Infoblox

VERBESSERN DER IT-INFRASTRUKTUR SICHERHEIT DURCH KONTROLLE DES DNS-VERKEHRS

Die meisten Cyber-Angriffe nutzen DNS - Machen Sie Ihre IT-Infrastruktur sicherer, indem Sie den DNS-Verkehr kontrollieren

Prepared by:
Stephan Fritsche
Central Europe Security Lead

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/

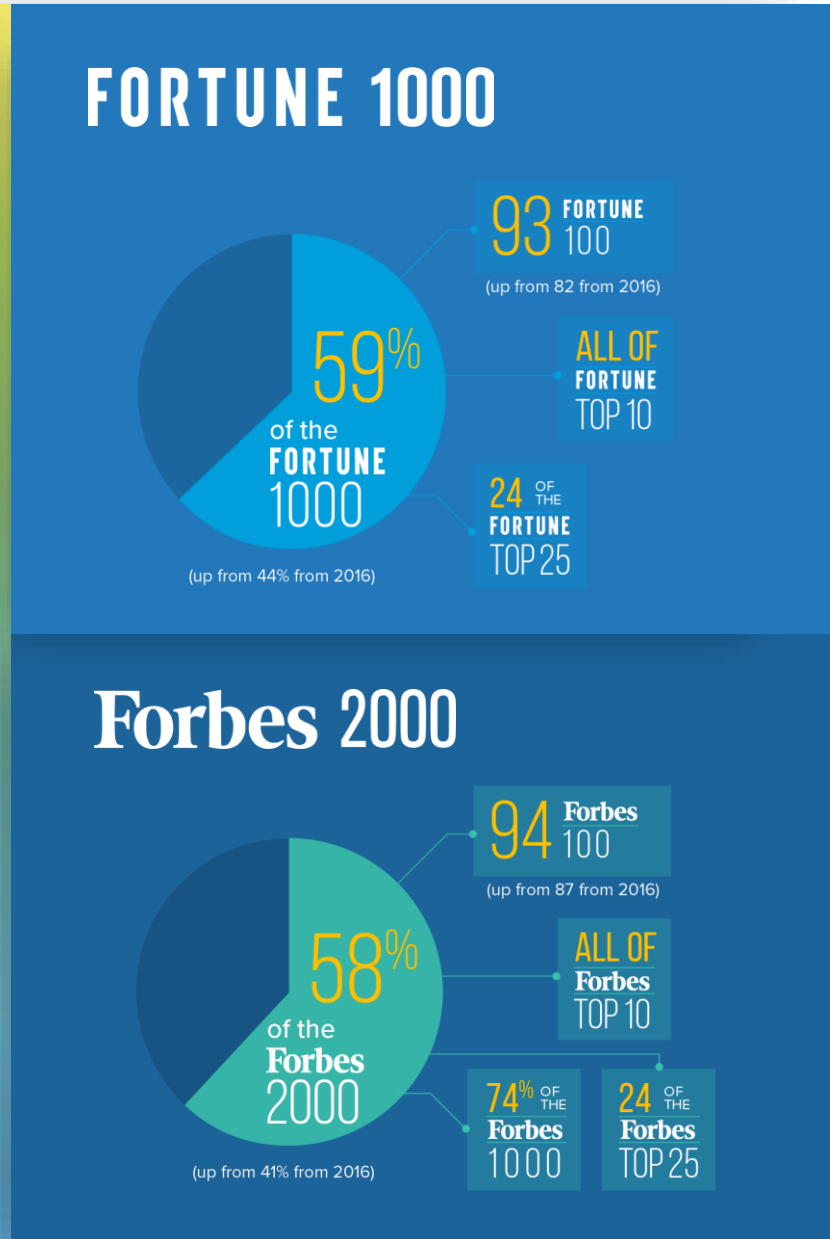
Leading the Industry

MISSION

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

OFFERINGS

Core Network Services, Cybersecurity, Secure Edge Services



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

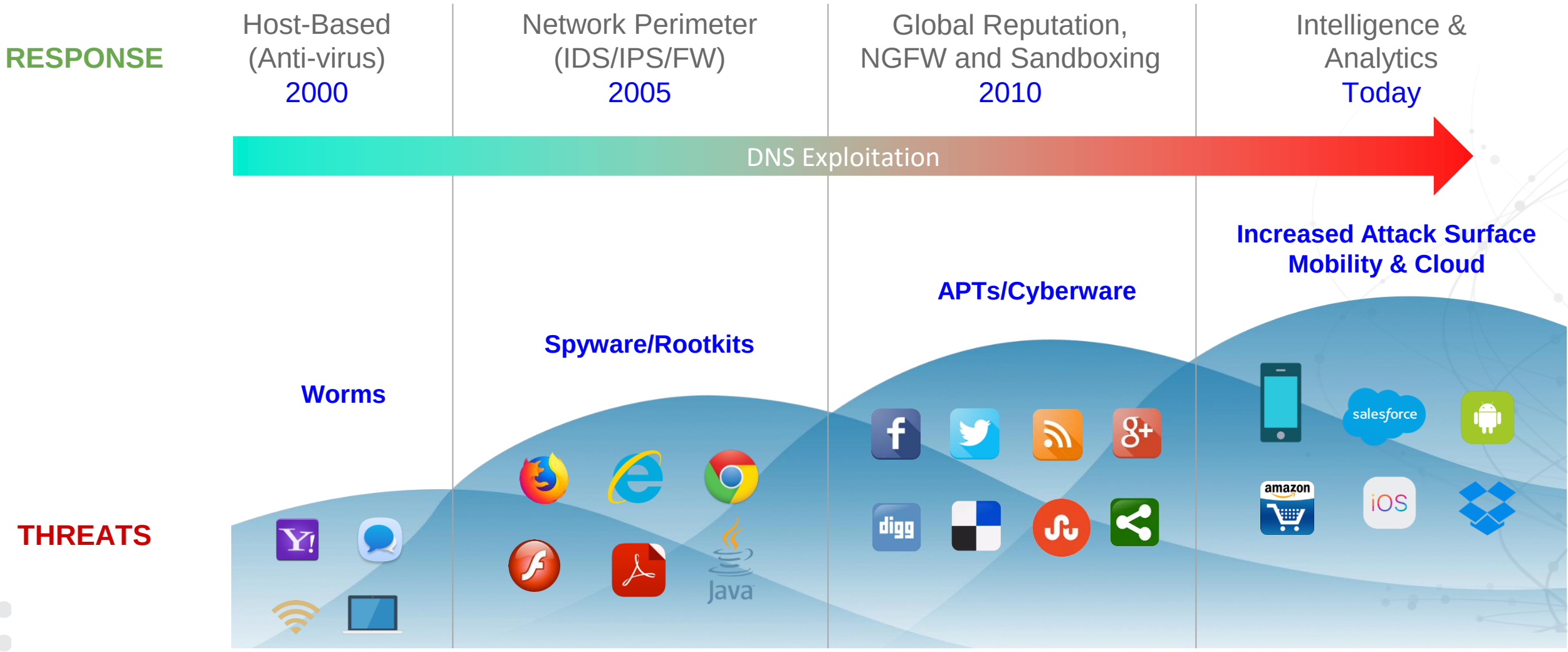
Strengthen and Optimize Security Posture

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

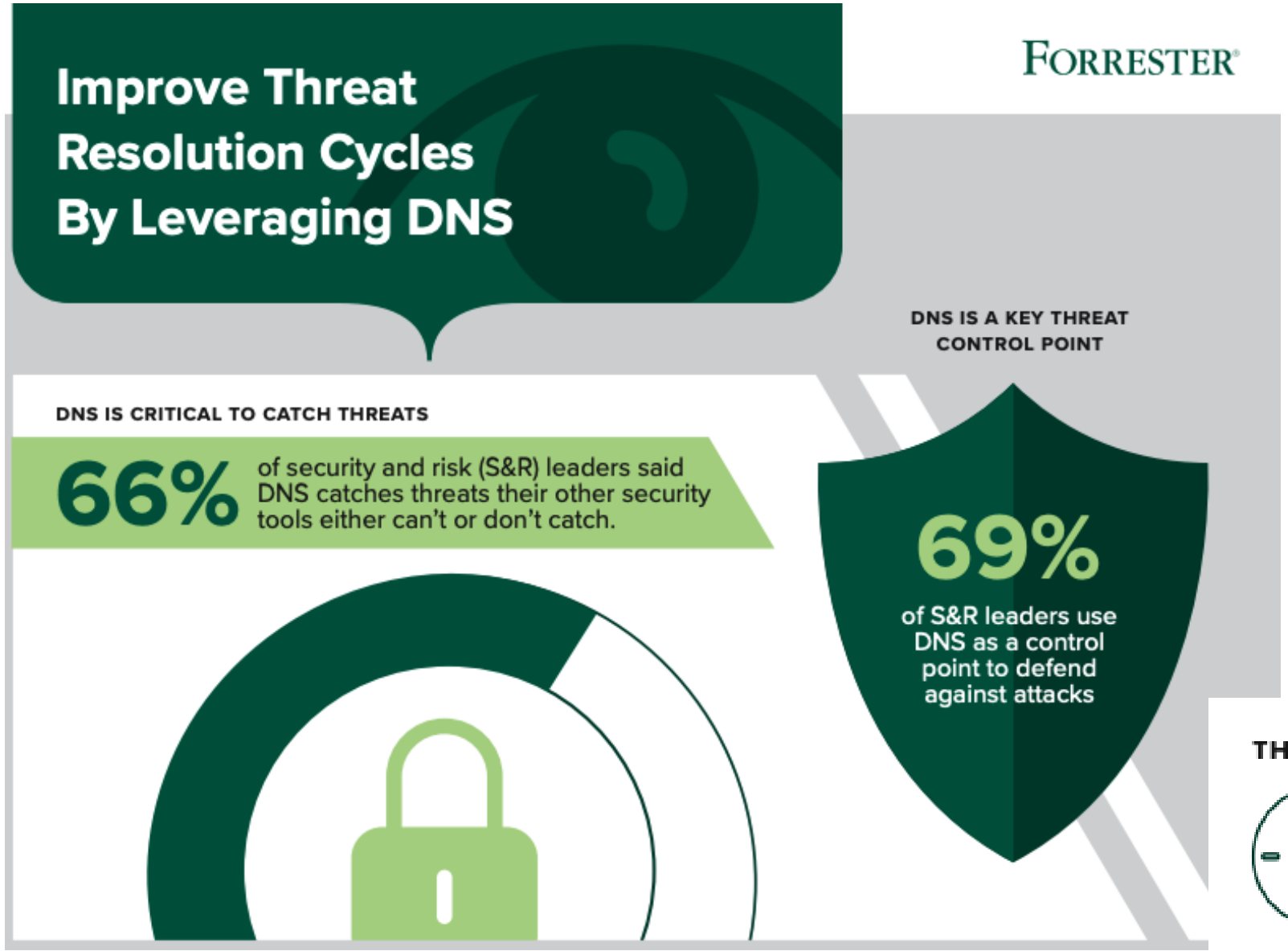
Cloud-native network and security services

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

The Threat Landscape Evolution



Forrester Research Paper Key Findings (July 2020)



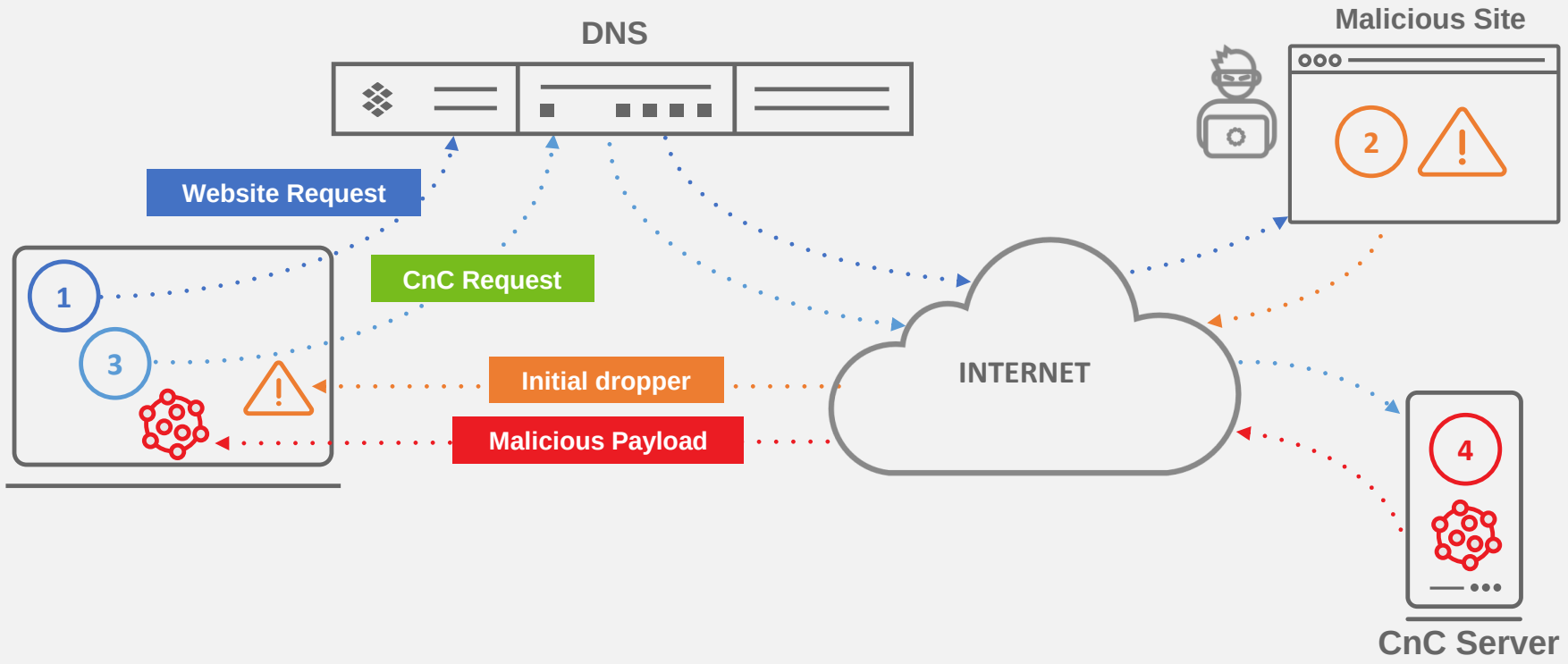
THREAT INVESTIGATIONS TAKE TOO LONG

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

Common Attack Steps Review

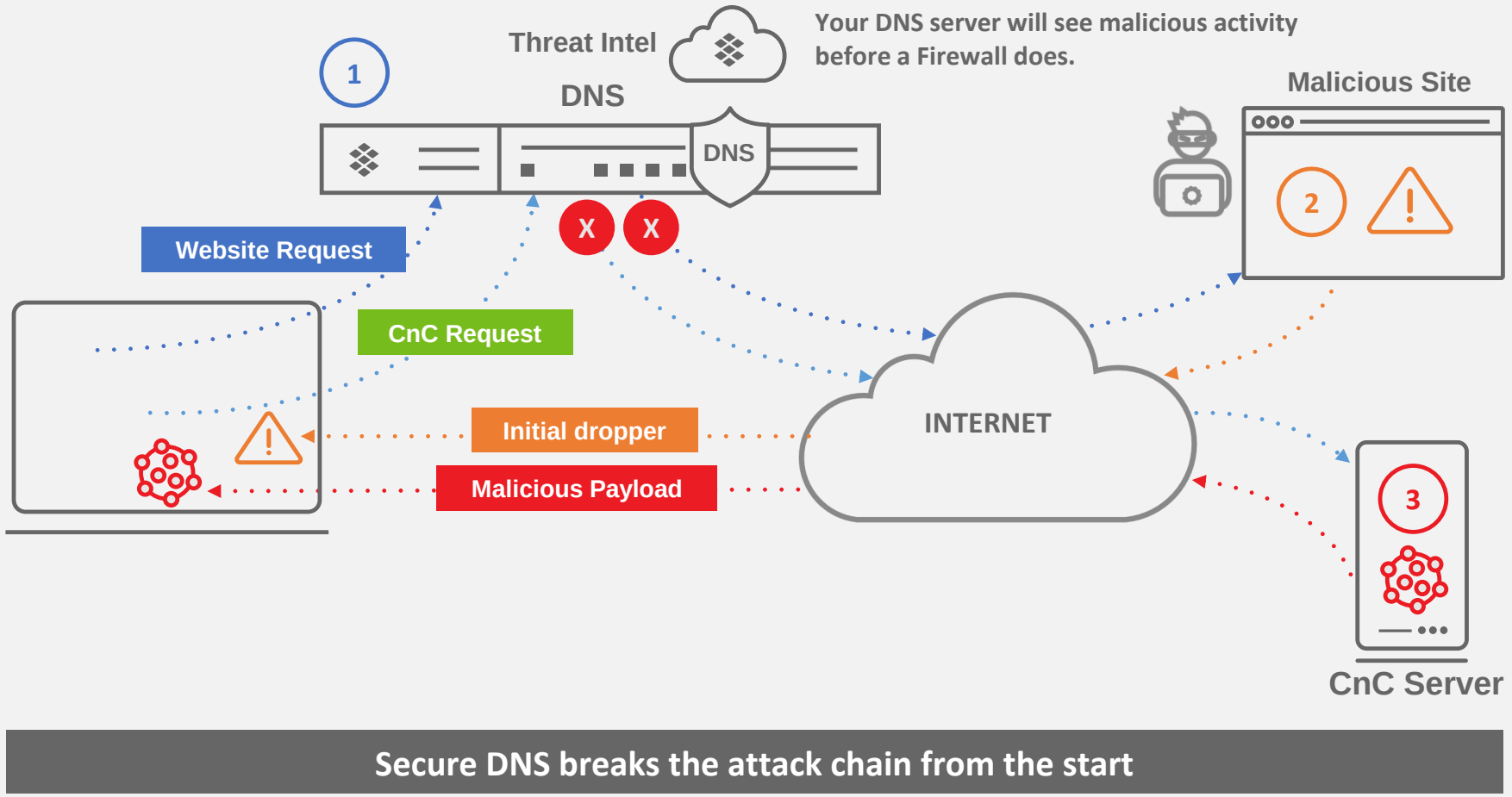
1. User directed to malicious site
2. Website delivers initial exploit
3. Exploit contacts Command and Control (CnC) server
4. Malicious payload downloaded



DNS is used for all outbound traffic requests

Leveraging DDI Intelligence for Foundational Security

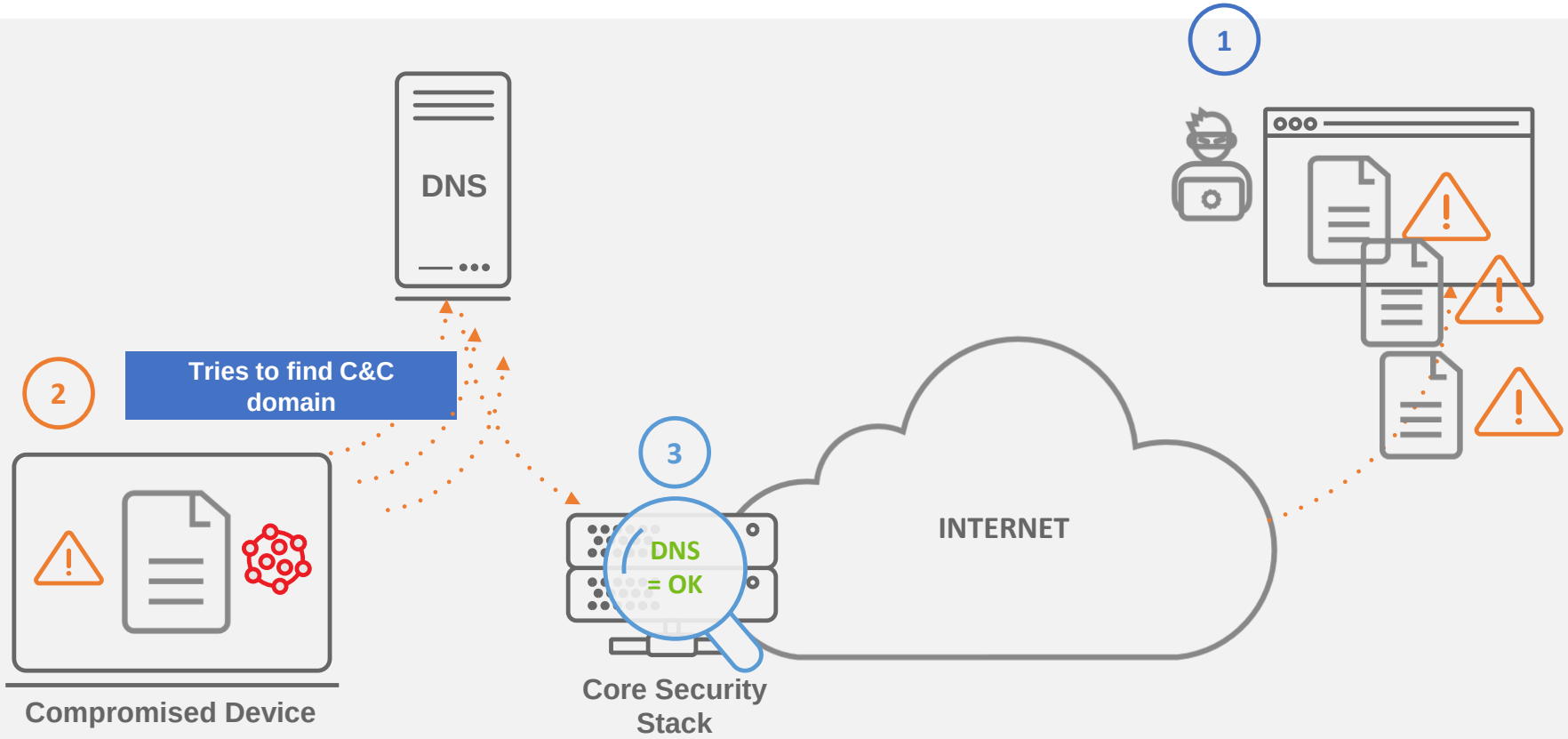
1. Curated threat intelligence for DNS
2. Connection to malicious website blocked at DNS
3. If already infected, system blocked from connecting to CnC at DNS



Secure DNS breaks the attack chain from the start

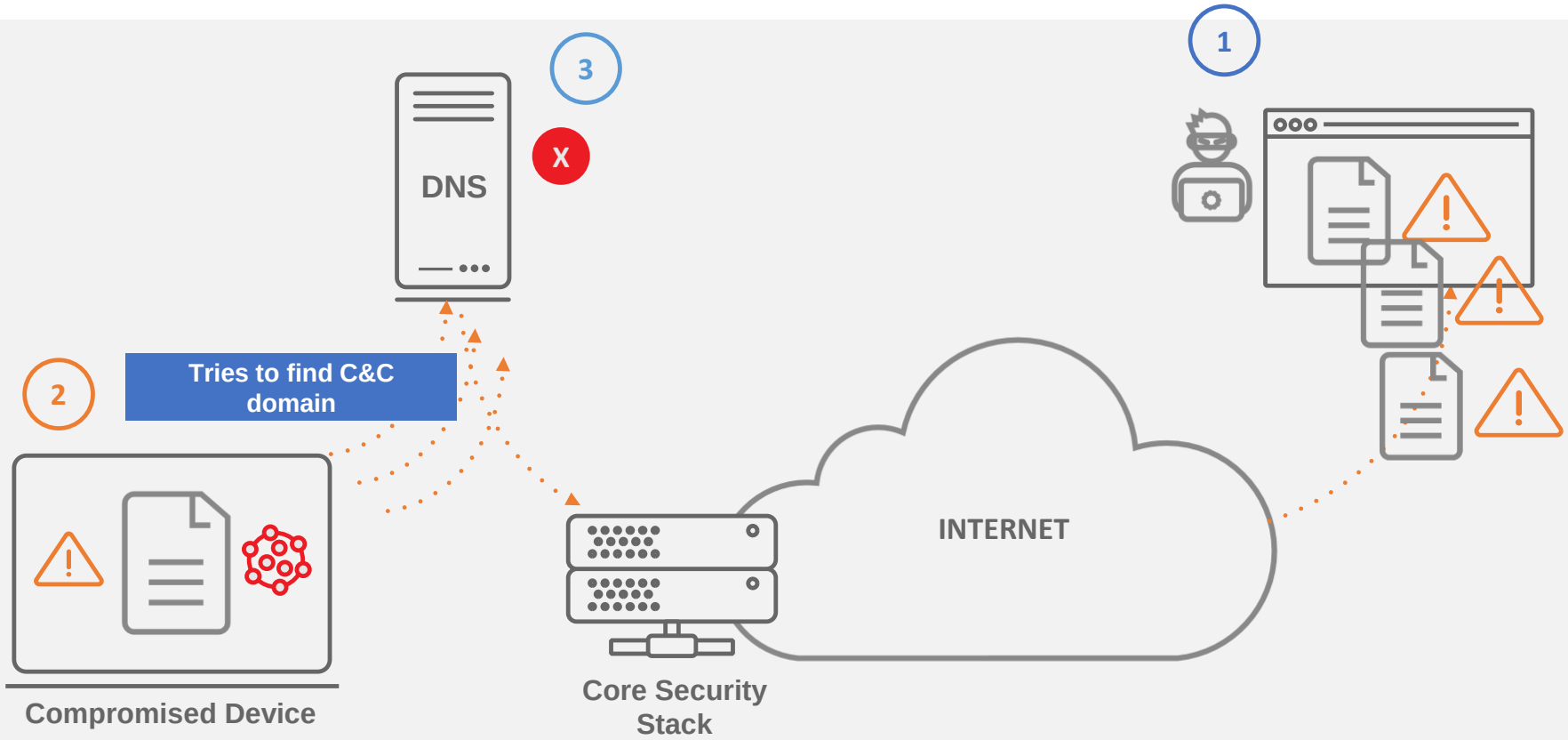
Dynamically Generated Domains

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



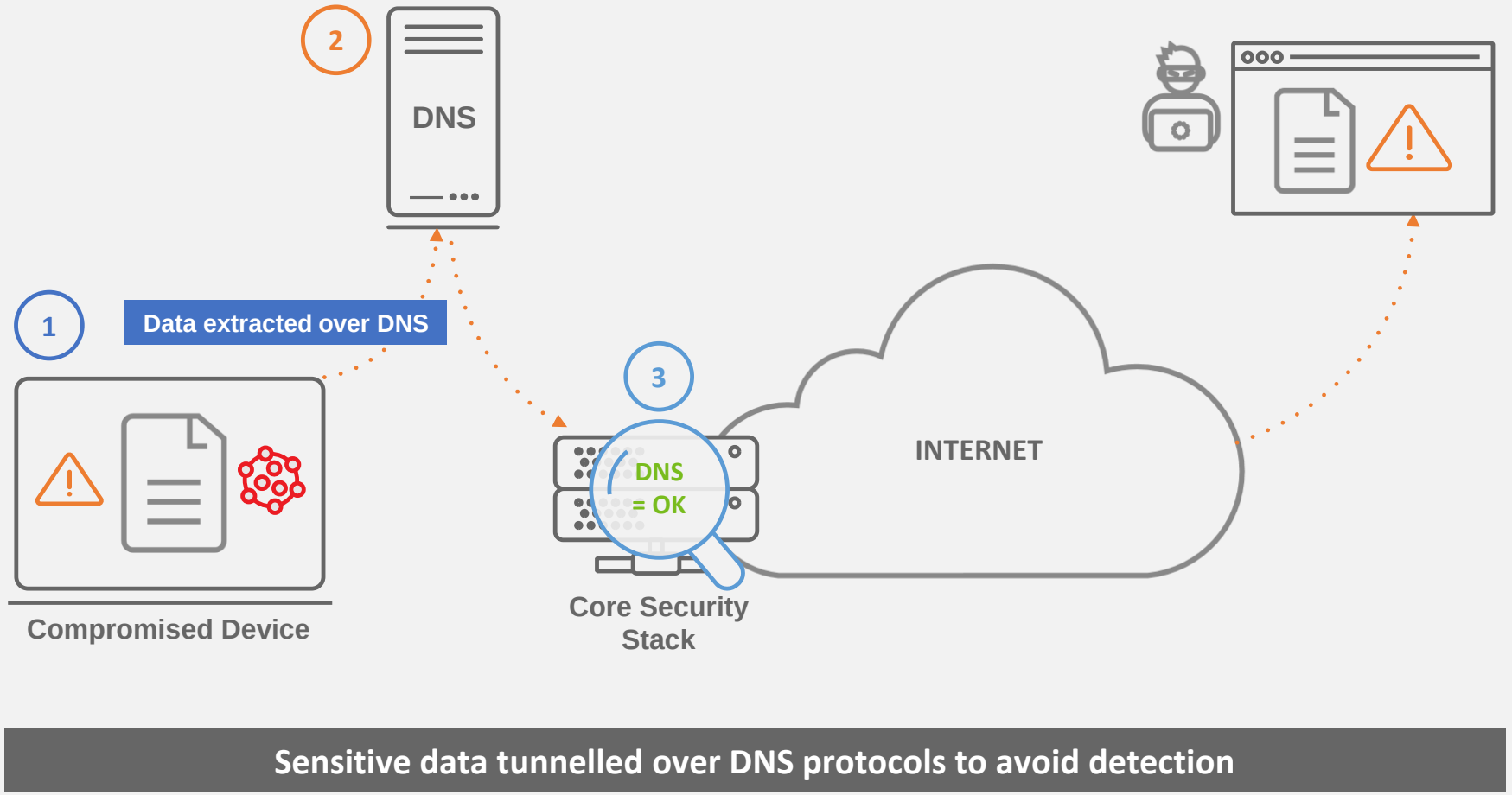
Dynamically Generated Domains Best Practices

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.



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

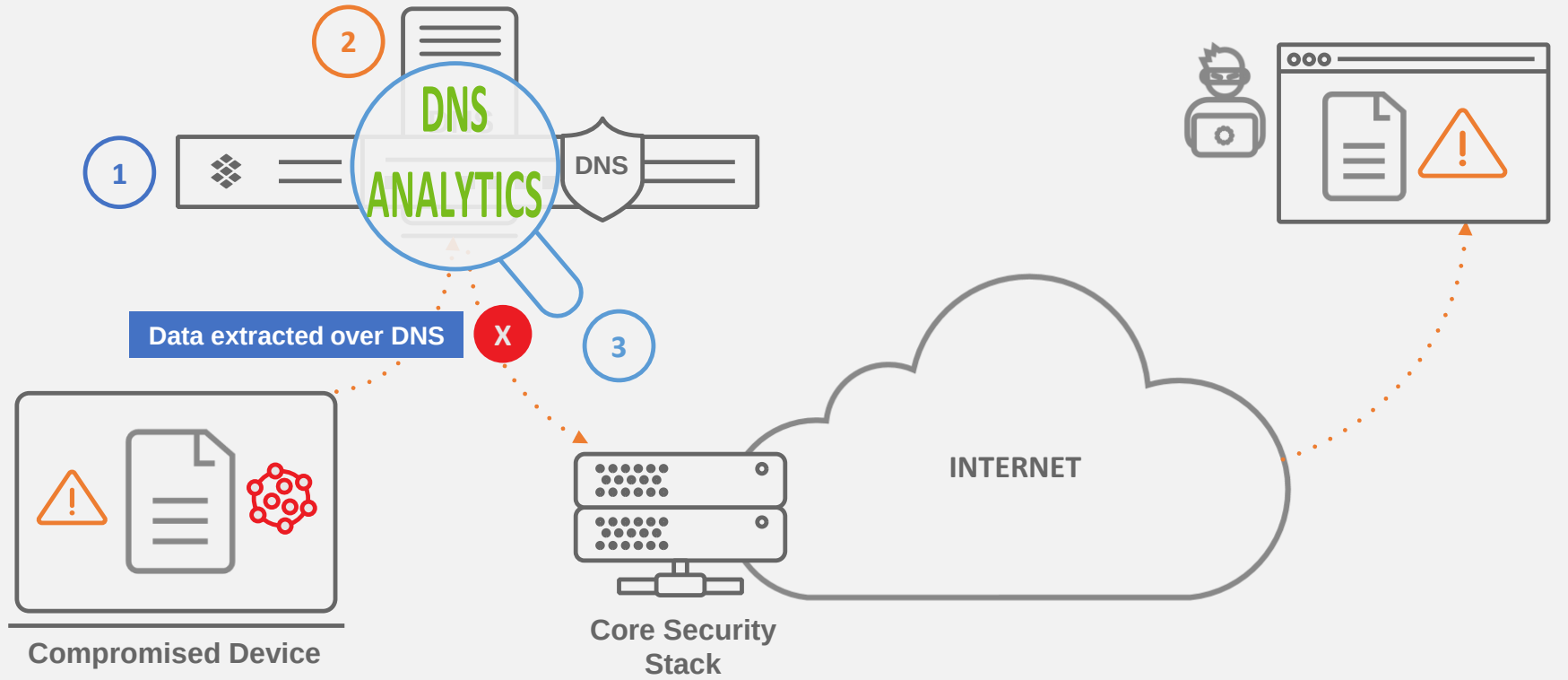


Sensitive data tunnelled over DNS protocols to avoid detection

 |

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

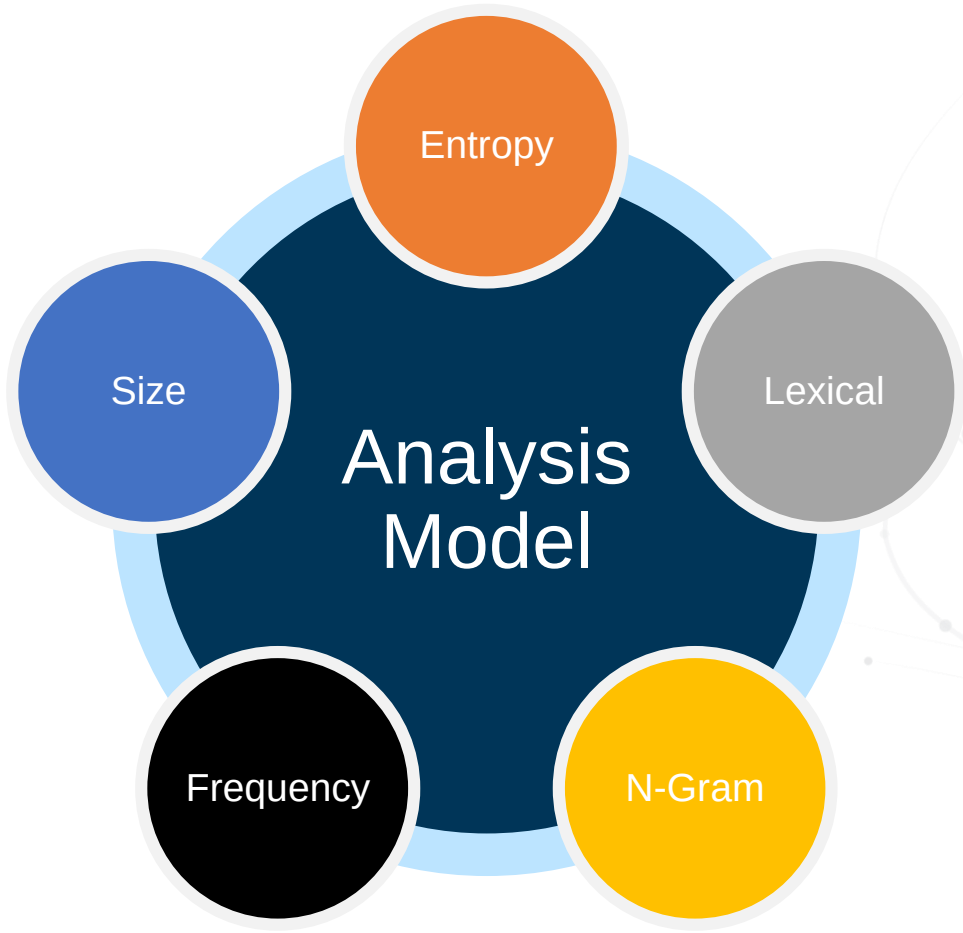


Attempted data exfiltration over DNS protocols detected and blocked

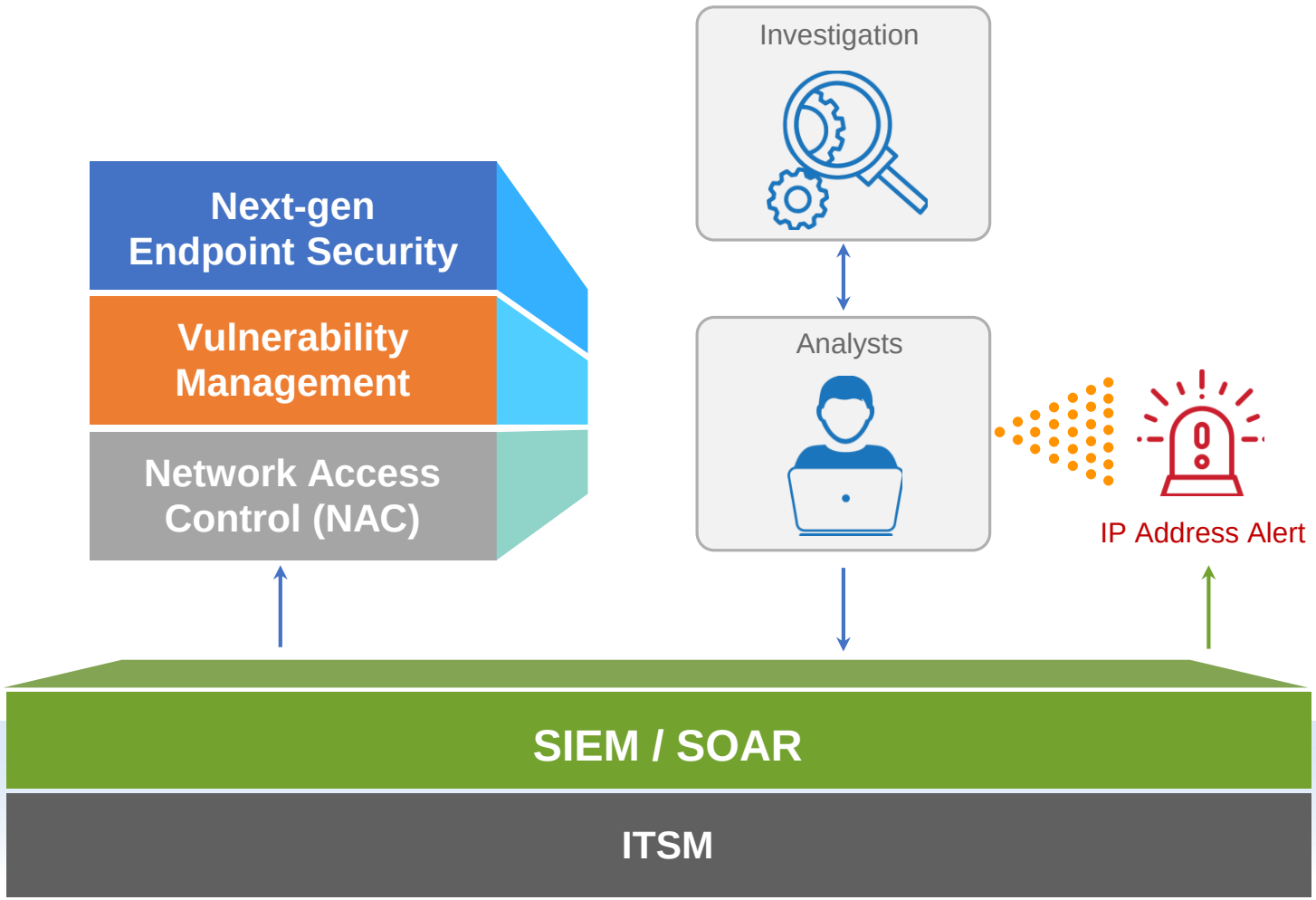
 |

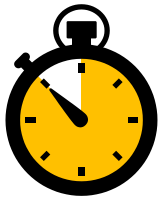
Threat Intelligence (Purpose Built for DNS) + Analytics + Infoblox Cyber Intelligence Unit = Advanced Threat Detection

- **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



Typical Incident Response



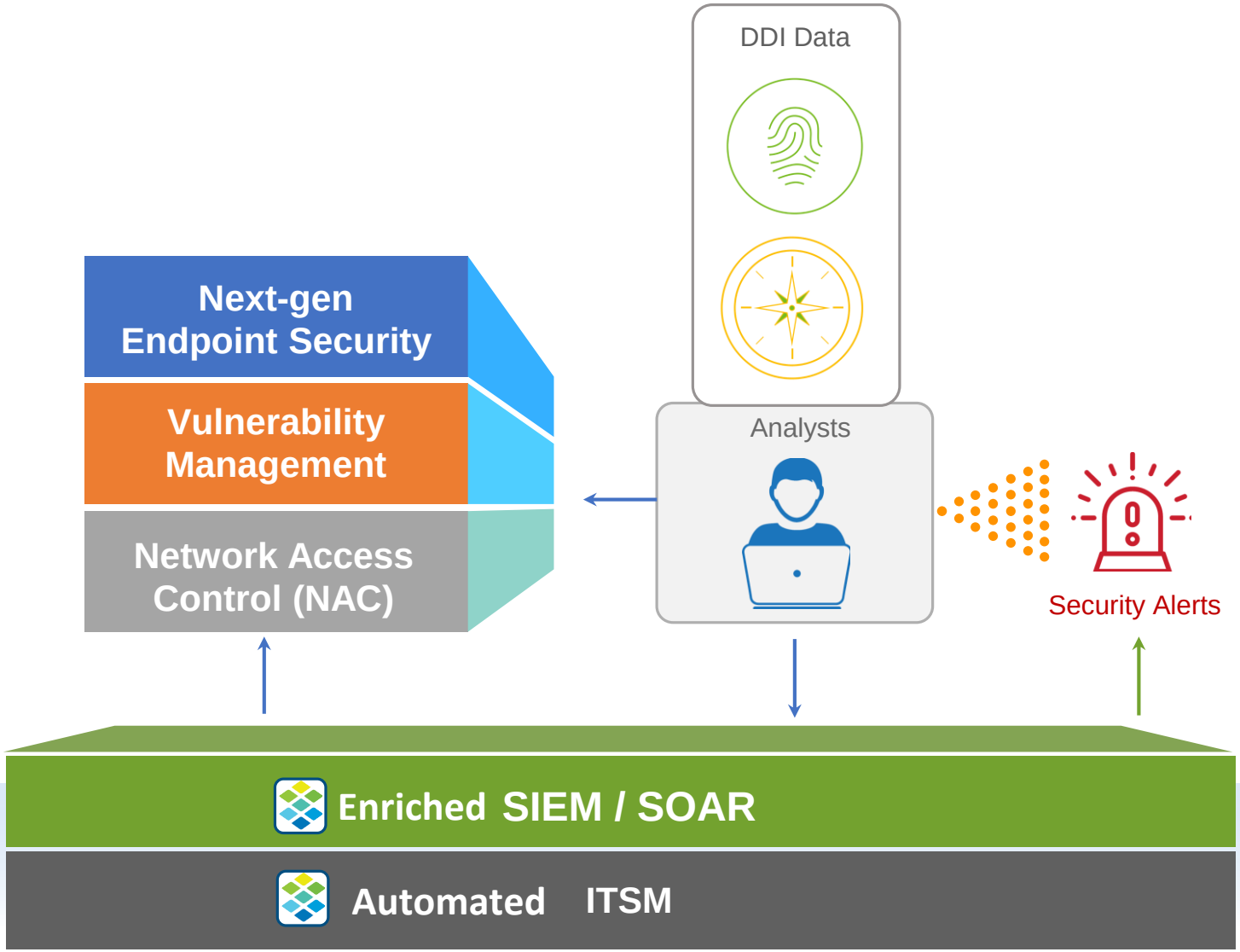


Lengthy Response Times

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

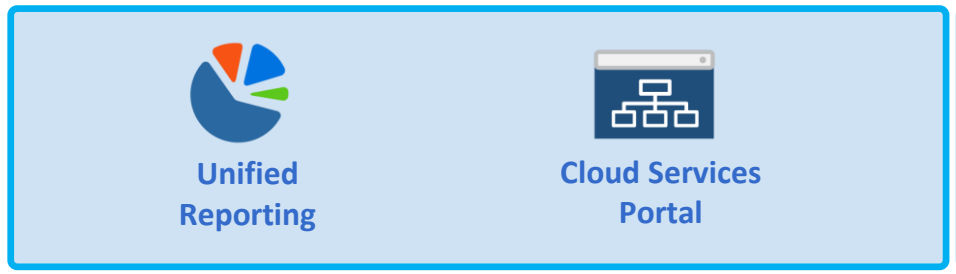
IPAM

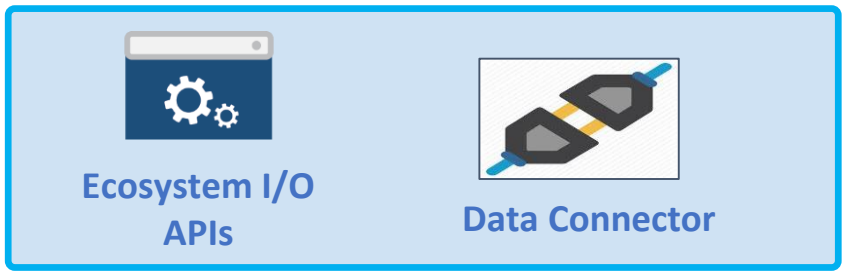
Application and Business Context

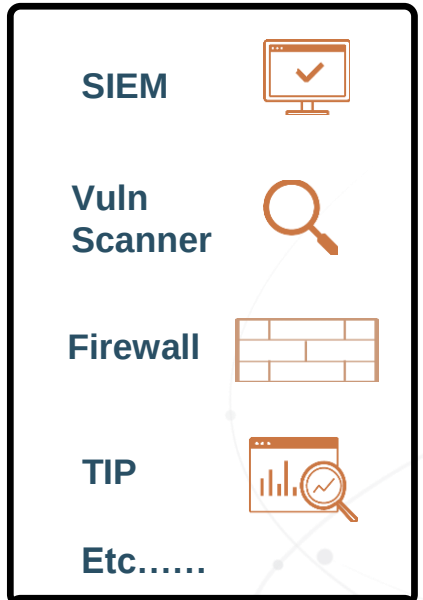
- "Metadata" via Extended Attributes: Owner, app, security level, location, ticket number
- Context for accurate risk assessment and event prioritization

 |

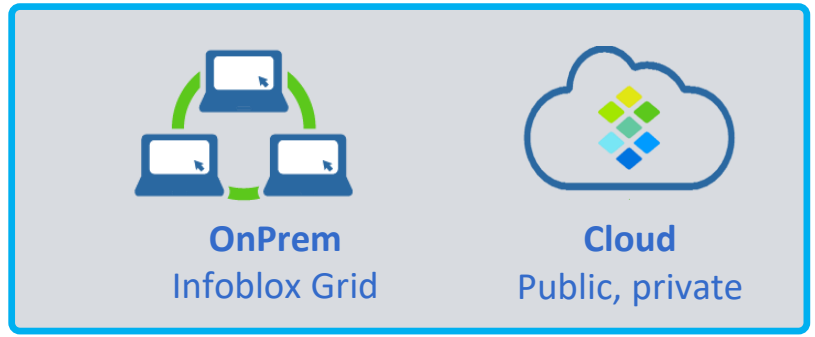
BloxOne® Threat Defense Advanced

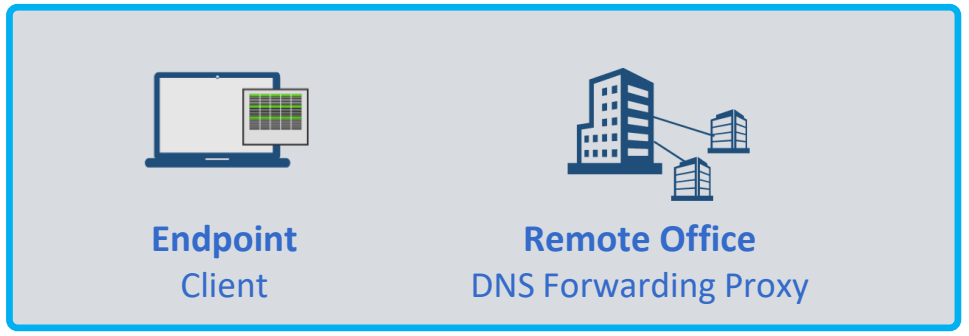


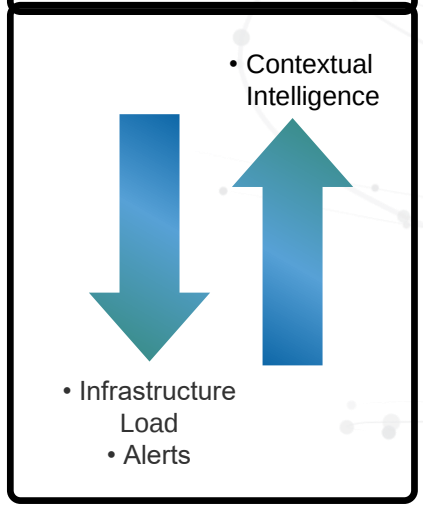




Globally available recursive DNS and web filtering








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