27.10.2016 – *“Schwiiz under Agriff”*

Lösungsansätze – systematische Eingrenzung von Sicherheitslücken und Gefahrenpotenzialen

- Michele Rapisarda, Channel Manager Radware Schweiz

IT-Sicherheit in Liechtenstein

Michele Rapisarda – Channel Manager Schweiz
micheler@radware.com

Über Radware

Marktführer in Application Availability Lösungen

Best Managed Security Service 2016

>$200M Umsatz

Über 10,000 Enterprise & Carrier Kunden

Bloomberg, ebay, at&t, verizon, orange, Telecom Italia, 中国银行 Bank of China, LG, DTCC, VeriSign, BNP Paribas, vodafone, Hilton

Globale Technology Partner

Check Point, Alcatel·Lucent, hp, IBM, Ericsson, NEC, Microsoft, Juniper Networks, OpenDaylight, Nokia Siemens Networks, Oracle, redhat, TATA, vmware, OpenFlow, Cisco, SAP

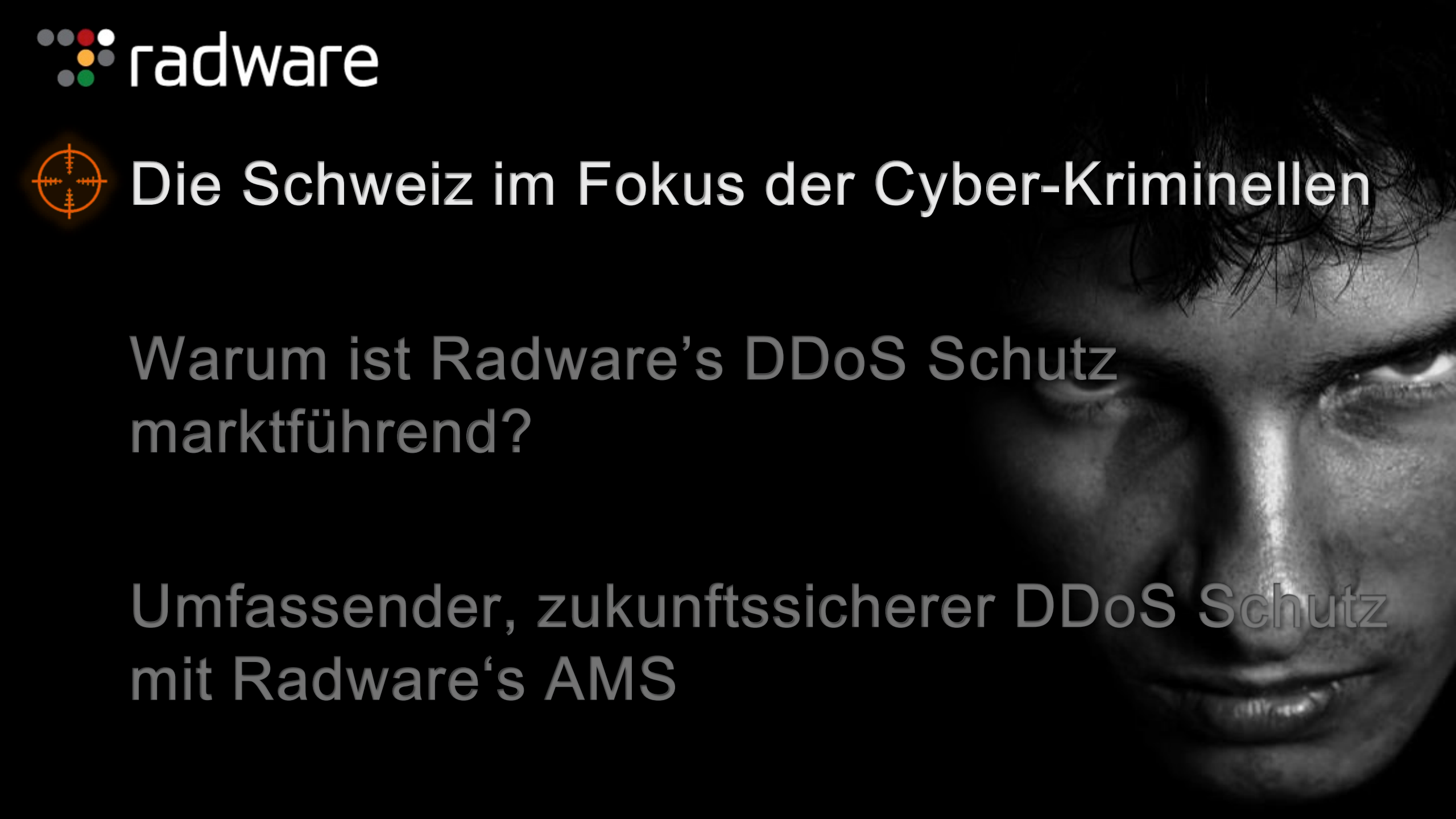
Radware (the hidden champions) in a nutshell

- 1050 Angestellte, 44 Niederlassungen weltweit (25 Mitarbeiter in DACH)
- Wir sind seit fast 20 Jahren Unternehmer-geführt am Markt (1997 durch die Familie Zisapel gegründet, Roy Zisapel nach wie vor CEO von Radware und Entwickler unseres ersten Loadbalancer)
- Einziger Anti-DDoS Hersteller welcher eine komplette Lösung gegen jegliche DDoS-Angriffe (nicht nur volumetrisch) anbietet und alles aus einer Hand herstellt und supportet (Hardware, Software, 7x24 Support, Updates, Cloud&Scrubbing)

  kein Dritthersteller involviert – wir supporten unsere Lösungen von A-Z
- Wir entwickeln und supporten all unsere DDoS-Produkte selbst (mit zahlreichen Patenten) und OEM-lizensieren diese an namhafte Hersteller (Check Point, Cisco)

radware

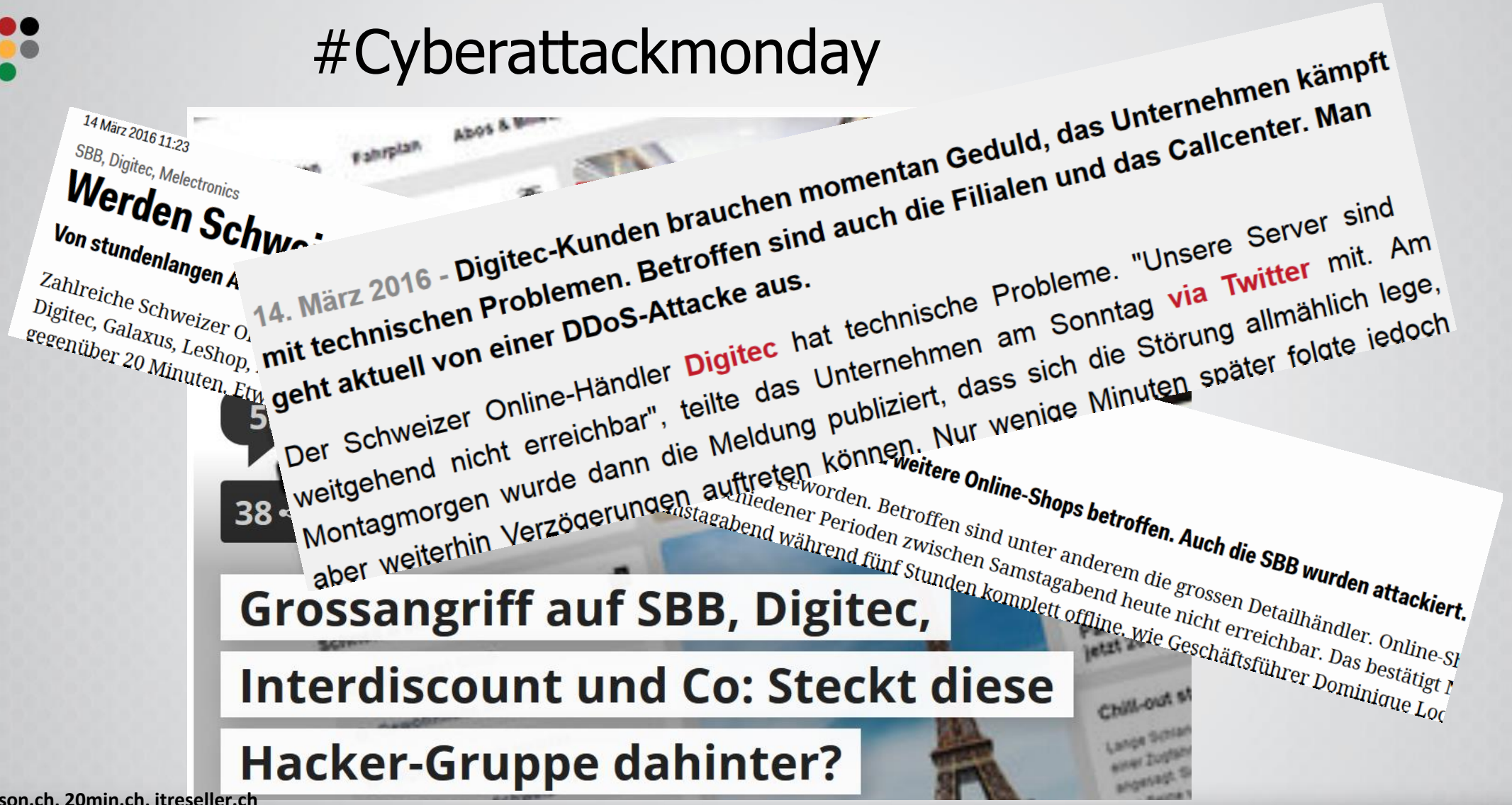
Die Schweiz im Fokus der Cyber-Kriminellen



Warum ist Radware's DDoS Schutz marktführend?

Umfassender, zukunftssicherer DDoS Schutz mit Radware's AMS

#Cyberattackmonday



Source: Watson.ch, 20min.ch, itreseller.ch

#Cyberattackmonday

- Die Attacken dauerten zum Teil die ganze Woche:
  - Digitec.ch
  - Fust.ch
  - Microspot.ch
  - Interdiscount.ch
  - Denner.ch
  - Leshop.ch
  - Coop.ch
  - Galaxus.com
  - SBB.ch
  - Brack.ch

Source: Watson.ch, 20min.ch, itreseller.ch

Es ist korrekt, dass unser Webshop am Montagnachmittag wiederholt nicht funktionierte», sagt Interdiscount-Mediensprecherin Nadine Käser auf Anfrage. Man gehe aktuell davon aus, dass es sich beim Angriff um eine DDoS-Attacke («Distributed Denial of Service», «Dienstblockade») handle.

Wir können bestätigen, dass die Kundendaten sicher und nicht betroffen sind», so Käser. Auch bei Microspot seien die Kundendaten nicht gefährdet, sagt Microspot-Leiter Markus Kwincz sagt. Man arbeite mit Hochdruck an einer Lösung des Problems.

Shenron Attack Tool

- Lizard Squads öffentliche stresser services
- 19,99$ => 15GB Angriff für 1200 Sekunden
  - DNS
  - SNMP

Lizard Squad hacked thousands of cameras to attack websites

The infamous outfit made a botnet out of connected devices to flood banks and governments.

Jon Fingas , @jonfingas
07.03.16 in Security

11 Comments

1234 Shares

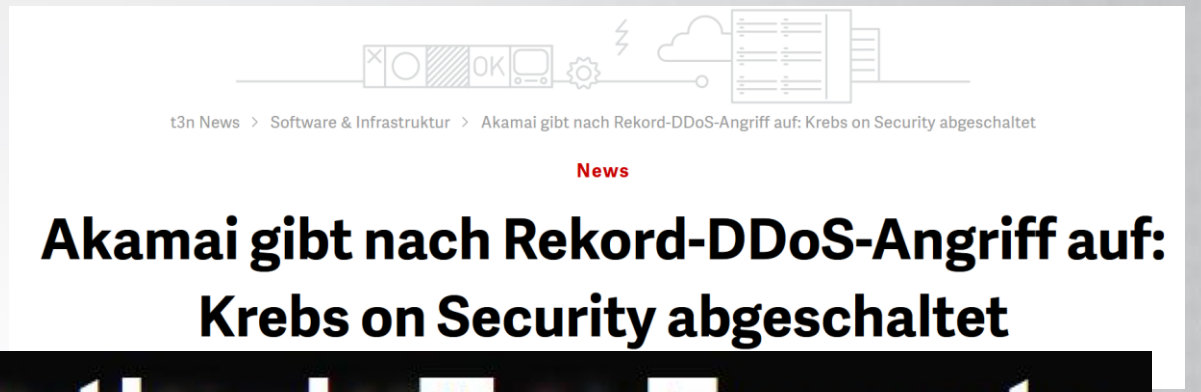
Getty Images/iStockphoto

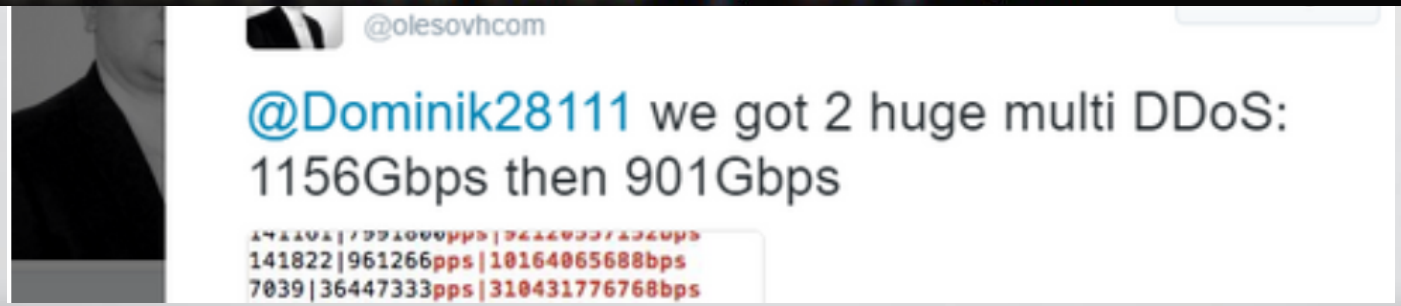
The hacking collective Lizard Squad isn't relying solely on masses of compromised PCs to cause some grief online. Security researchers at Arbor

radware

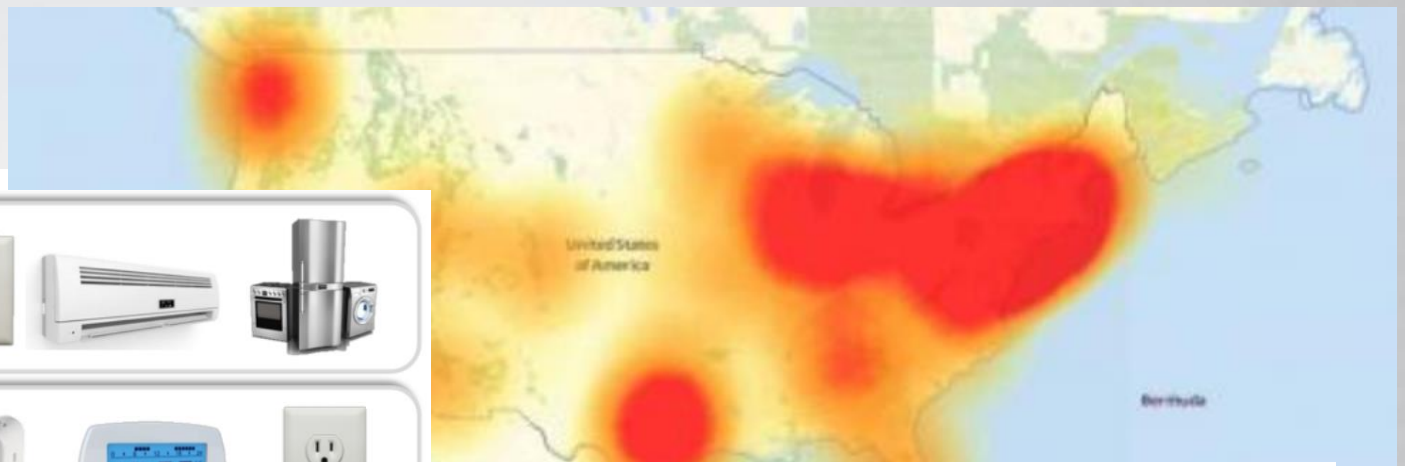
Die Angriffe werden immer grösser und raffinierter…

- Angriffe übersteigen Terabitgrenze
- IoT-Geräte werden
-





#dynattack 24.10.2016



The Pearl Harbor of Internet Attacks happened on Friday. The end of the internet may be near...

Published on October 24, 2016 | Featured in: Information Privacy & Security , Technology

Source: radware.com, blick.ch, theiotlearninginitiative.com, identityweek.com

radware

Die Schweiz im Fokus der Cyber-Kriminellen

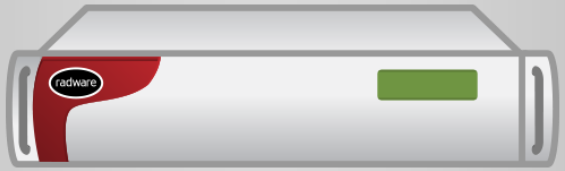
Warum ist Radware’s DDoS Schutz marktführend?

Umfassender, zukunftssicherer DDoS Schutz mit Radware‘s AMS

Unsere Lösungen

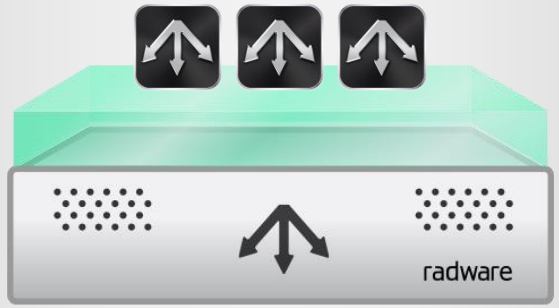
Security

AMS
Attack Mitigation Solution



- Führende hybride Angriffs-Mitigations-Lösung
- Führende Detektion und akkurate Mitigation
- Kürzeste time to protect
- 7x24 Emergency Response Team (ERT)

Next Generation
Application Delivery
(Uebernahme Nortel Alteons 2009)



Garantierte Resscouren per Applikation via vADC (Virtualisierung)
Patentierte Applikations-Beschleunigung (FastView)
Integriertes service-level monitoring
Integrierte Applikations-Security

Application Delivery

Von Grund auf **von uns** entwickelt um  den **Applikations Service-Level** immer aufrecht zu halten

(offizielle) weltweite Referenzen

8 der Top 12 Börsen

12 der Top 25 Banken

BB&T · ADP · Deutsche Bank · Bloomberg · ING · DTCC · WELLS FARGO · E*TRADE · NYSE

Führende Online Businesses

Top Retailers & Travel

Shopping.com · Papa Johns · HSN · PayPal · GROUPON · Hanes · boku · GAP · twitter · DELTA · ebay · STAPLES

5 der Top 10 Carriers

3 der Top 7 Cloud Service Providers

Telefónica · Telecom Italia · vodafone · SUNGARD · SOFTLAYER · EarthLink · CISCO · salesforce · at&t · verizon · Akamai · SAP · Atos

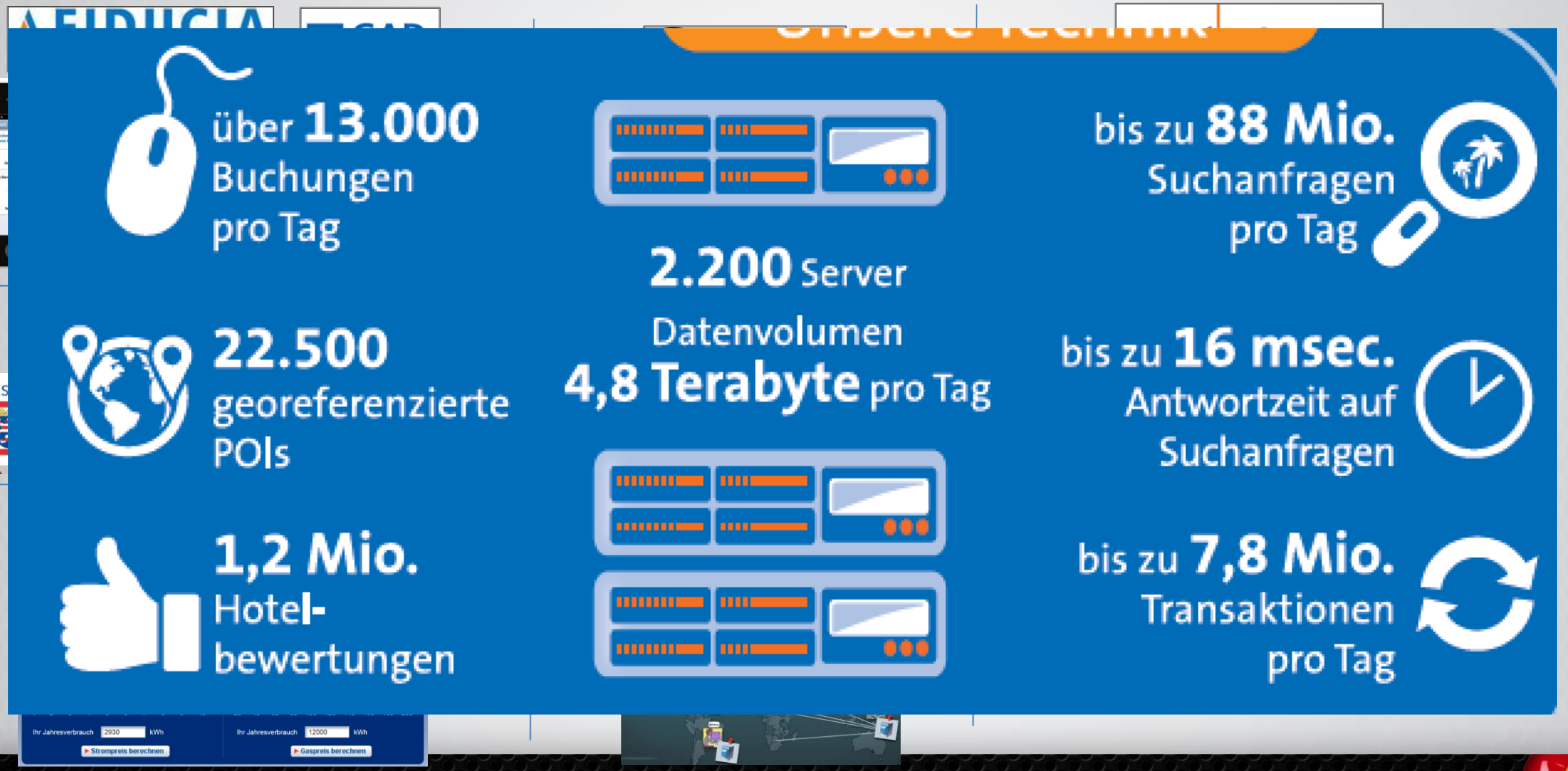
Top Organisationen nutzen Radware Security Services

Borgata Hotel Casino & Spa · asianbge · servercentral · ING · Level 3 Communications · ups · coles · Availity · ESL · DriveWealth · HKEx 香港交易所 · The Limelight Group · Playtika · MoneyGram · Barnabas Health

Check Point Software Technologies Ltd. · CISCO

Ausgewählter OEM partner für Cisco Firepower NGFW und Checkpoint NGFW

(offizielle) deutsche Referenzen



(offizielle) Referenz Schweiz

ProtonMail

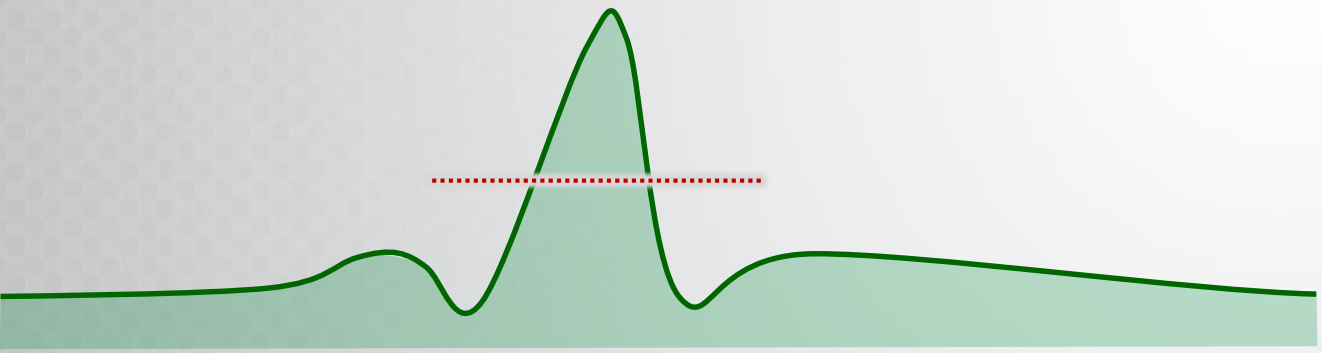
Secure Email Based in Switzerland

ProtonMail Chooses Radware Attack Mitigation System to Successfully Mitigate Multiple Advanced Persistent DDoS Attacks

Verhaltensbasierte vs. ratebasierte Erkennung

Non-Radware

Rate-basierte Erkennung



Radware

Verhaltens-basierte Erkennung

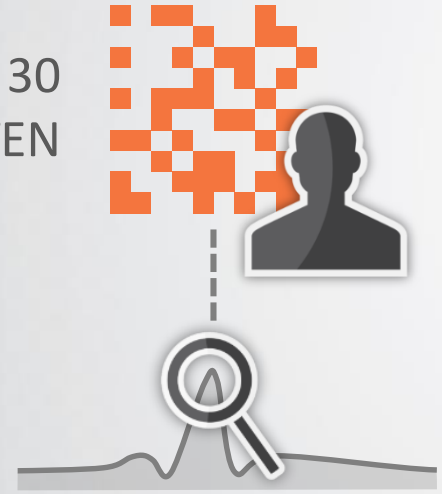
Um SLA-Beeinflussung des legitimen Verkehrs zu vermeiden

Echtzeit Signatur Erstellung vs. Manuell

Non-Radware

Manuelle Signatur Erstellung

30
MINUTEN



Radware

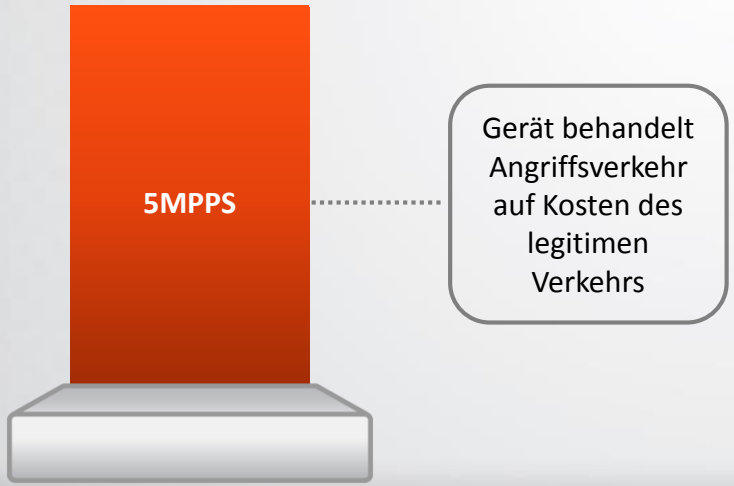
Echtzeit Signatur Erstellung

18
SEKUNDEN

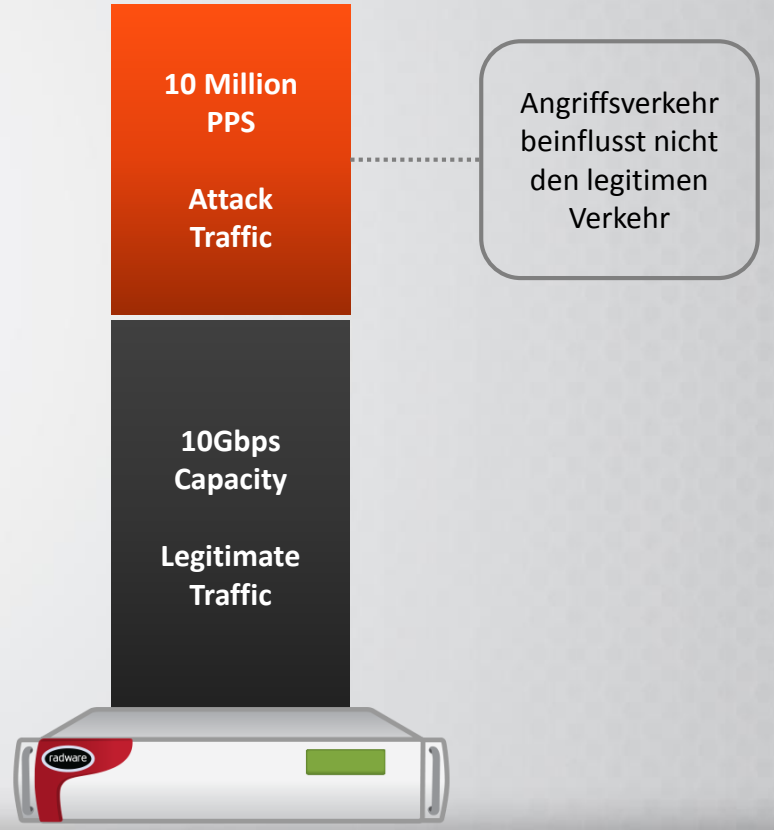
Manuelle Signatur Erstellung benötigt bis zu **30 Minuten.**
Die Radware Echtzeit Signatur benötigt nur **bis zu 18 Sekunden.**

Dedizierte Hardware um gegen Angriffe vorzugehen

Non-Radware



Radware



Wir gehen über primitives Source IP blockieren hinaus

Non-Radware

Nur Source IP Addresse

X.X.X.X

Radware

Signatur mit multiplen Parametern

Smart traffic blocking basiert auf Echtzeit Signaturen welche **multiple Parameters** inkludieren im Vergleich zu primitiven source IP address blocking

radware

Die Schweiz im Fokus der Cyber-Kriminellen

Warum ist Radware’s DDoS Schutz marktführend?

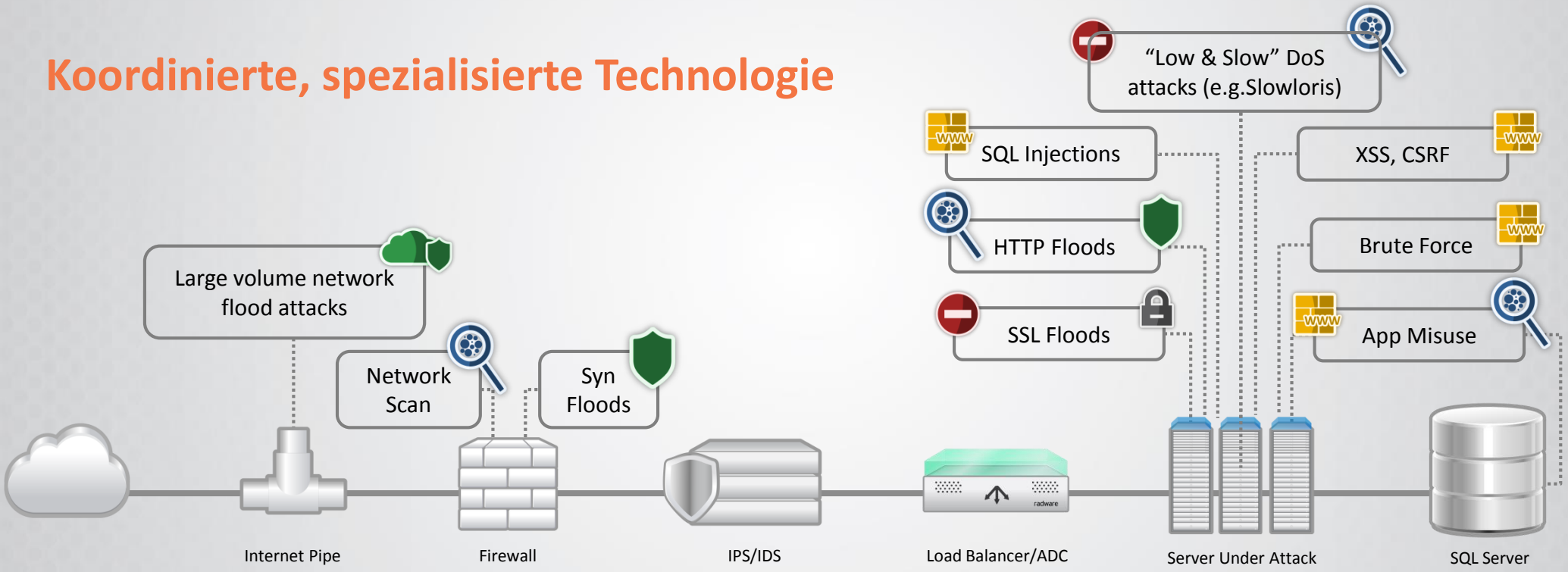
Umfassender, zukunftssicherer DDoS Schutz mit Radware‘s AMS

Was müssen Sie bei der Auswahl des richtigen Schutzes berücksichtigen

Assets:	Welche assets wollen Sie schützen (Applikationen/Netzwerk)?
Wo:	Sind die Applikationen in einem Datacenter center oder in der cloud?
Latenz:	Wie empfindlich ist Ihr Business in Bezug auf Latenz in “Friedenszeit”?
Umleitung:	Wie empfindlich sind Ihre Applikationen auf Unterbrüche aufgrund einer Umleitung des Verkehrs?
Expertise:	Verfügen Sie über in-house expertise um Ihre on-premise appliances zu managen und zu monitoren?
Security:	Wie empfindlich ist Ihr Business ggü. SSL-Bedrohungen auf Ihre Applikationen?

Die Multi-Vector Herausforderung

Koordinierte, spezialisierte Technologie



Unsere Anti-DDoS-Geschmacksrichtungen

Cloud DDoS Protection Service

1. **Hybrid Cloud (best practise)**
2. **Always-on Cloud**
3. **On-Demand Cloud**

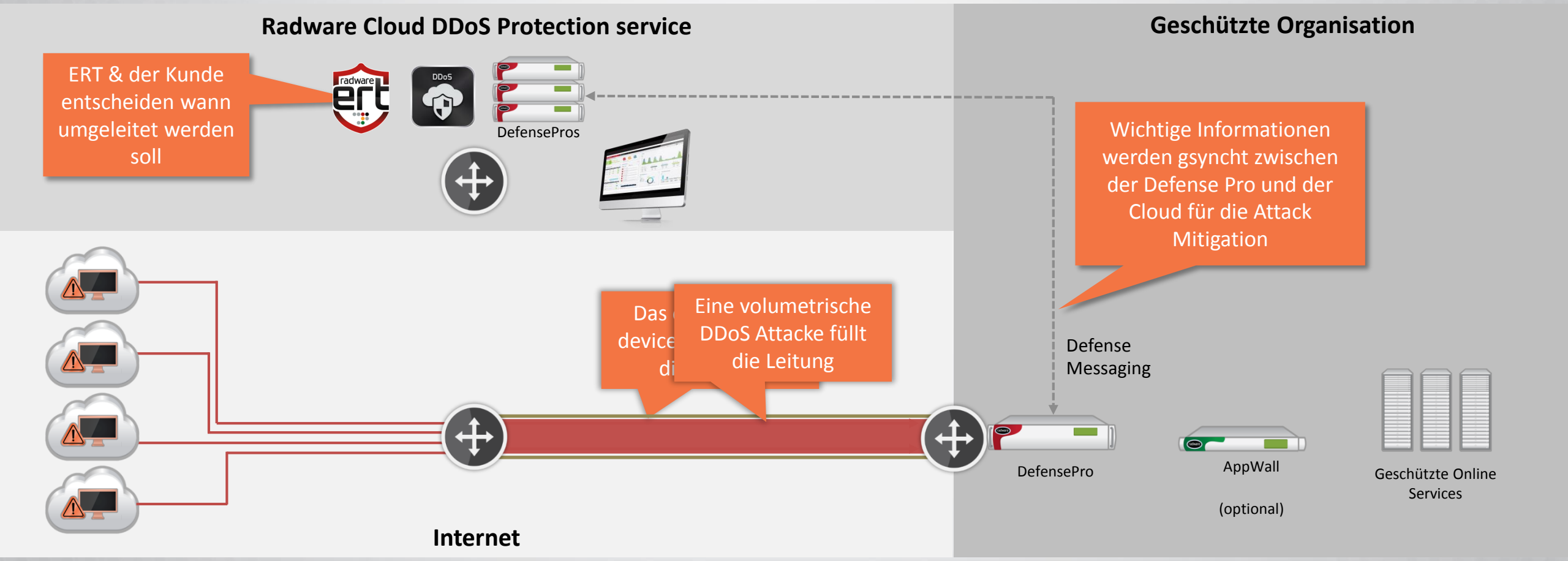
1 Hybrid Cloud DDoS Protection Service

- Detect where you can. Mitigate where you should.

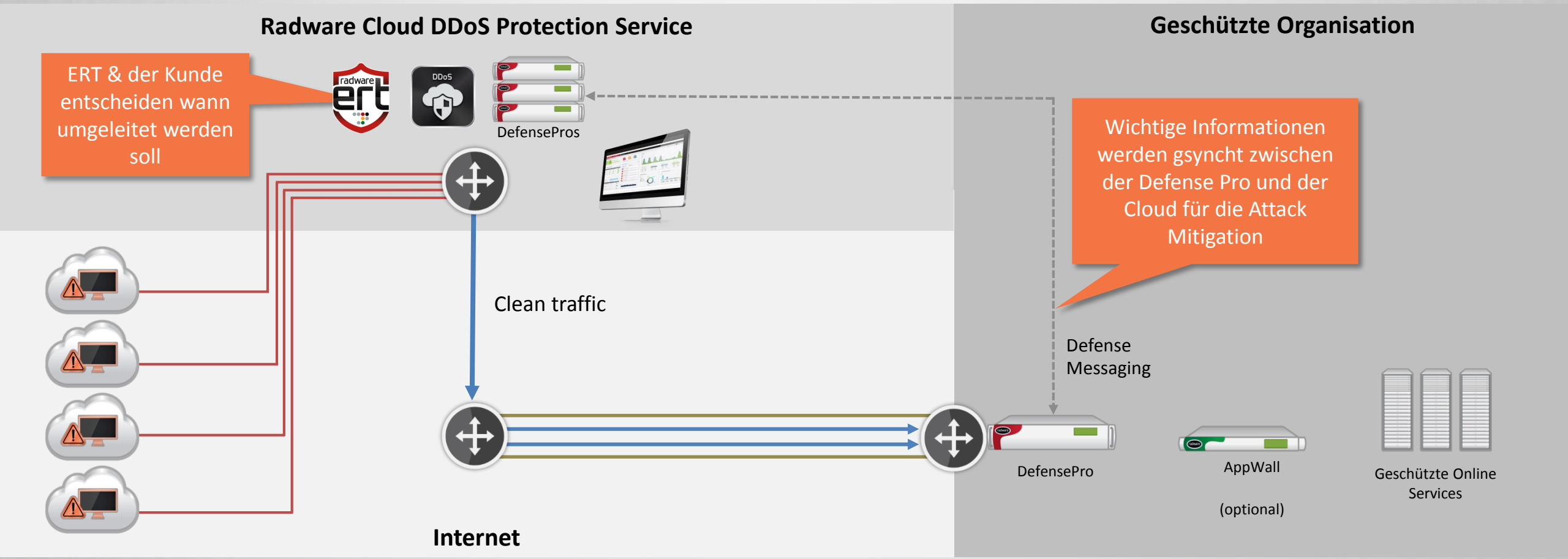
  - Integrierte Lösung mit on premise Box vor Ort
  - **Minimale Latenz in “Friedenszeiten”- Umleitung nur bei Ueberlaufen der Leitung**
  - **Schnellster Schutz - Mitigation startet sofort on-premise**
  - Keine Schutzlücke bei Umleitung in die Cloud - DefenseMessaging für synchronisierten Schutz
  - Single point of contact und (optionale) managed services - **ERT Standard oder Premium**

Für Organisationen welche eine appliance in ihren DC’s deployen können

1 Hybrid Cloud DDoS Protection Service



1 Hybrid Cloud DDoS Protection Service



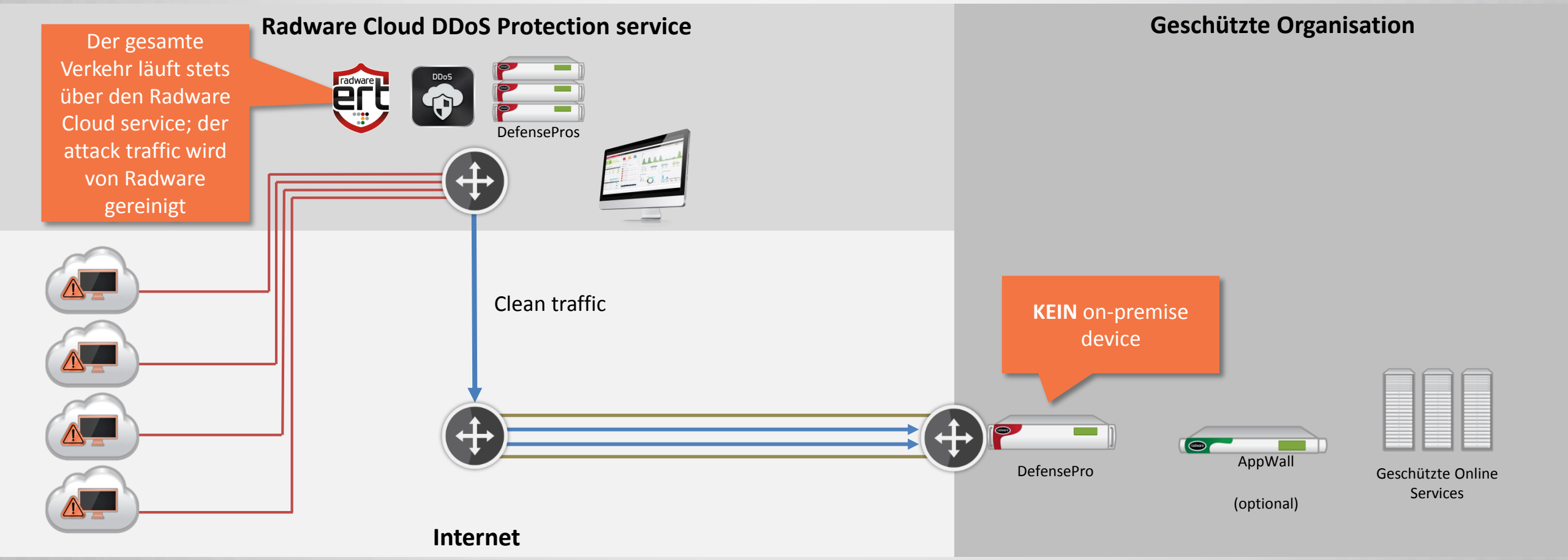
2 Always-On Cloud DDoS Protection Service

- As simple as it gets: Let Radware handle it all

  - **Kürzeste time to protection** – Der gesamte Verkehr läuft immer über die Radware's cloud POPs
  - **Minimalste Kunden-Interaktion–** proaktiv fully-managed vom Radware ERT
  - Unlimited service – Unlimiterte # of attacks, Grösse & Dauer
  - **Zusatzkosten für den umgeleiteten traffic**

Für Organisationen, welche Applikationen in der public cloud haben oder keine Appliance in ihren DC's deployen können

2 Always-On Cloud DDoS Protection Service



3 On-Demand Cloud DDoS Protection Service

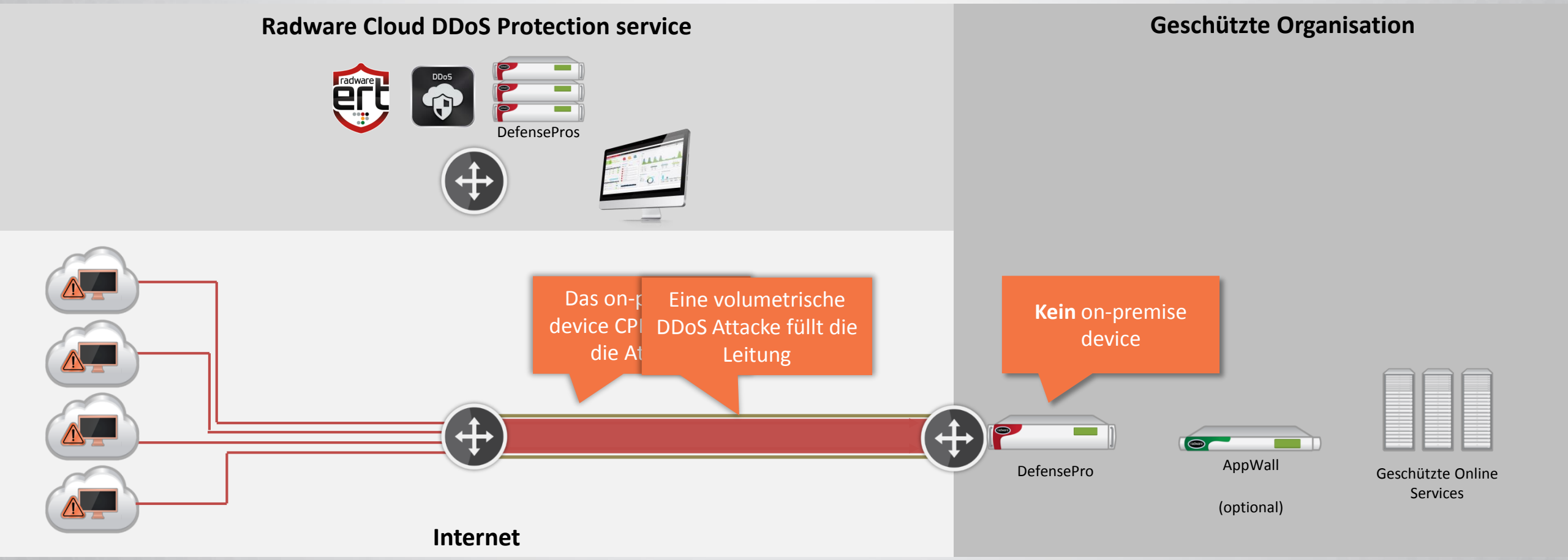
- Günstigste Variante; Einfachstes Deployment

  - Der Verkehr wird nur bei Angriff über die cloud geleitet. **Keine on-premise appliance.**
  - Umleitung basierend auf link utilization thresholds oder flow stats
  - Unlimitierte Angriffsgrösse - limitierte Umleitungen pro Jahr
  - Nur ERT Standard service verfügbar

  - Eingeschränkte Möglichkeit application-level und SSL-basierte DDoS Attacken abzuwehren

Für Organisationen welche keinen Bedarf an real-time detection von applikations-level and SSL-based DDoS Angriffen haben

3 On-Demand Cloud DDoS Protection Service



Unsere Anti-DDoS-Geschmacksrichtungen

DefensePro

1 Hybrid Cloud
Best Practise

- Traffic Umleitung nur bei pipe saturation
- Minimale Latenz in peacetime
- Unlimiterte # of attacks, Grösse & Dauer
- ERT Standard oder Premium (managed service)

Für Organisationen welche eine appliance in ihren DC's deployen können

---

2 Always-on Cloud

- Minimalste Kunden-Interaktion nötig
- Unlimiterte # of attacks, Grösse & Dauer
- Nur ERT Premium service level verfügbar
- Zusatzkosten für den umgeleiteten traffic

Für Organisationen, welche Applikationen in der public cloud haben oder keine appliance in ihren DC's deployen können

---

3 On-Demand Cloud

- Günstigste Variante; Einfachstes Deployment
- Detection basierend auf link utilization thresholds oder flow stats
- Unlimitierte Angriffsgrösse - limitierte Umleitungen pro Jahr
- Nur ERT Standard service verfügbar
- Eingeschränkte Möglichkeit application-level und SSL-basierte DDoS Attacken abzuwehren

Für Organisationen welche keinen Bedarf an real-time detection von applikations-level and SSL-based DDoS Angriffen haben

Radware's Security Lösung - der Multi-Vector Herausforderung getrotzt

Radware Emergency Response Team
24x7 Security Experts

Zentralisiertes Management & Reporting
APSolute Vision

On-Demand Cloud DDoS | DoS protection | Behavioral analysis | IPS | Defense SSL protection | WAF

On-Demand Cloud DDoS Service
DefensePipe
2.8TB+ Mitigations Kapazität
Hybrid, Always-on oder On-Demand

Attack Mitigation Device
DefensePro
Durchsatz von 200Mbps – 300Gbps

Web Application Firewall
AppWall, Cloud WAF Service

Alles aus einer Hand: Fully-Managed Cloud Security Service

Emergency Response Team (ERT) – 7x24 dedizierte Security Experten für schnelle Mitigation unter Angriff

24/7 DDoS Schutz

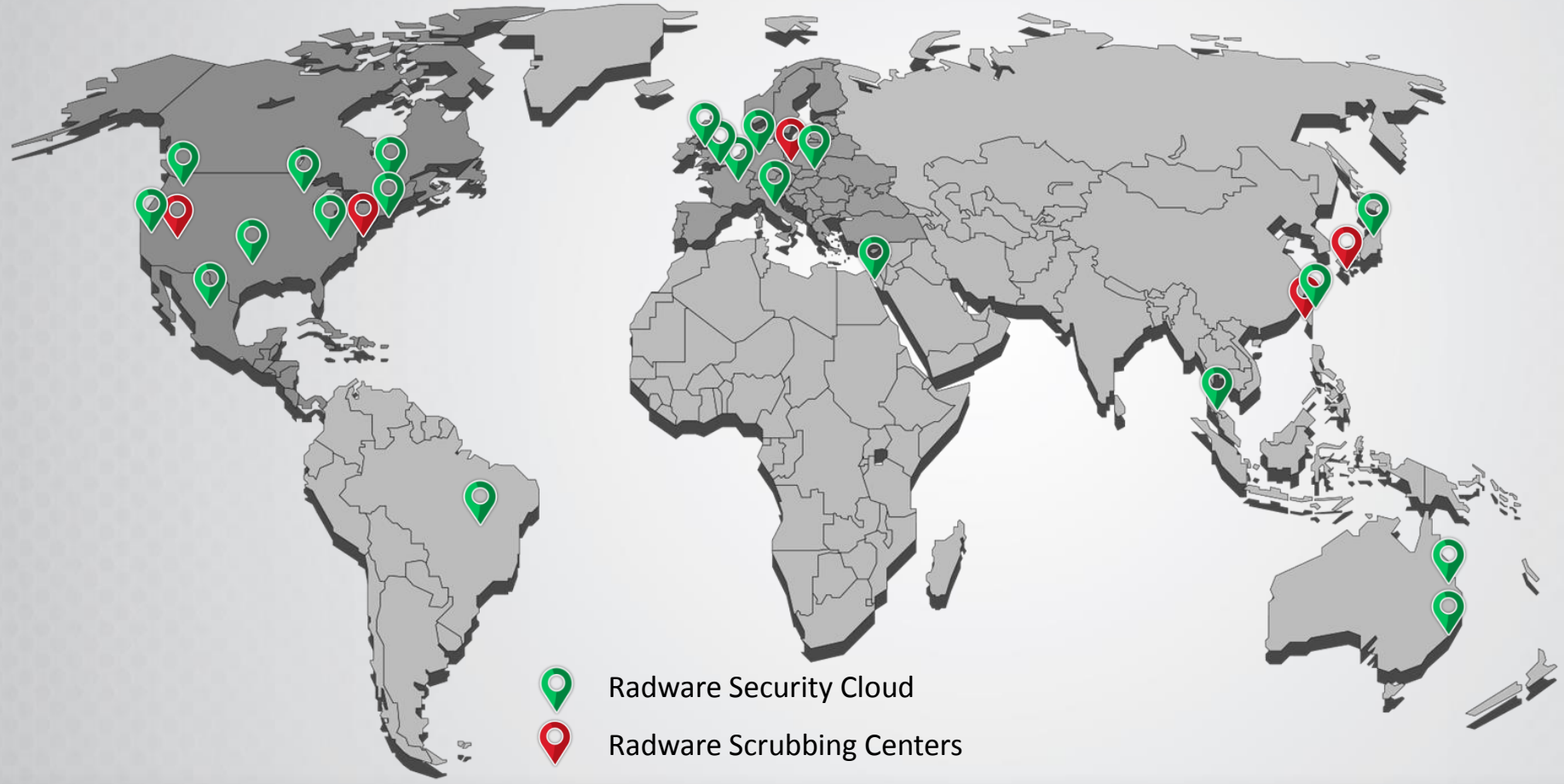
On-Premise Device Management

Regelmässiges Security Consulting

Online Portal & Reporting

Outsourcen Sie das Monitoring und Management komplett zu den Radware Security Experten

Radware's globales Cloud Security Netzwerk



Ueber 2.8Tbps+
globale
Mitigationskapazität

Trennung von clean und attack traffic
mit dedizierten
scrubbing centern

Zusammenfassung der Lösungen

Lösung	Abdeckung	Time-to-Protect	Service Optionen
1 **Hybride Attack Mitigation mit WAF und SSL Mitigation**	★★★★★ DDoS, verschlüsselte Angriffe & Web Attacken	**Am Besten** Echtzeit, Sekunden	Fully managed mit ERT Premium
2 **Radware Cloud WAF**	★★★★ DDoS & Web Attacken	**Am Besten** Echtzeit, Sekunden	Cloud Service ERT Premium option
3 **On-Demand Cloud DDoS Standalone**	★★★ DDoS	**Limitiert** Keine Echtzeiterkennung	Cloud Service keine ERT Premium option
4 **DDoS Standalone**	★★★ DDoS	**Gut** SSL-Inspektion nur möglich, wenn Keys in der Cloud sind, kleine Latenz	Cloud Service ERT Premium option

Radware in a nutshell - Lizensierung

- Unsere Hardware ist via Lizenzkey upgradebar, so dass der Initialinvest im kleinen Rahmen ist
- Wir lizensieren nach legitimate (clean) traffic – **nicht** nach Angriffs-traffic
- FAIR: Keine Einschränkung in Anzahl Umleitungen oder Dauer der Umleitung bei unserem Scrubbing-Service (Cloud-scrubbing Service ex *DefensePipe*)
- Auch reines Service-Modell verfügbar um OPEX/CAPEX Anforderungen zu erfüllen

Kampagnen / www.radware.de

Radware erneut "Leader" im Gartner Magic Quadrant

Geld oder Daten!

Cyberattacken mit Lösegeldforderung sich dafür wappnen.

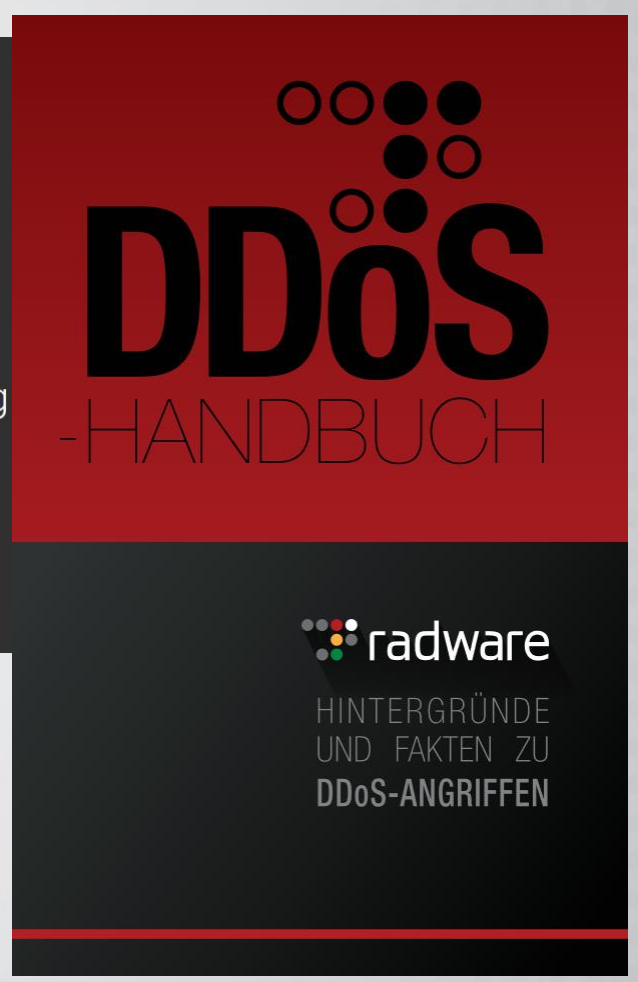
Jetzt lesen

Zunehmende Automatisierung führt zum „Battle of the Bots“

Jetzt lesen: “*Global Application & Network Security Report 2015/16*”

vom Radware Emergency Response Team

Jetzt lesen



Merci – Danke –Thank you

Michele Rapisarda, Channel Manager Radware Schweiz

www.Radware.com
www.Radware-ddos.ch