

DNS NO ECOSISTEMA DE CIBERSEGURANÇA
A Próxima Camada de Segurança

redShift consulting

Paulo Favero, M.Sc.

Infoblox Country Manager Portugal

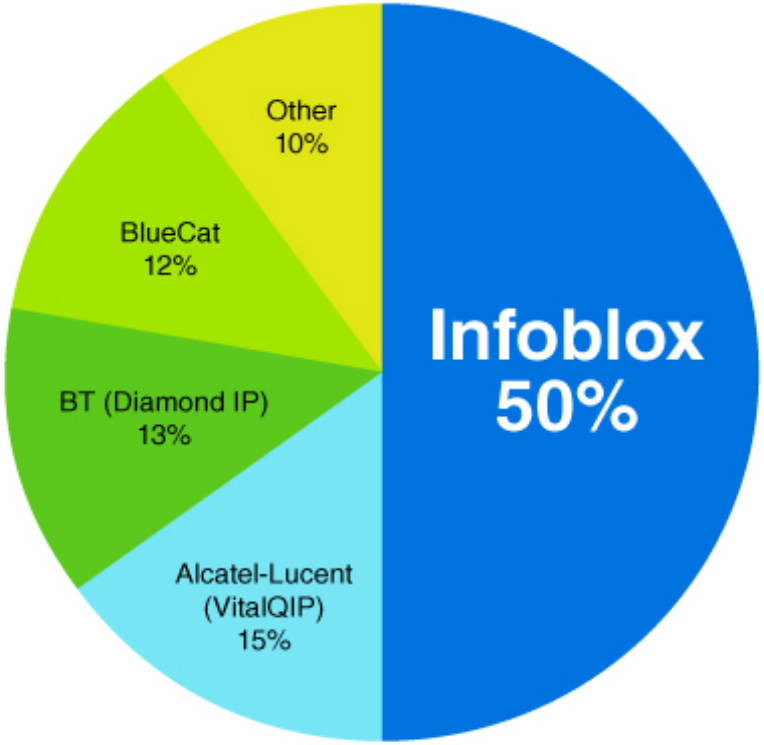
pfavero@infoblox.com

Infoblox
CONTROL YOUR NETWORK

Infoblox Overview & Business Update

- Founded in 1999, IPO in 2012: NYSE BLOX
- Headquartered in Santa Clara, CA with global operations in 25 countries
- Leader in technology for network control
- Market leadership
  - DDI Market Leader (Gartner)
  - 50% DDI Market Share (IDC)
- 8,000+ customers
- 64,000+ systems shipped
- 38 patents, 25 pending
- Annual revenue $300M, 27% CAGR
- Infoblox acquired IID in 2016
  - Leader in providing verified Machine Readable Threat Intelligence (MRTI)

Worldwide DDI Market Share



Source: IDC, Worldwide DDI Market Update, April 2014

 © 2015 Infoblox Inc. All Rights Reserved. CONFIDENTIAL

Diverse Customer Base in All Key Verticals

EXPOSURE TO INDUSTRY TOP 10 LEADERS

7 of the Aerospace and Defense Companies

9 of the Auto and Truck Manufacturers

8 of the Retailers

8 of the Major Banks

7 of the Telecommunications Providers

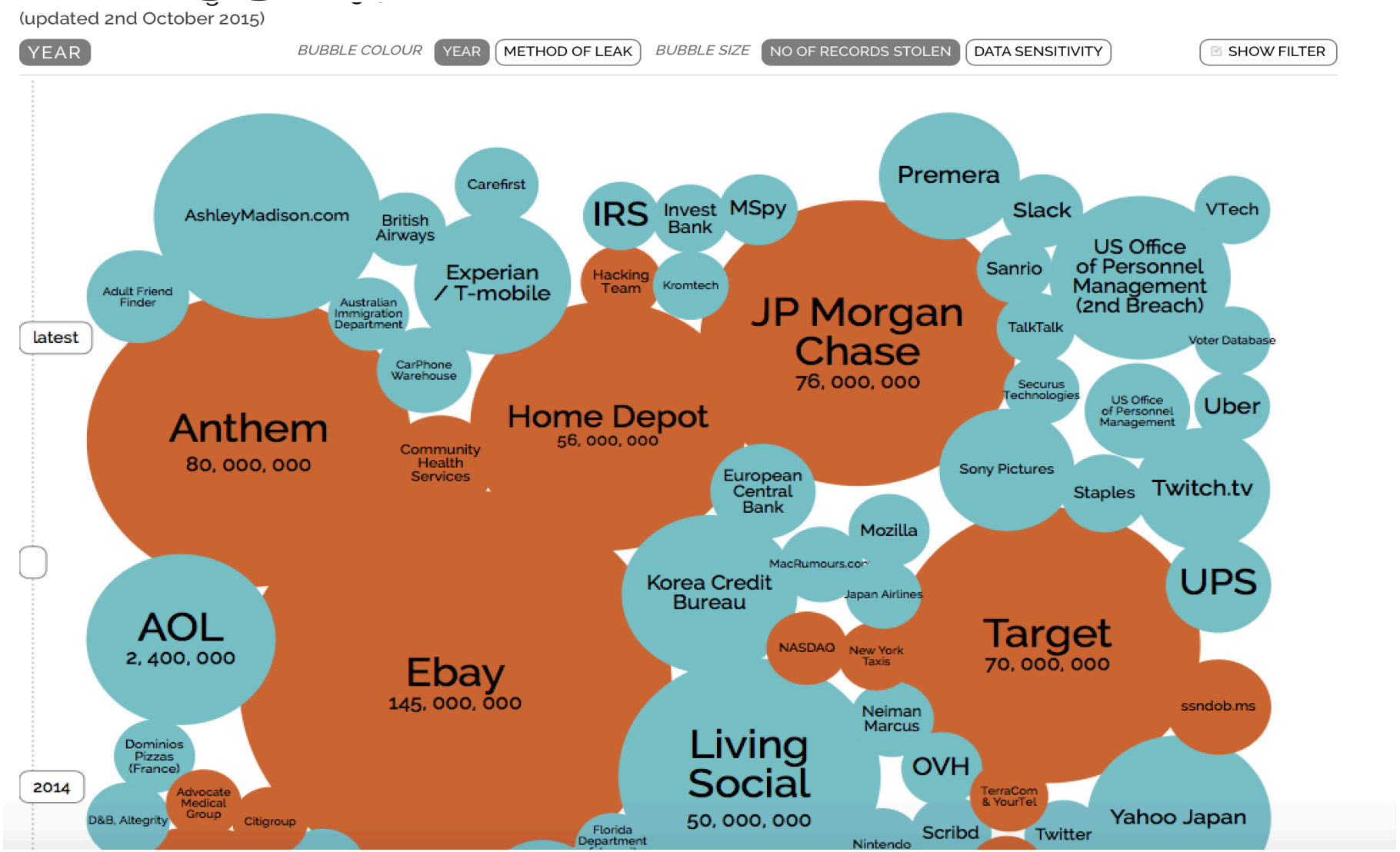
 © 2015 Infoblox Inc. All Rights Reserved. CONFIDENTIAL

Trends in Security



 © 2015 Infoblox Inc. All Rights Reserved. CONFIDENTIAL

World Biggest Data Breaches



* http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

 © 2015 Infoblox Inc. All Rights Reserved.

What the Bad Guys are After and Why

PII (Personally Identifiable Information)	Information like social security numbers of employees or customers that cybercriminals can use to steal identity, or sell in the underground market for profit
Regulated Data	Data related to PCI DSS and HIPAA compliance that can be misused
Intellectual Property	Data that can give an organization a competitive advantage
Other Sensitive Information	Credit card numbers, company financials, payroll and emails



Hacktivism



Espionage



Financial Profit

 © 2015 Infoblox Inc. All Rights Reserved. CONFIDENTIAL

Malware Exploiting DNS



- Over 91% percent malware uses DNS
  - To gain command and control
  - To exfiltrate data
  - To redirect traffic
- Despite adversaries' reliance on DNS, 68% organizations do **not** monitor recursive DNS
- Advanced attacks and data breaches persist and impact all sizes and types of organizations
- Average total cost of data breach ~$3.8M USD
- The question isn't if, but when you will be attacked, and how effectively you can respond

Anthem

SONY PICTURES

TARGET

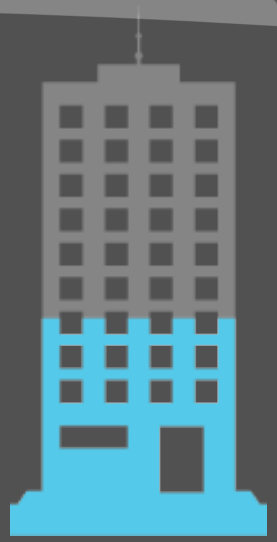
Source: Cisco 2016 Annual Security Report

 © 2015 Infoblox Inc. All Rights Reserved.

DNS and Data Exfiltration

DNS tunneling attacks let infected endpoints or malicious insiders exfiltrate data.

Attackers have recently used DNS tunneling in cases involving the theft of **millions of accounts**.[1]



46%

of large businesses have experienced DNS exfiltration.[2]

$3.8 M

Average consolidated cost of a data breach[3]



A recent high-profile data breach is likely to cost more than[4]

$100M.

1. *SANS Institute paper referencing Ed Skoudis as speaker at RSA Conference,* June 2012
2. *DNS attacks putting organizations at risk, survey finds, SC Magazine,* December 23, 2014
3. Ponemon Institute, 2015 Cost of Data Breach Study
4. *Anthem data breach cost likely to smash $100 million barrier, ZDNet,* February 12, 2015

 © 2015 Infoblox Inc. All Rights Reserved.

CONFIDENTIAL

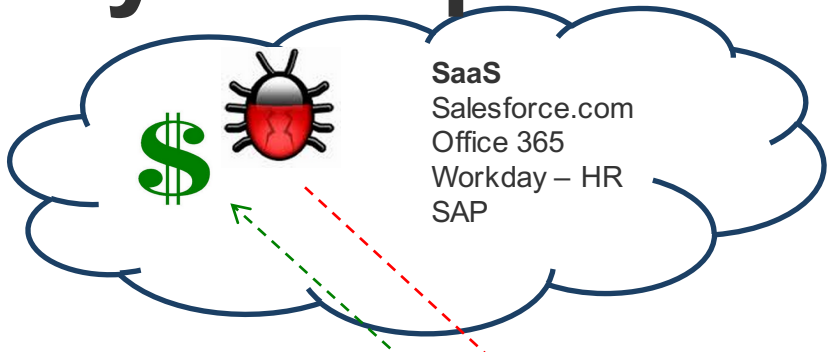
Infoblox

Security Solution Landscape



 © 2015 Infoblox Inc. All Rights Reserved. CONFIDENTIAL

Why DNS Security is important?



Firewall/NGFW

IPS/IDS

Web Proxy

Email/SPAM

APT/Sandbox
DLP

DNS communicates via Port 53 and is NOT protected by these tools

53

SIEM Solution
Your centralized logging and reporting

Infoblox
CONTROL YOUR NETWORK

- ✓ Secure DNS at the source
- ✓ Reporting
- ✓ Proactive block malware and understand who's infected
- ✓ Prevent IP leaving your DC

Biz IP/Data



DNS

DHCP

 | © 2015 Infoblox Inc. All Rights Reserved.

CONFIDENTIAL

U.S. DEPARTMENT OF HOMELAND SECURITY WARNING



- US-CERT has observed an increase in Domain Name System (DNS) traffic from client systems within internal networks to publically hosted DNS servers.
- Cricket's blog: http://www.blog.infoblox.com/uncle-sam-wants-you-to-control-outbound-dns/
- US-Cert announcement: https://www.us-cert.gov/ncas/alerts/TA15-240A/

 © 2015 Infoblox Inc. All Rights Reserved.

Peak Attack Size Year over Year

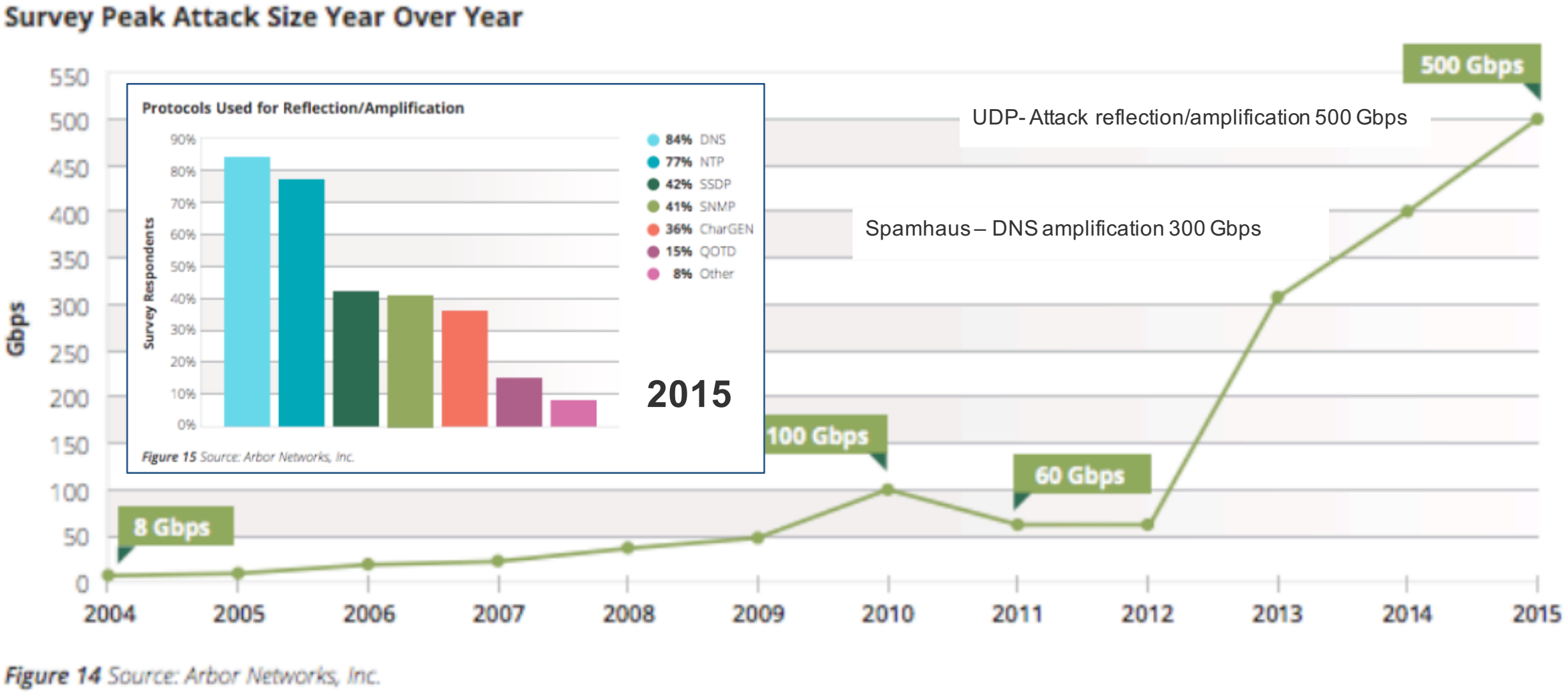


Figure 14 Source: Arbor Networks, Inc.

 © 2015 Infoblox Inc. All Rights Reserved.

DNS Security Challenges

1. Defending against DNS DDoS attacks



2. Stopping APTs/malware from using DNS

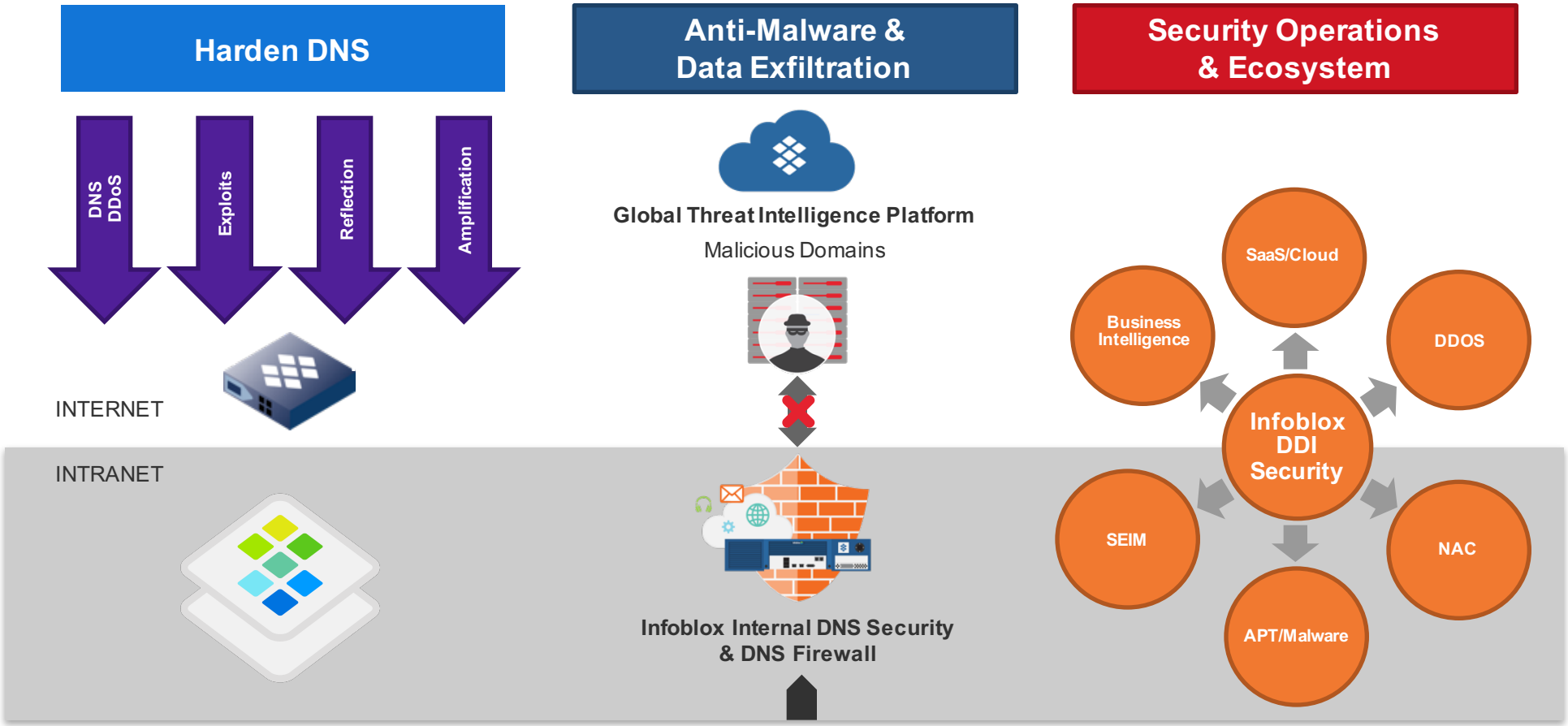


3. Preventing data exfiltration via DNS



 © 2015 Infoblox Inc. All Rights Reserved. CONFIDENTIAL

Infoblox Defense-In-Depth Strategy

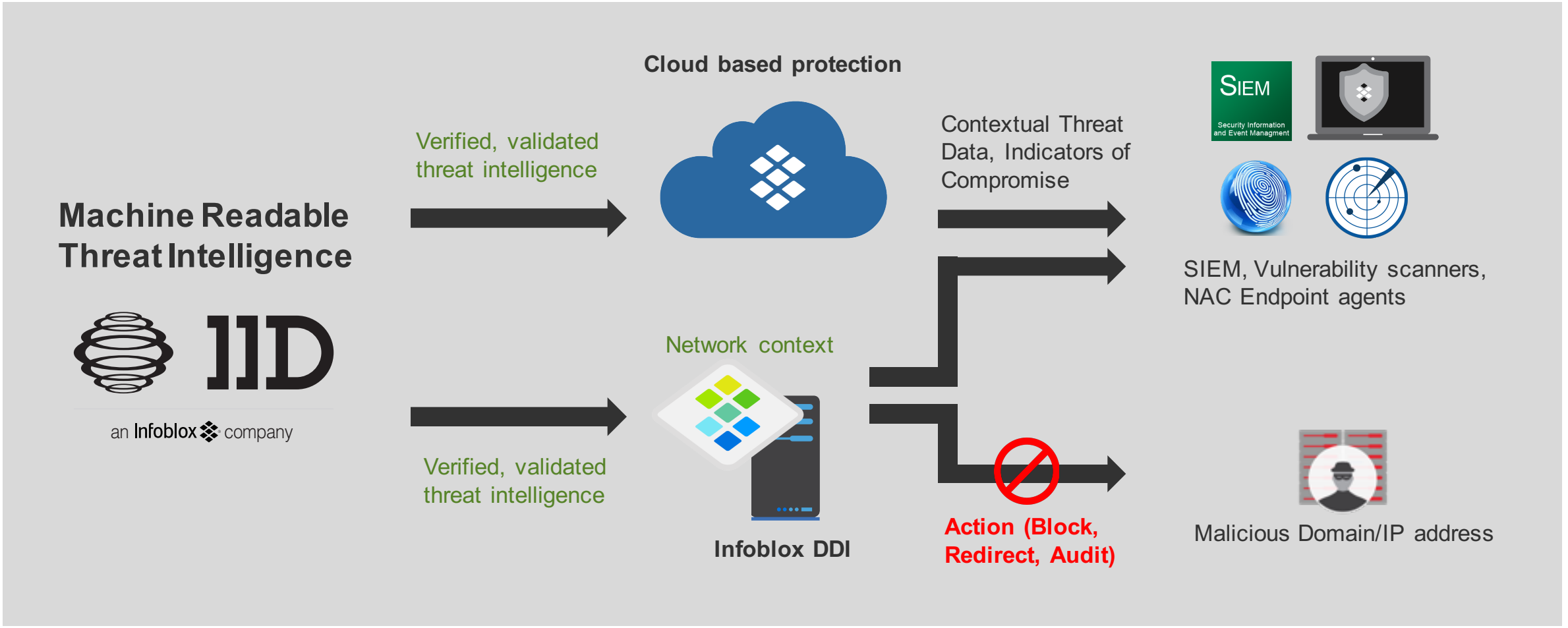


 | © 2015 Infoblox Inc. All Rights Reserved.

CONFIDENTIAL

Infoblox

Infoblox Platform Powered by IID



 | © 2015 Infoblox Inc. All Rights Reserved.

CONFIDENTIAL

What Makes Infoblox + IID Unique

Bringing together threat intelligence and enterprise context…



Prioritize

Respond to threats based on security and enterprise context and risk



Protect

Block malicious activity for both on-premise and off-premise devices



Predict

Preempt security compromises based on federated vertical and geo threat intelligence

Context-Aware Security

… to take action at the control point of the network

 © 2015 Infoblox Inc. All Rights Reserved. CONFIDENTIAL

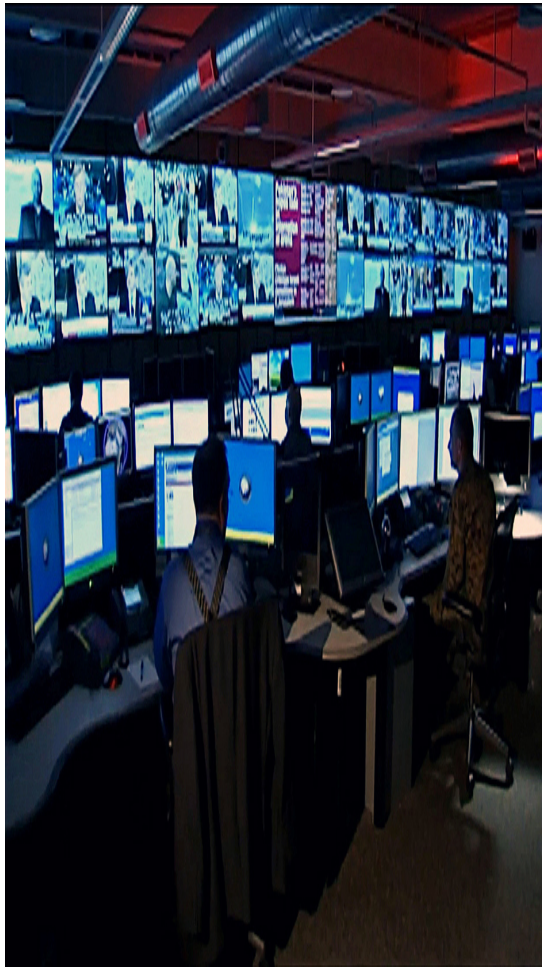
Infoblox as part of Cybersecurity Ecosystem



 | © 2015 Infoblox Inc. All Rights Reserved.

CONFIDENTIAL

Security Case – US Federal Defense Agency



Problem

Malware Infection

- 40M outbound queries per week to suspicious/malicious domains
- Struggled to maintain blacklists
- Difficulty identifying infected devices

Infoblox Solution

Infoblox DNS Firewall

- Automatically detected and blocked malware queries to malicious destinations
- Customer now has visibility (reporting) and control
- Automatically pinpointed the infected devices

Automated APT/Malware Protection Using DNS

 © 2015 Infoblox Inc. All Rights Reserved. CONFIDENTIAL

Infoblox as Authoritative Network Database

- What IP?
- When?
- Which MAC?
- Device Type?
- Hostname?
- User Behind?
- Where is It?
- Infected?



What has happened in the past?

IP, User, hostname, RPZ, lease…

Tracking History?

Infoblox

 © 2016 Infoblox Inc. All Rights Reserved.

Thank You

Infoblox

