



# Infoblox DNS, DHCP – czy biznes może bez nich żyć?

Rafał Szewczyk Regional Sales Manager Eastern Europe

# AGENDA

1

DNS, DHCP – czy biznes może bez nich żyć??

2

Czy stosujesz dobre praktyki bezpieczeństwa?

3

Ale ja już mam X rozwiązań bezpieczeństwa

4

Ostatnia niezabezpieczona furka – protokół 53/DNS

# DNS, DHCP – czy biznes może bez nich żyć??



# Skutki niedostępności DHCP I DNS

DDI



Redundancja  
serwerów



Krytyczne usługi  
sieciowe:  
DNS, DHCP, IP



Redundancja  
sieci

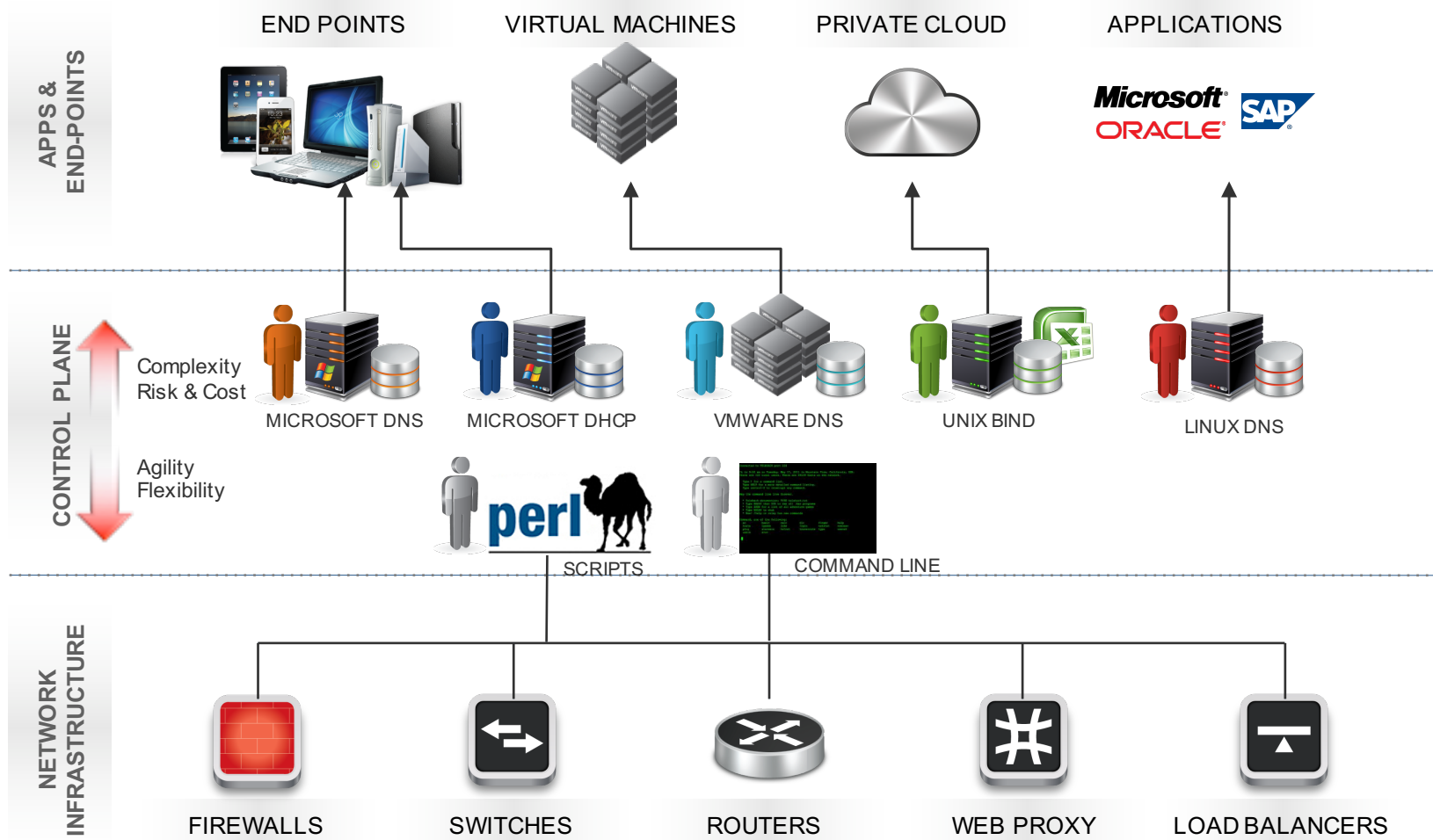


# DNS to naprawdę krytyczna usługa sieciowa!

**DNS**  
....  
**JEST  
KRYTYCZNY  
DLA  
APLIKACJI**



# Świat obecny znany od lat

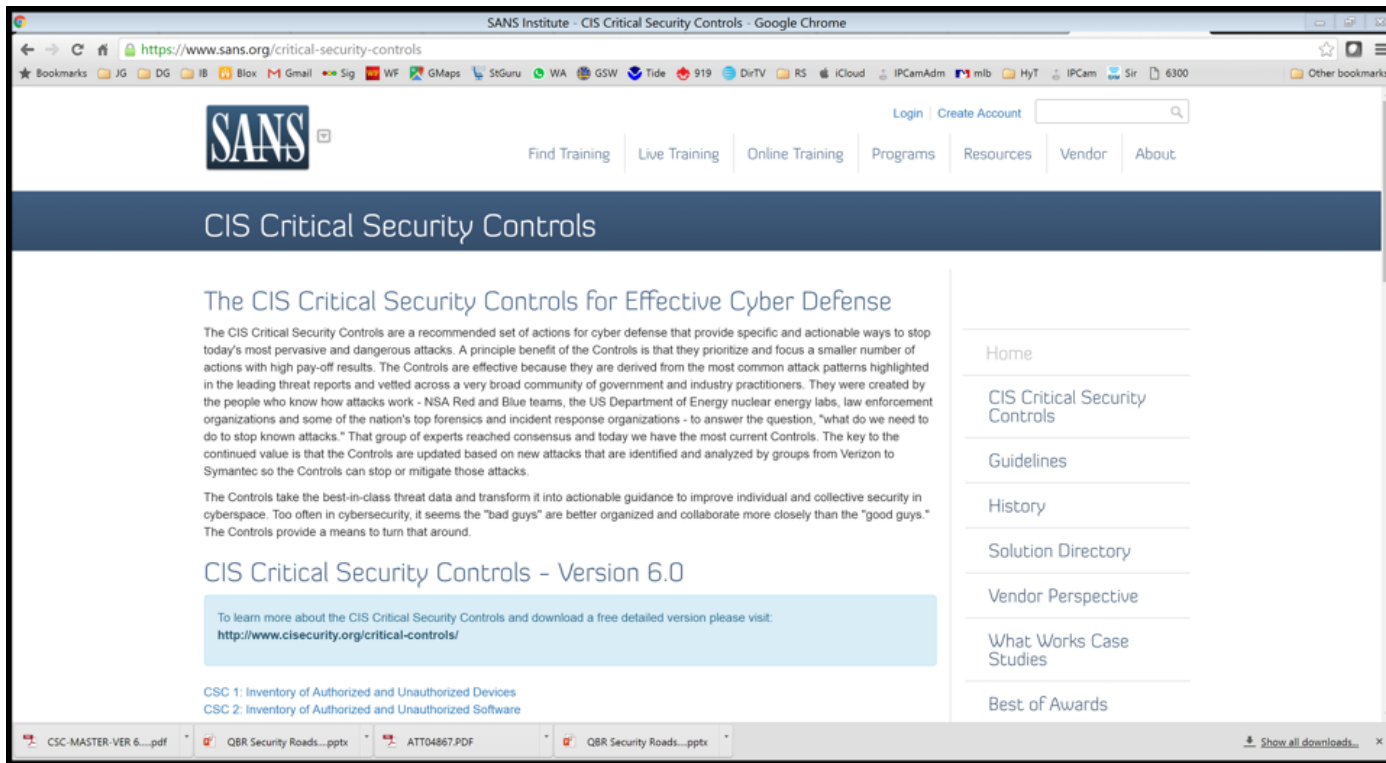


# Czy stosujesz dobre praktyki bezpieczeństwa?



# SANS Top 20 Critical Security Controls

## Well-respected security baseline



The screenshot shows a web browser window displaying the SANS Institute website. The address bar shows the URL <https://www.sans.org/critical-security-controls>. The page features the SANS logo and a navigation menu with links for Find Training, Live Training, Online Training, Programs, Resources, Vendor, and About. The main heading is "CIS Critical Security Controls". Below this, there is a section titled "The CIS Critical Security Controls for Effective Cyber Defense" with a detailed paragraph explaining the purpose and origin of the controls. A blue box contains a link to <http://www.cisecurity.org/critical-controls/>. The page also lists "CIS Critical Security Controls - Version 6.0" and includes a sidebar with links to Home, CIS Critical Security Controls, Guidelines, History, Solution Directory, Vendor Perspective, What Works Case Studies, and Best of Awards. The browser's taskbar at the bottom shows several open files, including PDFs and PPTX files.

<https://www.sans.org/critical-security-controls>



# Control #1: Inventory of Devices!

You can't protect or defend what you can't see

## CIS Critical Security Controls - Version 6.0

To learn more about the CIS Critical Security Controls and download a free detailed version please visit:  
<http://www.cisecurity.org/critical-controls/>

- 
- CSC 1: Inventory of Authorized and Unauthorized Devices
  - CSC 2: Inventory of Authorized and Unauthorized Software
  - CSC 3: Secure Configurations for Hardware and Software on Mobile Device Laptops, Workstations, and Servers
  - CSC 4: Continuous Vulnerability Assessment and Remediation
  - CSC 5: Controlled Use of Administrative Privileges
  - CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
  - CSC 7: Email and Web Browser Protections
  - CSC 8: Malware Defenses
  - CSC 9: Limitation and Control of Network Ports, Protocols, and Services
  - CSC 10: Data Recovery Capability
  - CSC 11: Secure Configurations for Network Devices such as Firewall Routers, and Switches
  - CSC 12: Boundary Defense
  - CSC 13: Data Protection
  - CSC 14: Controlled Access Based on the Need to Know
  - CSC 15: Wireless Access Control
  - CSC 16: Account Monitoring and Control
  - CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
  - CSC 18: Application Software Security
  - CSC 19: Incident Response and Management
  - CSC 20: Penetration Tests and Red Team Exercises

*“Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.”*

<https://www.sans.org/critical-security-controls>

# Control #1: Inventory of Devices!

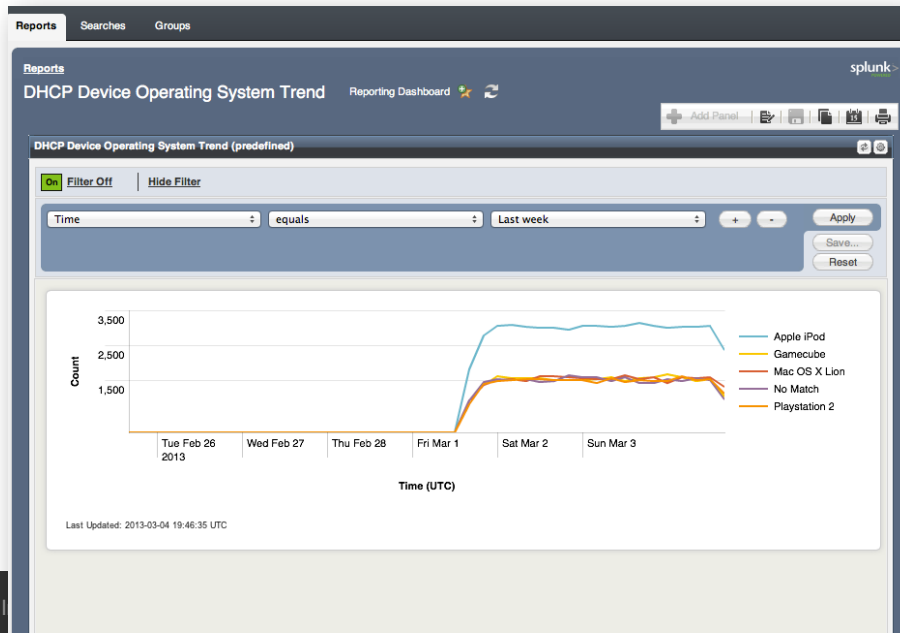
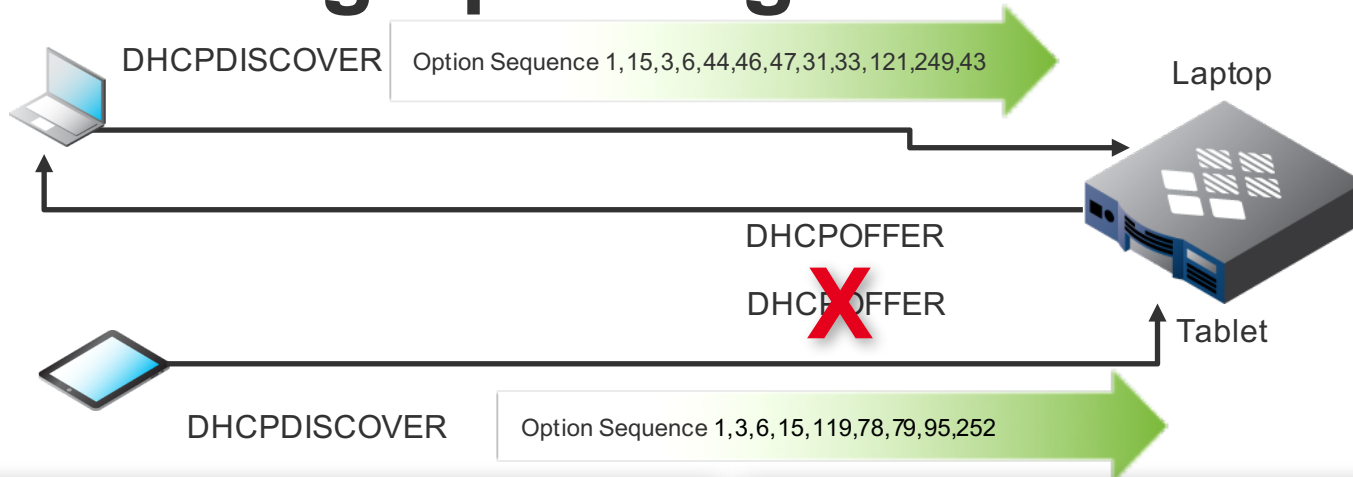
Use SANS to gain credibility and help find the pain!

CSC 1: Inventory of Authorized and Unauthorized Devices		
Family	Control	Control Description
System	1.1	<u>Deploy an automated asset inventory discovery tool</u> and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.
System	1.2	If the organization is dynamically assigning addresses using DHCP, then <u>deploy dynamic host configuration protocol (DHCP) server logging</u> , and use this information to improve the asset inventory and help detect unknown systems.
System	1.3	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.
System	1.4	Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. <u>The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.</u>

*"I'm sure you're aware that the SANS Top 20 control #1 is network device inventory. How you doing on that control?!"*

<https://www.sans.org/critical-security-controls>

# DHCP Fingerprinting



**DHCP Top Device Operating System**

Time: equals Last day


TopN: equals 10

Fingerprint	Total	% of all devices
1 Apple iPod	17536	22
2 Mac OS X Lion	9031	12
3 Gamecube	8878	11
4 Playstation 2	8709	11
5 Xbox 360	8442	11
6 No Match	8417	11
7 Playstation 3 or Playstation Portable (PSP)	8371	11

**MAC/DUID and Lease IP for Fingerprint= Playstation 3 or Playstation Portable (PSP)**

Lease IP	MAC/DUID
1 10.65.44.100	00:7d:5f:16:e9:5f
2 10.65.44.100	00:7d:5f:16:e9:5f

# Find & Remediate Potential Security Breaches

IPAM Home > 192.168.0.0/16 > 192.168.1.0/24  
192.168.1.22 IPv4 Address 

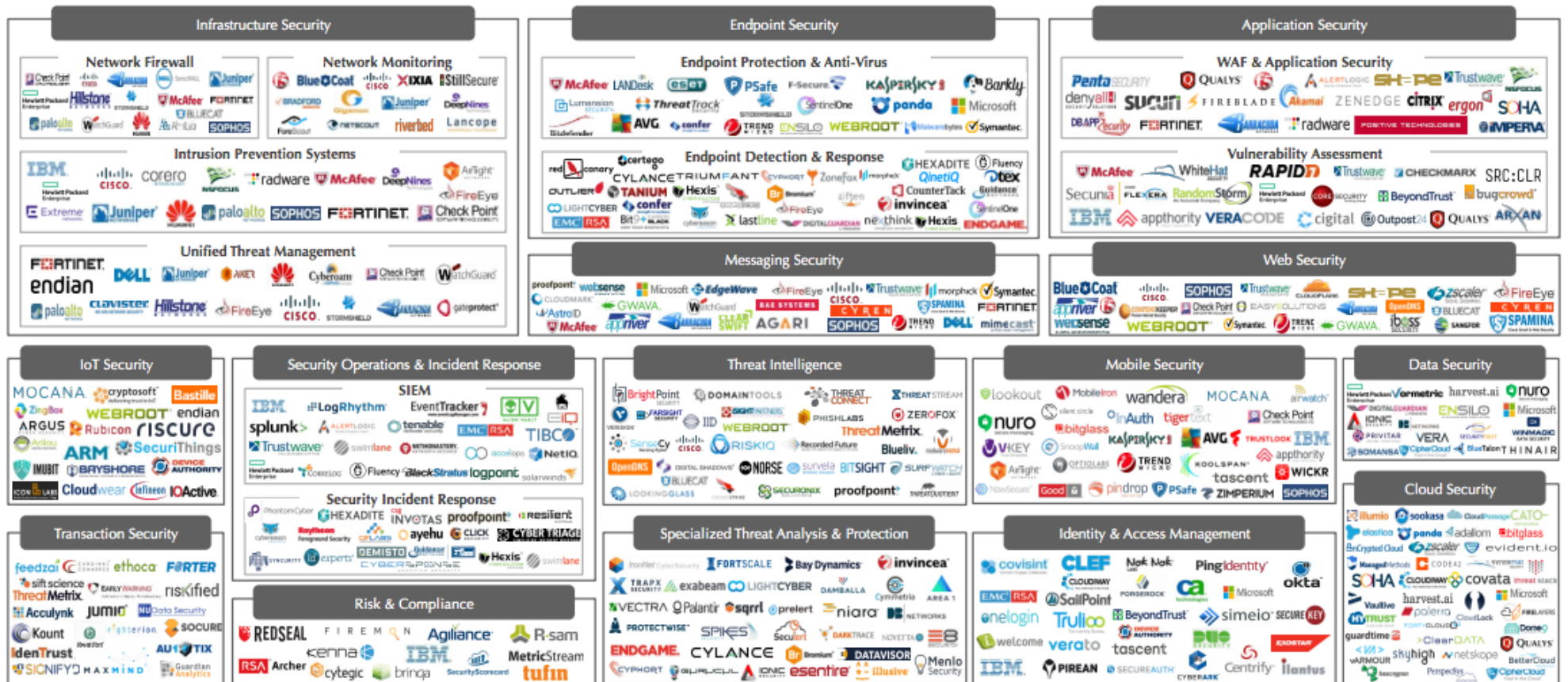
### Discovered Data

NetBIOS Name: <b>WIN-4SCOBLFST1</b>	OS: <b>Microsoft Windows Server 2008 R2 (64-bit)</b>
Discovered MAC Address: <b>00:50:56:bb:e3:6d</b>	Last Discovered: <b>2014-02-21 11:01:07 CET</b>
First Discovered: <b>2014-01-11 01:11:38 CET</b>	Discovered Name: <b>WIN-4SCOBLFST1.infobloxdemo.com</b>
Discoverer: <b>gm1p1.infoblox.com</b>	Attached Device Description: <b>Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M), Version 12.2(55)SE3, RELEASE SOFTWARE (f c1) Technical Support: <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> Copyright (c) 1986-2011 by Cisco Systems, Inc. Compiled Thu 05-May-11 15:40 by prod_rel_team</b>
Attached Device Address: <b>192.168.1.254</b>	Attached Device Name: <b>tae-demo</b>
Attached Device Port Description: <b><a href="#">link to Main ESXI DEMO server</a></b>	Attached Device Port Name: <b>Gi3/0/1</b>
Attached Device Port: <b>109</b>	Port Duplex: <b>Full</b>
Port Link: <b>Connected</b>	Port Speed: <b>1G</b>
Port Status: <b>Up</b>	VLAN Description:
VLAN Name: <b>default</b>	Virtual Host Adapter: <b>vmnic1</b>
Virtual Datacenter: <b>ha-datacenter</b>	Virtual Cluster:
Virtual Entity Name: <b>G-ms3</b>	Virtual Entity Type: <b>Virtual Machine</b>
Virtual Host: <b>DNSDEMO.TME.Inca.infoblox.com</b>	Virtual Switch: <b>vSwitch1</b>

# Ale ja już mam X rozwiązań bezpieczeństwa



# Security Landscape: Welcome to the Jungle!



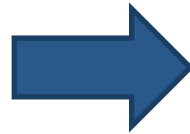
Source: Momentum Partners.

**Ilu było producentów?**

**Jakieś sugestie??**

**406 producentów!!!**

# Customer Security Challenges



**Security They Want**

**Security They Often Get**

Customer Security Challenges

Inability to Prioritize Events

Lack of Visibility

Lack of Vendor Integration

Manual Processes

Inability to Respond




# What do Security Types Deal With Day to Day?

- Making sure systems are operational. Examples:
  - Is my logging system collecting all the data?
  - Is the newly connected user compliant relative to my security devices?
- Monitoring and visibility of overall security situation
- Floods of alerts – way more than they can handle
  - Very hard to prioritize based on actual risk
- Incident Handling & Response
  - Trying to decide what's the Scope/Severity/Veracity of the threat?
  - Assembling data from disparate sources to decide what to do
  - Actual response: What actions to take and where?
- Keeping up with the general threat landscape
- Trying to make sense of vendor and “expert” claims and advice




# Gartner Security Recommendations: Include a Focus on Cross-Product Integration

## End-User Recommendations

- 
- **Seek solutions with cross-product integration that enables improvements towards context-based decision making.**
  - Use price negotiation in lower demand segments to save money.
  - Maximize the use of product suites and avoid shelfware situations.
  - Examine advanced threat protection as market consolidates this function.

## Technology Provider Recommendations

- 
- Focus on improving efficacy (No. 1 Buying Criteria).
  - Focus on delivering suite or bundled solutions.
  - **Continue to leverage cross-product integration efforts to utilize context information and automated response capabilities.**
  - Providers in segments with decreased demand should increase marketing efforts or consider new product development/M&A.

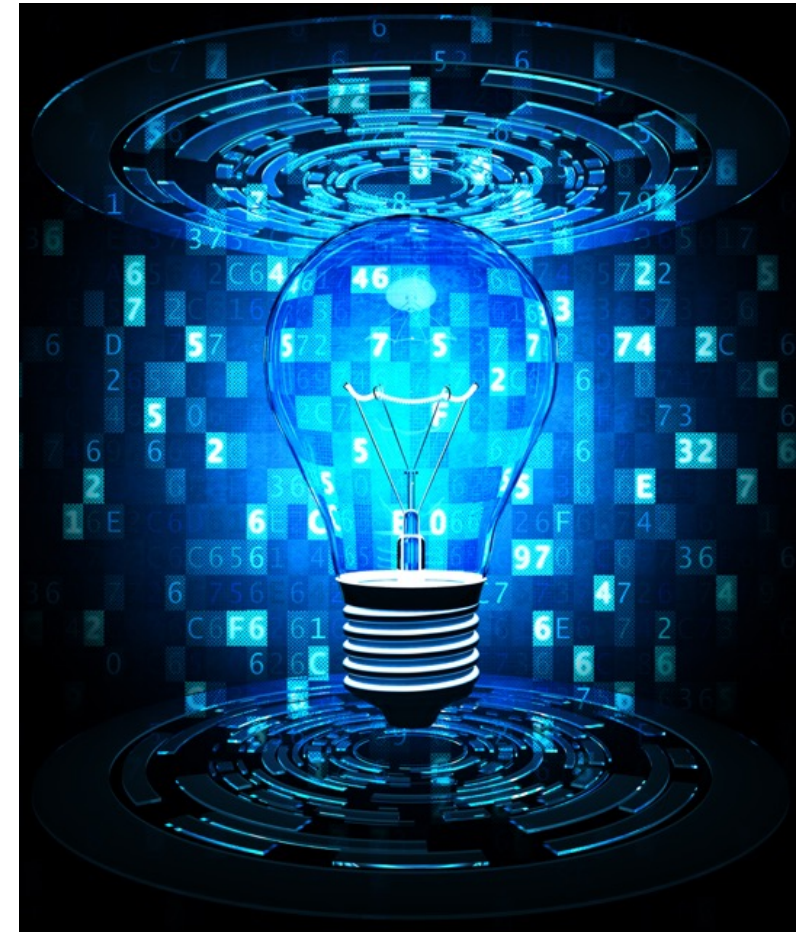
# Infoblox Security Strategy in Two Bullets

- **Security Integration & Ecosystem**

- Our unique position in the network creates a rich data source to be shared with customer security systems and architectures
- Infoblox Grid data provides business context that security systems lack and badly need

- **DNS Security**

- DNS is a unique threat vector that deserves a dedicated solution
- Infoblox is best positioned to plug this increasingly critical gap



# Infoblox Data and Its Relevance to Security



**A DHCP assignment signals the insertion of a device on to the network**

- Includes context: Device info, MAC, lease history
- DHCP is an audit trail of devices on the network

## IPAM



**Fixed IP addresses are typically assigned to important devices:**

- Data center servers, network devices, etc.
- IPAM provides “metadata” (additional business context) via EAs: Owner, app, security level, location, ticket number
- *And the business importance of the asset determines level of risk!*



**DNS is the first step in almost every activity, good or bad.**

**DNS query data provides a “client-centric” record of activity**

- Includes internal activity *inside the security perimeter*
- Includes BYOD and IoT devices
- This provides an excellent basis to profile device & user activity

Security Relevant Data and Context Using Network Infrastructure

# Ostatnia niezabezpieczenia furtka – protokół 53/DNS



# Malware Exploiting DNS



Source: Cisco 2016 Annual Security Report



## DNS

**91.3%**  
of malware uses  
DNS in attacks



**68%**  
of organizations  
don't monitor  
recursive DNS

Source: Cisco Security Research

  
CISCO

Cisco 2016  
Annual Security Report

# The Rising Tide of DNS Threats

Are You Prepared?

In the last year alone there has been an increase of

**216%**  
DNS attacks<sup>1</sup>

**47%**  
DDoS attacks<sup>2</sup>



With possible amplification up to **100x** on a DNS attack, the amount of traffic delivered to a victim can be huge



**28M**

Pose a significant threat to the global network infrastructure and can be easily utilized in DNS amplification attacks<sup>3</sup>



**33M** Number of open recursive DNS servers<sup>3</sup>



With enterprise level businesses receiving an average of **2 million** DNS queries every single day, the threat of attack is significant

1. Prolexic Quarterly Global DDoS Attack Report, Q4, 2013 2. Prolexic Quarterly Global DDoS Attack Report, Q1, 2014 3. [www.openresolverproject.org](http://www.openresolverproject.org)

# The Rising Tide of DNS Threats

Are You Prepared?

## Financial Impact is huge

Estimated cost of a DDoS attack can be upwards of

**\$100,000**  
per hour<sup>5</sup>

## Resulting in:



Revenue Loss



Customer Defection



Brand Damage



Data theft from "smokescreening"

55% of DDoS targets were also victims of theft<sup>5</sup>

## Top Industries Targeted<sup>6</sup>

16%

Media & Entertainment

9%

High Tech

Commerce

Consumer Goods  
Hotels  
Retail

20%

Public Sector

28%

Enterprise  
Business Services  
Financial Services  
Healthcare  
Automotive

27%

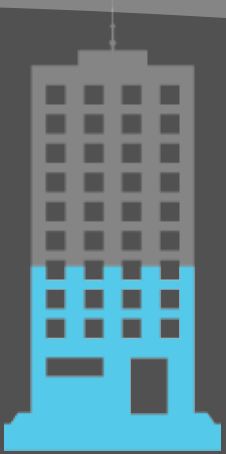


# DNS and Data Exfiltration

**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**.<sup>1</sup>



**46%** of large businesses have experienced DNS exfiltration.<sup>2</sup>

**\$3.8 M**

Average consolidated cost of a data breach<sup>3</sup>



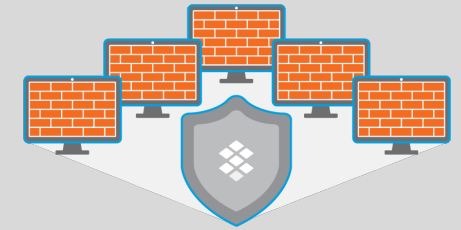
A recent high-profile data breach is likely to cost more than<sup>4</sup>

**\$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

# DNS Security Challenges

1 Defending against DNS DDoS attacks



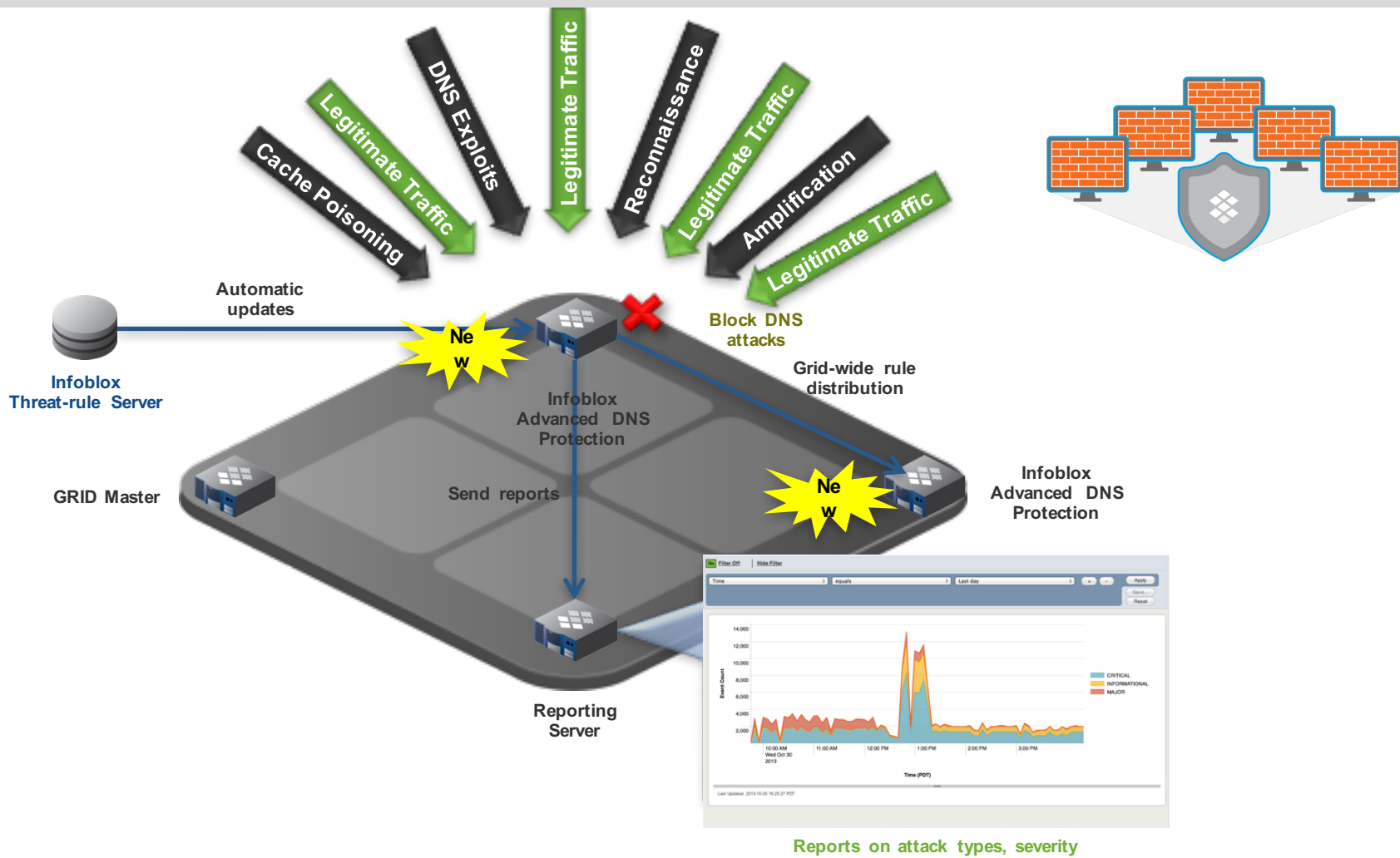
2 Stopping APTs/malware from using DNS



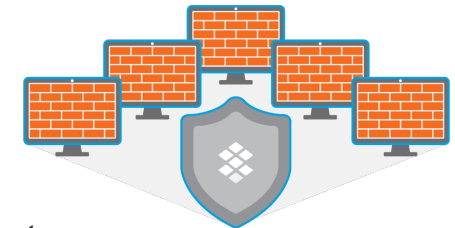
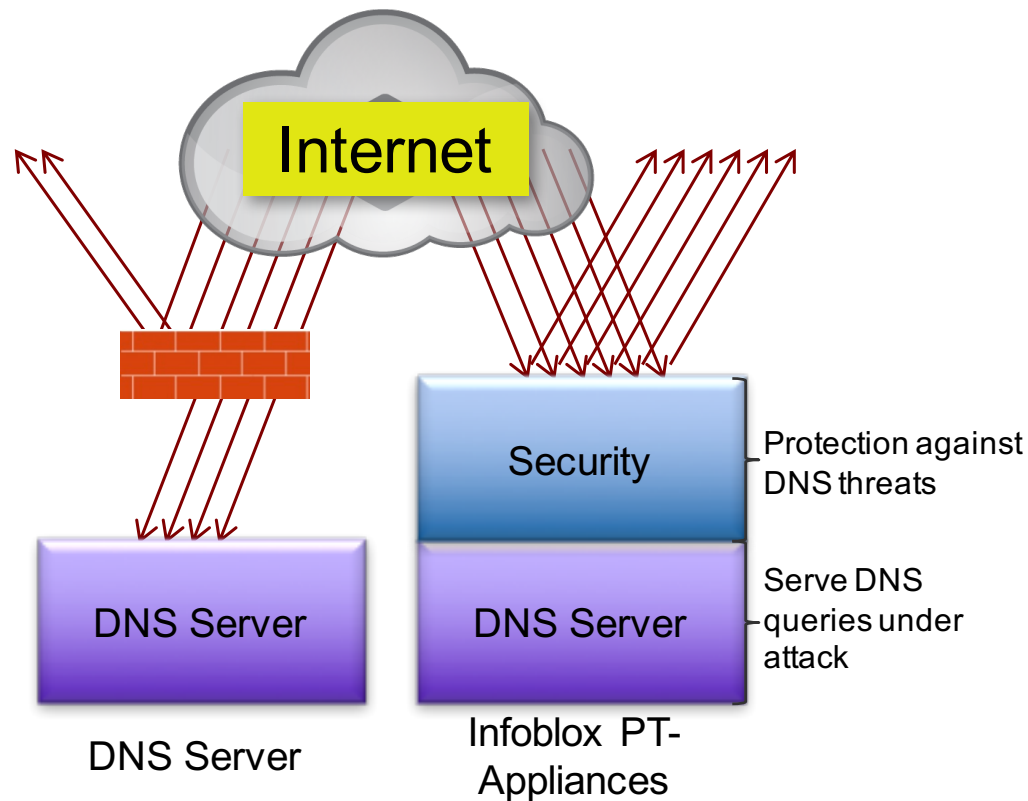
3 Preventing data exfiltration via DNS



# 1 Advanced DNS Protection - Defending against DNS DDoS attacks



# 1 Advanced DNS Protection - Defending against DNS DDoS attacks



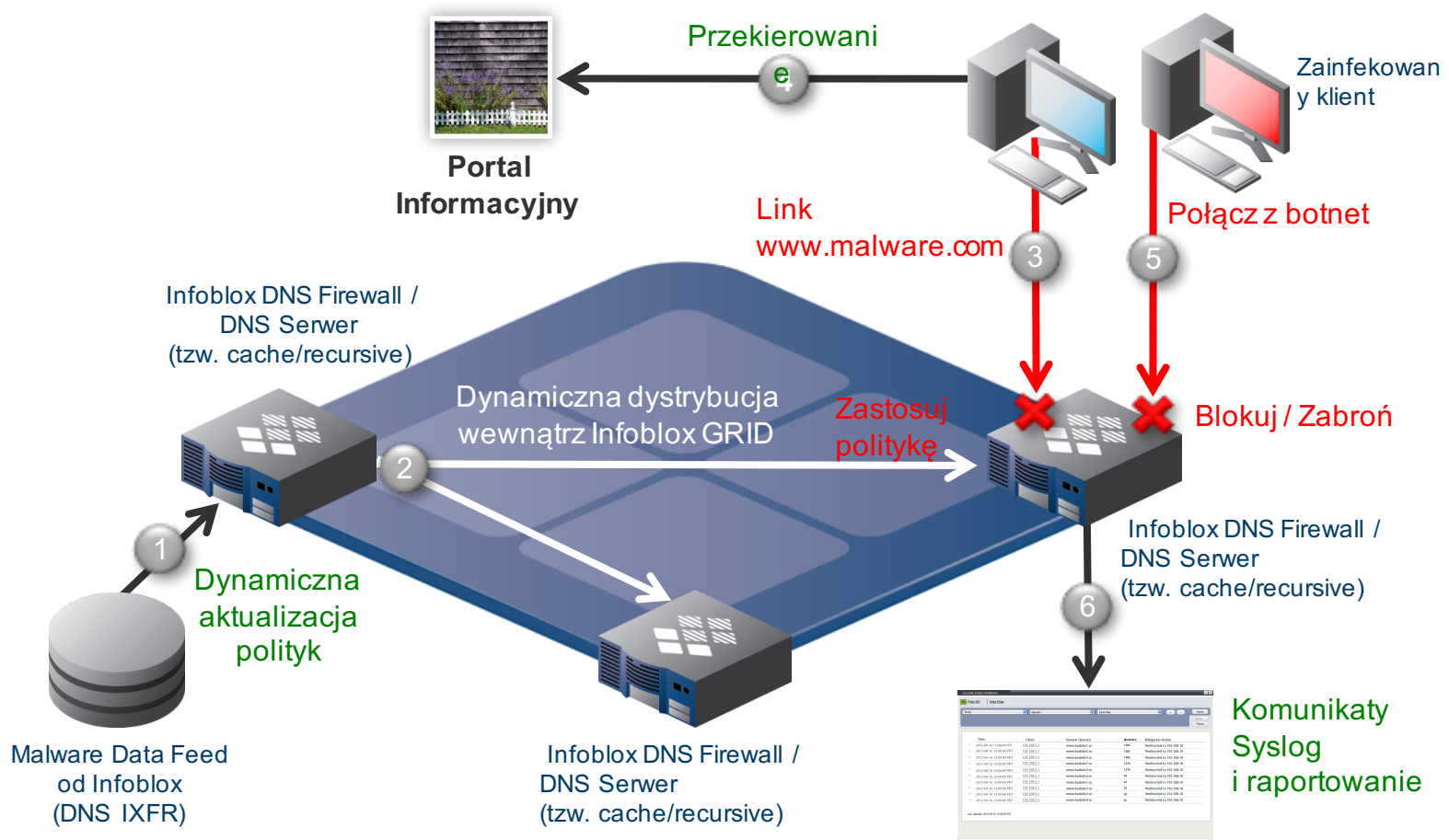
## Use Cases

- Enterprise Customers
  - External authoritative DNS server
  - Internal DNS- Enterprise / Universities with open networks
- Service Providers
  - Recursive Caching
  - Authoritative DNS services

Traditional security appliances mitigate only partial attacks against DNS

# 2

## DNS Firewall - Stopping APTs/malware from using DNS



## 3

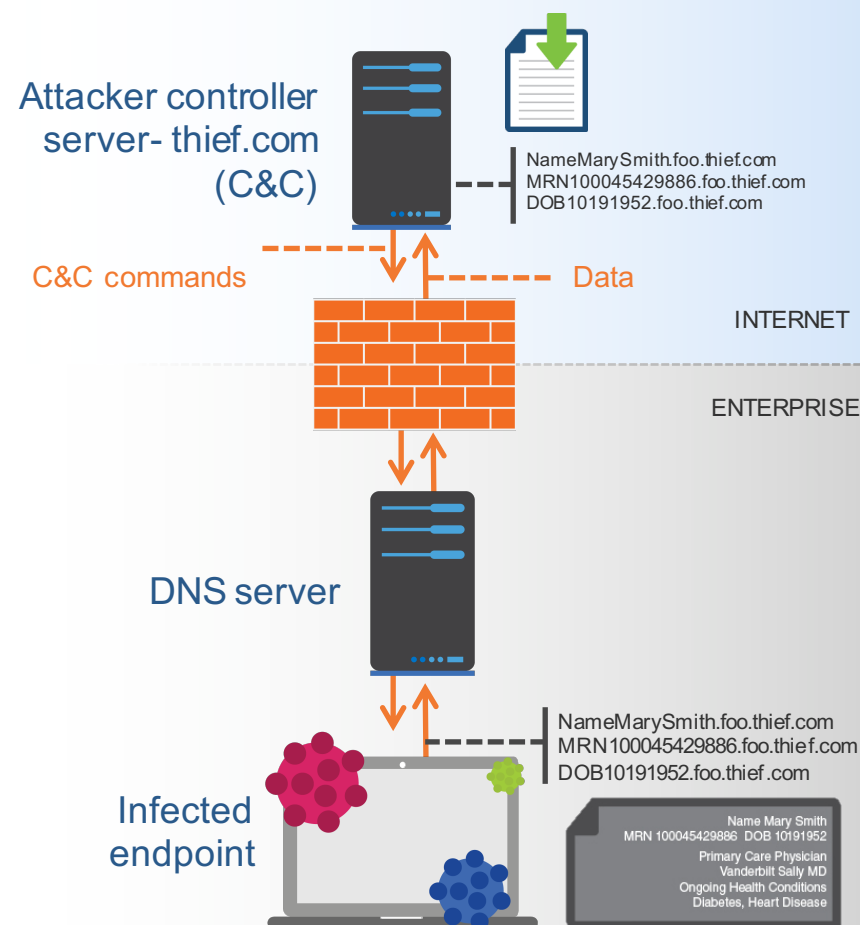
## DNS Threat Insight - Preventing data exfiltration via DNS



- Sophisticated (zero-day)
- Infected endpoint gets access to file containing sensitive data
- It encrypts and converts info into encoded format
- Text broken into chunks and sent via DNS using hostname.subdomain or TXT records
- Exfiltrated data reconstructed at the other end
- Can use spoofed addresses to avoid detection

### Data Exfiltration via host/subdomain Simplified/unencrypted example:

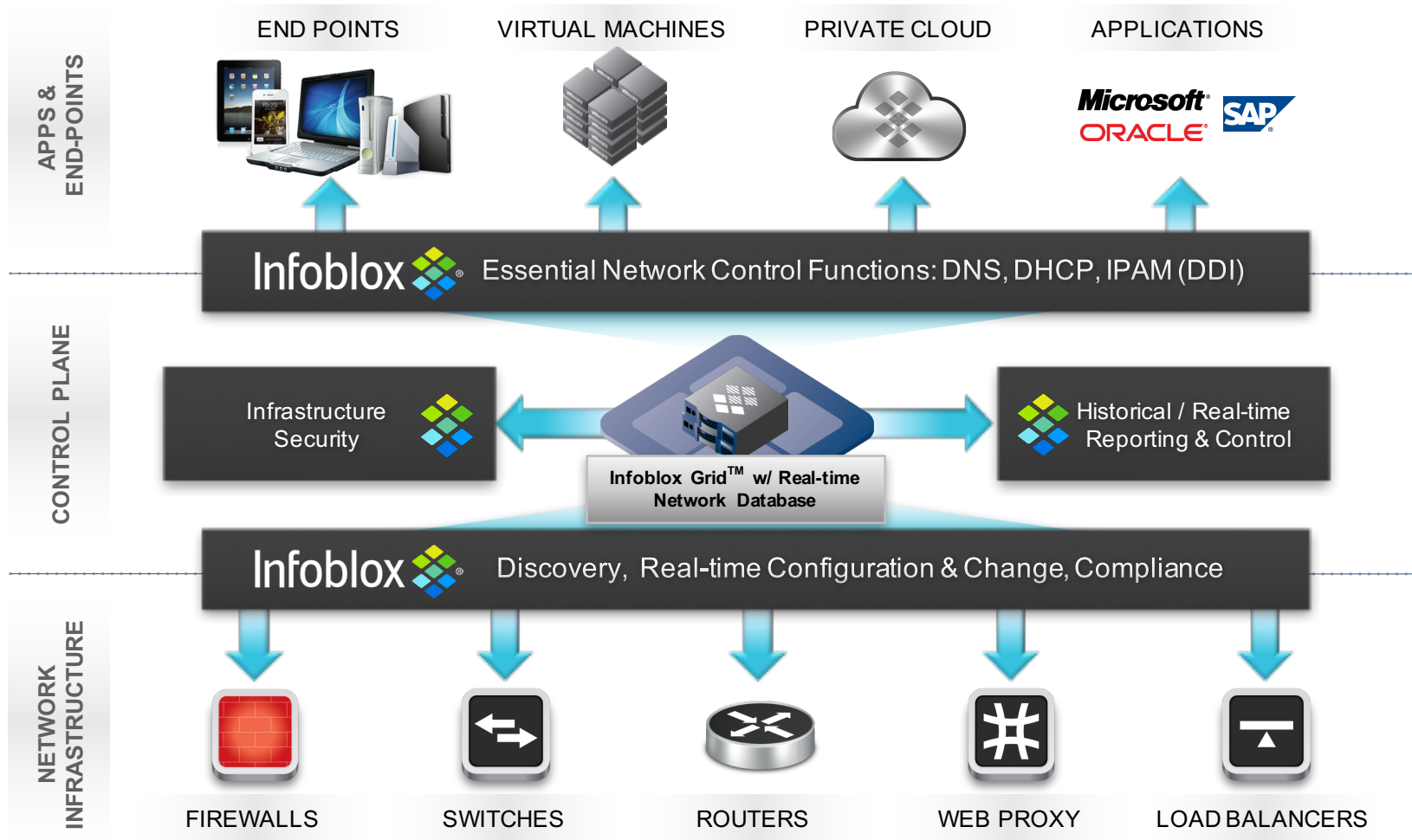
MarySmith.foo.thief.com  
SSN-543112197.foo.thief.com  
DOB-04-10-1999.foo.thief.com  
MRN100045429886.foo.thief.com



# Our Security Ecosystem – Expanding Aggressively



# Alternatywna wizja świata





# Nieprzekonany?

Wyślij nam plik PCAP a my zobaczymy co w trawie piszczy

- Infoblox analyzes and provides insights on malicious activity in seconds
- Report on findings to take back to management

## ADP Categories

Category	Matches	Unique IPs
Default Pass/Drop	960	1
DNS Tunneling	148	6
DNS DDoS	100	1
DNS Amplification and Reflection	60	1
DNS Protocol Anomalies	11	1
TCP/UDP Floods	5	1

## ADP statistics by rules

ID	Rule name	Domain	Severity	Unique IPs	Alert	Drop
110100700	EARLY DROP UDP query invalid question class <i>This rule drops UDP DNS packets when the RR (resource record) class being queried is invalid.</i>		Critical	1		11
130000500	RATELIMIT UDP high rate inbound large DNS queries (anti tunneling) <i>This rule warns if any source IP sends large UDP DNS queries (which could be DNS tunneling attacks) until the traffic hits the rate limit. It then drops all such traffic for some time, which is user configurable.(subcategory: Large Query/Response)</i>	*.sophosxl.net	Major	5	116	

