



# Evolving Network Architectures and the Impact on Security

Craig Sanderson, VP Security Solutions  
Infoblox



# 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<sup>1</sup>

## Cloud

60% of web application attacks were to gain unauthorized access to cloud-based email servers<sup>2</sup>

## IoT

Half of top 12 Global exploits targeted IoT devices in Q4 2018<sup>3</sup>

## 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

Threat Landscape

---

Digital Transformation Driving New Architectures

---

Using a Foundational Approach for  
Enterprise Security

---

Market Trends in DNS Privacy



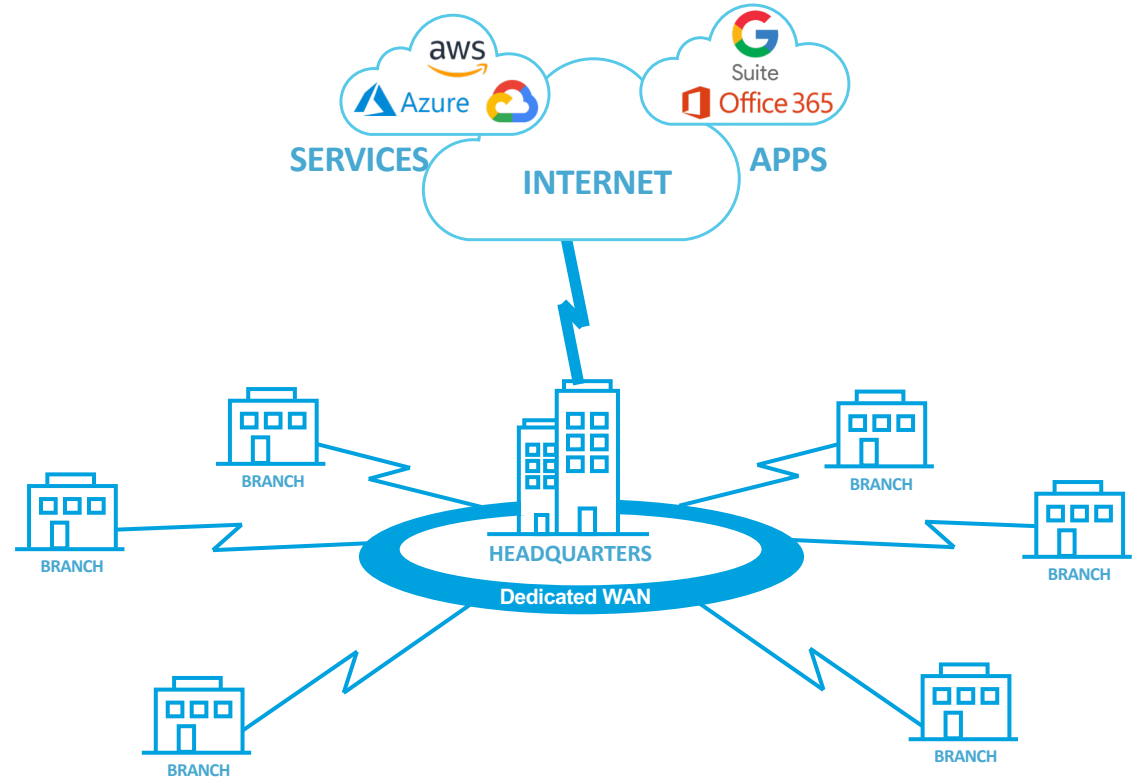
# The Traditional Architecture

Dedicated WAN circuits

Static configurations

Lack of automation

Centralized, perimeter-based security



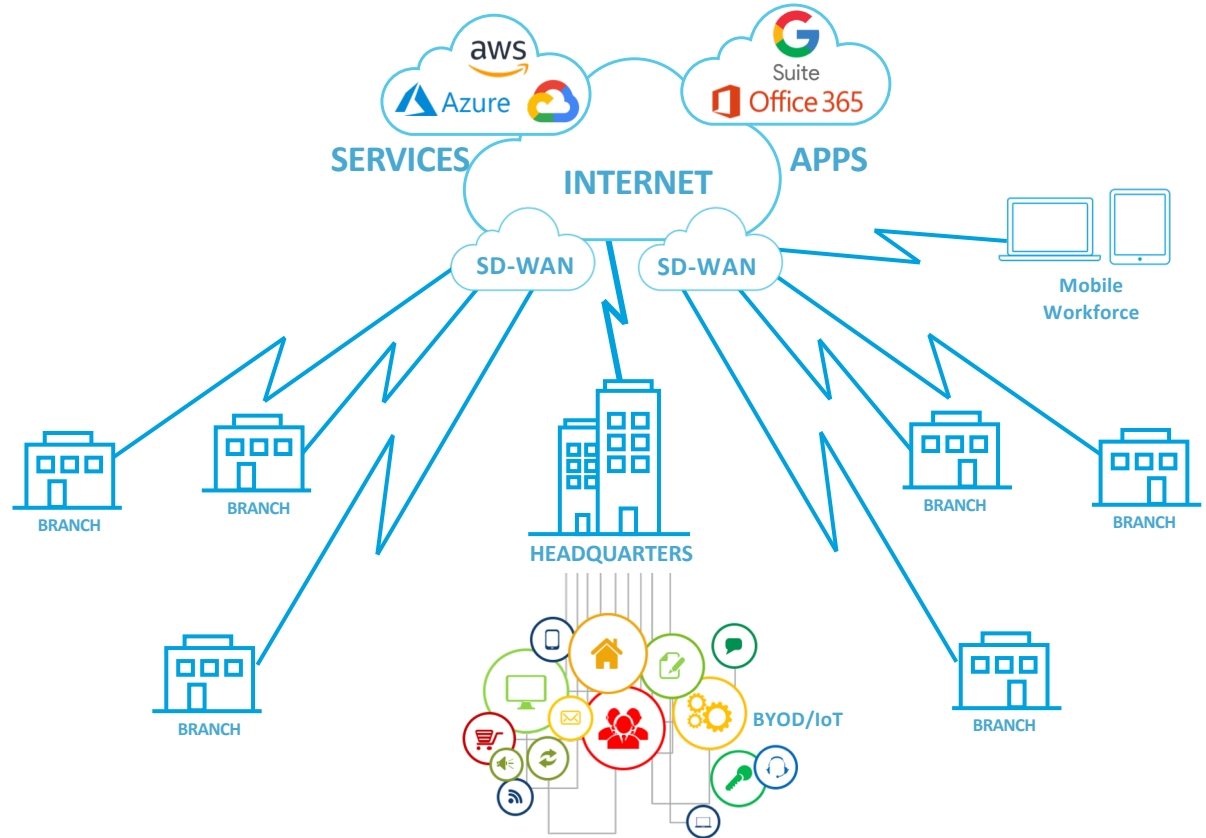
# The New Architecture: Cloud, SaaS, SD-WAN

SD-WAN for remote locations

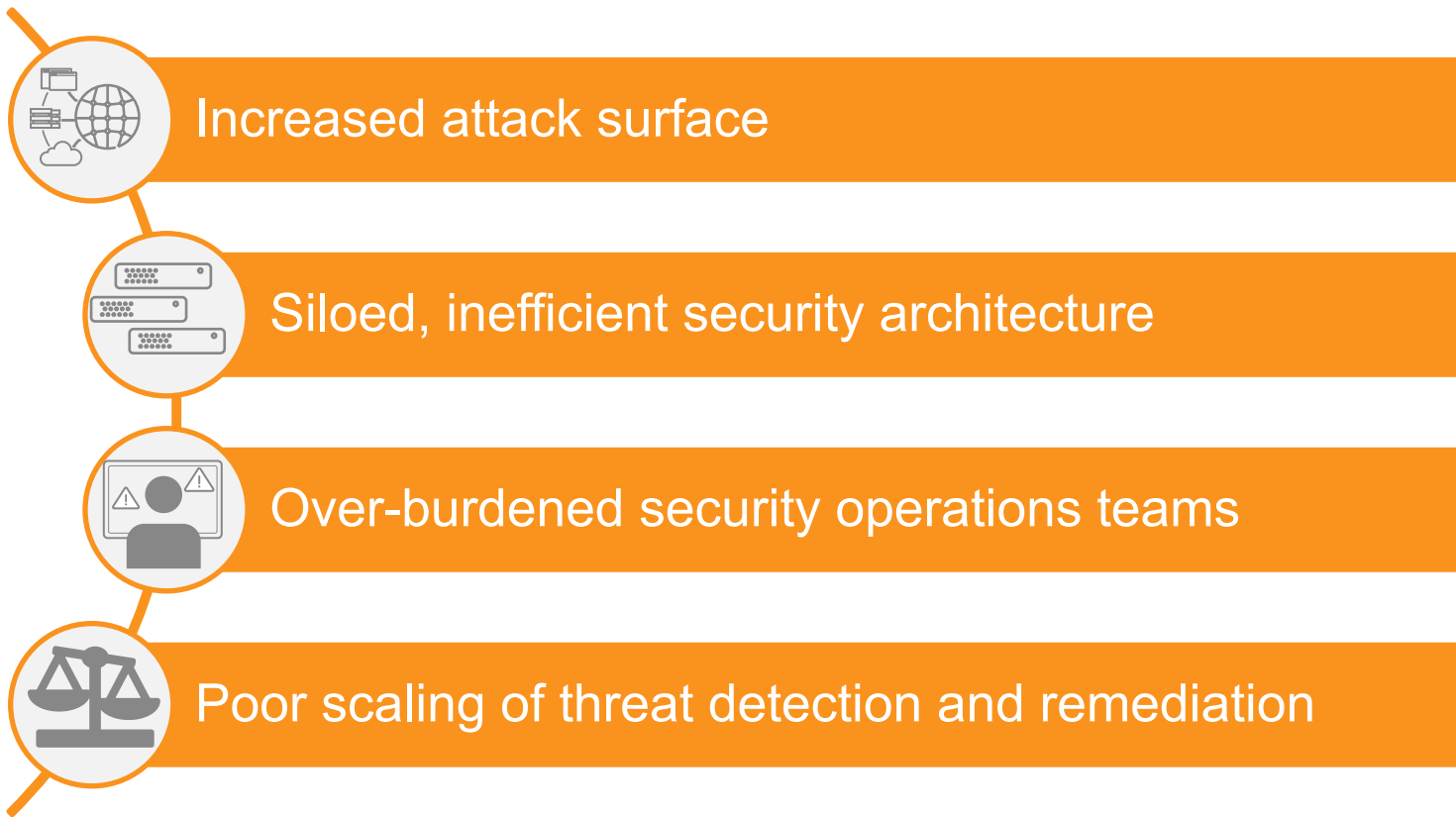
Decentralized infrastructure

BYOD/IoT

SaaS/Cloud



# Security Implications



# Foundational Services



DNS

DHCP

IP Address Management (IPAM)

DDI





# Core Foundation Elements for Any Architecture

## IP Address Management

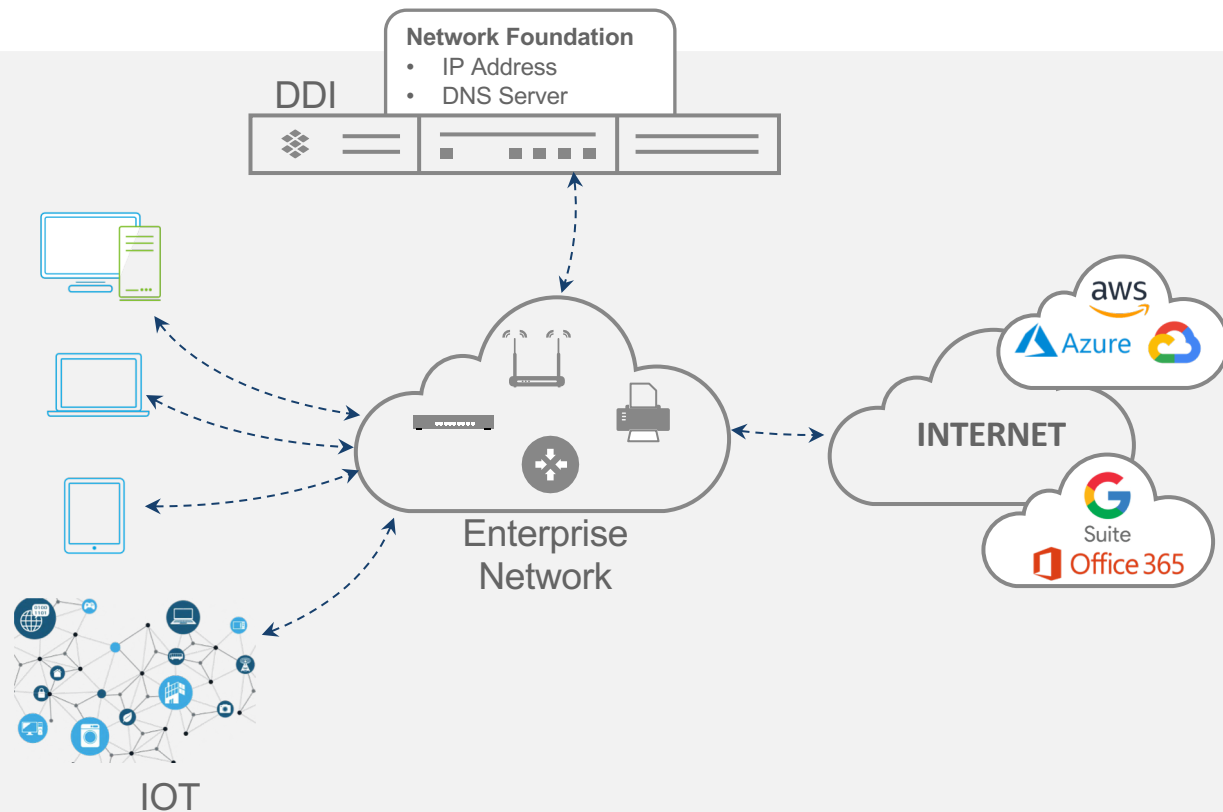
- Device IP Address
- Centrally managed
- Resolve network conflicts

## 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



# Agenda

Threat Landscape

---

Digital Transformation Driving New Architectures

---

Using a Foundational Approach for  
Enterprise Security

---

Market Trends in DNS Privacy



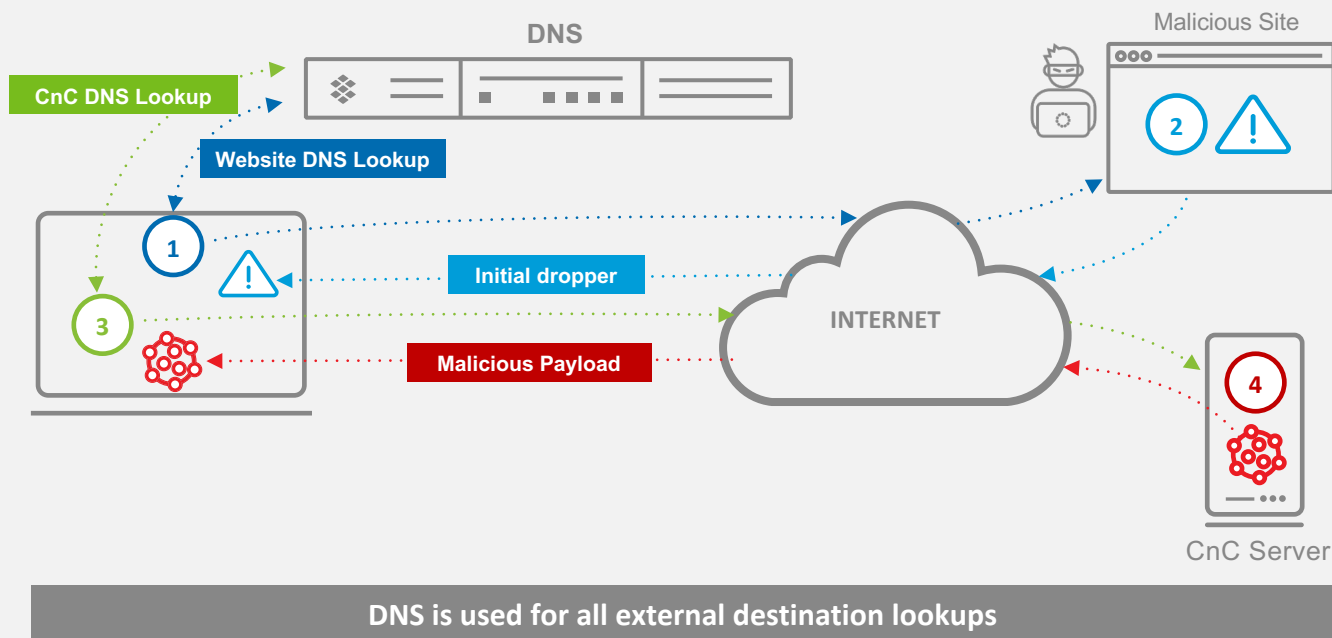
# Common Attack Steps Review

1 User directed to malicious site

2 Website delivers initial exploit

3 Exploit contacts CnC server

4 Malicious payload downloaded

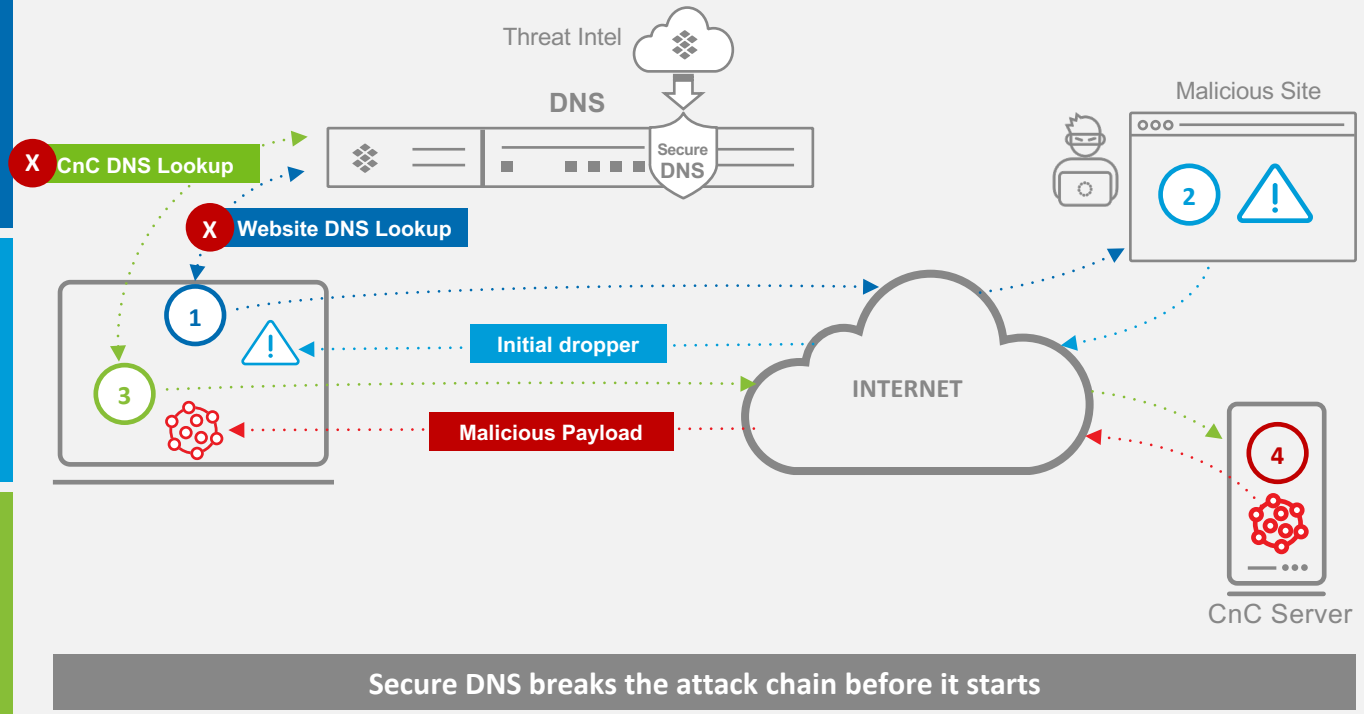


# Leveraging DNS Intelligence for Security

1 Curated threat intelligence for DNS

2 Connection to malicious website blocked at DNS

3 If already infected, CnC connection request blocked at DNS



# Optimizing Entire Security Stack

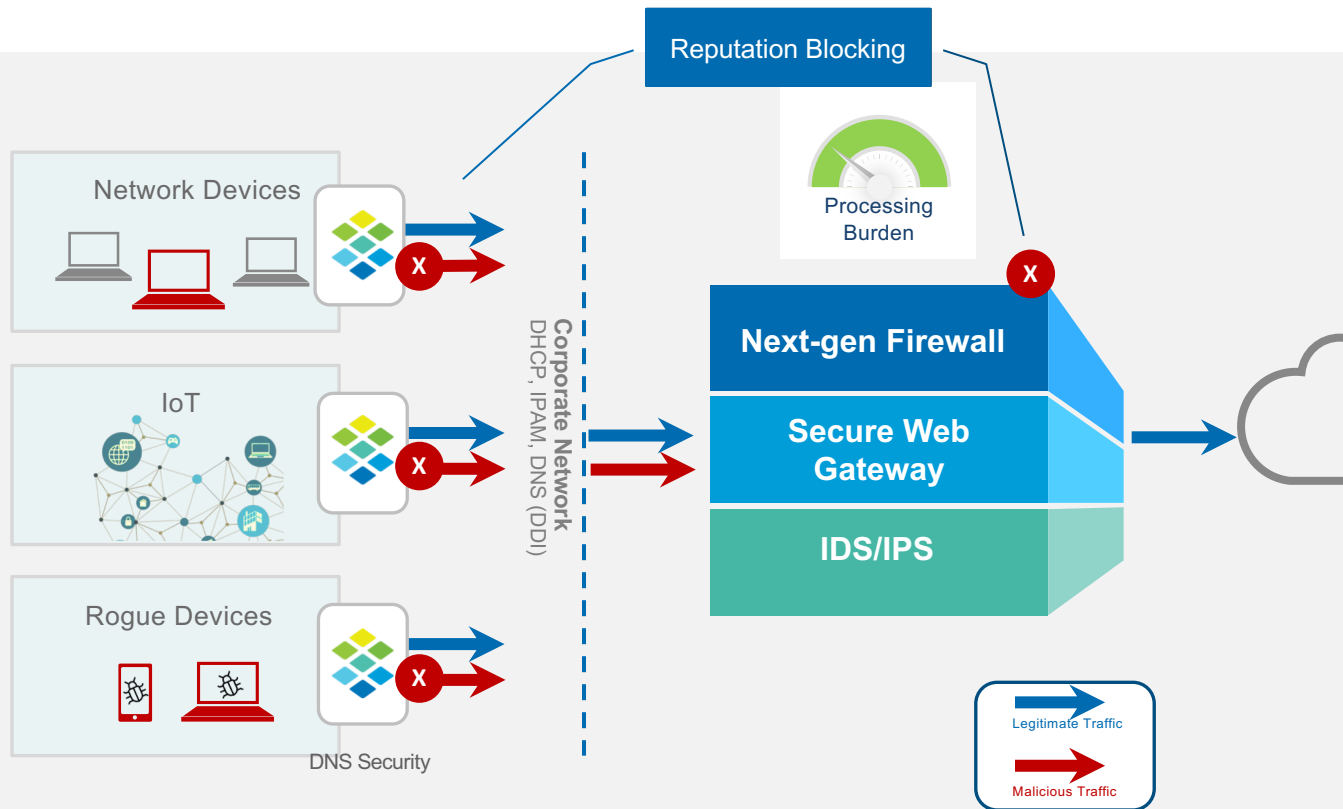
## Preserving Perimeter Security

### 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

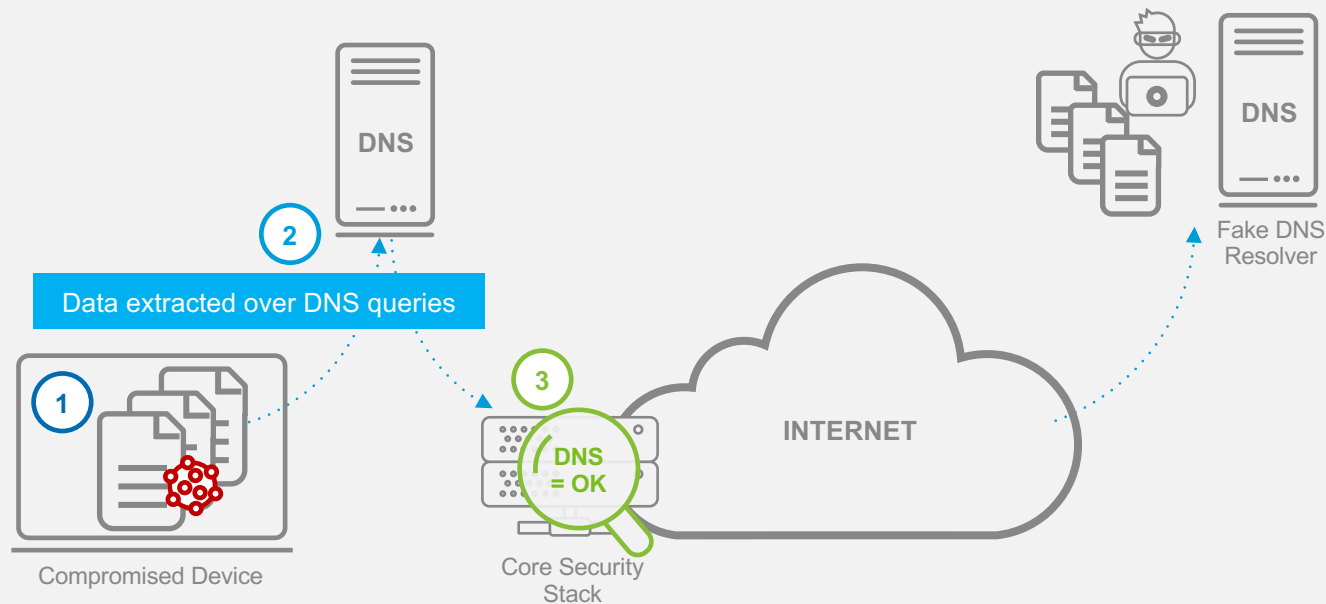


# Closing Gaps in Protection: Data Exfiltration over DNS

1 Malware seeks sensitive data on compromised device

2 Malware uses DNS channel to exfiltrate data

3 Defenses do not inspect DNS traffic



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

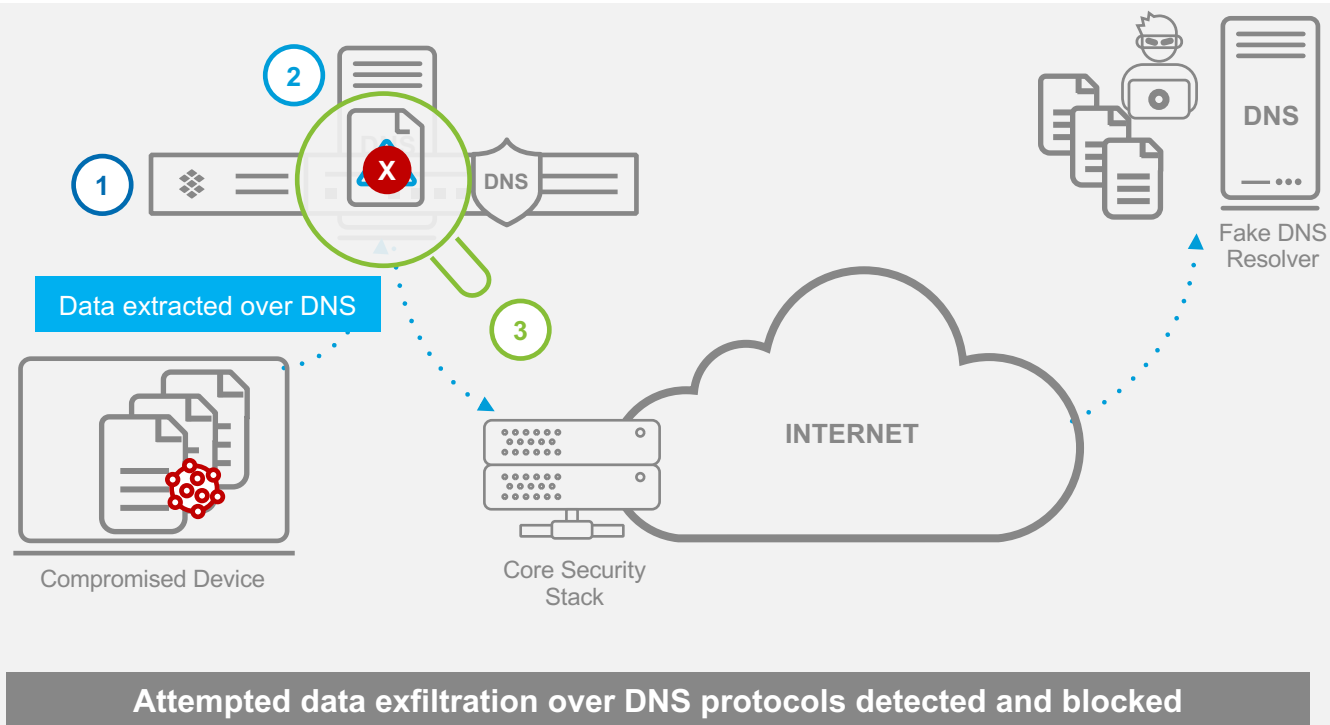


# Protecting from Data Exfiltration over DNS

1 DNS with threat intelligence and analytics

2 Machine learning analytics inspect DNS traffic for data exfiltration

3 Data secured by blocking DNS request

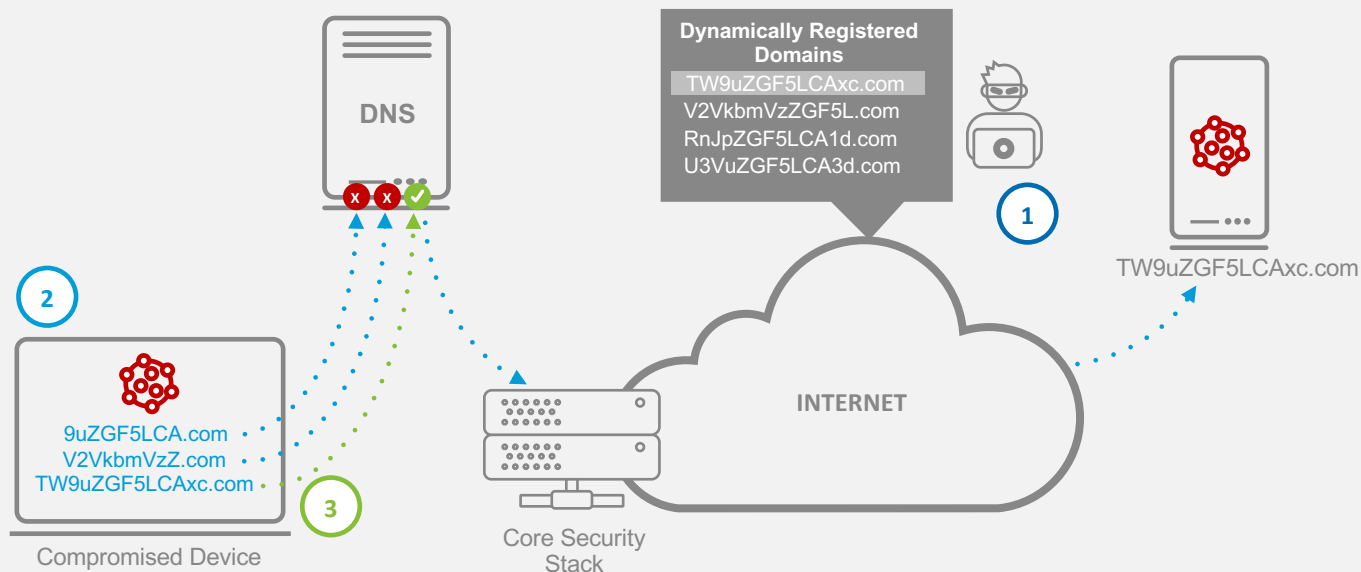


# Closing Gaps in Protection: Domain Generation Algorithms

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



Threat Intel/reputation is ineffective against this attack method



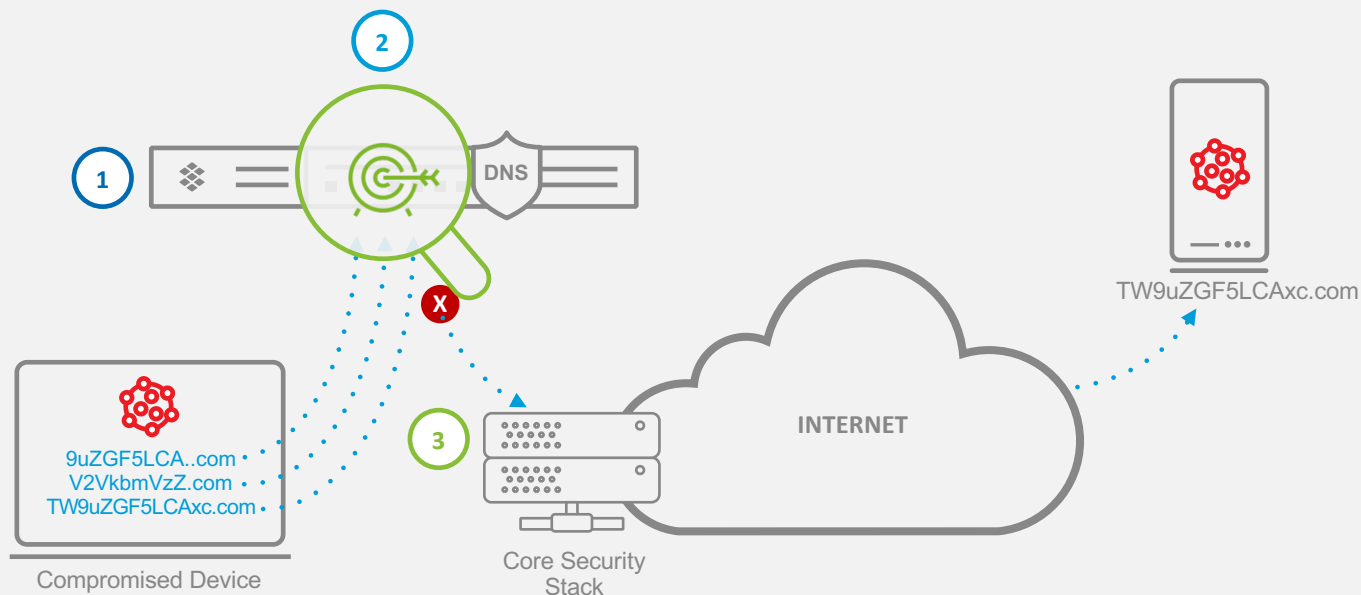


# Protecting Against Dynamically Generated Domains

1 Machine learning analytics inspect DNS queries

2 Identifies patterns that follow DGA methods

3 Block ongoing connections with the same pattern



Machine learning identifies algorithm-based domain lookups

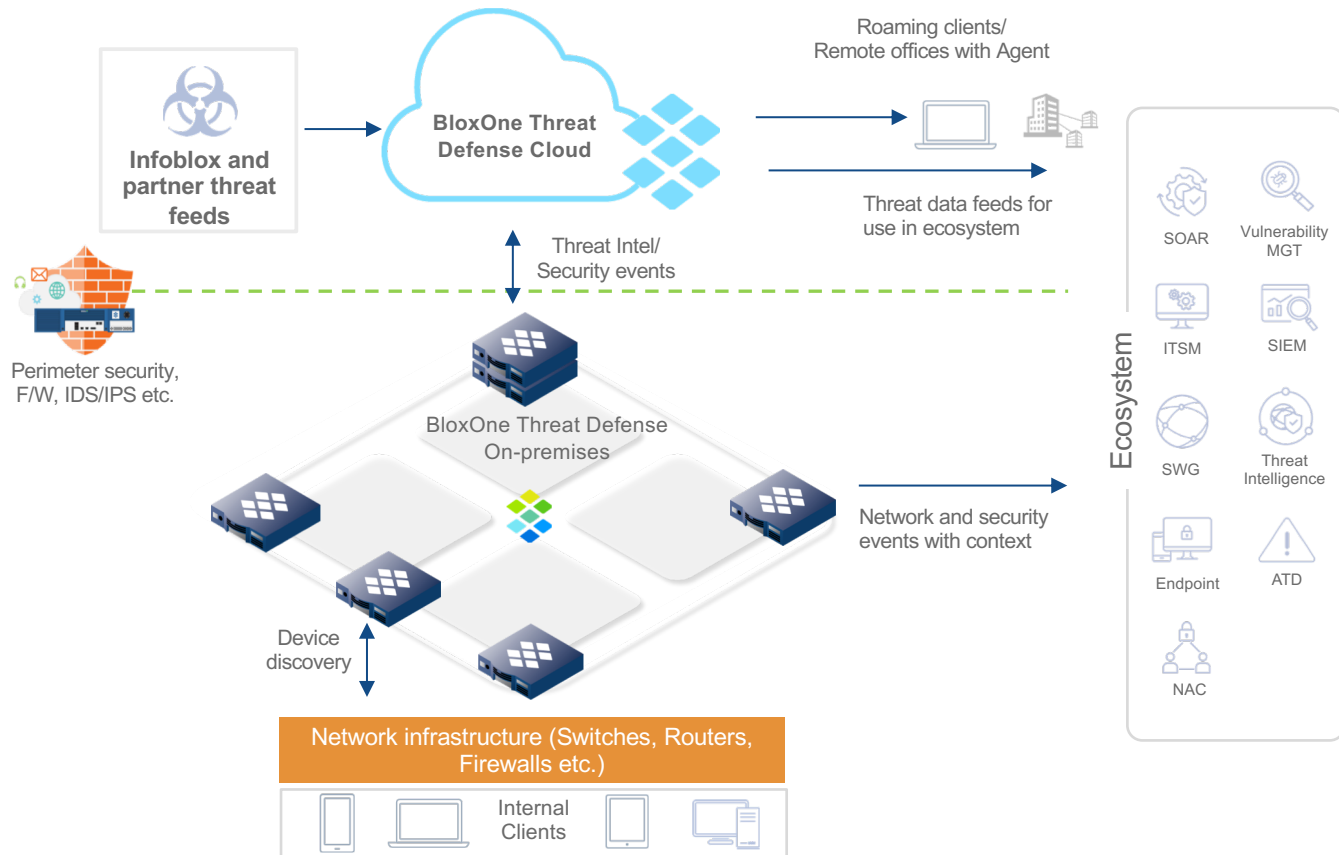


# Using a Hybrid Architecture

1 Hybrid architecture provides same protection on and off premises

2 Helps ensure resiliency and redundancy

3 Integrates with rest of ecosystem



# Agenda

Threat Landscape

Digital Transformation Driving New Architectures

Using a Foundational Approach for Enterprise Security

Market Trends in DNS Privacy

# 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



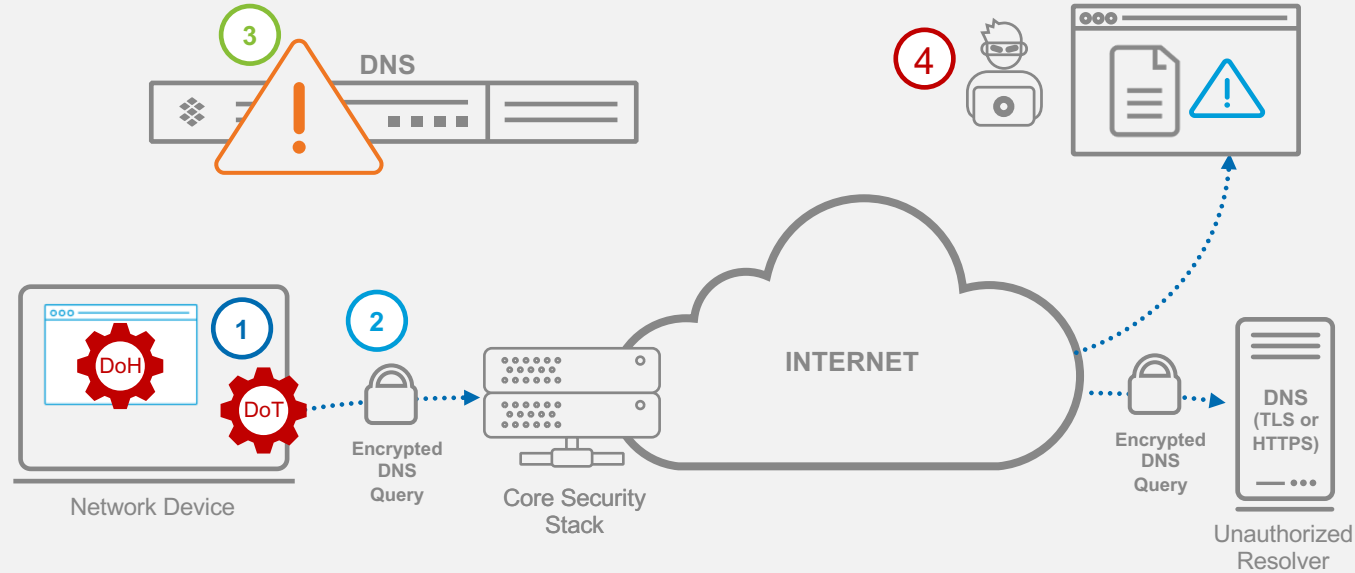
# DoT/DoH: Bypass of Enterprise DNS is a Challenge

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



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



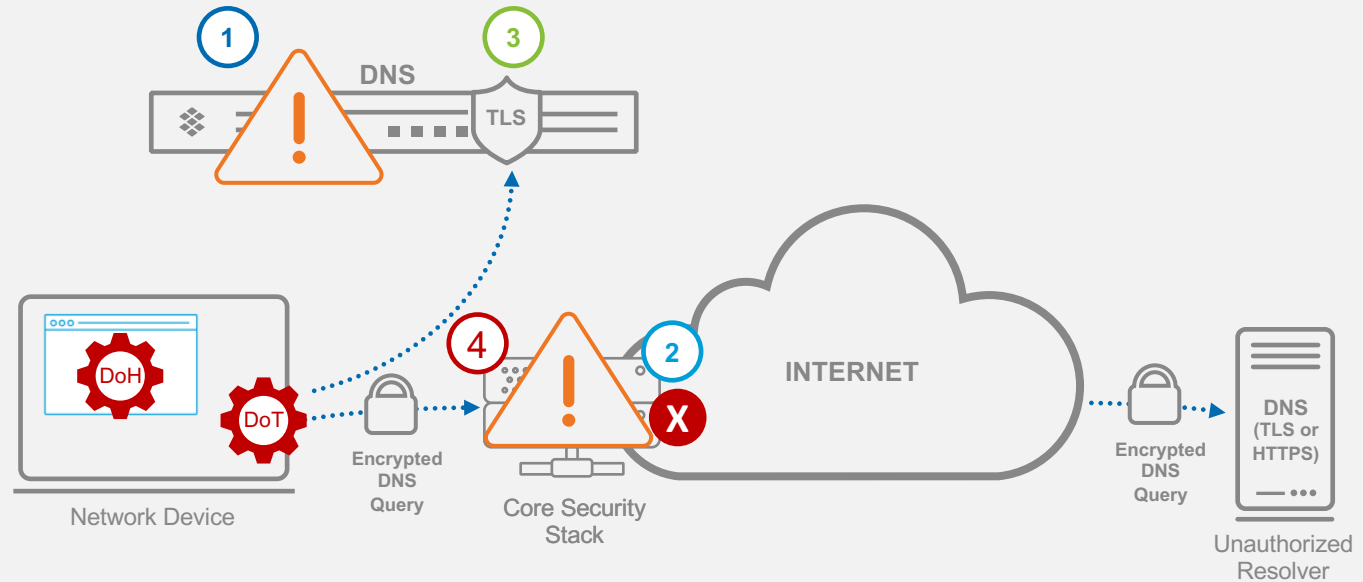
# DoT/DoH Best Practices

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



DoT/DoH Best Practices protects your users and devices



# Use Case: A National Cyber Security Center

## DNS Security Use Case:

- Protect 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)



# 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





# Next Steps: Subscribe to our Complimentary Threat Reports

- **Cyber Intel Unit has 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



**Infoblox**  
NEXT LEVEL NETWORKING

## PsiXBot InfoStealer Uses DNS over HTTPS

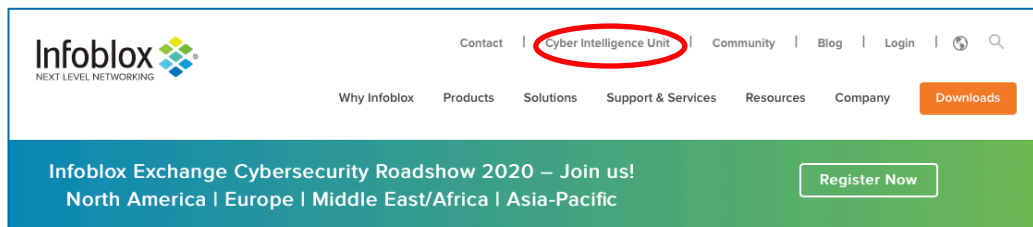
Author: Jonathan Armer

### 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).<sup>1</sup> PsiXBot steals information, adds computers to its botnet and uses DNS over HTTPS (DoH).<sup>2</sup>

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

Next →



**Infoblox**  
NEXT LEVEL NETWORKING

Contact | **Cyber Intelligence Unit** | Community | Blog | Login | 🔍

Why Infoblox | Products | Solutions | Support & Services | Resources | Company | Downloads

Infoblox Exchange Cybersecurity Roadshow 2020 – Join us!  
North America | Europe | Middle East/Africa | Asia-Pacific

Register Now

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



# Q & A

