



The unspoken backdoor

DNS the Foundational Enterprise Security

Alvin Rodrigues
Field Chief Security Officer
arodrigues@infoblox.com

25 February 2021

infoblox.com
© 2020 Infoblox Inc.



1



DNS a vulnerability,

becomes foundation for enterprise security



infoblox.com
© 2020 Infoblox Inc.

2

AGENDA

◆ Network transformation

Cyber Security for transforming network

Criticality of securing DNS

beyond securing DNS

3

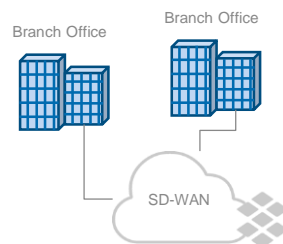
The network is constantly transforming

Cloud is the New Network



Shifting perimeter. Direct access to cloud applications from everywhere

SD-WAN drives network transformation



Direct connection to Internet with no ability to replicate full HQ security stack

IoT leads to explosion of devices

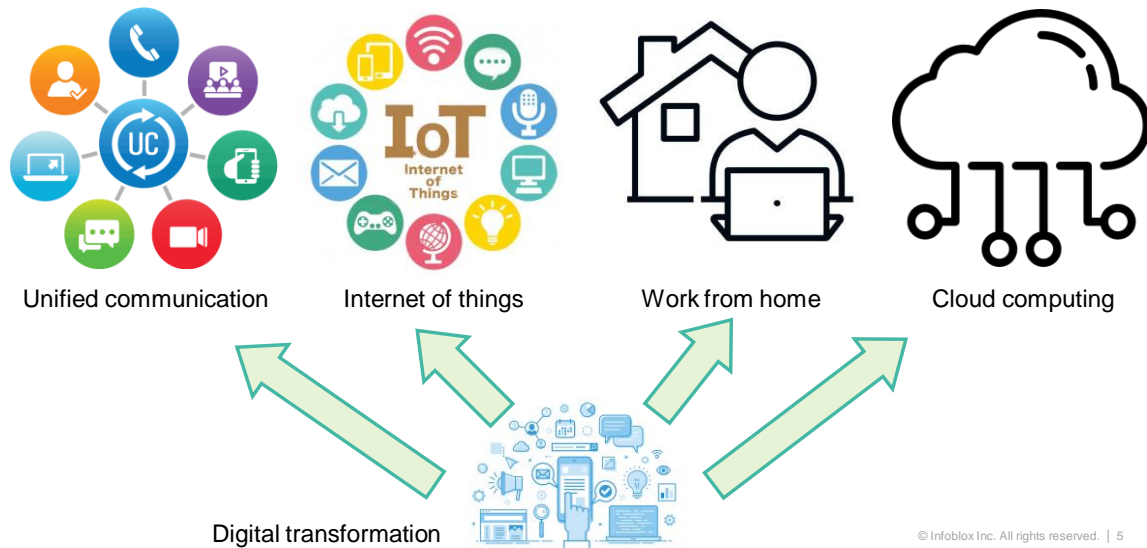


Endpoint security cannot be deployed on lightweight IoT devices

4

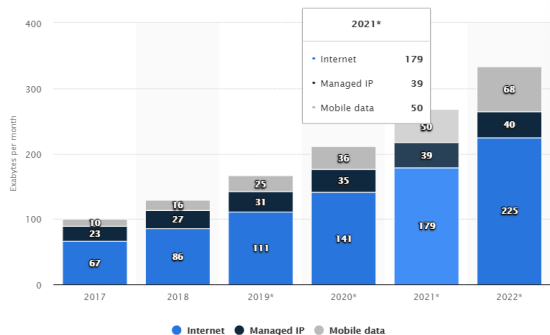


Drivers for network transformation



5

DNS is growing



Data volume of global consumer IP traffic from 2017 to 2022, by connection type

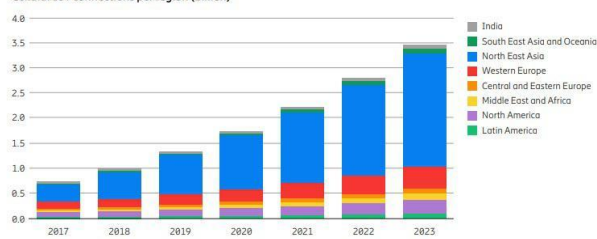
observations

- Global consumer IP traffic rose. Global Internet user grows.
- Cellular IOT connection grows. (North East Asia largest growth)
- DNS foundation of all IP connections. Therefore, DNS is growing.

Source:

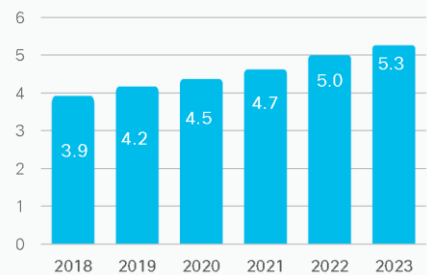
<https://www.forbes.com/sites/louiscolombus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/?sh=2d9d427c7d83>
Cisco annual Internet report, 2018 to 2023

Cellular IoT connections per region (billion)



6% CAGR
2018-2023

Billions of
Internet
Users

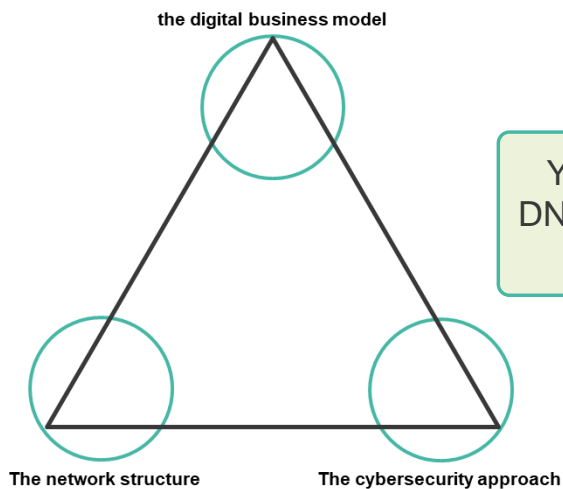


Global Internet user growth

© Infoblox Inc. All rights reserved. | 6

6

Symbiotic relationship - business, network and security



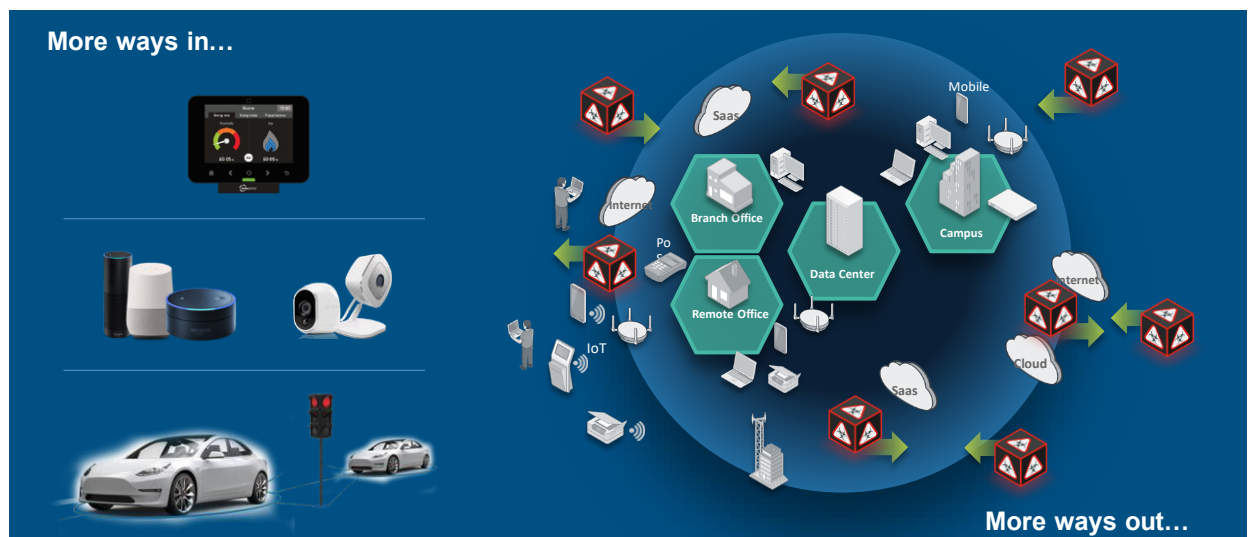
Your network is your business.
DNS – foundation of your network.
Visibility is the cornerstone.

© Infoblox Inc. All rights reserved. | 7



7

More points of infiltration into the business



© Infoblox Inc. All rights reserved. | 8



8

AGENDA

Network transformation

- ◆ Cyber Security for transforming network

Criticality of securing DNS

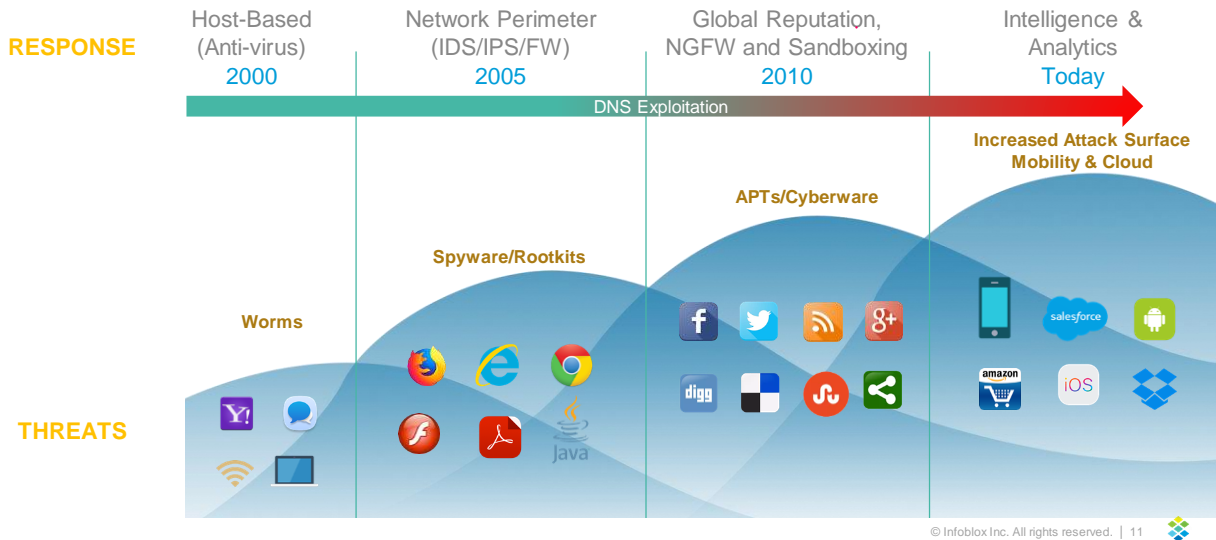
beyond securing DNS

9



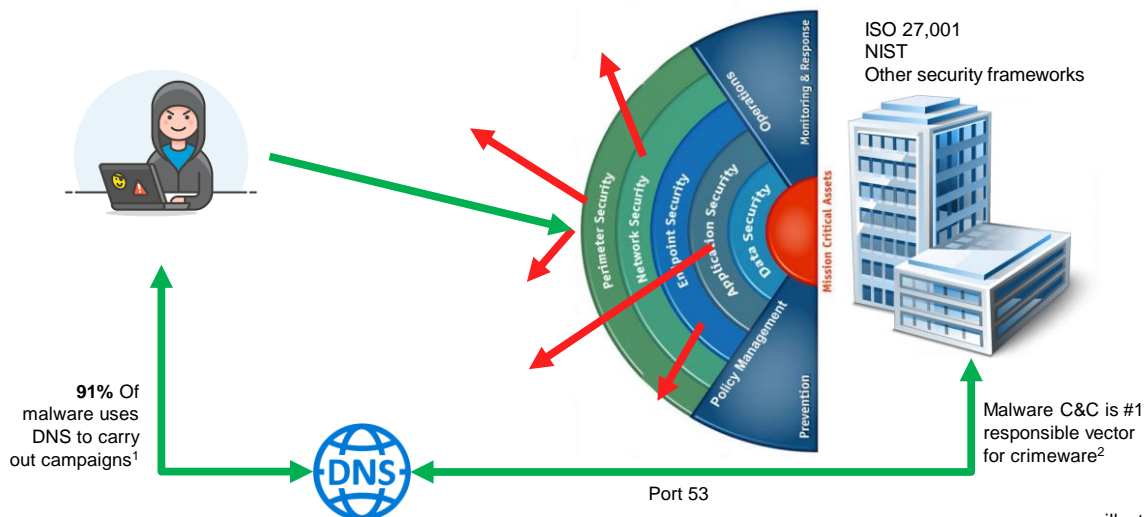
10

The threat and cyber response landscape evolution



11

Circumvent “Defense-In-Depth” through DNS traffic



1. Source: Cisco 2016 Annual Security Report 2. Source: Verizon 2016 Data Breach Investigations Report






© Infoblox Inc. All rights reserved. | 12

illustration

12

Why Should Securing DNS Be a Focus?

Security Teams At a Disadvantage with DNS

 <p>DNS is everywhere and critical</p>	 <p>DNS was designed to be open and allow everything</p>	 <p>DNS is the first touch point</p>	 <p>95% of today malware attack involve DNS</p> <p>68% of organization don't monitor recursive DNS</p>	 <p>Ownership is in silos: NetOps teams typically own DNS – not SecOps</p>
--	--	--	---	--

© Infoblox Inc. All rights reserved. | 13



13

Critical gaps address by securing DNS



Data exfiltration



C2 malware communication and propagation



Visibility of infected devices and host

© Infoblox Inc. All rights reserved. | 14



14

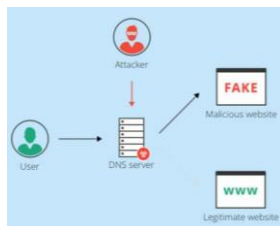
Gaps address by securing DNS



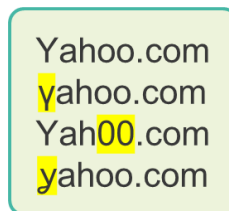
Malicious website



Phishing



DNS hijacked / Poison



Lookalike domain



© Infoblox Inc. All rights reserved. | 15



15

AGENDA

Network transformation

Cyber Security for transforming network

Criticality of securing DNS

◆ Beyond securing DNS

16

DNS becoming the 1st line of defence



- Time to detect
- Time to investigate, respond and contain.

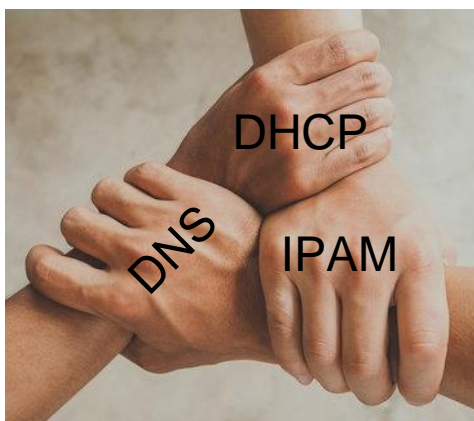
Security Ecosystem integration •

© Infoblox Inc. All rights reserved. | 17



17

DNS partners



DDI

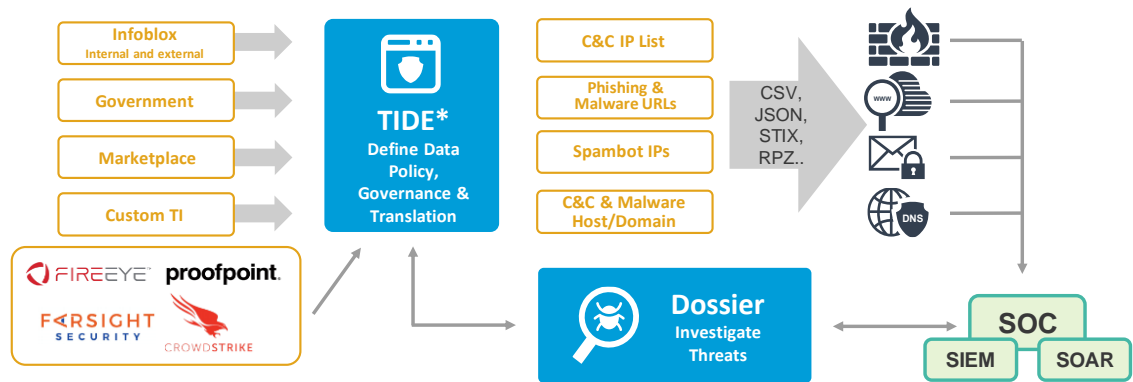
© Infoblox Inc. All rights reserved. | 18



18

Single source multiple feeds and applications

Threat Intel Data Sharing reduces 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

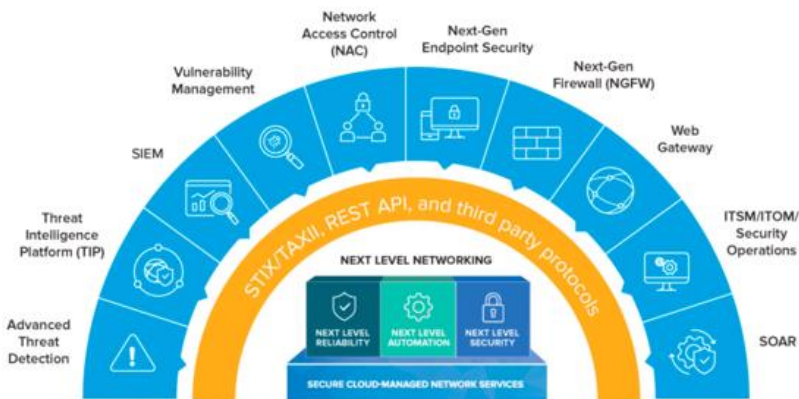
* Threat Intelligence Data Exchange

© Infoblox Inc. All rights reserved. | 19



19

Security ecosystem integration

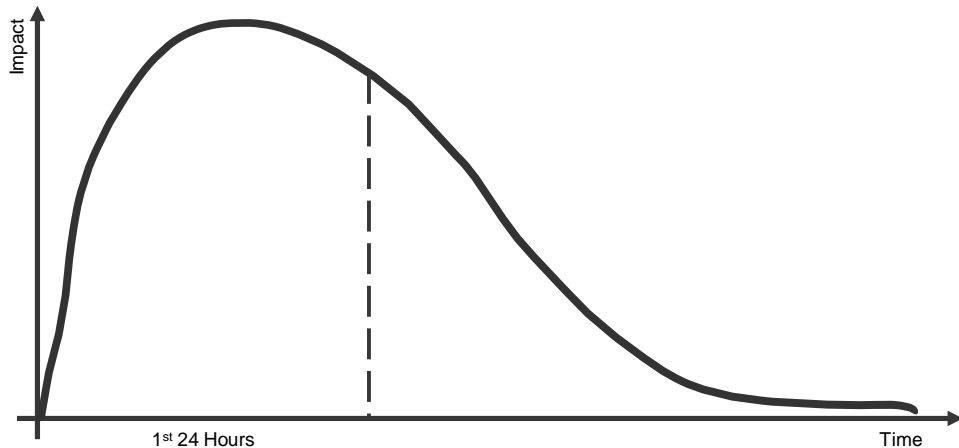


© Infoblox Inc. All rights reserved. | 20



20

Breach impact over time



illustration

© Infoblox Inc. All rights reserved. | 21



21

Compliance – single source of truth – MAS IBTRM

Incident Reporting Template

Instructions:

	All Incidents	For Cyber Incidents Only
1. Incident Notification to MAS <i>(as soon as possible, within an hour)</i>	<ul style="list-style-type: none"> Submit Section (A) of this Incident Reporting Template 	For CII institutions: <ul style="list-style-type: none"> To also submit the National Cyber Security Incident Reporting Form available from the Cyber Security Agency of Singapore (CSA) website, or via the link here: https://www.csa.gov.sg/legislation/forms For all other FIs: <ul style="list-style-type: none"> To also submit Annex in this Incident Reporting Template
2. Subsequent update(s) to MAS <i>(updates to be provided as and when there are changes in the current situation, or as requested by MAS)</i>	<ul style="list-style-type: none"> Submit any updates to Section (A) 	For CII institutions: <ul style="list-style-type: none"> Submit any updates to the National Cyber Security Incident Reporting Form For all other FIs: <ul style="list-style-type: none"> Submit any updates to the Annex
3. Full Incident Report to MAS <i>(as required under the relevant legislation)</i>	<ul style="list-style-type: none"> Submit Section (A) and (B) 	

Section D: Other Information

D1. IP addresses

Provide the list of IP addresses surfaced from incident. Please state the involvement of the IP addresses in the incident (e.g. Victim, Malware Command & Control Servers, etc.). If IP addresses were resolved from domain names, please specify the domain names and the date/time of resolution of IP addresses from the domain names.

IP Address	Involvement	Domain name from which IP address was resolved	Date/Time of Resolution of IP address from Domain name

E2. Domain Names

Provide the list of domains surfaced from incident. Please state the involvement of the domain names in the incident. (E.g. Drive-by-download Servers, Malware Control & Command Servers, defaced website)

Domain Name	Involvement of Domain name

© Infoblox Inc. All rights reserved. | 22



22

