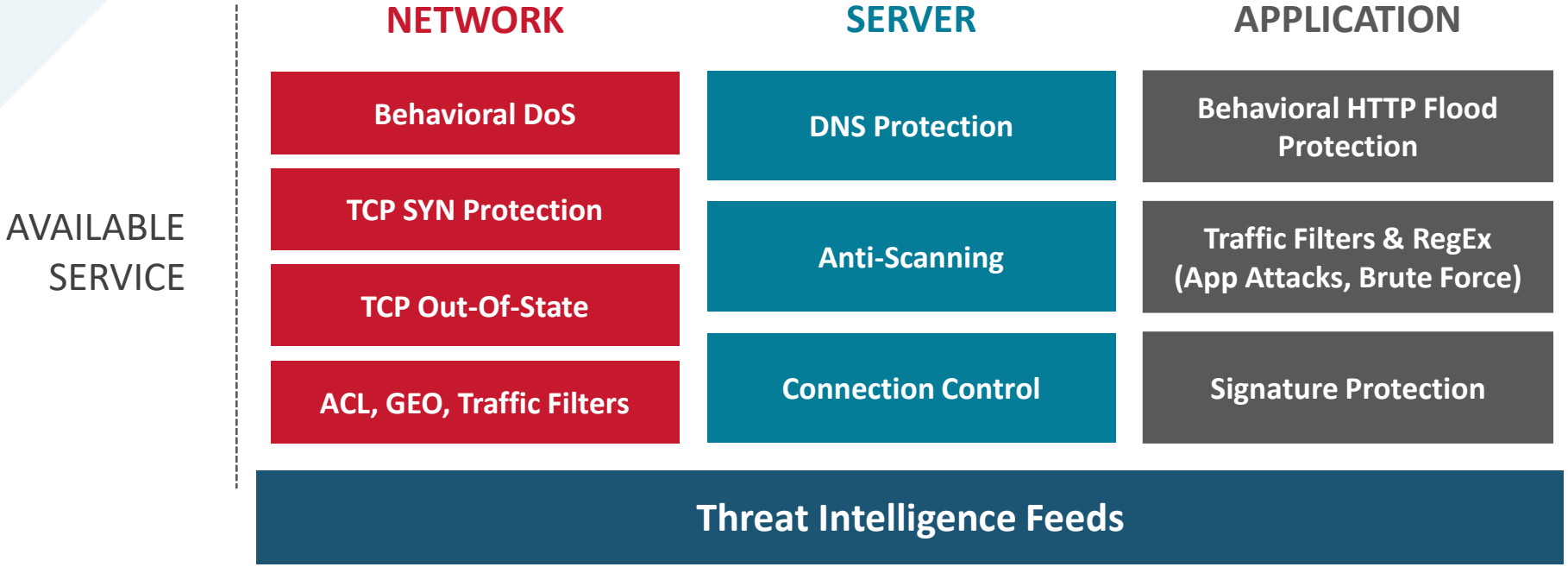


Erkennung basierend auf volumetrischen Daten

- Günstiger Ansatz basierend auf “Out-of-Path” Methode
- Erkennung von volumetrischen Angriffen basierend auf Netflow Daten
- Niedrig-volumige Angriffe können erst nach Umleitung erkannt werden

Worauf ist bei der Auswahl einer Lösung zu achten?

Unterschiedliche Schutz-Module für die einzelnen Arten von Angriffen



Welche Service Level Agreements stellt der Anbieter zur Verfügung?

TIME TO DETECT

TIME TO ALERT

TIME TO DIVERSION

TIME TO MITIGATE

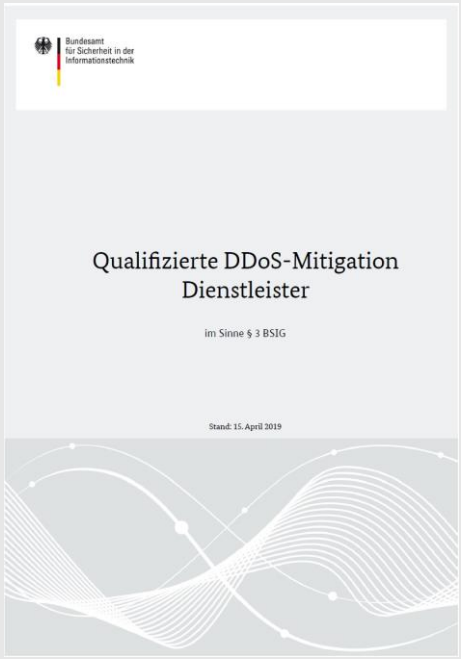
CONSISTENCY OF MITIGATION

SERVICE AVAILABILITY

Welche Standards werden unterstützt?

ISO 27001	Information Security Management Systems
ISO 27002	Information technology — Security techniques — Code of practice for security controls
ISO 27032	Security Techniques -- Guidelines for Cybersecurity
ISO 27017	Information Security for Cloud Services
ISO 27018	Information Security Protection of Personally identifiable information (PII) in public clouds
ISO 28000	Specification for Security Management Systems for the Supply Chain
EU GDPR	EU General Data Protection Regulation
PCI-DSS	Payment Card Industry Data Security Standard
HIPAA	Health Insurance Portability and Accountability Act
US SSAE16	SOC-1 Type II, SOC-2 Type II

Liste qualifizierter Anbieter vom BSI



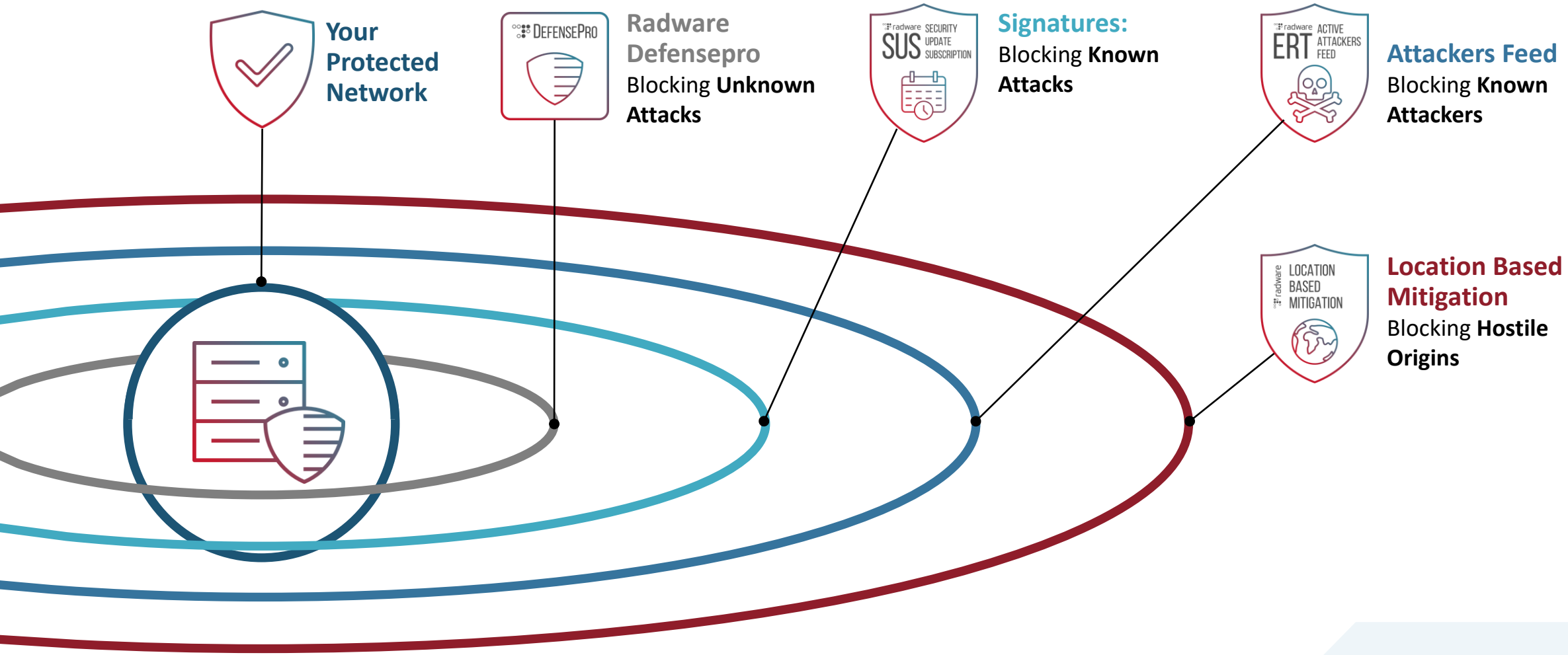
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation-Liste.html

Wie geht man mit verschlüsseltem Traffic um?

Welche Optionen gibt es für verschlüsselten Traffic?

- **Keyless SSL Protection**
- **First Request SSL Protection**
- **Selective Full SSL Protection**
- **Full SSL Protection**

Gibt es Signaturen und/oder ein Security-Feed?

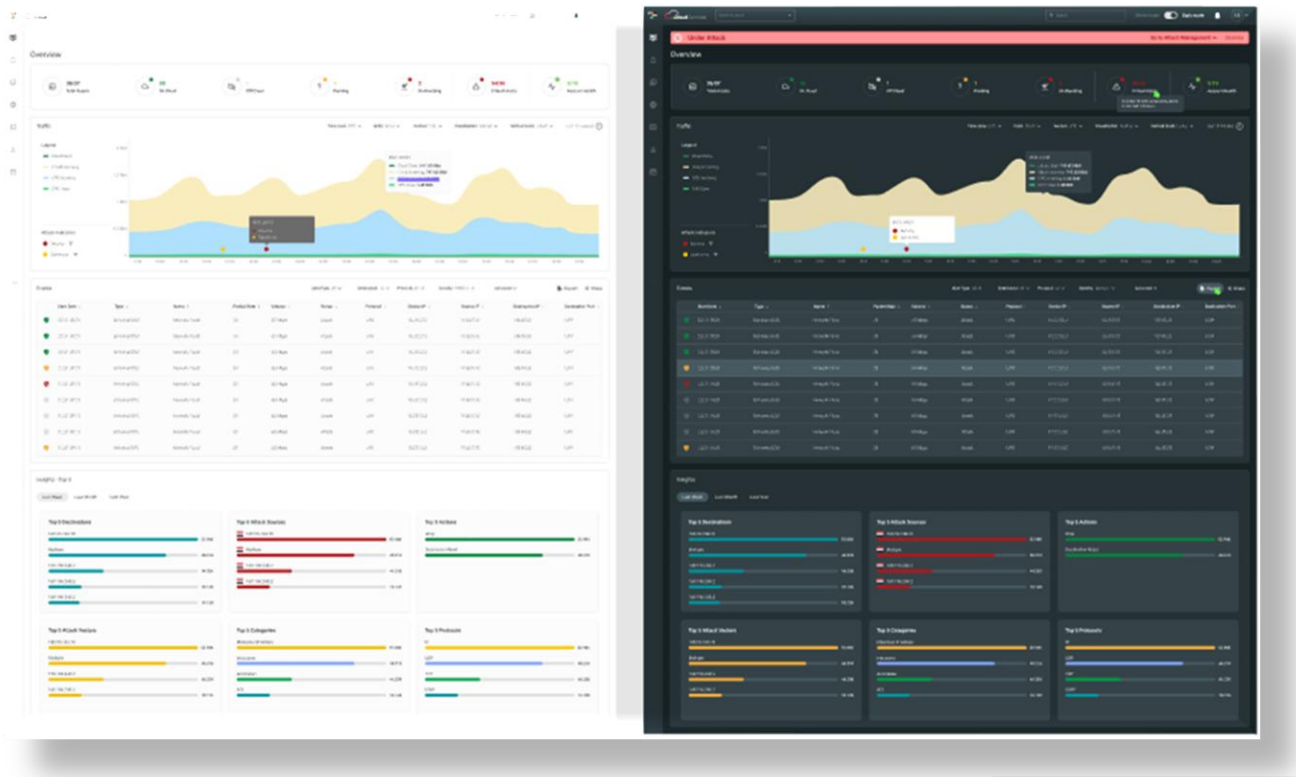


Bei globalen Organisationen: Weltweit verteilte Scrubbing Center

Wichtig für Behörden:
Gibt es die Option den Cloud-Schutz nur in Deutschland zu halten?

Cloud DDoS Management System - Demonstration

- **Attack Centric**
  - In case of an Attack – related info is consolidated
- **Prompt response time**
- **Visibility**
  - Traffic details
  - Context sensitive reporting
  - Advanced analytics
  - Peacetime information
- **Control**
  - Self provisioning
- **Peacetime**
  - Traffic Monitoring
- **Intuitive GUI**



Live Demo

radware

Fragen?

Kontakt

Radware GmbH
Robert-Bosch-Str. 11a
63225 Langen

Tel: +49-6103-70657-0
Fax: +49-6103-70657-66
Email: info_de@radware.com


radware
Thank You!