Effective Zero Trust:

Nutzen Sie DNS-Daten zur Bedrohungsanalyse

Ralf Geisler, Regional Manager D-A-CH & EE

IT-SA: October 10th 2019

efficient iP™

Agenda

1. Introduction
2. Zero Trust Basics
3. Warum ist der Schutz von DNS entscheidend für Zero Trust ?
4. Nutzen von DNS für Security: Zusammengefasst in drei Vorteilen
5. Key Takeaways
6. Q&A

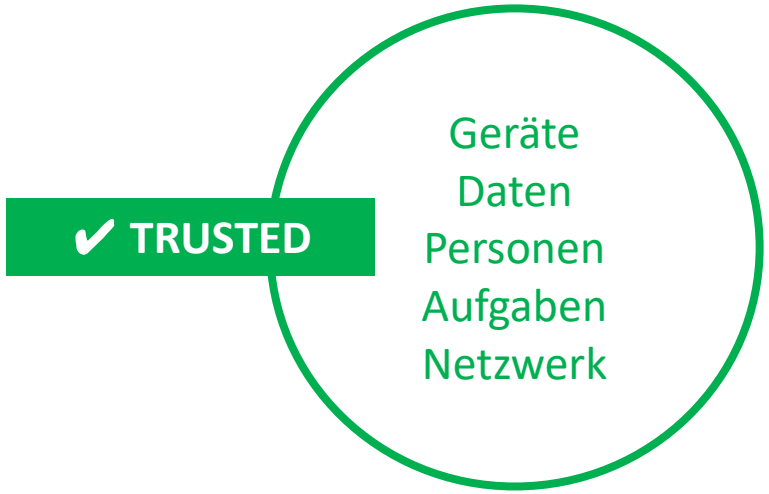
EfficientIP im Überblick

Zero Trust

Was verstehen wir unter Zero Trust?

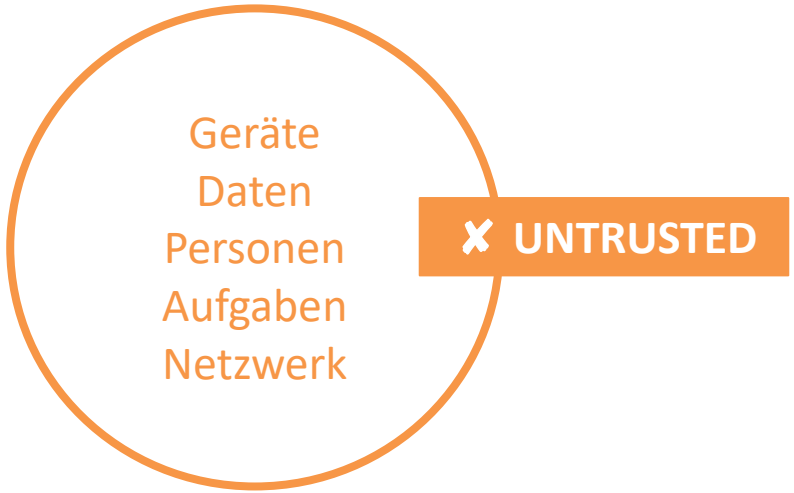
Das Zero-Trust-Sicherheitskonzept wurde von Forrester Research als Alternative zum Perimeter-Sicherheitskonzept vorgestellt

Perimeter-Sicherheitsmodell



Alles, was sich innerhalb des Netzwerks eines Unternehmens befindet, kann als vertrauenswürdig angesehen werden.

Zero-Trust-Sicherheitskonzept

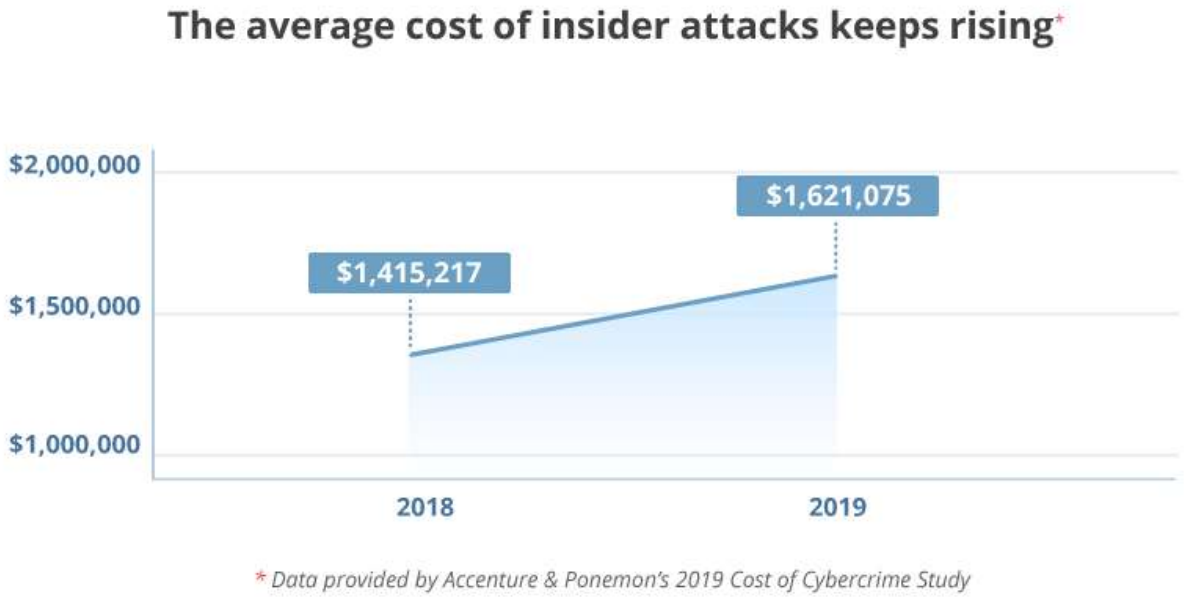


Alles ist standardmäßig nicht vertrauenswürdig, auch wenn es sich bereits im Netzwerk befindet.

efficient iP™

Warum Zero Trust?

Der Perimeter-Sicherheits-Ansatz ist nicht ausreichend, um Bedrohungen aus dem Inneren des Netzwerkes standzuhalten



1. Interne Bedrohungen werden immer ausgefeilter, vielfältiger und leistungsfähiger:
   - infizierte Dokumente, Malware, Ransomware, Phishing, Verbreitung über E-Mail und gefährdete Websites, nutzen von Zero-Day-Schwachstellen
2. Verteilte Topologien und Multi-Cloud komplexieren die Sicherheit
3. Die Betrachtung nach "Makro-Segmenten" wie intern, extern, DMZ ist nicht ausreichend, um vor internen Bedrohungen zu schützen

Zero Trust Grundlagen

Granulare Transparenz

Wechsel zur Betrachtung der Sicherheit nach Mikrosegmentierung, wie z. Bsp. ein einzelner Client, eine Anwendung oder ein Server

Echtzeit-Analyse

Identifizieren Sie einen Client oder eine Nutzung und überprüfen Sie das Verhalten in Echtzeit

Automatisierung & Orchestrierung

Dynamische Konfiguration von Netzwerk- und Sicherheitssystemen mit Durchsetzung von Policies

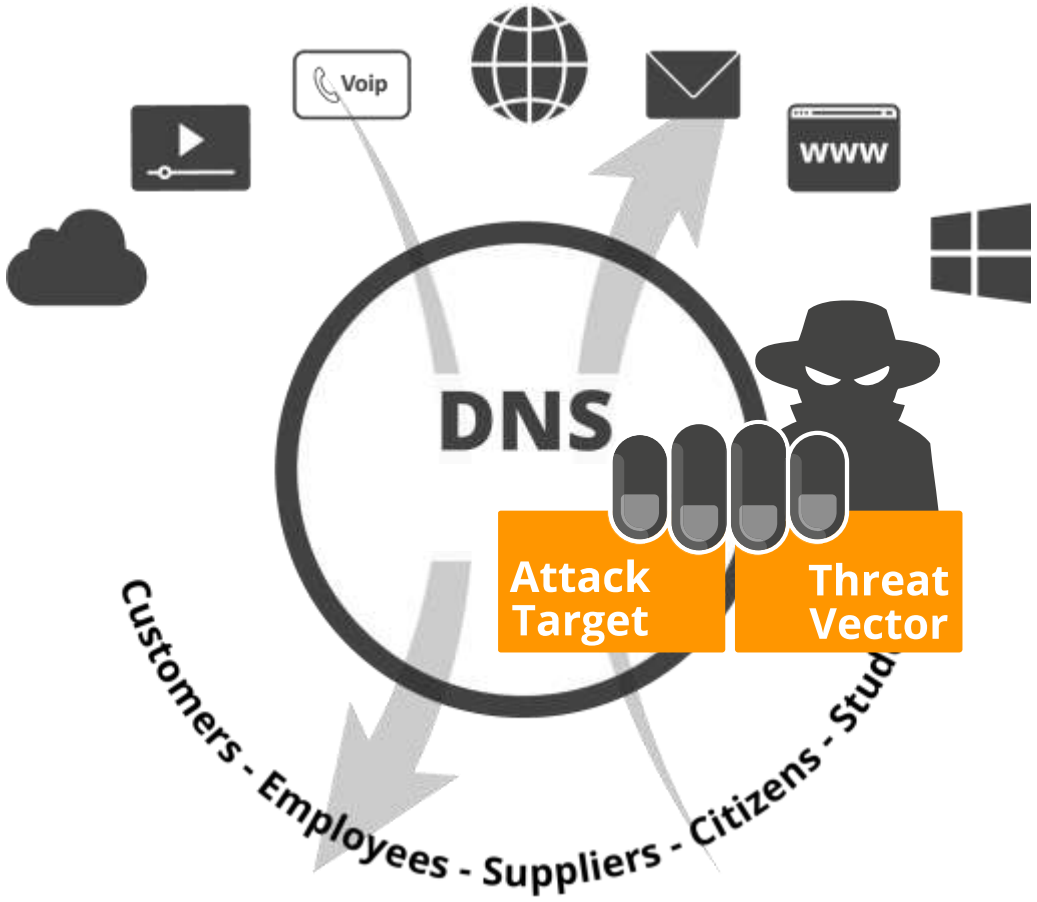
efficient iP™

Warum ist der Schutz von DNS entscheidend für Zero Trust ?

Zero Trust und DNS

DNS spielt eine zentrale Rolle im "Application Traffic Routing" und stellt die Verbindung zwischen Benutzern und Anwendungen her

Da per Definition offen, nutzen Hacker die DNS-Doppelrolle in der "Kill-Chain" entweder als Bedrohungsvektor oder als direktes Ziel

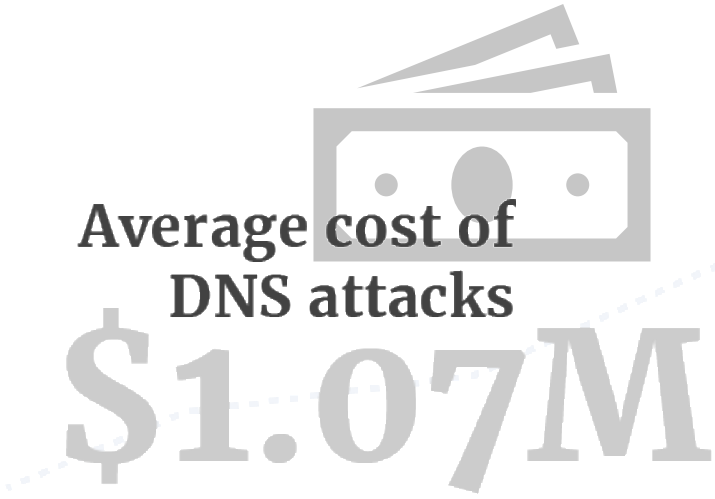


DNS steht ganz oben auf der Liste der Hacker

TOP primary application layer **Targets**

Arbor Network 2018 Security Report

Cisco 2016 Security Report



IDC 2019 DNS Threat Report

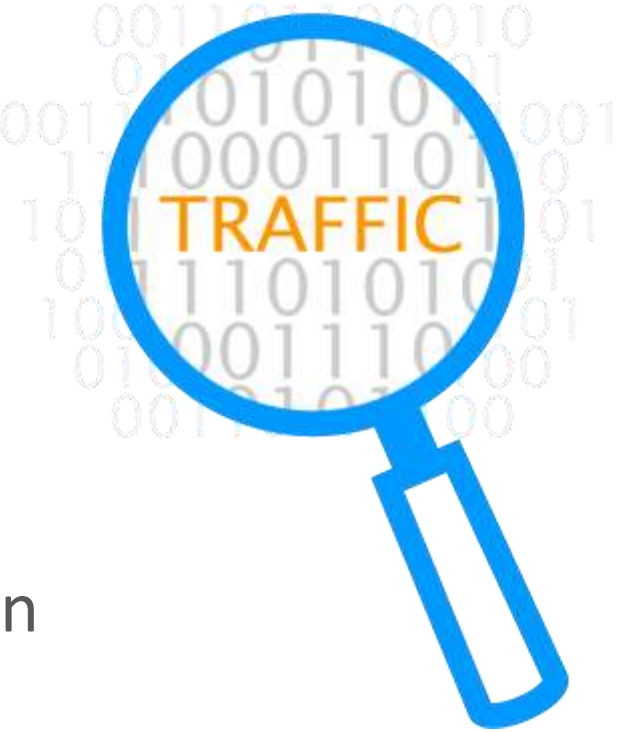
Die DNS-Protokollanalyse ist eine Schlüsselkomponente der Netzwerksicherheit, um fortgeschrittene Bedrohungen zu erkennen, die im Netzwerkverkehr verborgen sind

efficient iP™

Nutzen von DNS für Security: Zusammengefasst in drei Vorteilen

Nutzen Sie DNS-Daten, um die Netzwerk-transparenz auf Benutzerebene zu erhöhen

- DNS hat eine perfekte Transparenz über den gesamten Datenverkehr auf einen sehr detaillierten Niveau
  - für jeden Benutzer, jede App, jede Ressource und jeden Server im Netzwerk



- DNS-Daten bieten wertvolle Kontext-informationen für die Erkennung verhaltensbedingter Bedrohungen
  - Kunden-ID, Zieldomäne, Abfragetyp, Fragmentierung, Dauer etc.....

Analysieren Sie Daten mit erweiterten Echtzeit-Analysen.

"End-to-End"-Sicherheit - von der Quelle bis zum Ziel

Erkennen von Angriffen, indem jedes Verhalten des DNS-Clients analysiert wird

Erkennung von DNS-Angriffen

Daten-Exfiltration

“DNS Tunneling” (CnC)

DGA

“Zero Day” schadhafte Domain

Identifizieren schadhafter Ziele mit Hilfe von Bedrohungs-informationen der Domäne-Reputation

efficient iP™

DNS-Integration im Security Eco-System zur Automatisierung und Orchestrierung von Antworten

Aufbrechen von Sicherheitssilos und Bereitstellen einer durchgängigen Automatisierung und Kontrolle

Verhindert die Ausbreitung von Angriffen,

verbessert die Erkennung und

beschleunigt die Abhilfemaßnahmen durch die gemeinsame Nutzung von Informationen über Bedrohungen und Sicherheitsmöglichkeiten

efficient iP™

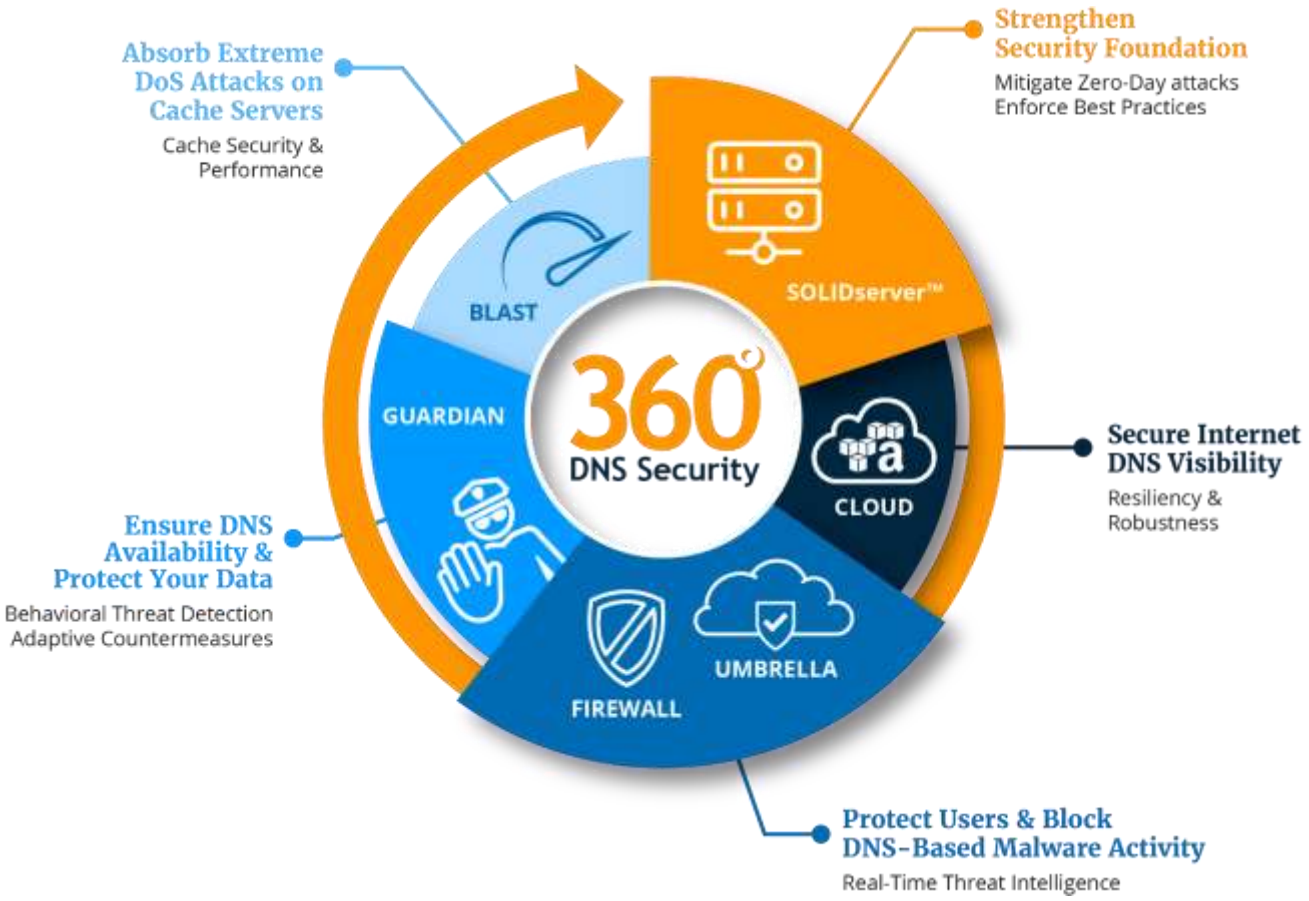
Die wichtigsten Schlussfolgerungen
Key Takeaways

Die wichtigsten Schlussfolgerungen / Takeaways

1. 91% der Malware missbraucht DNS für Angriffe auf Netzwerke -> dabei ist die Sicherung von DNS durch den EfficientiP 360° DNS-Security Ansatz realisierbar

2. DNS sieht den gesamten Internetverkehr und kann somit wertvolle Daten liefern, um Daten-Exfiltrationen und andere Bedrohungen zu erkennen

3. Die Kombination von Client-Verhaltens-analysen mit Bedrohungsinformationen bringt vorausschauende Sicherheit für Ihre Zero Trust Strategie



Sichern Sie Ihr DNS, Sichern Sie Ihr Netzwerk

Vielen Dank!

Halle: 9
Stand: 9-139

efficient iP