Evolving IT Architectures and the Impact on Security

Agenda

Threat Landscape

Digital Transformation Driving New Architectures

Using a Foundational Approach for
Enterprise Security

Market Trends in DNS Privacy

Threat Landscape in the Age of Digital Transformation

Edge

Attacks on edge services top the list of threats tracked in Q3 2019[1]

Cloud

60% of web application attacks were to gain unauthorized access to cloud-based email servers[2]

IoT

Half of top 12 Global exploits targeted IoT devices in Q4 2018[3]

What to lookout for in 2020

- More mobile threats

- All online accounts are fair game

- Ransomware is rising to crisis level

- Continued increase in cybersecurity skills gap

Sources:
1. Fortinet threat landscape report Q3 2019
2. Verizon DBIR 2019
3. Fortinet threat landscape report Q4 2018

Other sources: Infoblox CIU, Forbes, CIO Dive, Trendmicro
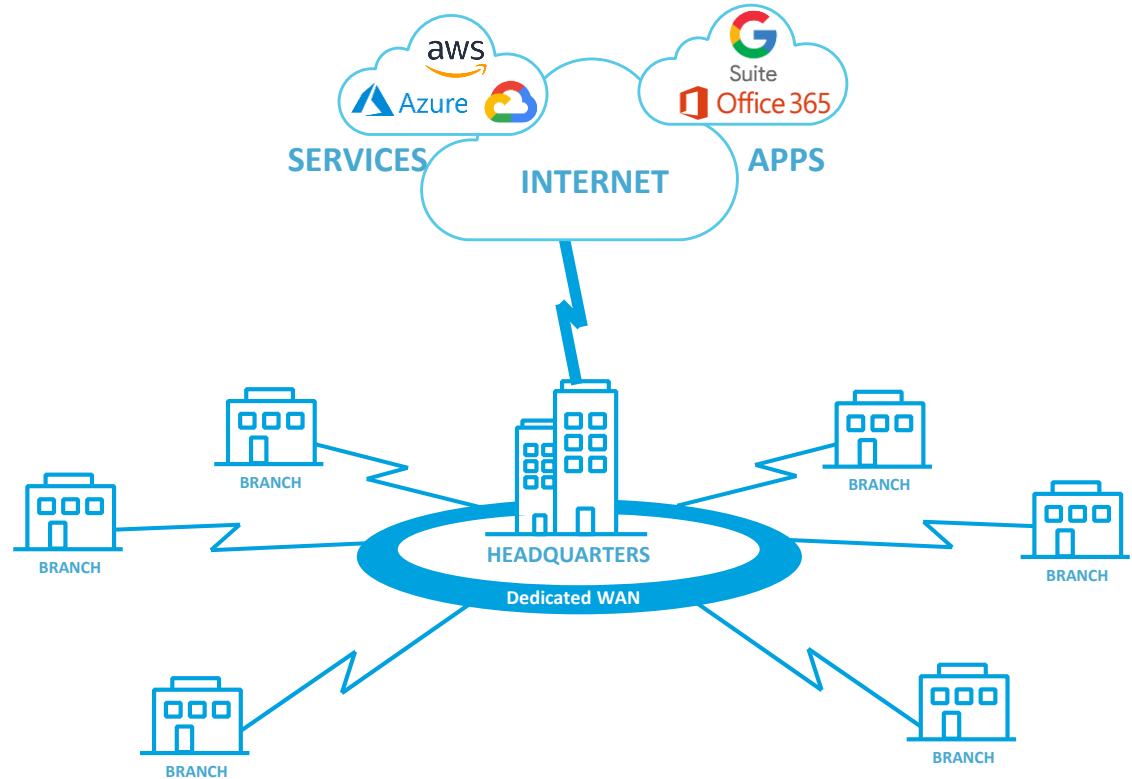
Agenda

The Traditional Architecture

Dedicated WAN circuits

Static configurations

Lack of automation

Centralized, perimeter-based security
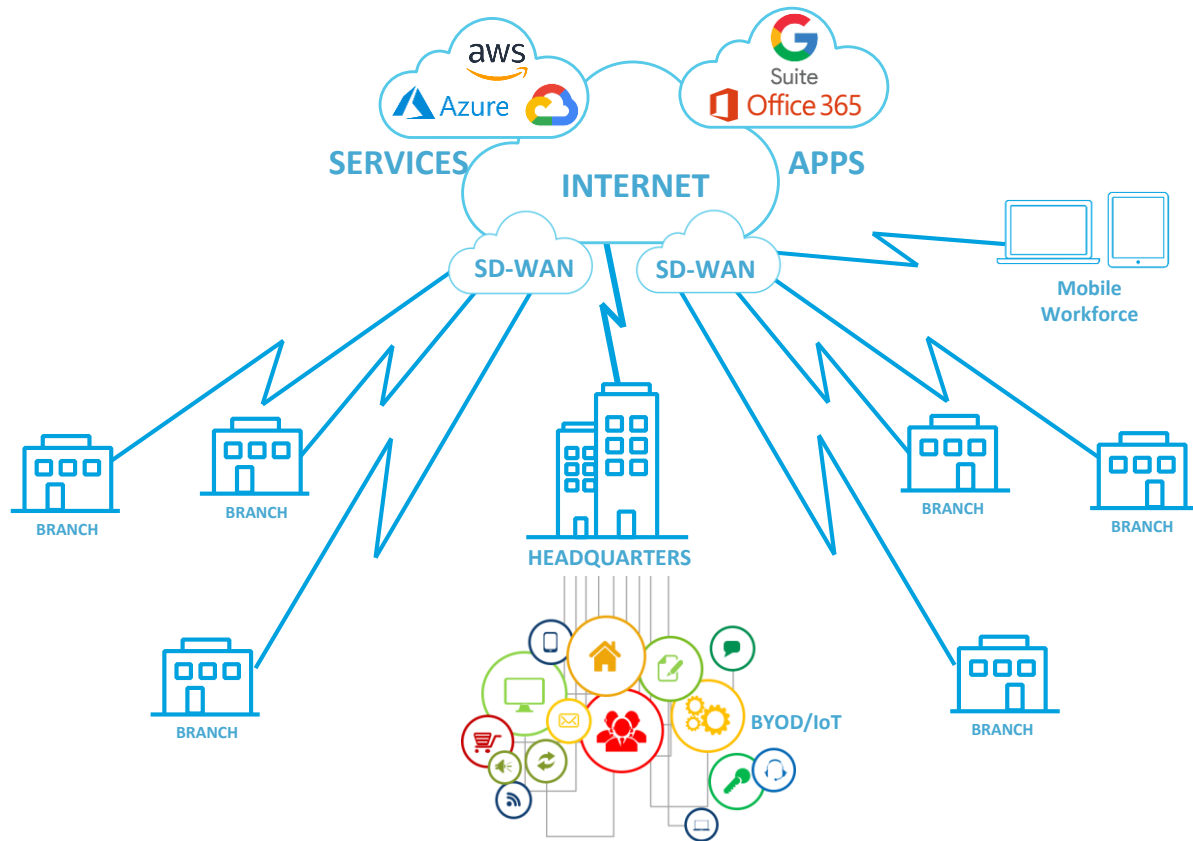

SERVICES

APPS

INTERNET

BRANCH

BRANCH

BRANCH

BRANCH

HEADQUARTERS

Dedicated WAN

BRANCH

BRANCH

The New Architecture: Cloud, SaaS, SD-WAN

SD-WAN for remote locations

Decentralized infrastructure

BYOD/IoT

SaaS/Cloud

And Impacts Security

Increased attack surface

Siloed, inefficient security architecture

Over-burdened security operations teams

Poor scaling of threat detection and remediation

Foundational Services

DNS

DHCP

IP Address Management (IPAM)

DDI

Core Foundation Elements for Any Architecture

Network Foundation
- IP Address
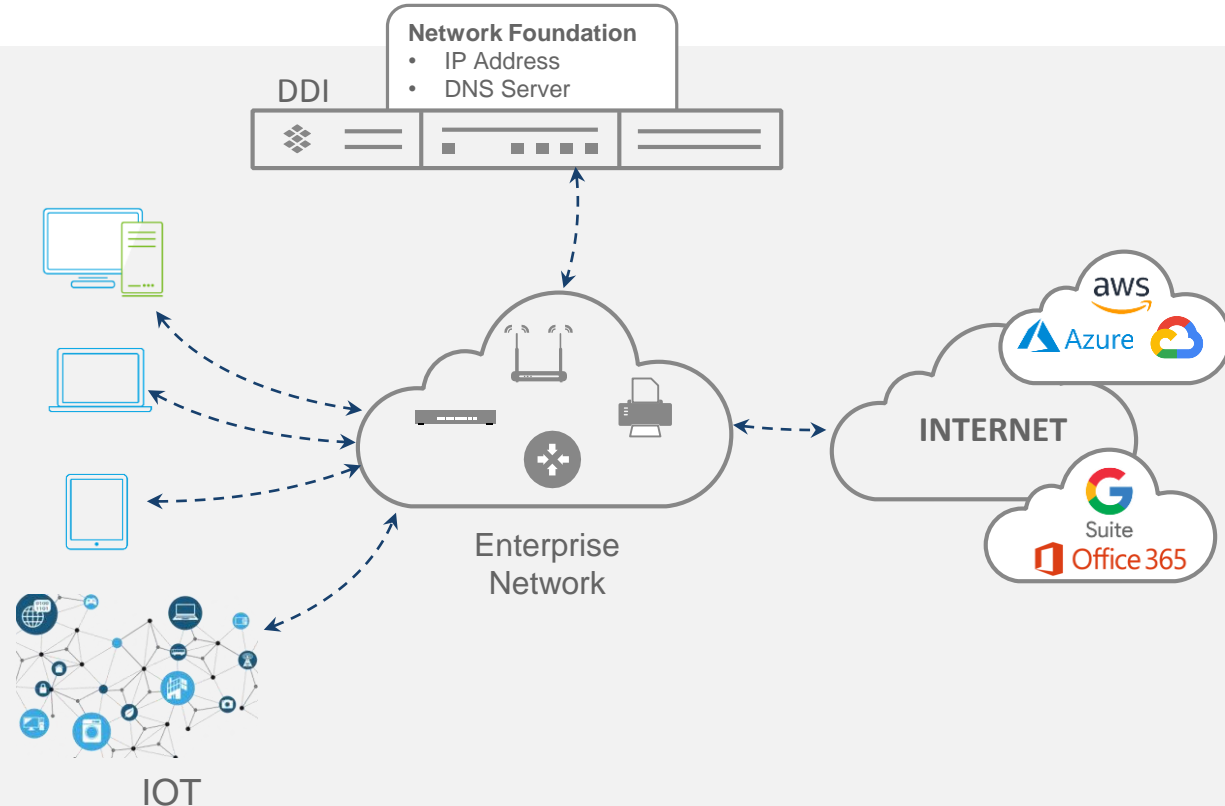- DNS Server

DDI

IP Address Management

- Device IP Address
- Centrally managed
- Resolve network conflicts

Provides Internet Connectivity
- DNS used to locate services/destinations
- DNS server location

Asset Management and Discovery
- Automated device discovery
- Authoritative inventory of physical and virtual network assets

Enterprise
Network

IOT

aws
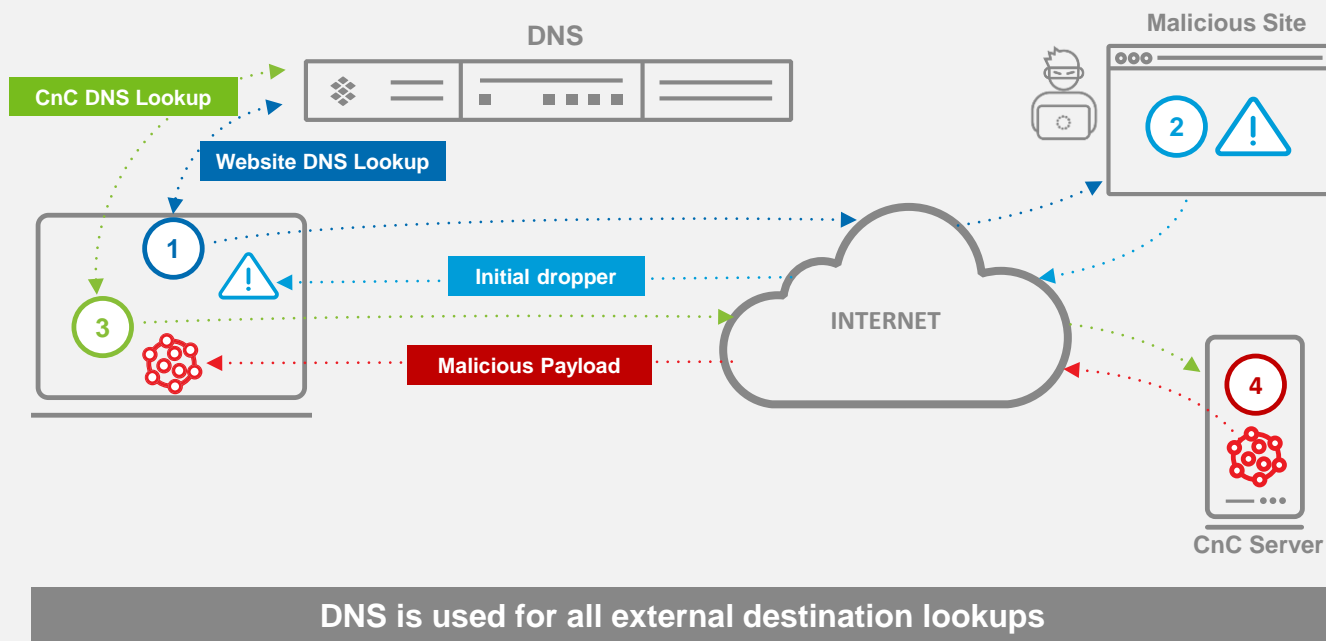Azure

INTERNET

G Suite
Office 365

Agenda

Common Attack Steps Review

1 User directed to malicious site

2 Website delivers initial exploit

3 Exploit contacts CnC server

4 Malicious payload downloaded

DNS

CnC DNS Lookup

Website DNS Lookup

Initial dropper

Malicious Payload

INTERNET

Malicious Site

CnC Server

DNS is used for all external destination lookups

Leveraging DNS Intelligence for Security

1 **Curated threat intelligence for DNS**

2 **Connection to malicious website blocked at DNS**

3 **If already infected, CnC connection request blocked at DNS**

Threat Intel

DNS

Secure DNS

X CnC DNS Lookup

X Website DNS Lookup

Malicious Site

2

Initial dropper

INTERNET

Malicious Payload

1

3

4

CnC Server

Secure DNS breaks the attack chain before it starts
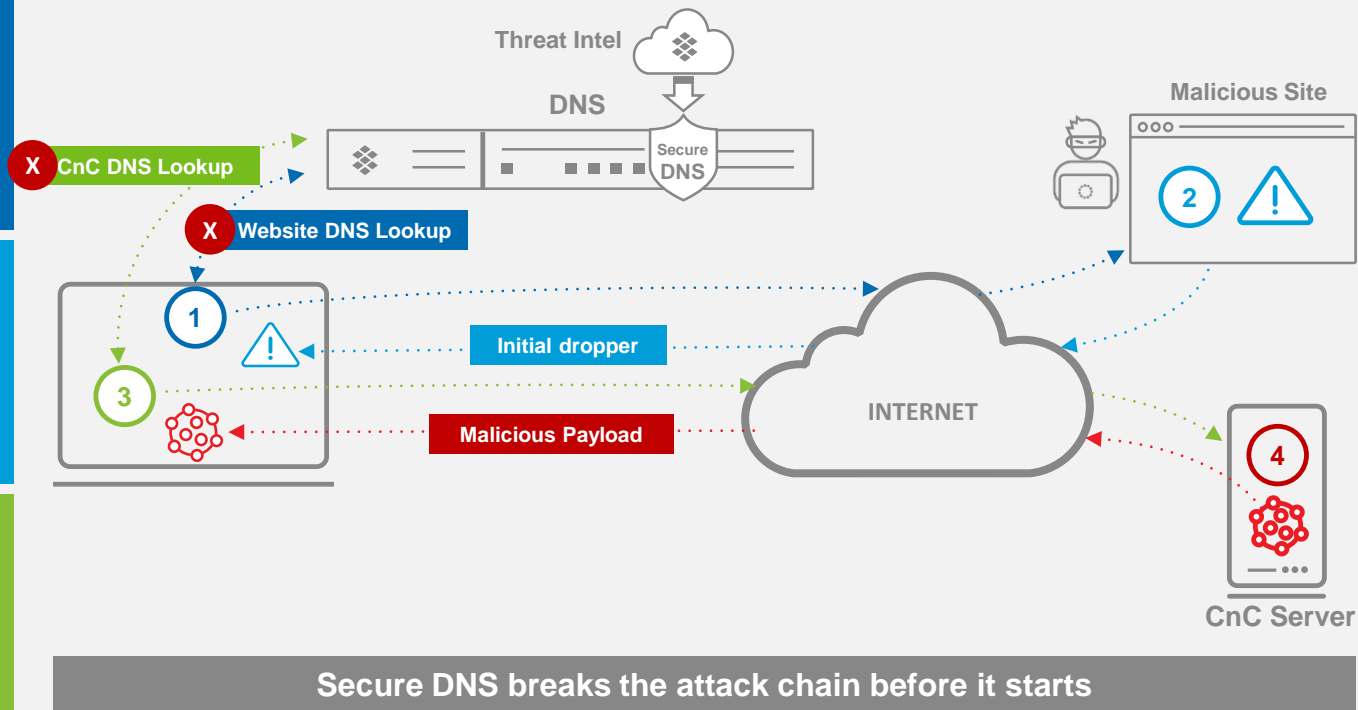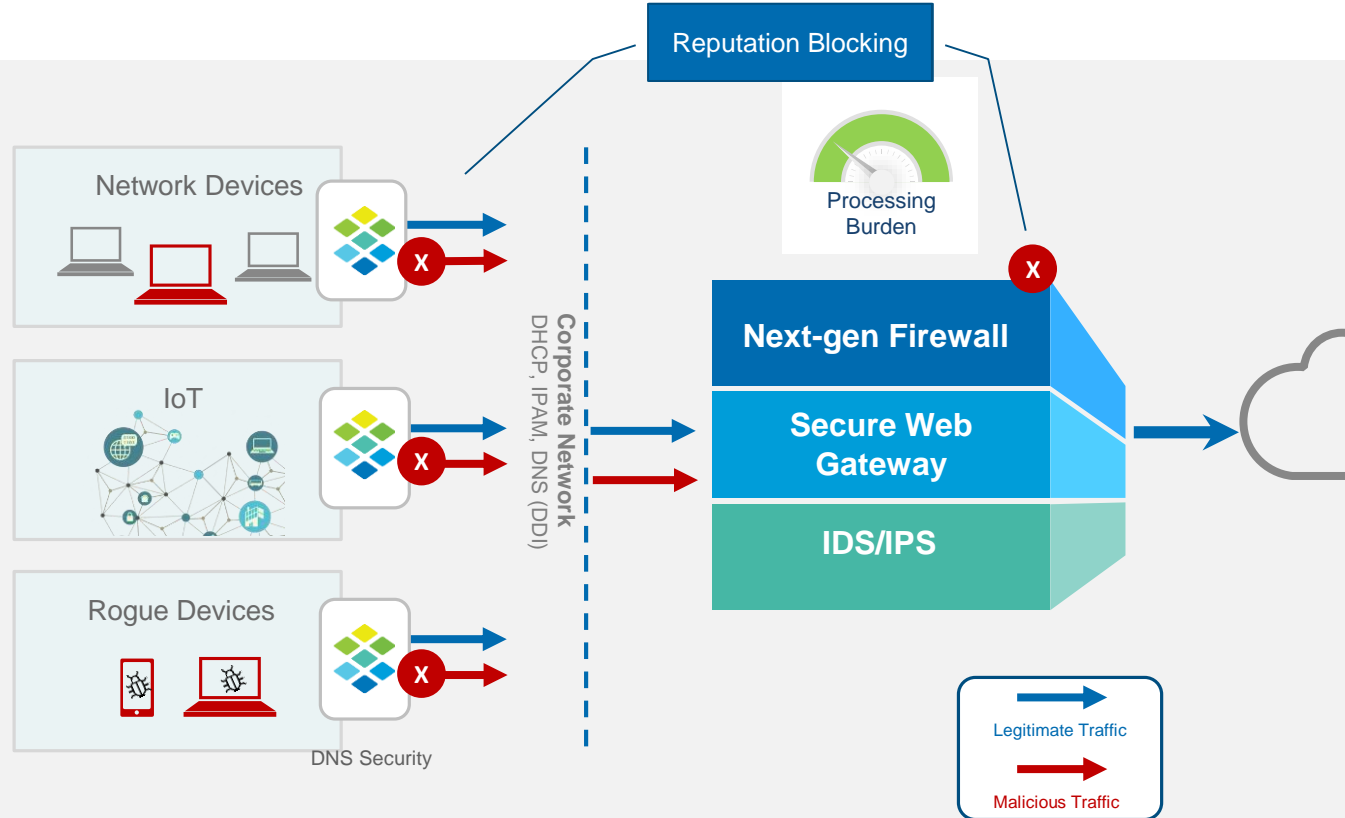
Optimizing Entire Security Stack

Preserving Perimeter Security

Giving Back Scalability

- Offloading blocking of known threats
- Reducing "junk" traffic to NGFWs, SWGs and IDS/TPS
- Preserving processing power of perimeter security

Protect All Devices

- Foundation of **DHCP, IPAM**, **DNS**
- Widespread protection for
  - All enterprise devices
  - All IoT devices
  - Rogue devices
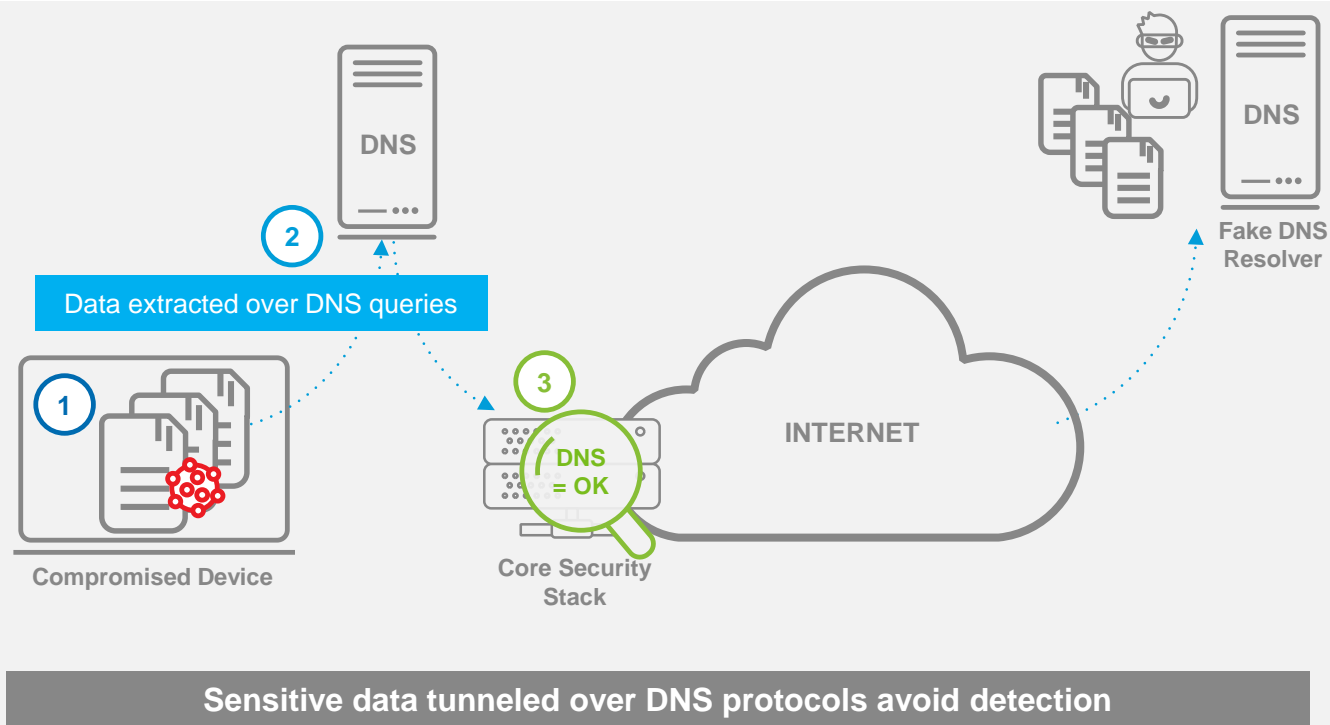
Reputation Blocking

Processing Burden

Network Devices

IoT

Rogue Devices

DNS Security

Corporate Network
DHCP, IPAM, DNS (DDI)

Next-gen Firewall

Secure Web Gateway

IDS/IPS

Legitimate Traffic

Malicious Traffic

Closing Gaps in Protection: Data Exfiltration over DNS

1 Malware seeks sensitive data on compromised device

2 Malware uses DNS channel to exfiltrate data

3 Defenses do not inspect DNS traffic

DNS

2

Data extracted over DNS queries

1

Compromised Device

3

DNS = OK

Core Security Stack

INTERNET

Fake DNS Resolver

DNS

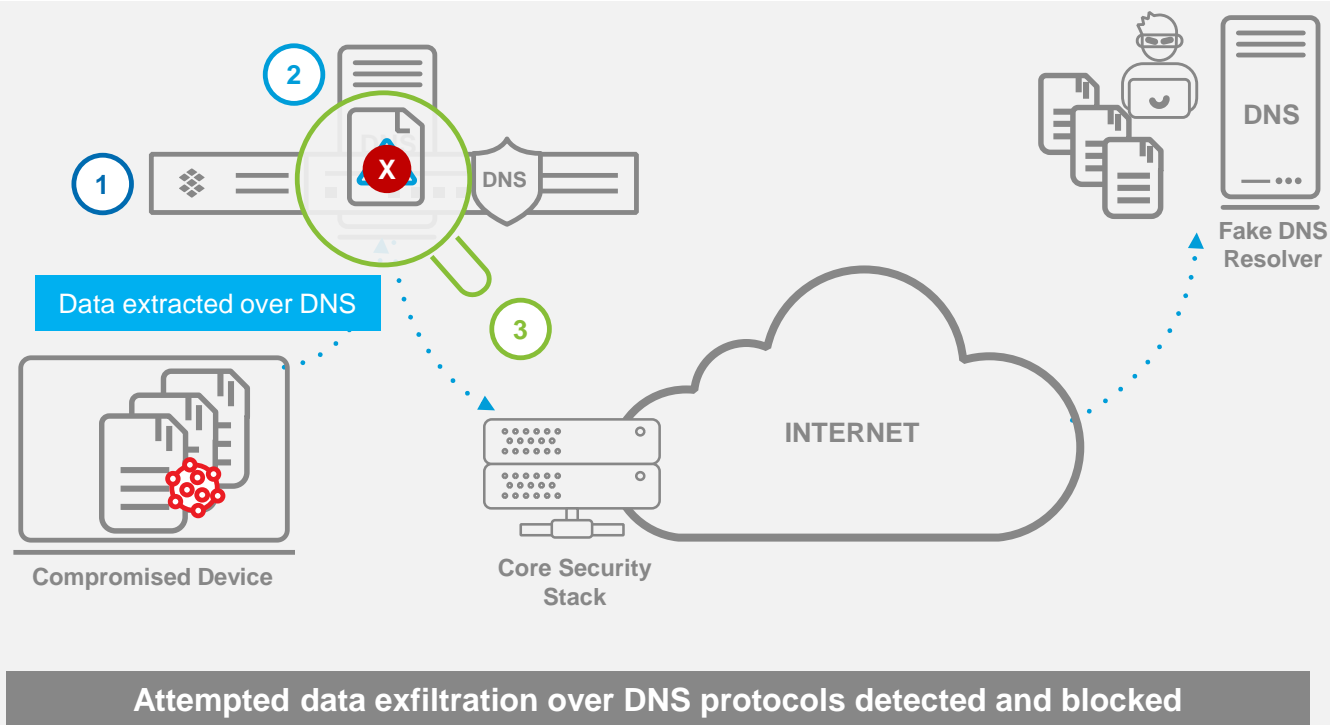**Sensitive data tunneled over DNS protocols avoid detection**

Protecting from Data Exfiltration over DNS

1 DNS with threat intelligence and analytics

2 Machine learning analytics inspect DNS traffic for data exfiltration

3 Data secured by blocking DNS request

2

1

DNS

Data extracted over DNS

3

INTERNET

Compromised Device

Core Security Stack

DNS

Fake DNS Resolver

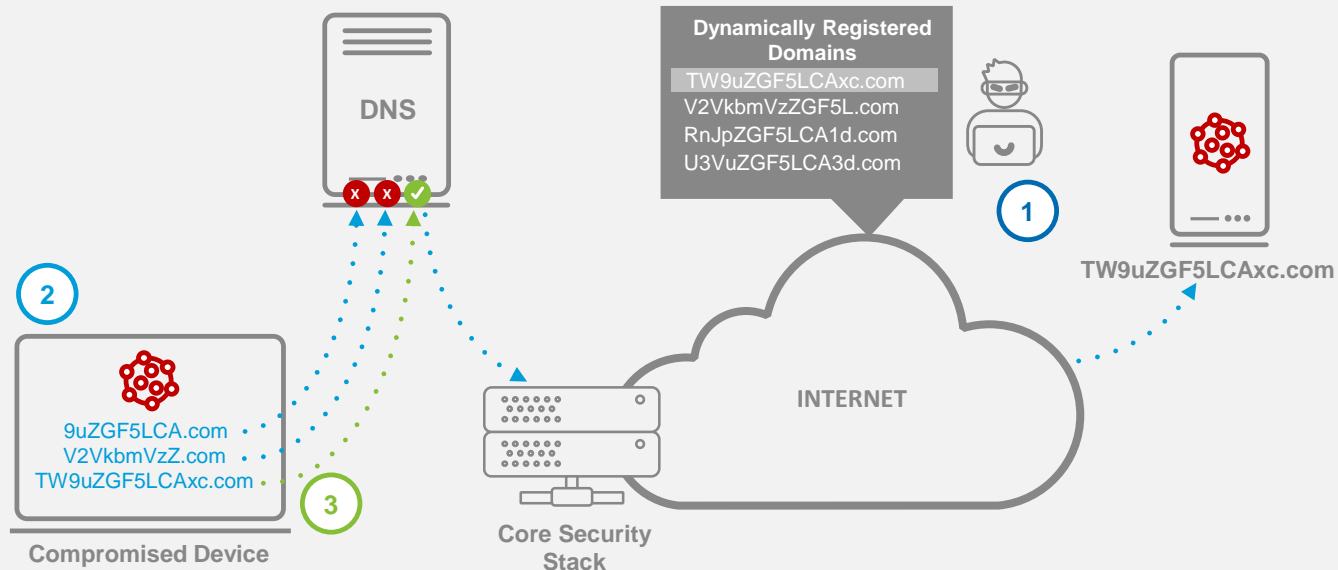Attempted data exfiltration over DNS protocols detected and blocked

Closing Gaps in Protection: Dynamically Generated Domains

1 Attacker uses algorithm for dynamic domain creation

2 Malware uses same algorithm to "look" for CnC

3 Successful domain allows malware to connect to CnC

DNS

Dynamically Registered Domains
TW9uZGF5LCAxc.com
V2VkbmVzZGF5L.com
RnJpZGF5LCA1d.com
U3VuZGF5LCA3d.com

1

TW9uZGF5LCAxc.com

2

9uZGF5LCA.com
V2VkbmVzZZ.com
TW9uZGF5LCAxc.com

Compromised Device

3

INTERNET

Core Security Stack

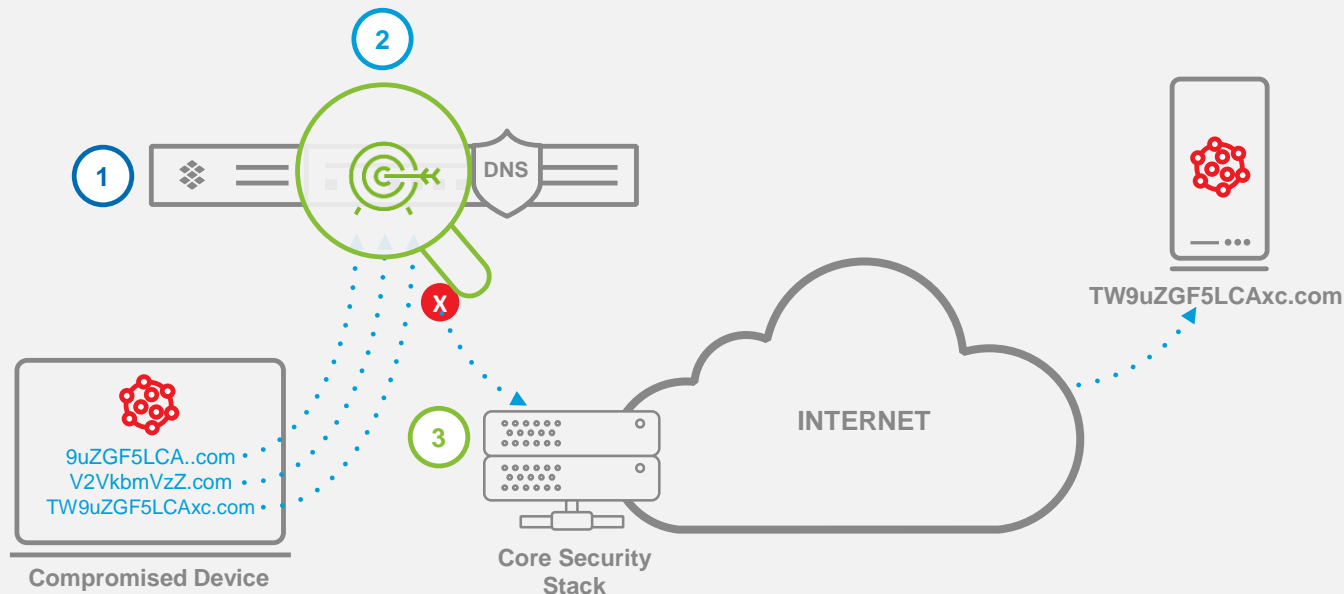**Threat Intel/reputation is ineffective against this attack method**

Protecting Against Dynamically Generated Domains

1 Machine learning analytics inspect DNS queries

2 Identifies patterns that follow DGA methods

3 Block ongoing connections with the same pattern

DNS

INTERNET

TW9uZGF5LCAxc.com

9uZGF5LCA..com
V2VkbmVzZZ.com
TW9uZGF5LCAxc.com

Compromised Device

Core Security Stack

Machine learning identifies algorithm-based domain lookups

Agenda

Market Trends in DNS Privacy

- Two evolving improvements to DNS privacy have recently made the news:
  - DNS over TLS (Transport Layer Security) or "DoT"
  - DNS over HTTPS or "DoH"

- Mechanisms promote consumer privacy but allow users to circumvent established enterprise DNS controls.
  - Exposure to data exfiltration and malware proliferation

DoT/DoH: Bypass of Enterprise DNS is a Challenge

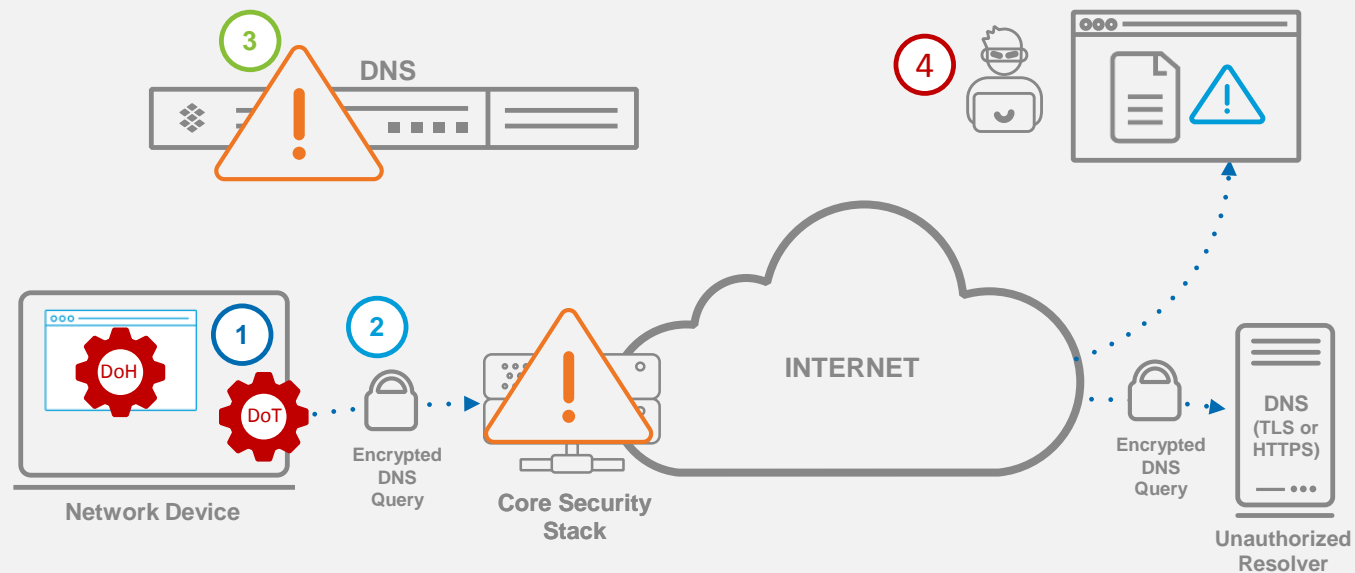**1** Device (TLS) or browser (HTTPS) is configured with unauthorized DNS Resolver

2 Encrypted DNS queries sent to external resolver

3 Internal DNS Resolver bypassed, and DNS traffic not inspected

4 Attackers can exploit DoT for their own purpose

DNS

Network Device

Encrypted DNS Query

Core Security Stack

INTERNET

Encrypted DNS Query

DNS (TLS or HTTPS)

Unauthorized Resolver

**DoT/DoH "HIDES" DNS traffic from your security tools**

DoT/DoH Best Practices

1 Circumventing internal DNS is a bad idea

2 Block Access to unauthorized DNS servers

3 Use internal DNS vendor that supports DoT to retain control and security

4 Block DoH using Threat Intel List of Canary and unauthorized resolvers

Network Device

Encrypted DNS Query

Core Security Stack

INTERNET

Encrypted DNS Query

DNS (TLS or HTTPS)

Unauthorized Resolver
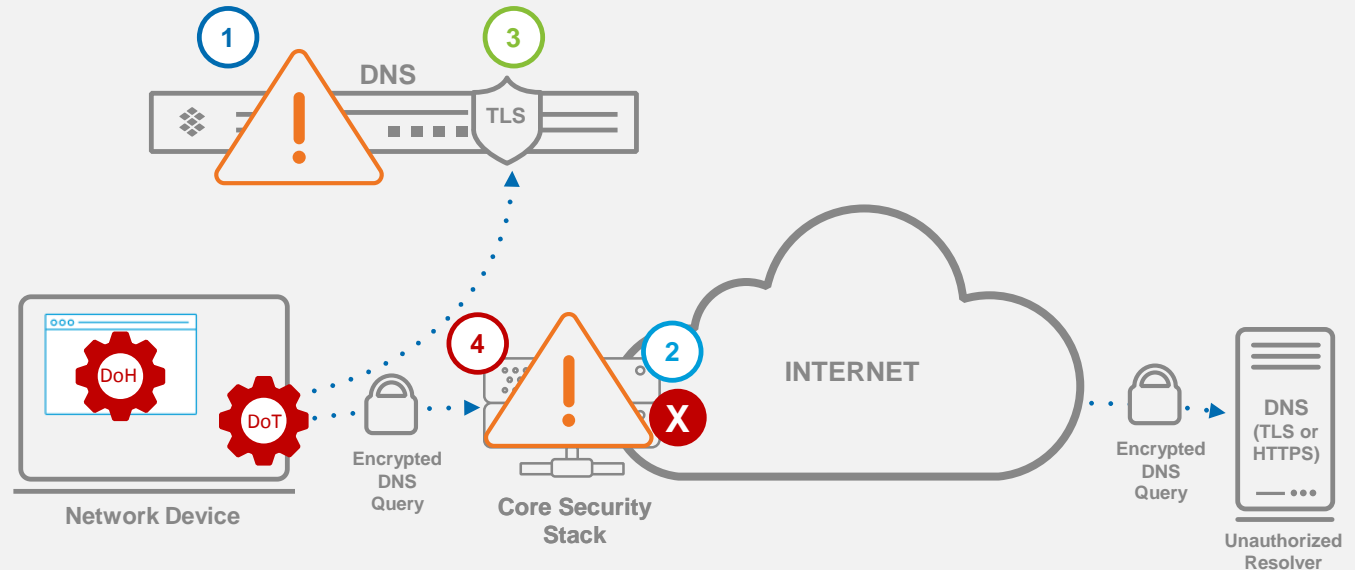
DoT/DoH Best Practices protects your users and devices

Customer Story: UK National Cyber Security Center

Customer Use Case:

- Protect UK government departments from cyberattacks

Solution: BloxOne Threat Defense for foundational security using DNS control plane

Outcomes:

- 273,329 requests blocked, of which 5,768 were unique in a single week
- 3 terabytes of DNS data analyzed for security threats
- 134,825 unique DNS queries blocked in 1 year
- Nearly all organizations benefited from blocking of (malicious) DNS queries
- Identified previously unknown methods that avoid threat detection (DGAs)

https://www.ncsc.gov.uk/information/active-cyber-defence-one-year

Summary

Evolving IT Architectures
and Impact on Security

Digital transformations put new demands on IT, security

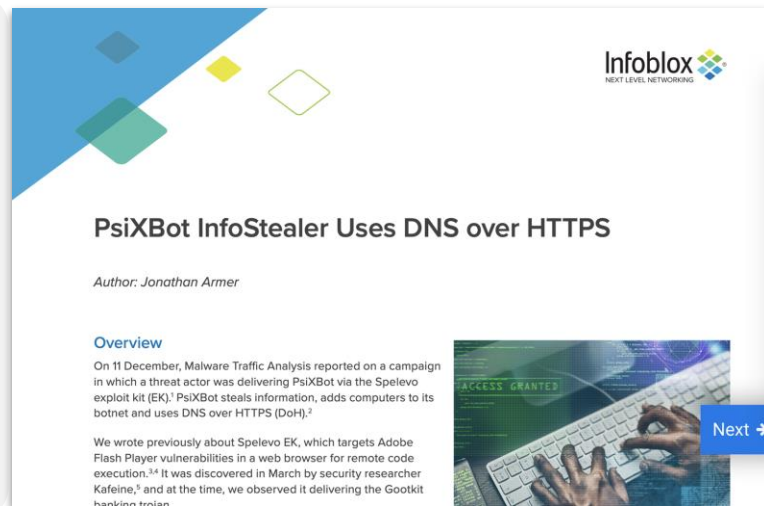DDI can be leveraged to provide foundational security for any architecture

Keeping control of your DNS is critical for security

Infoblox Cyber Intelligence Unit

- **10+ years** of experience
- Publishes **hundreds of thousands** of valuable indicators daily
- Provides actionable intelligence that is **high quality, timely** and **reliable**
- Publishes valuable cyber threat reports

Subscribe

PsiXBot InfoStealer Uses DNS over HTTPS

Author: Jonathan Armer

Overview

On 11 December, Malware Traffic Analysis reported on a campaign in which a threat actor was delivering PsiXBot via the Spelevo exploit kit (EK).[1] PsiXBot steals information, adds computers to its botnet and uses DNS over HTTPS (DoH).[2]

We wrote previously about Spelevo EK, which targets Adobe Flash Player vulnerabilities in a web browser for remote code execution.[3,4] It was discovered in March by security researcher Kafeine,[5] and at the time, we observed it delivering the Gootkit banking trojan.

https://insights.infoblox.com/
threat-intelligence-reports