Controlware Security Day 2022

Cyberrisk - die unterschätzte Gefahr im DNS

DNS enthält einzigartige Sicherheitseigenschaften, die oftmals übersehen werden oder völlig unbekannt sind

Infoblox

Marcom V1.1 2019

Infoblox

Cyberrisk - die unterschätzte Gefahr im DNS

DNS enthält einzigartige Sicherheitseigenschaften, die oftmals übersehen werden oder völlig unbekannt sind

Prepared by: Stephan Fritsche

Infoblox

Stephan Fritsche
Central Europe Security Lead
Mobil: +49 170 58 52 443
sfritsche@infoblox.com
www.infoblox.com

https://www.infoblox.com/products/bloxone-ddi/
https://www.infoblox.com/products/bloxone-threat-defense/

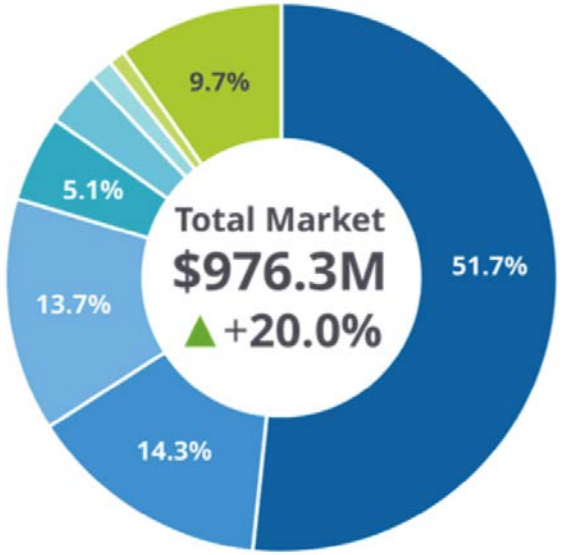
Leading the Industry

MISSION

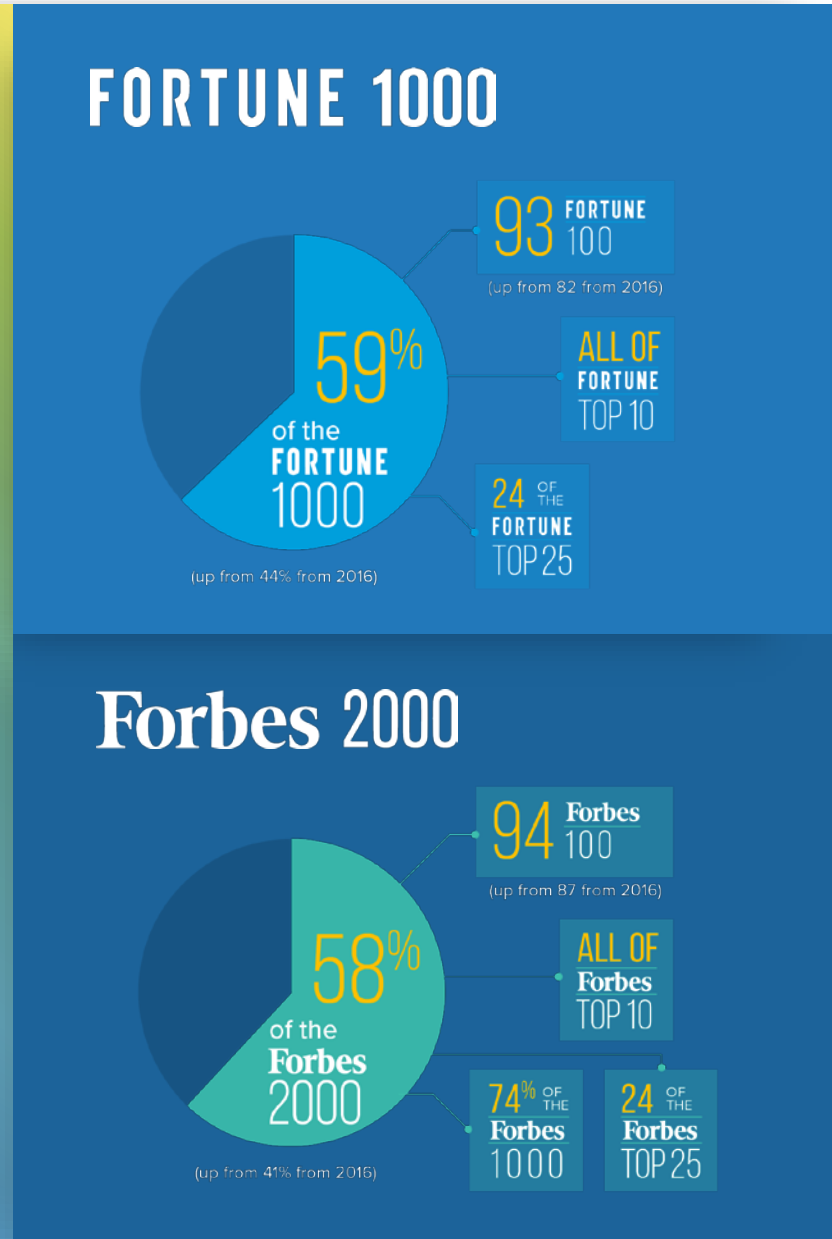
Empowering organizations to manage their continuously evolving growing networks simply and securely.

OFFERINGS

Core Network Services, Cybersecurity, Secure Edge Services



Worldwide DDI Market Shares, 2020



Infoblox Overview

Cloud-first Network Experience

CORE MARKETS

DDI

DNS | DHCP | IPAM

Deliver business-critical network services

Security

Protect the business in new threat landscape

Edge

Deploy secure edge services at scale

PRODUCT PORTFOLIO

Network Service & Protocol Delivery (DDI)

- Application Load Balancing (DTC)
- Reporting • Network Visibility and Configuration Management
- Network Intelligence

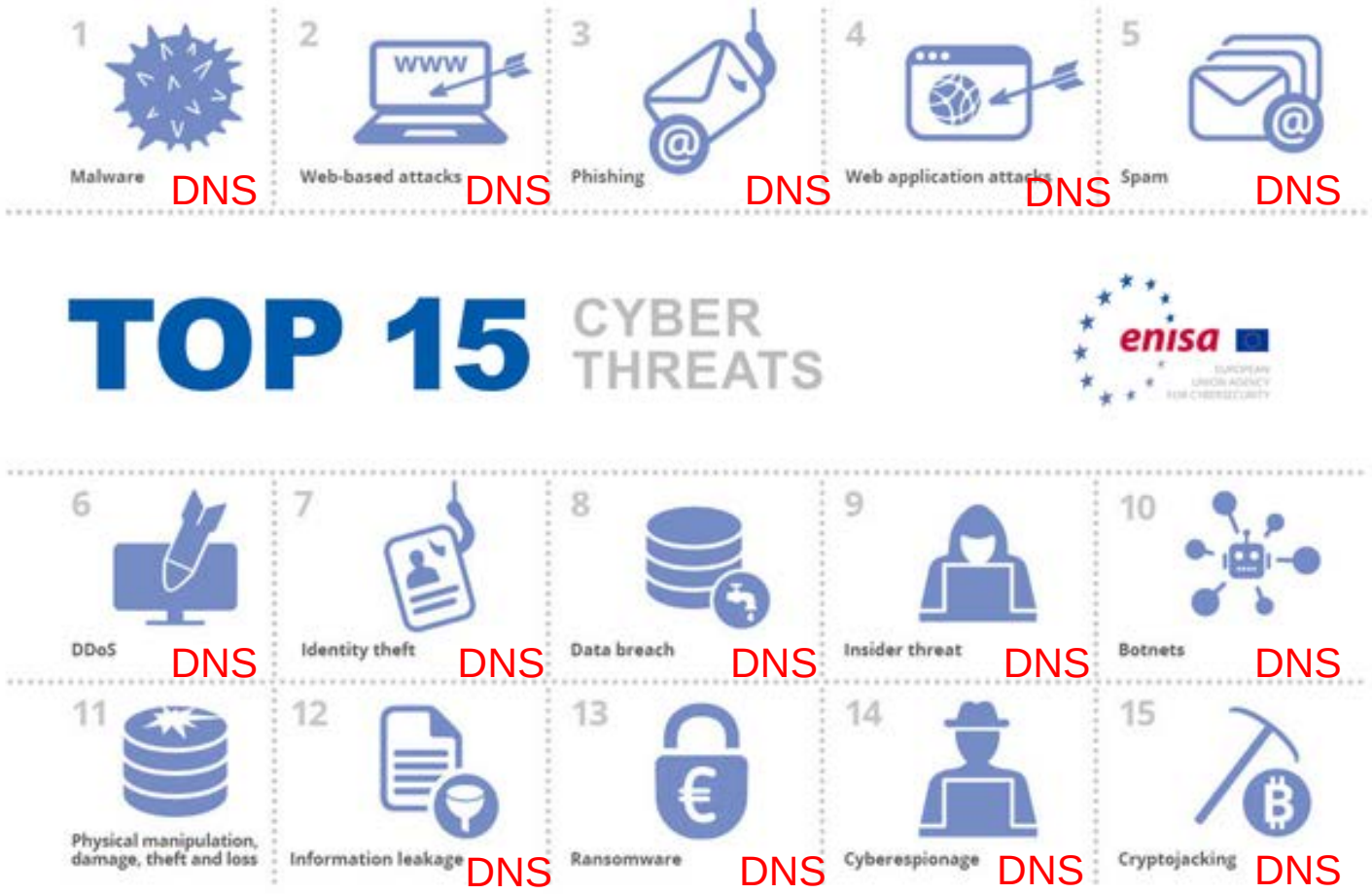
Strengthen and Optimize Security Posture

- Security visibility and discovery
- Detect and block modern malware, data exfiltration
- Threat Intelligence Optimization
- Ecosystem Enrichment, Security Automation and Orchestration
- Infrastructure Protection (ADP)

Cloud-native network and security services

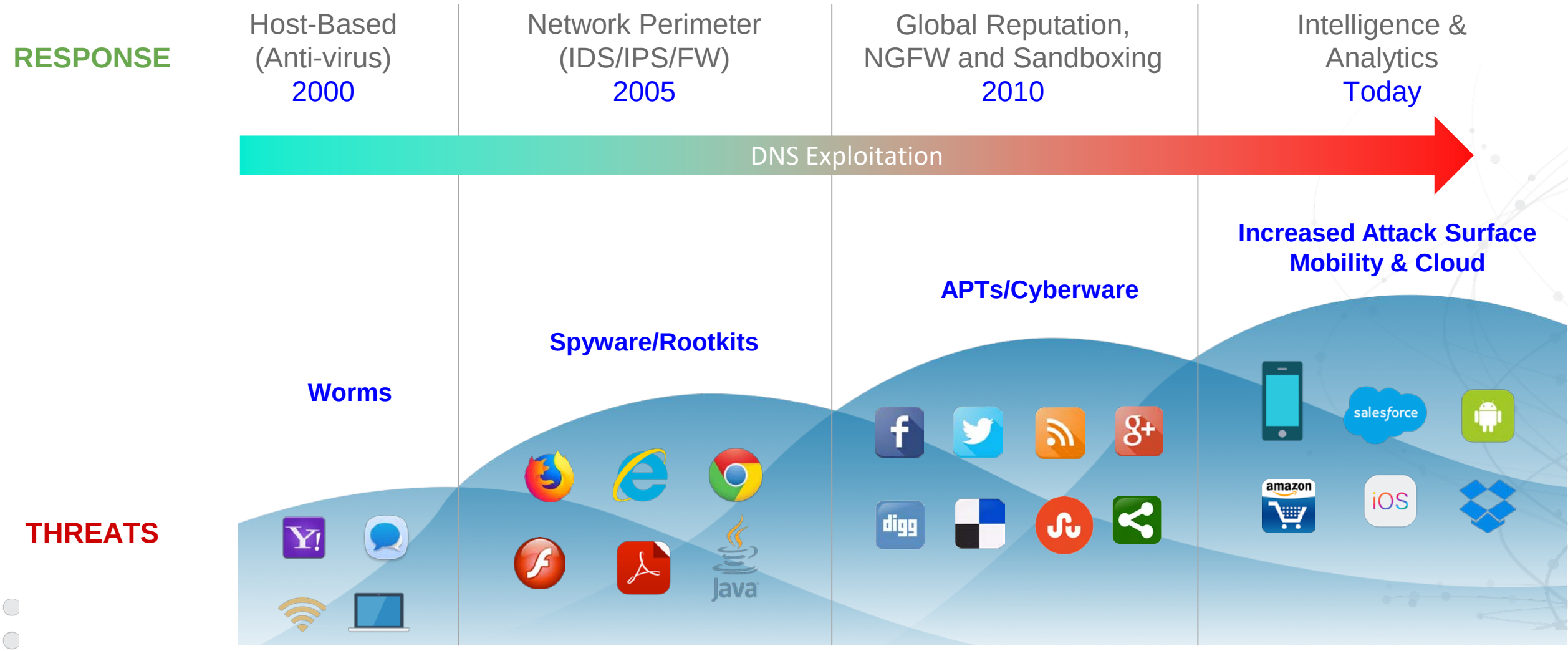
- SaaS based delivery of DDI and adjacent network/security services
- Agility and scale
- On-premise or As-a-service
- Cloud managed simplicity

ENISA (European Union Agency for Cybersecurity)
Threat Landscape 2020 - Insider Threat Report



https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

The Threat Landscape Evolution

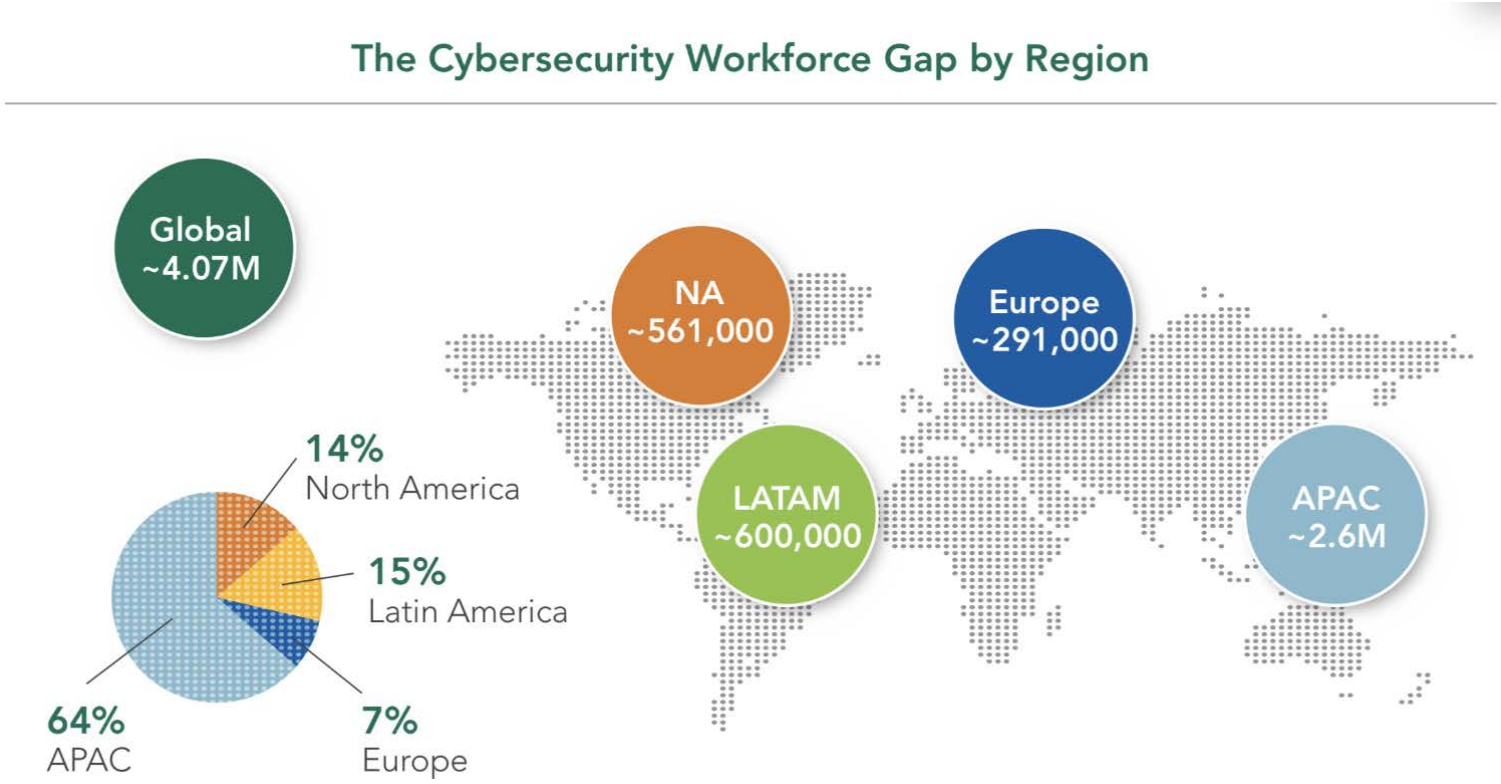


And Throwing More People at the Problem is not Possible

92% of companies get more than 500 alerts per day; a single cyber analyst can handle only 10

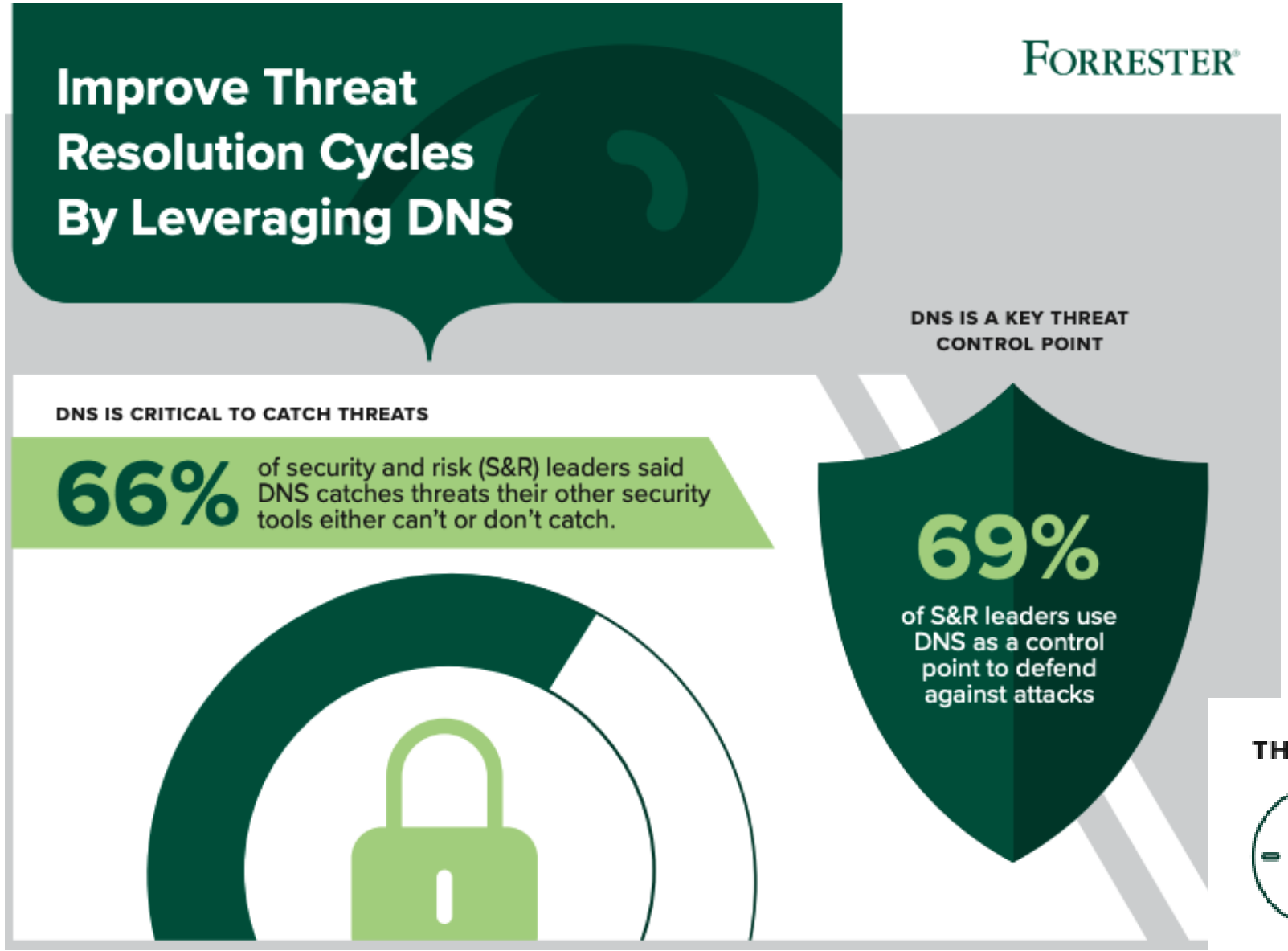
4% of alerts, only, are investigated; not enough humans to keep organizations safe

30+ security tools in operation, with staff and expertise to manage 12



ISC2 Cybersecurity Workforce Study, 2019

Forrester Research Paper Key Findings (July 2020)



THREAT INVESTIGATIONS TAKE TOO LONG

74% of security operations teams spend more than 4 hours investigating a single threat incident.

https://info.infoblox.com/resources-whitepapers-accelerate-threat-resolution-with-dns

How DNS is used by malware?

1

Reconnaissance

Harvesting email addresses, conference information, etc.

DNS Reconnaissance

2

Weaponization

Coupling exploit with backdoor into deliverable payload

3

Delivery

Delivering weaponized bundle to the victim via email, web, USB, etc.

DNS Resolution
DNS Infiltration

4

Exploitation

Exploiting a vulnerability to execute code on victim's system

DNS Protocol Anomalies
DNS Exploits
DNS Hijacking

5

Installation

Installing malware on the asset

6

Command & Control (C2)

Command channel for remote manipulation of victim

DNS Resolution
DNS Callback
DNS Tunneling

7

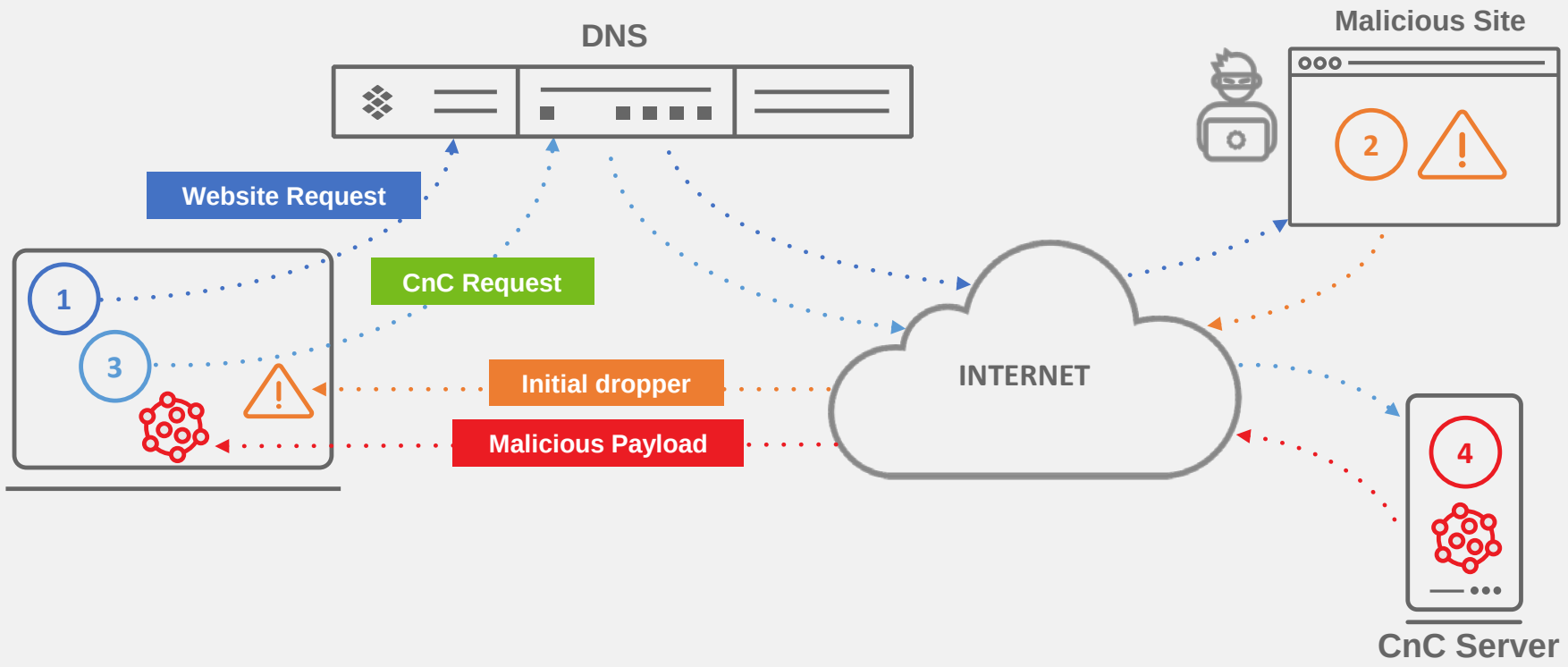
Actions on Objectives

With "Hands on Keyboard" access, intruders accomplish their original goal

DNS Tunneling
DNS Exfiltration
DNS DDoS

Common Attack Steps Review

1. User directed to malicious site
2. Website delivers initial exploit
3. Exploit contacts Command and Control (CnC) server
4. Malicious payload downloaded

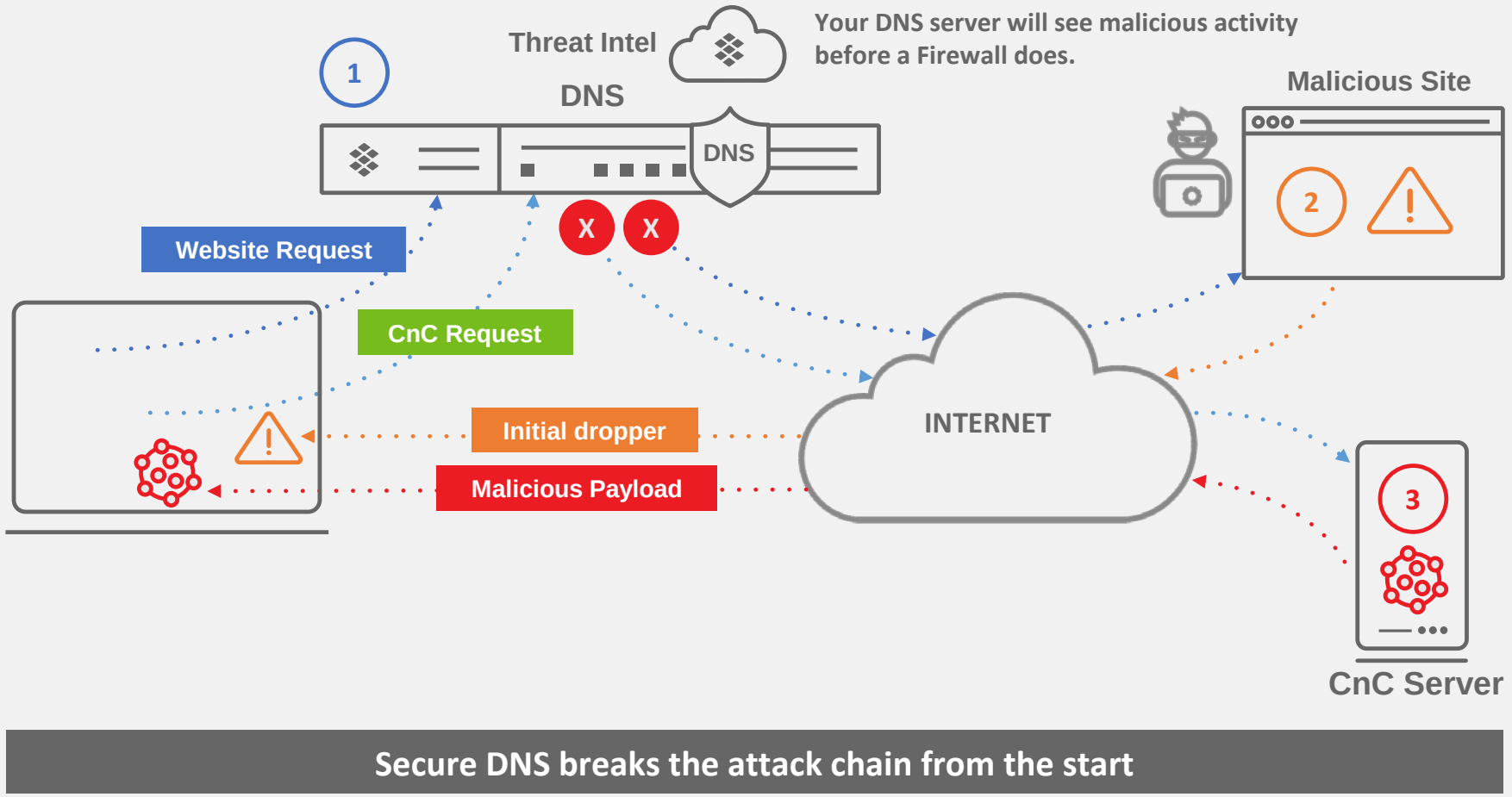


DNS is used for all outbound traffic requests

 |

Leveraging DDI Intelligence for Foundational Security

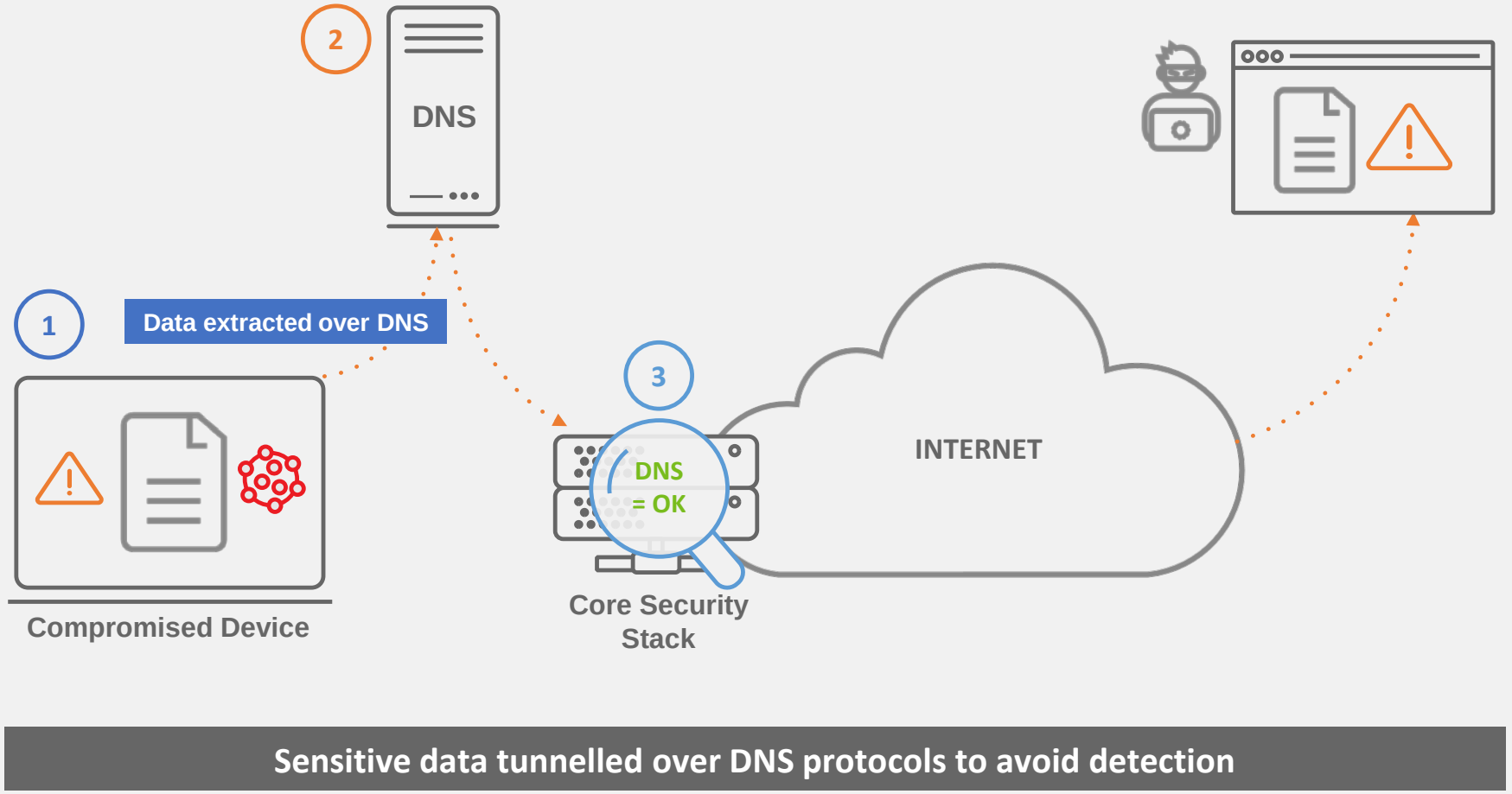
1. Curated threat intelligence for DNS
2. Connection to malicious website blocked at DNS
3. If already infected, system blocked from connecting to CnC at DNS



Secure DNS breaks the attack chain from the start

Data Exfiltration over DNS

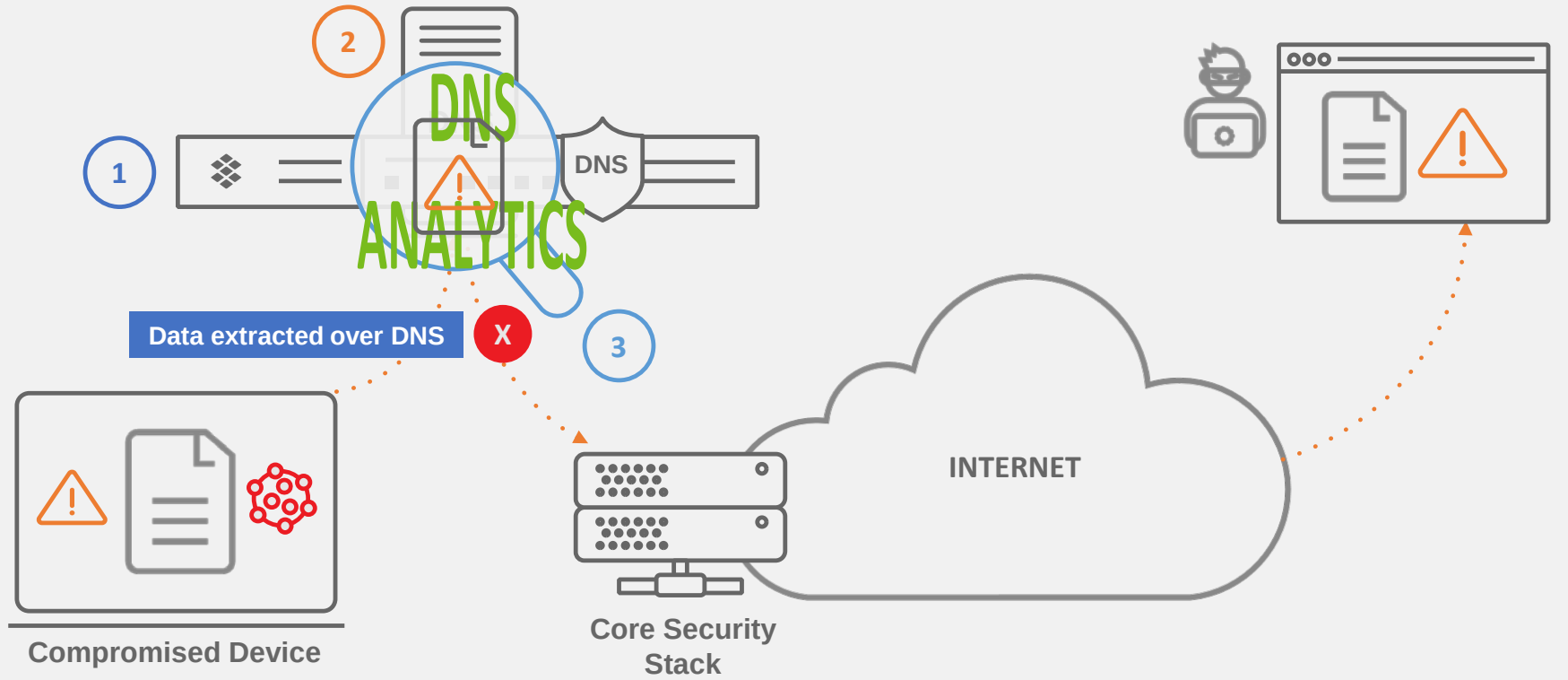
1. Malware on device seeks sensitive data
2. Malware uses DNS channel to send data
3. Traditional security does not inspect DNS traffic



Sensitive data tunnelled over DNS protocols to avoid detection

Protecting Against Data Exfiltration over DNS

1. DNS with threat intelligence and analytics
2. Machine learning analytics inspects DNS traffic, detects data exfil
3. Data prevented from exiting enterprise by blocking DNS request to destination

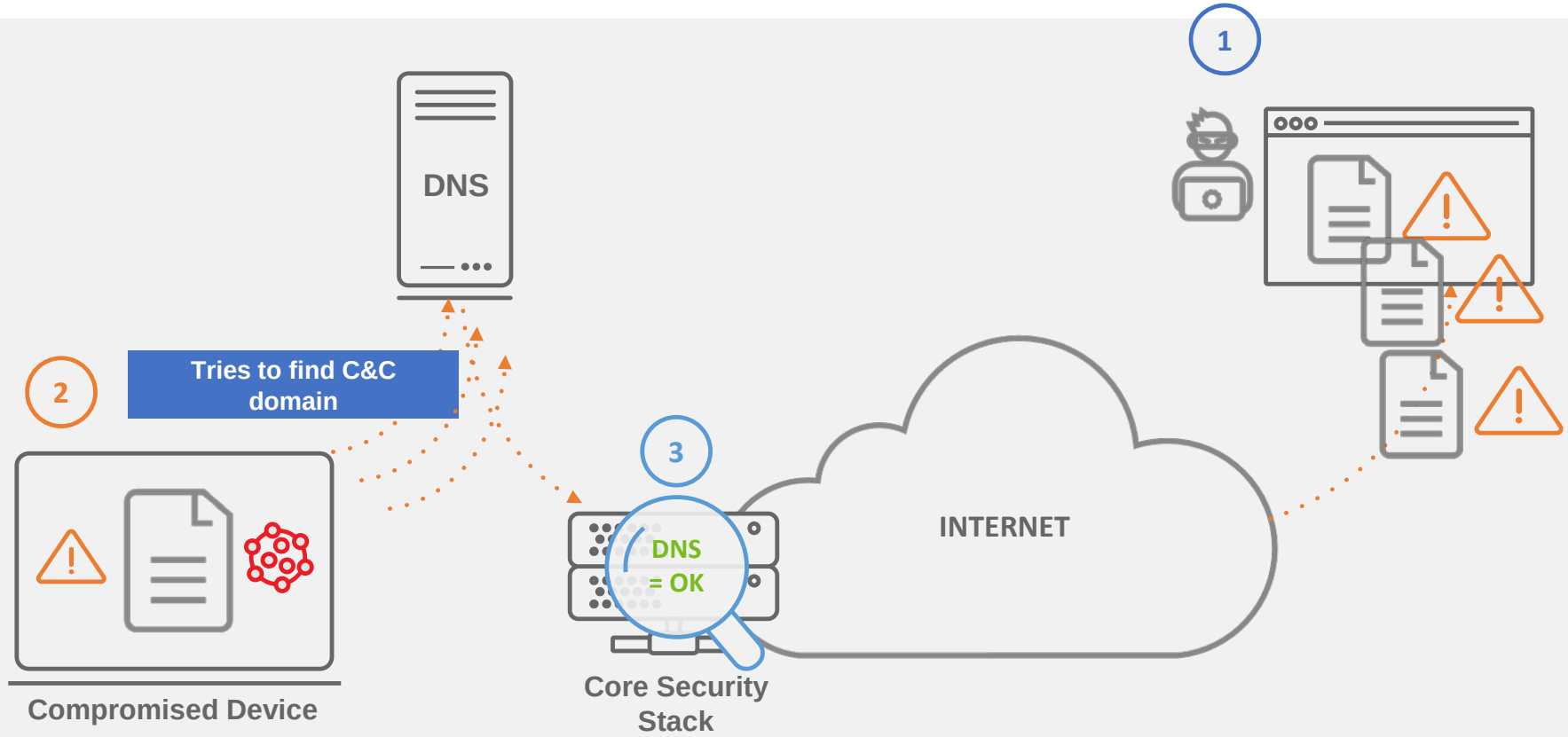


Attempted data exfiltration over DNS protocols detected and blocked

 |

Dynamically Generated Domains

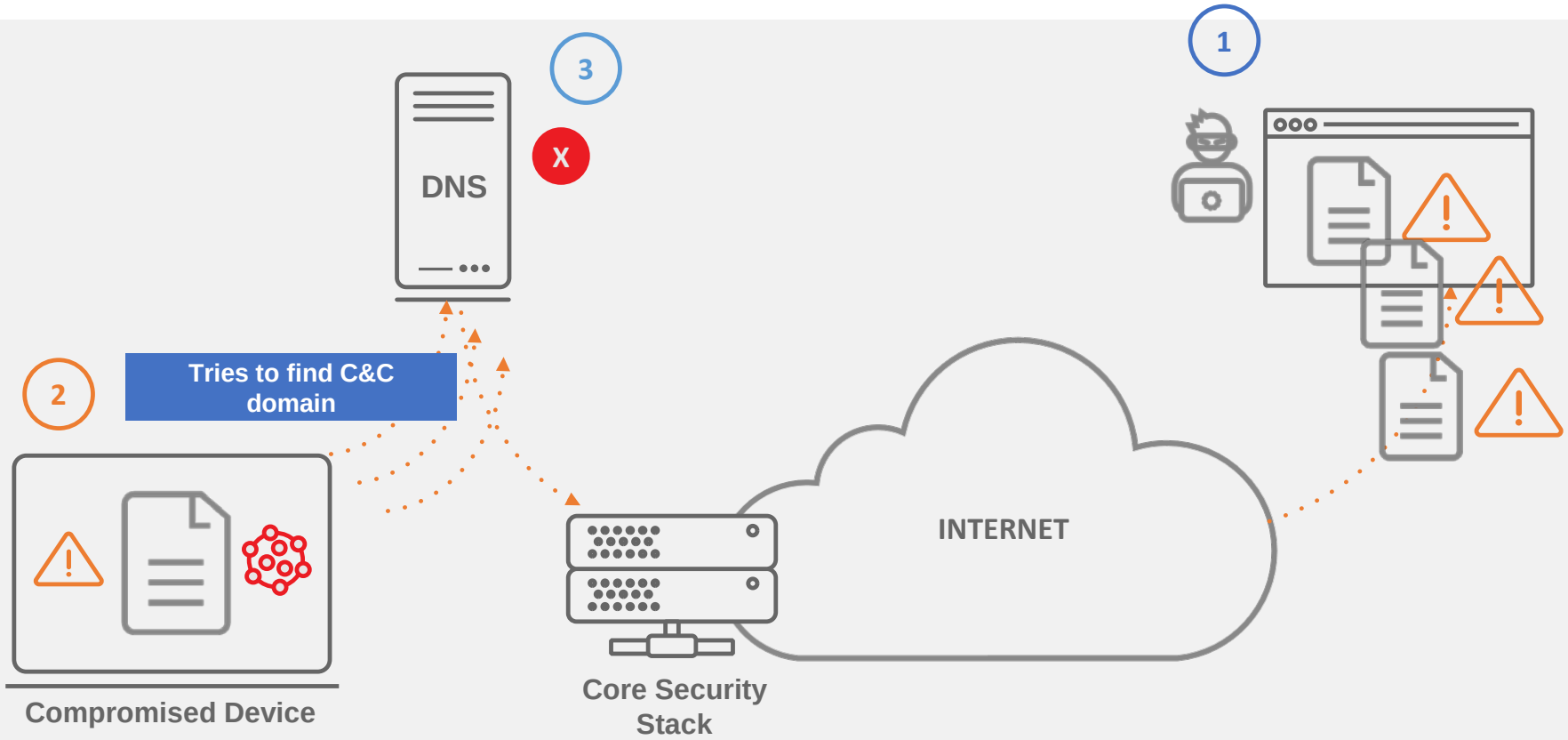
1. Attacker uses an algorithm to register lots of domains
2. Malware infected device reaches out to these domains
3. Malware gets a match



 |

Dynamically Generated Domains Best Practices

1. Attacker uses an algorithm to register lots of domains
2. Malware infected device reaches out to these domains
3. Infoblox notices pattern with mashin learning and blocks further tries.



 |

DoT & DOH

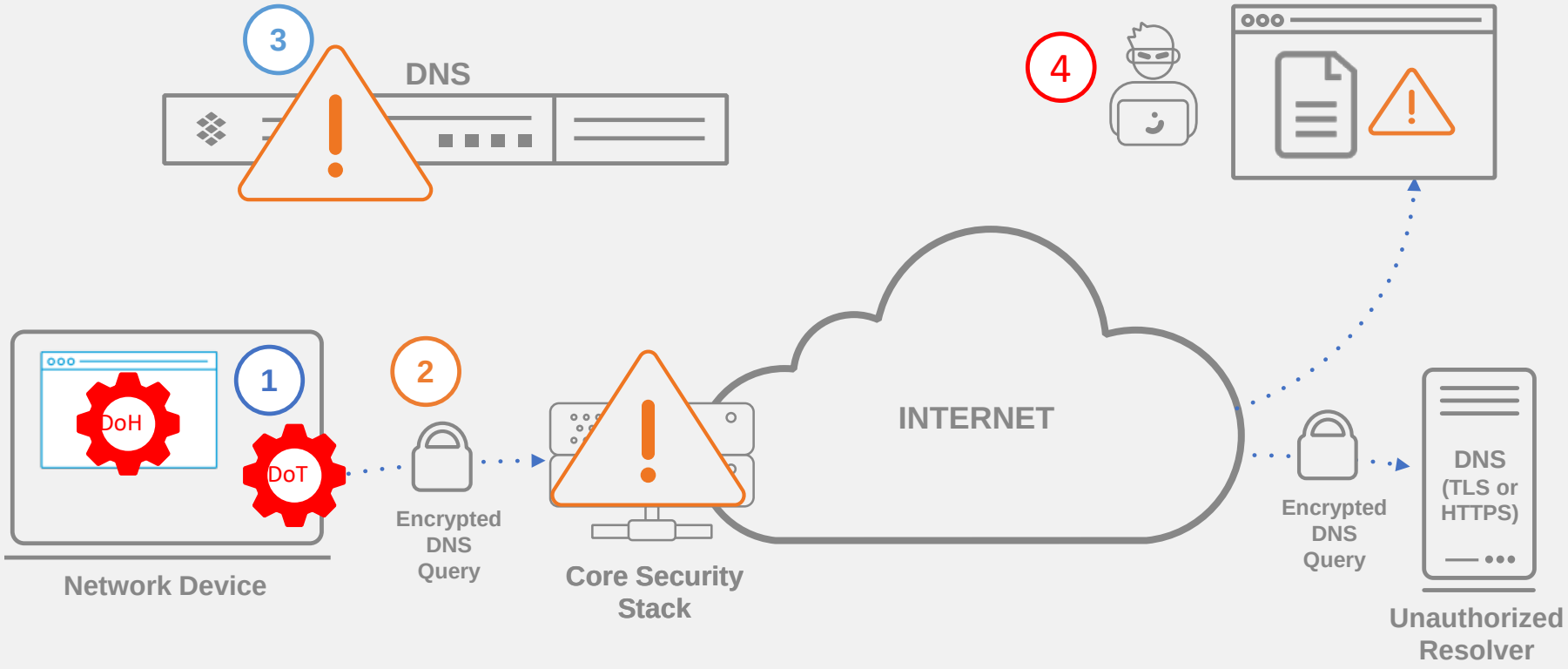
- Two evolving improvements to DNS privacy have recently made the news:
  - DNS over TLS (Transport Layer Security) or "DoT”
  - DNS over HTTPS or "DoH”
- Mechanisms promote consumer privacy but allow users to circumvent established enterprise DNS controls.
  - Exposure to data exfiltration and malware proliferation

Privacy

Security

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

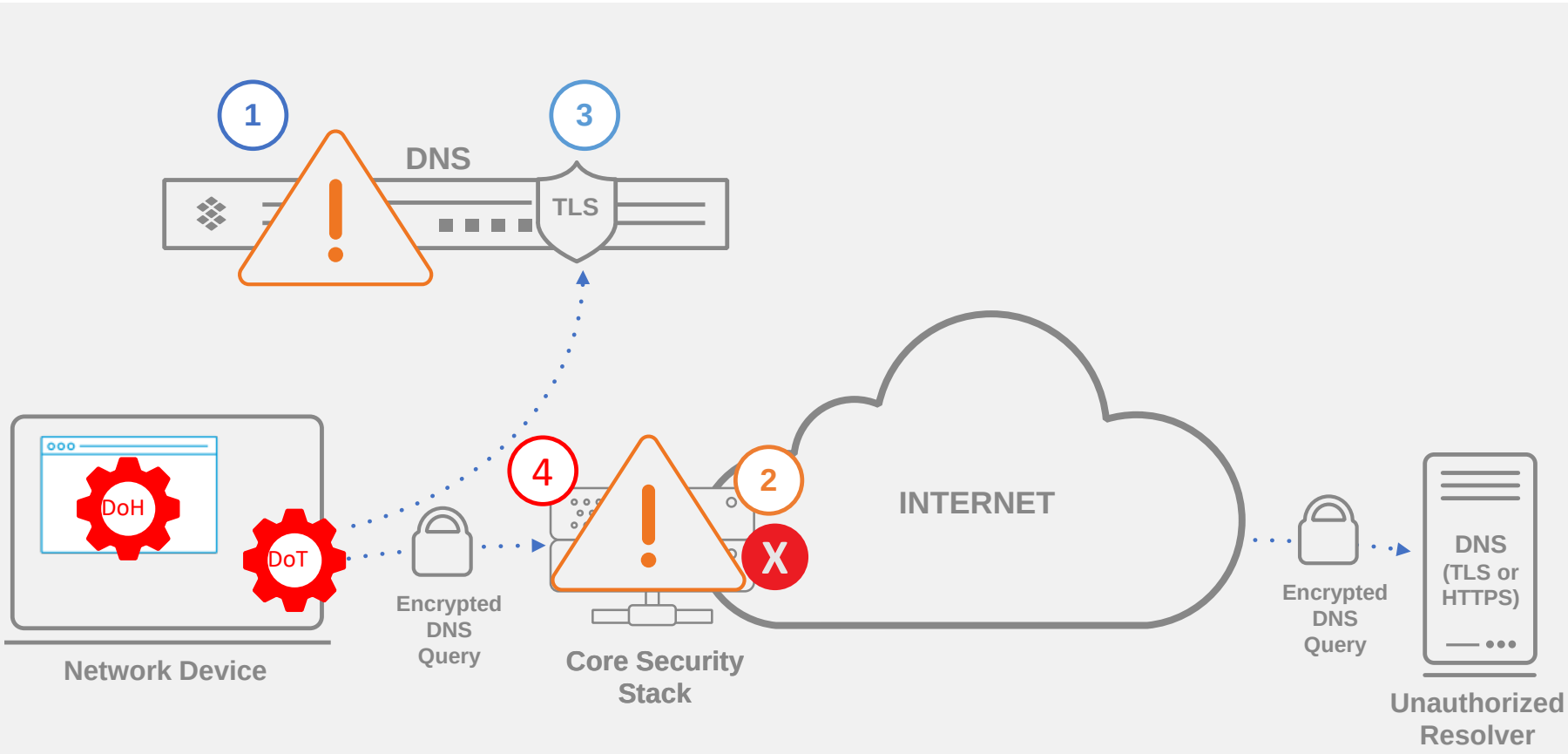


DoT/DoH "HIDES" DNS traffic from your security tools

 |

DoT/DoH Best Practices

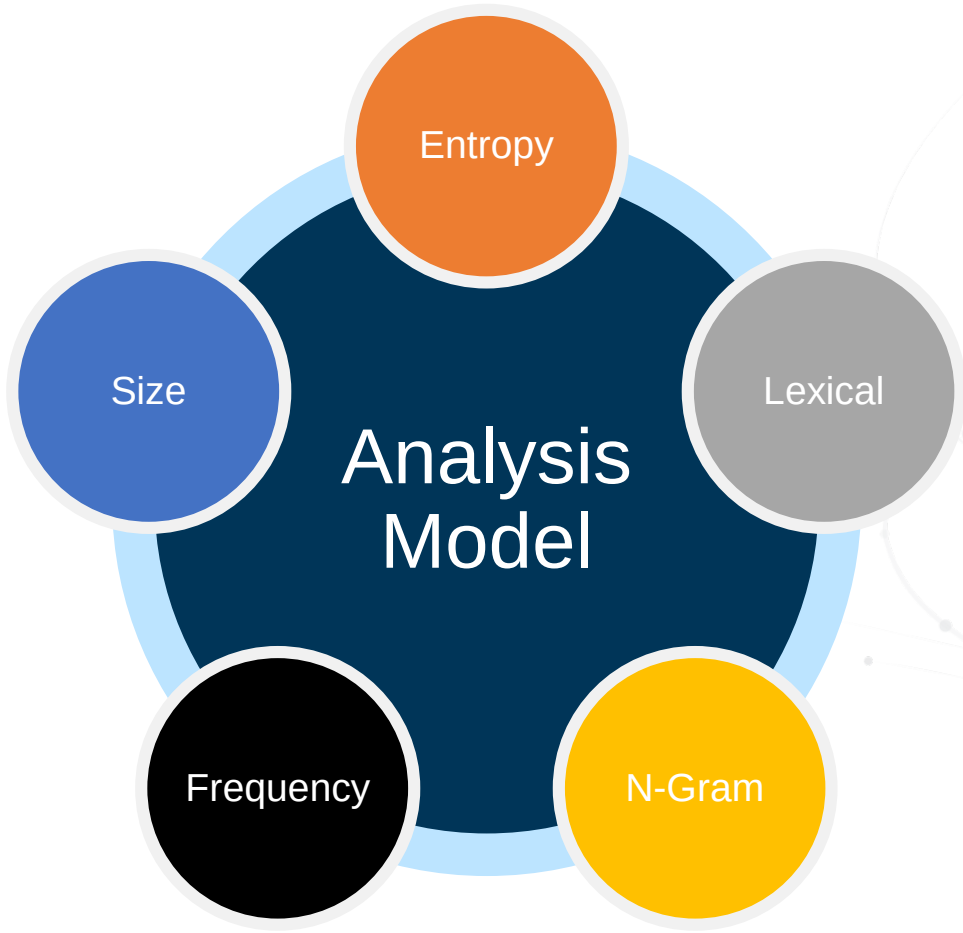
1. **Circumventing internal DNS is a bad idea**
2. **Block Access to unauthorized DNS servers**
3. **Use internal DNS vendor that supports DoT to retain control and security**
4. **Block DoH using Threat Intel List of Canary and unauthorized resolvers**



DoT/DoH Best Practices protects your users and devices

Threat Intelligence (Purpose Built for DNS) + Analytics + Infoblox Cyber Intelligence Unit = Advanced Threat Detection

- **Behavioral Models - Machine learning based analytics**
  - DNS Data Exfiltration
  - DGA, Fast Flux, Allowlist
  - Fileless Malware, Zero-day
- **High accuracy IOCs**
  - Extensive IOC collection network
  - Reverse engineering, hunting
  - High accuracy scoring algorithms
  - Protection against modern malware - ransomware, malware C&C, phishing, exploit kits, APTs
- **DNS Attack Signatures**
  - Secure the name service from protocol attack
  - Protect against protocol misconfiguration



BloxOne® Threat Defense Advanced

Unified Reporting

Cloud Services Portal

Ecosystem I/O APIs

Data Connector

Threat Insight Behavioral

Reputational Threat Intel

DNS Firewall

Cloud/On-Prem/Hybrid

Dossier Threat Research

TIDE Intel Sharing

Globally available recursive DNS and web filtering

OnPrem
Infoblox Grid

Cloud
Public, private

Endpoint
Client

Remote Office
DNS Forwarding Proxy

SIEM

Vuln Scanner

Firewall

TIP

Etc……

• Contextual Intelligence

• Infrastructure Load
• Alerts

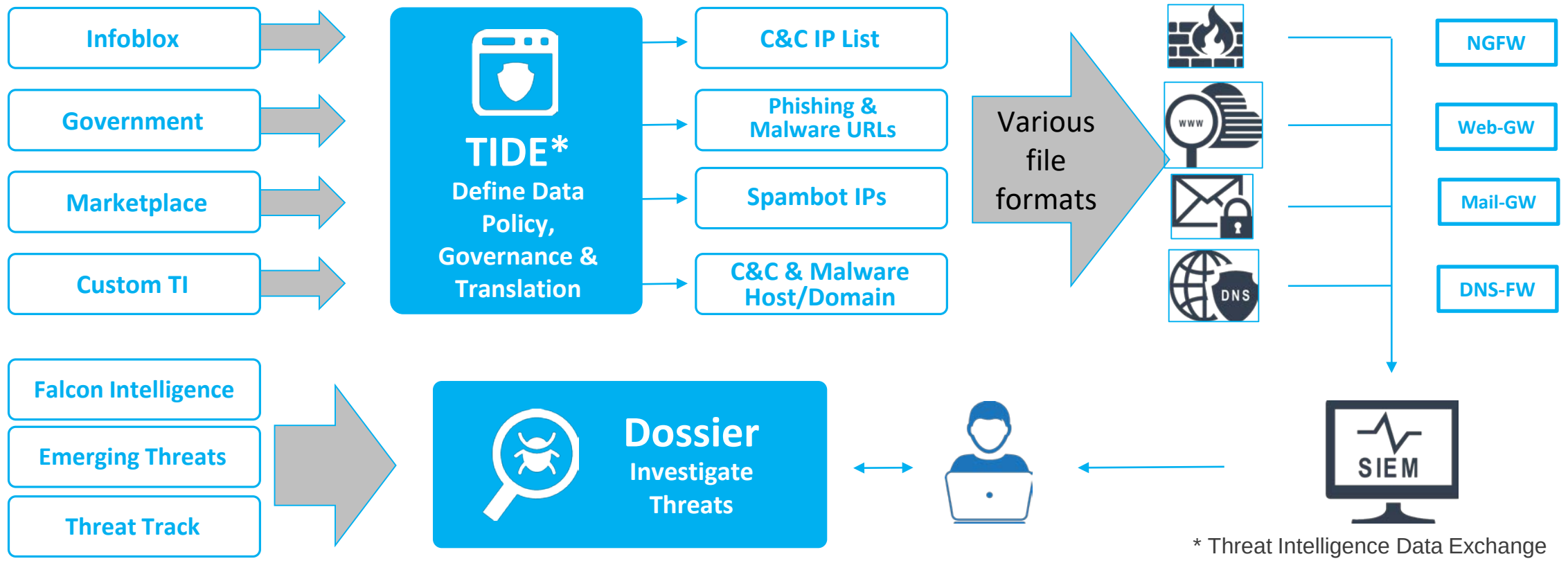
 |

Overlapping between Threat intelligence is pretty low

Note: IID is an Infoblox brand

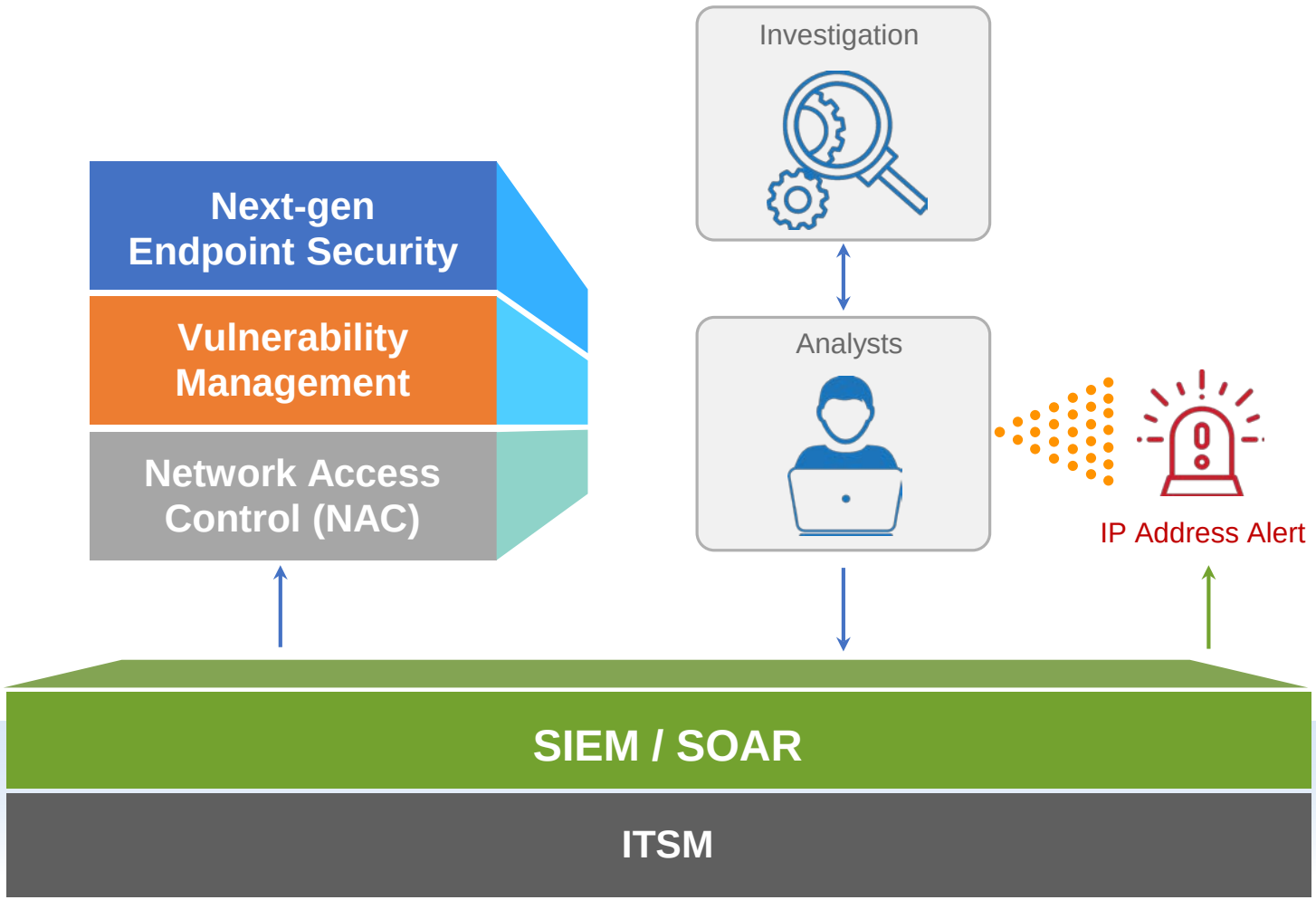
Threat Intel Data Sharing

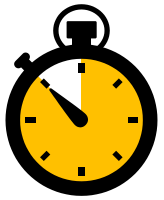
- Reduce cost of threat feeds while improving effectiveness across entire security portfolio



Single-source of TI management | Automate investigation & triage | Orchestrate common security policy across multi-vendor infrastructure

Typical Incident Response



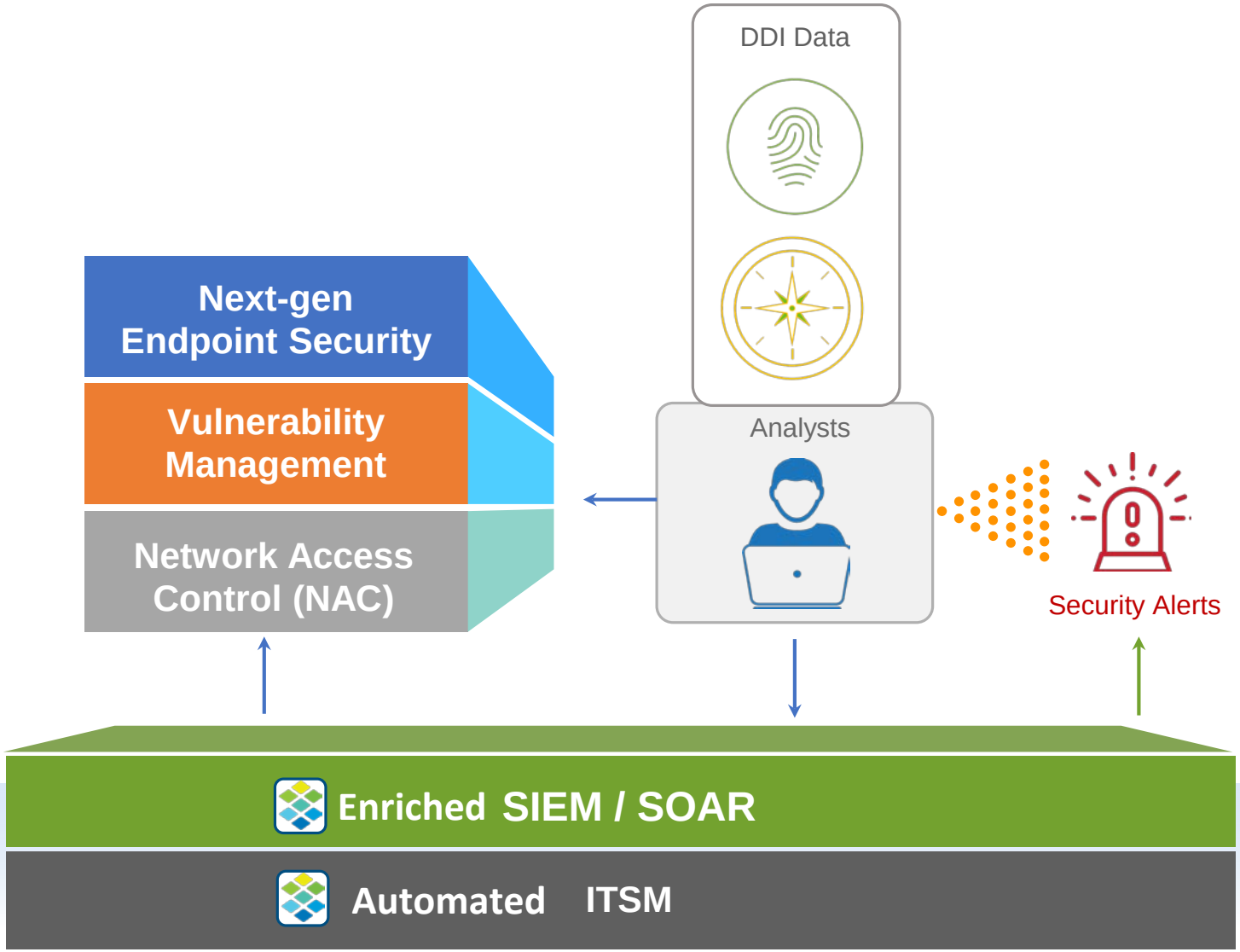


Lengthy Response Times

Manual Investigation

- MAC Address
- User details
- Network Location
- Physical location
- Network devices
- Device type
- OS information
- Current IP
- Historical IP's and locations

DDI Data Accelerates Incident Response



Lower Response Times

DNS

- Malicious activity inside the security perimeter
- Includes BYOD and IoT device
- Profile device & user activity

DHCP

- Device Audit Trail and Fingerprinting
- Device info, MAC, lease history

IPAM

Application and Business Context

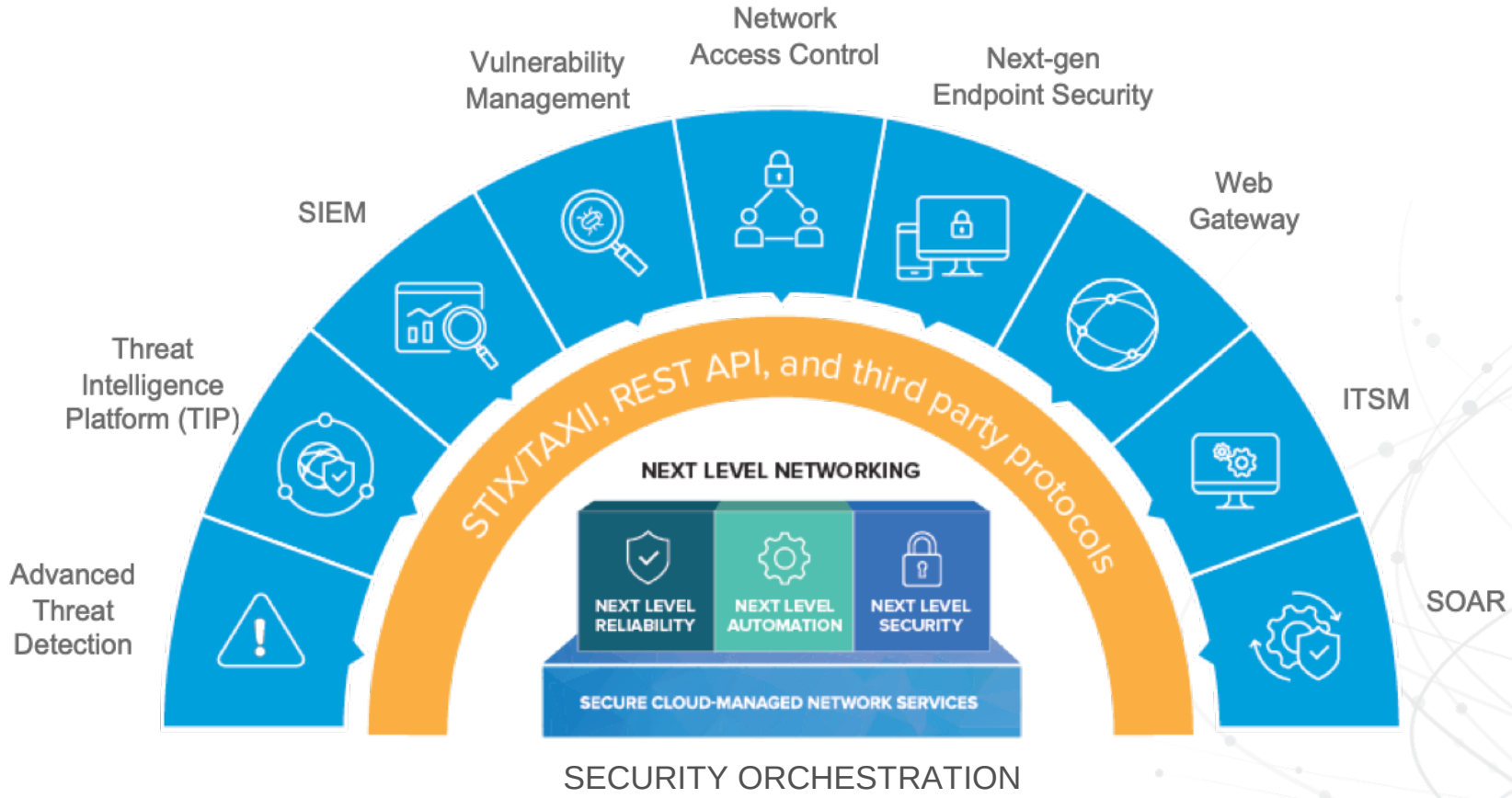
- "Metadata" via Extended Attributes: Owner, app, security level, location, ticket number
- Context for accurate risk assessment and event prioritization

The Hacker in the Hotel Room - A Sec Ops Analogy

- Stephan hacks the Casino systems from the guest wifi of the hotel, steals customer credit card details worth millions of dollars by exfiltrating the data over DNS, then checks into the Penthouse suite
- **Most systems**
  - Tells the Casino SOC that the attack came from a device in the lobby
  - Has no idea where it is now - could be any device, anywhere
- **Infoblox**
  - Tells the Casino SOC that it comes from a windows laptop that was connected in the lobby
  - It is now connected in room 2404
  - It is also the same laptop that tried to hack other guest wifi users the day before

Cybersecurity Ecosystem

- Automatically notify ecosystem of events in real time
- Trigger remediation action
- Share network context



- Faster remediation
- Improve ROI of ecosystem
- Bridge silos

Broad Ecosystem of Engaged Partners

Strategic & High Value Alliance Partners

Strategic Partners

High Value Partners

Ecosystem Partners

Technology Partners

Valued OEM Partners

Our Main focus

Service providers need new revenue streams and market differentiation. With security as a **top business concern**, security services are a prime driver for new revenue-generating opportunities.

Provide network-based security services at scale using Infoblox deployed infrastructure

Our focus: Enable new cost-effective sources of revenue

Support 4G & 5G Use Case Growth

Protect businesses, networks and subscribers from malware

Easy to Bundle

Attach to new or existing services

Expand Security Product Portfolio

Handle increasing amounts of data and devices

Enhance Quality of Experience

Provide anywhere protection to non-traditional devices

Increase Revenue

Boost revenue per user leveraging existing investments

Newly Observed Domains

“Innocent until proven guilty” is not always the best way

Newly Observed Domains can be good!!

I am innocent, I swear!!

Lookalike Domain Detection

paypal.com	pąypąl.com	paypal.com	Text
xn--pypl-53dc.com	xn--pypl-btac.com	paypal.com	Punycode

google.com	google.com	google.com	Text
google.com	xn--ggle-0nda.com	xn--ggle-55da.com	Punycode

 |

ROI: Reduces Cost of Existing Tech Stack

2/3

reduction in threat response time

3x

more productivity from threat analysts

Drastic reduction in malicious traffic sent to NGFWs

Based on real customer data

Independent Research Study: B1TD Delivers 243% ROI

Forrester Total Economic Impact Study found when customers deploy BloxOne Threat Defense there is a **243% ROI and less than 6 months total investment payback.**

Get report

Benefits for the Customer

Cost of Security	Risk Identification	Attack Surface	Security Posture
Security Before Security	Universal Source of Truth	Improve Time to Remediate	Automated Response

1 Reduce Security Cost

Payback 6 months

Security ROI 243%

"Decreased load on existing security tools and infrastructure (e.g.: SIEMs, NG firewalls, DPI)"

2 SecOps Efficiency UP

"Security operations (SecOps) gain 19% of their time back using contextualized BloxOne Threat Defense intelligence on investigations"

3 LOW Attack Exposure

"Reduce Risk of Material Breach 5%"

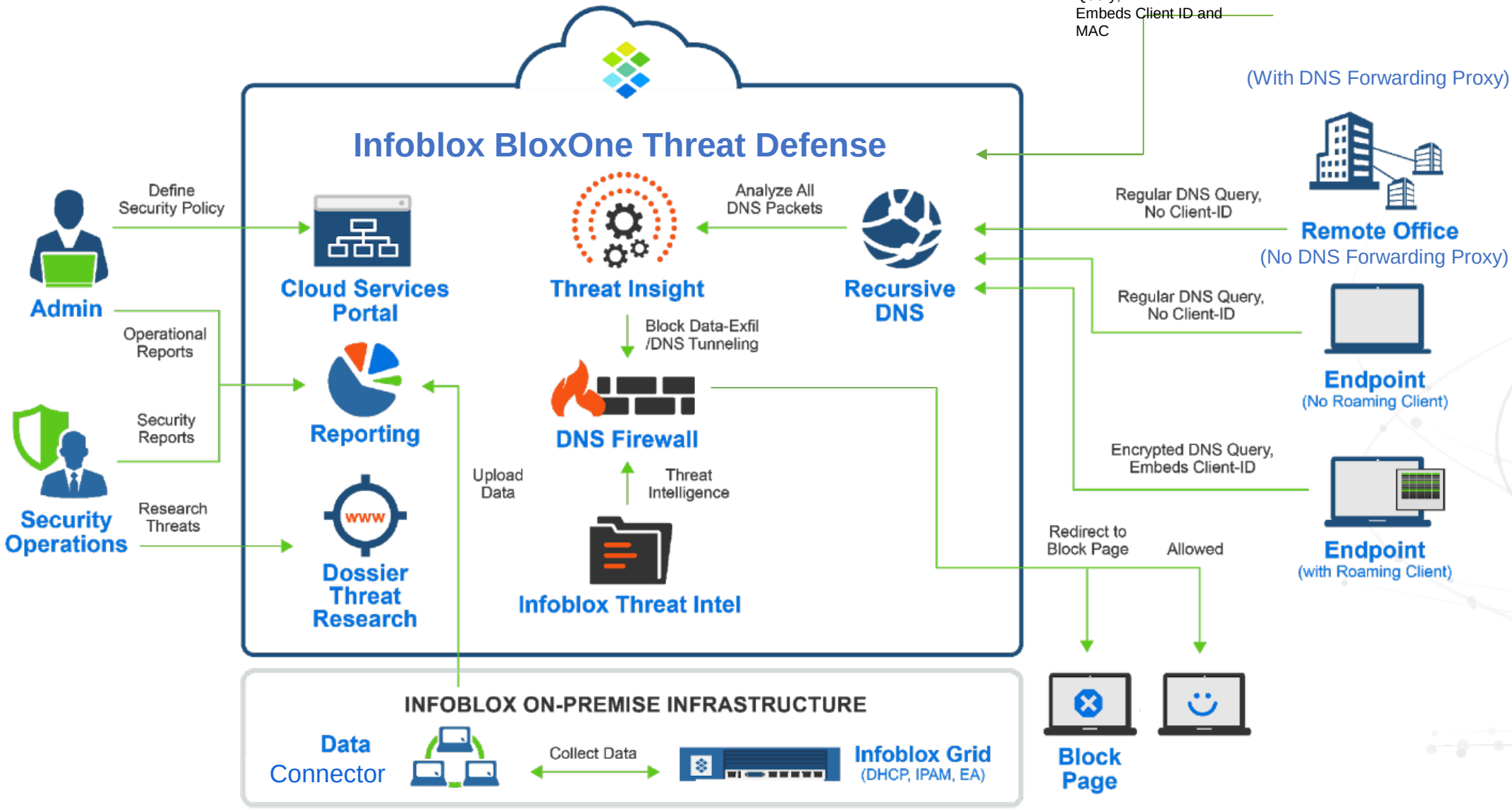
"Decrease your remediation time by providing automatically enriched network and event context (DDI-DNA)"

4 One Security Posture

"Increase your security posture by using DNS services to protect Work-From-Home employees"

"Increase your security posture by securing IoT and Operational security assets"

BloxOne Threat Defense: Overview



 |

Thank You

Vinaka köszönöm Kiitos Maake Asante Shukria Dhanyavadagalu
감사합니다 Dankscheen спасибо Kam Sah Hammida شكرا Manana Dankon
Dank Je Mauruuru Biyan Diolch i Chi Terima Kasih Matondo Taiku Tack
Blagodaram Ngiyabonga Dziekuje Chokrane Grazie
Juspaxar Arigato Mochchakkeram
நன்றி Bedankt Dakujem धन्यवाद Gracias Khap Paldies Tingki
Ua Tsaug Rau Koj Grazas cảm ơn bạn Gratias Tibi
Děkuji Nirringrazzjak Di Ou Mèsi Kia Ora Kop Khun Obrigado ありがとう
Suksama Rahmat Nuwun 谢谢 хвала Hvala Welalin Djiere Dieuf
Misaotra Matur Danke Merci Salamat Go Raibh Maith Agat Eskerrik Asko
ขอบคุณ Najis Tuke