Infoblox®
NEXT LEVEL NETWORKING

Building a Secure Architectural Foundation for Next Generation Networks and Digital Transformation

Victor Danevich, CTO, System Engineering

Key CISO Challenges

How can I do more with less?

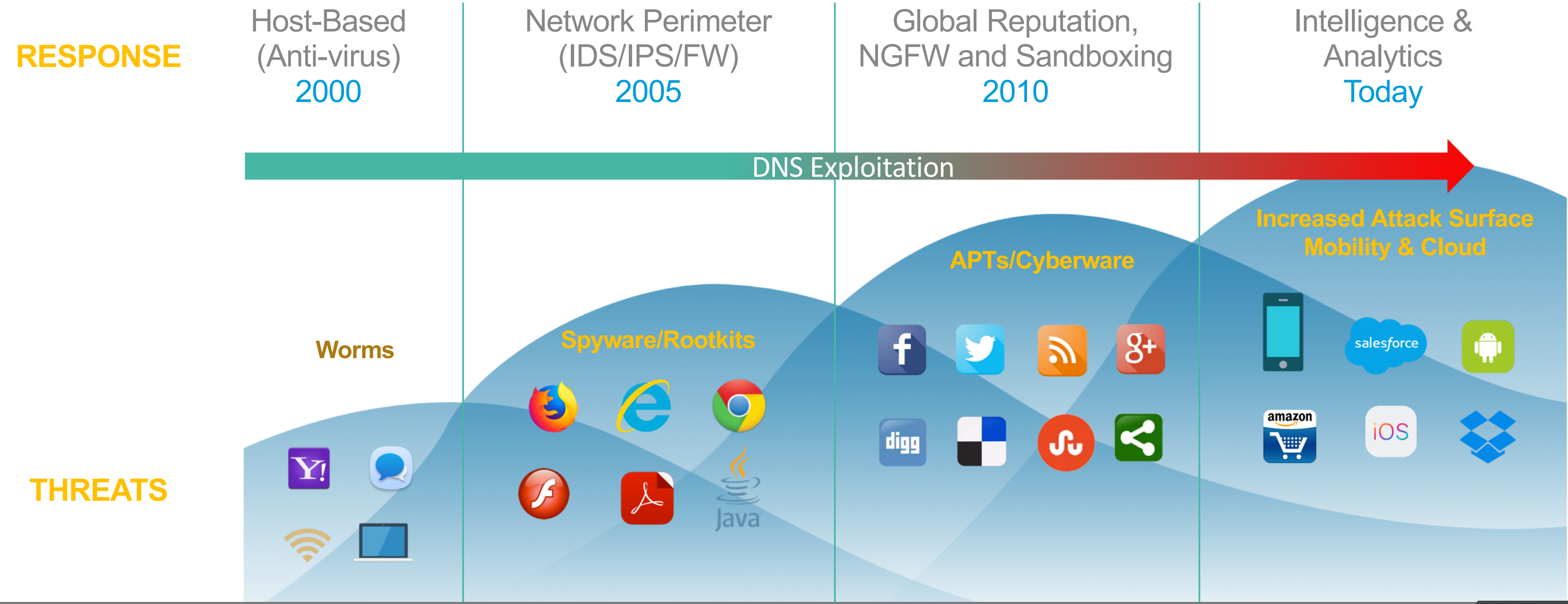
How do I simplify?

Build adaptive security architectures

Improve compliance scoring

Protect the enterprise

The Threat Landscape Evolution



RESPONSE

Host-Based (Anti-virus) 2000

Network Perimeter (IDS/IPS/FW) 2005

Global Reputation, NGFW and Sandboxing 2010

Intelligence & Analytics Today

DNS Exploitation

THREATS

Worms

Spyware/Rootkits

APTs/Cyberware

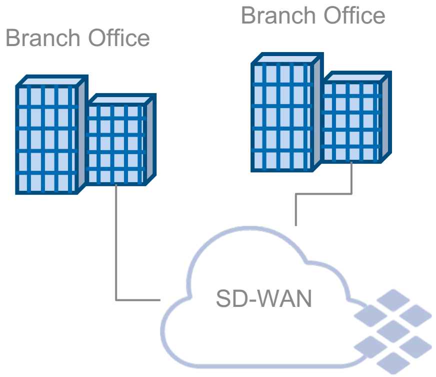
Increased Attack Surface Mobility & Cloud

Traditional Security Model Obsolete for Today's World

Cloud is the New Network

Shifting perimeter. Direct access to cloud applications from everywhere

SD-WAN, Virtualization drive network transformation



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

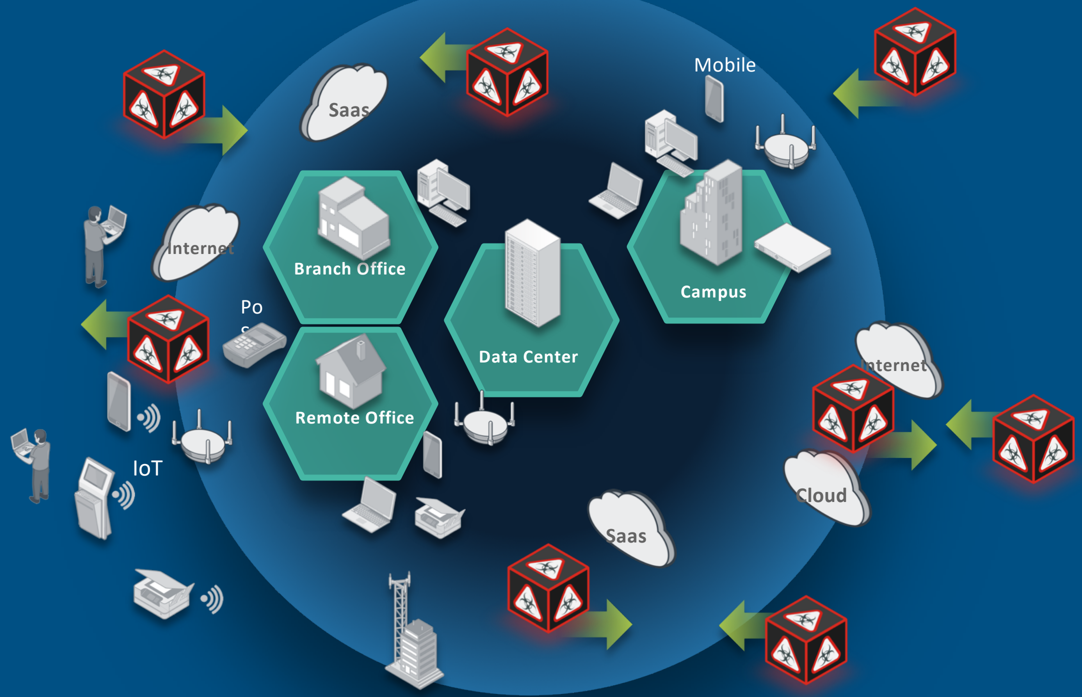
IoT leads to explosion of devices

Endpoint security cannot be deployed on lightweight IoT devices

But, new risk does not always equal need for a new tool!

Malware Can Infiltrate from Any Point

More ways in…



More ways out…

Business Disruptions are Costly and Impacts Brand

$40M

Initial loss from a recent ransomware attack

$119B

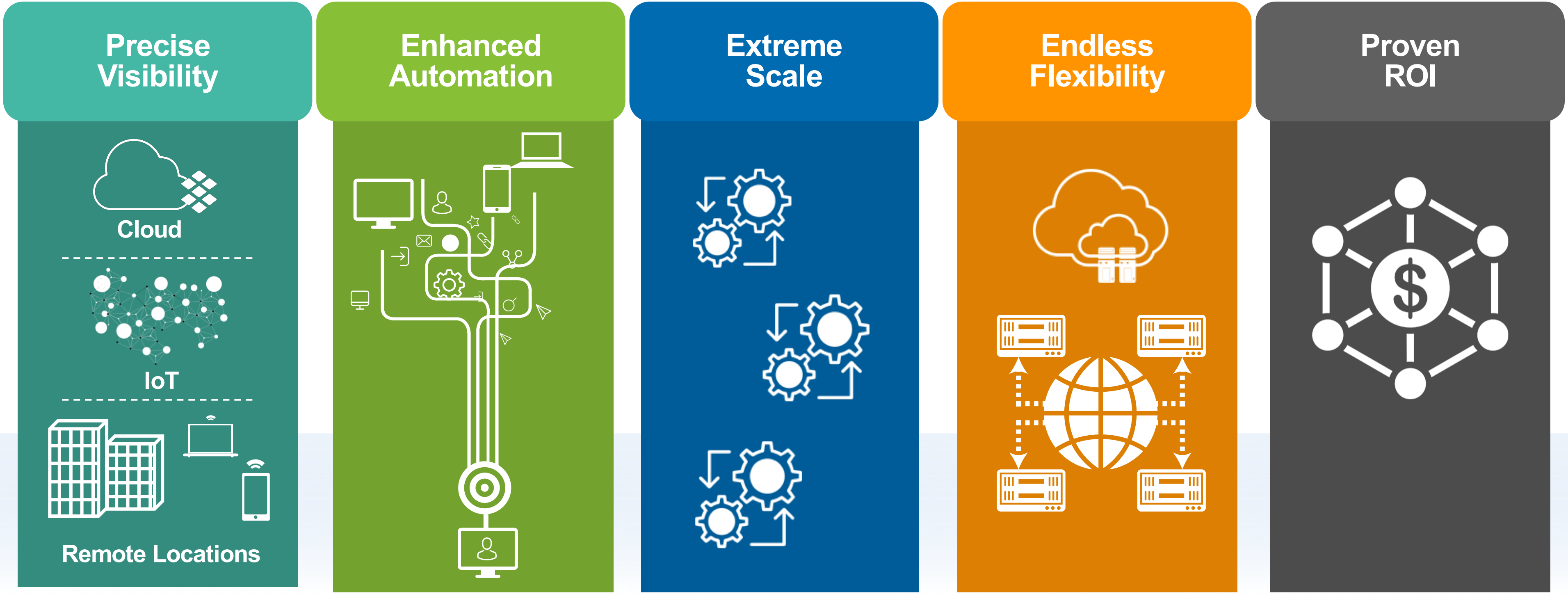
Wiped off from Facebook’s market cap after Cambridge Analytica breach

196 DAYS

Average time to identify a breach

Sources: Ponemon Institute, The Guardian

Key Tenets of a Next Gen Security Architecture



Precise Visibility

Cloud

IoT

Remote Locations

Enhanced Automation

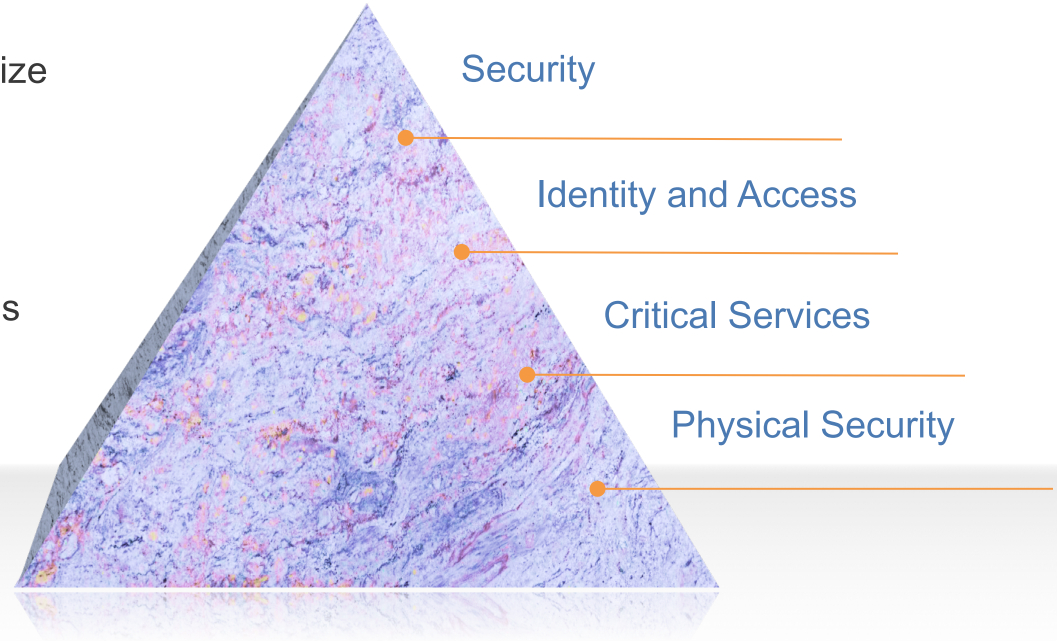
Extreme Scale

Endless Flexibility

Proven ROI

DDI as a Foundational Security Architecture

- The best opportunity to introduce efficiency in security architectures is to integrate foundational security
- Find Lowest Common Denominator to Maximize ROI
  - DNS is the foundation of every network conversation
  - DHCP is the foundation of network access
  - IPAM Database is the AUTHORITATIVE source of all network-connected assets



Customer Story: UK National Cyber Security Center

Customer Use Case:

- Protect UK government departments from cyberattacks

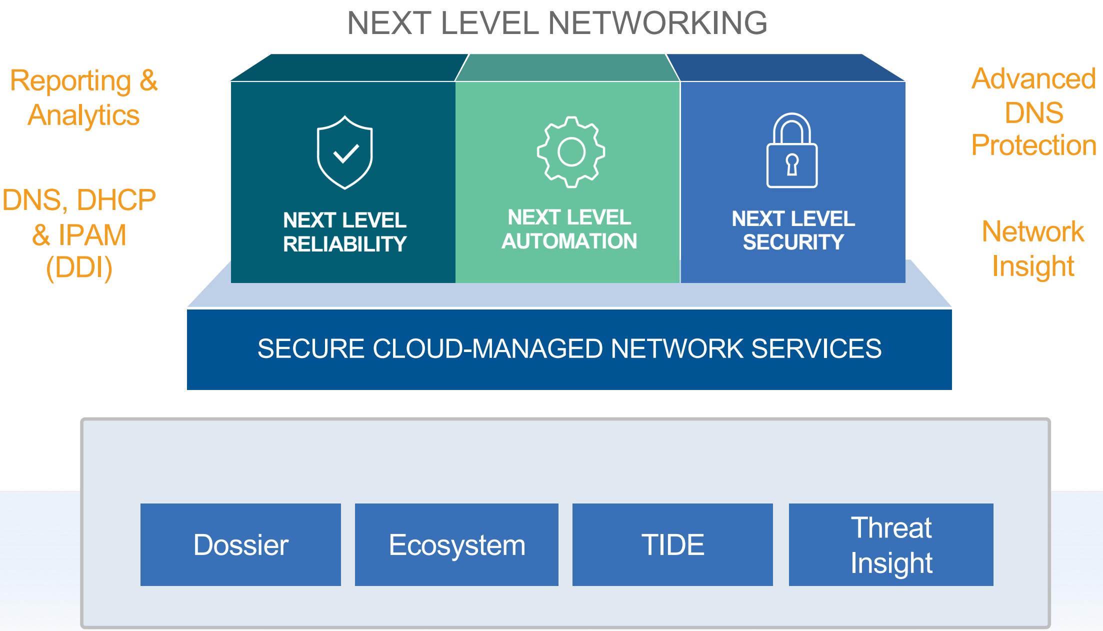
Solution: ActiveTrust for foundational security using DNS control plane

Outcomes:

- 273,329 requests blocked, of which 5,768 were unique in a single week
- 3 terabytes of DNS data analyzed for security threats
- 134,825 unique DNS queries blocked in 1 year
- Nearly all organizations benefited from blocking of (malicious) DNS queries
- Identified previously unknown methods that avoid threat detection (DGAs)

https://www.ncsc.gov.uk/information/active-cyber-defence-one-year

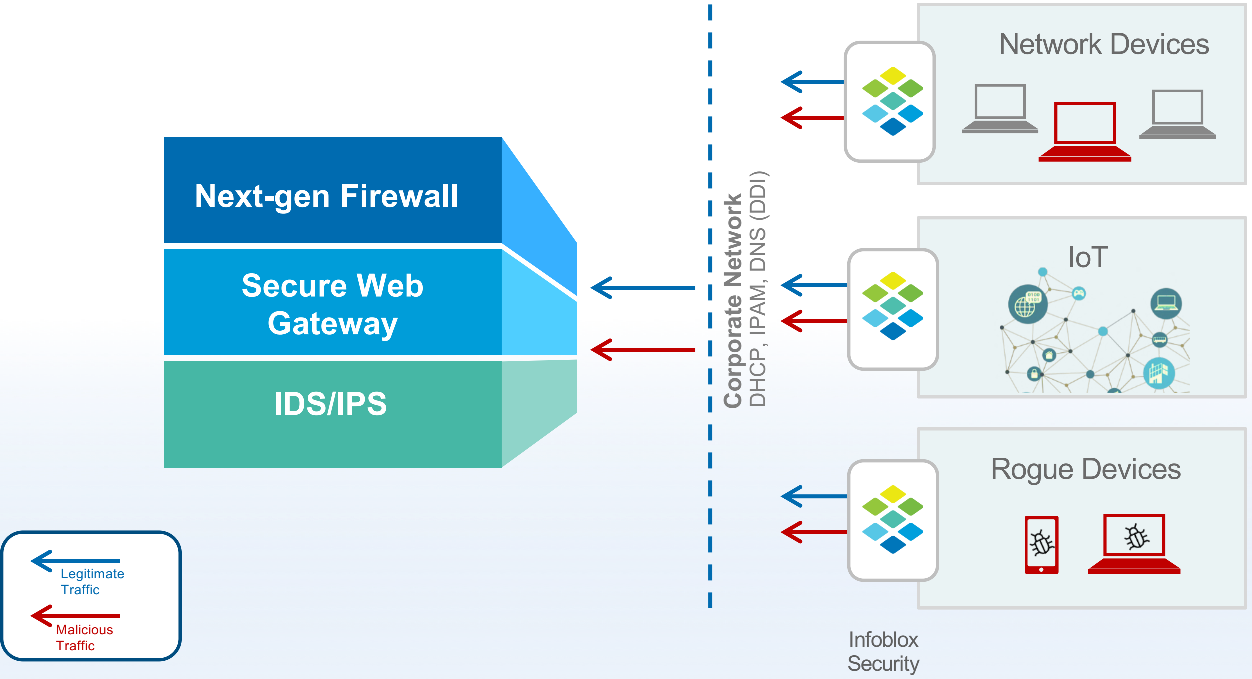
Infoblox Security



- Contextual Intelligence

- Infrastructure Load
- Alerts

Optimize Infrastructure with Expanded Enforcement



Preserving Perimeter Security

Giving Back Scalability

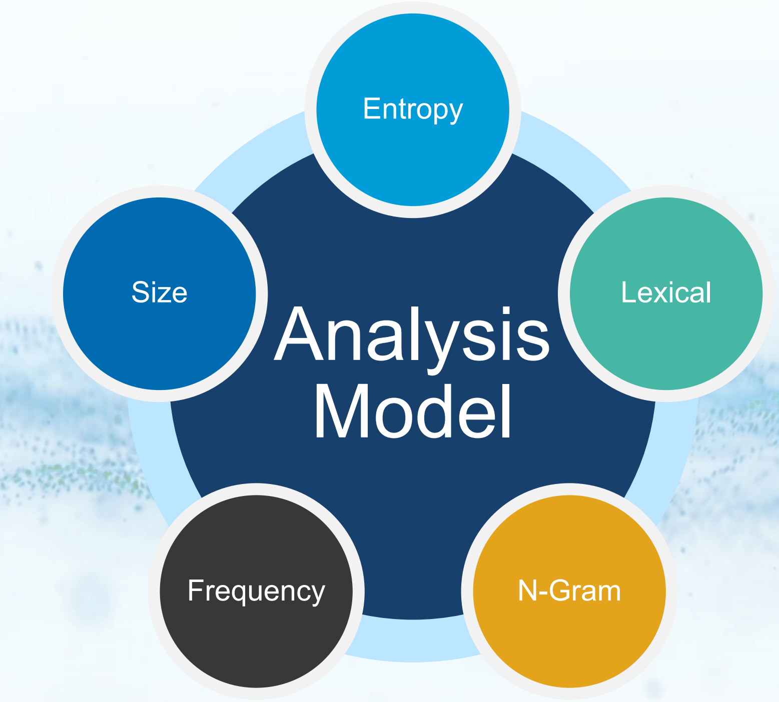
- Offloading blocking of known threats
- Reducing "junk" traffic to NGFWs, SWGs and IDS/TPS
- Preserving processing power of perimeter security

Protect All Devices

- Foundation of **DHCP, IPAM, DNS**
- Widespread protection for
  - All enterprise devices
  - All IoT devices
  - Rogue devices

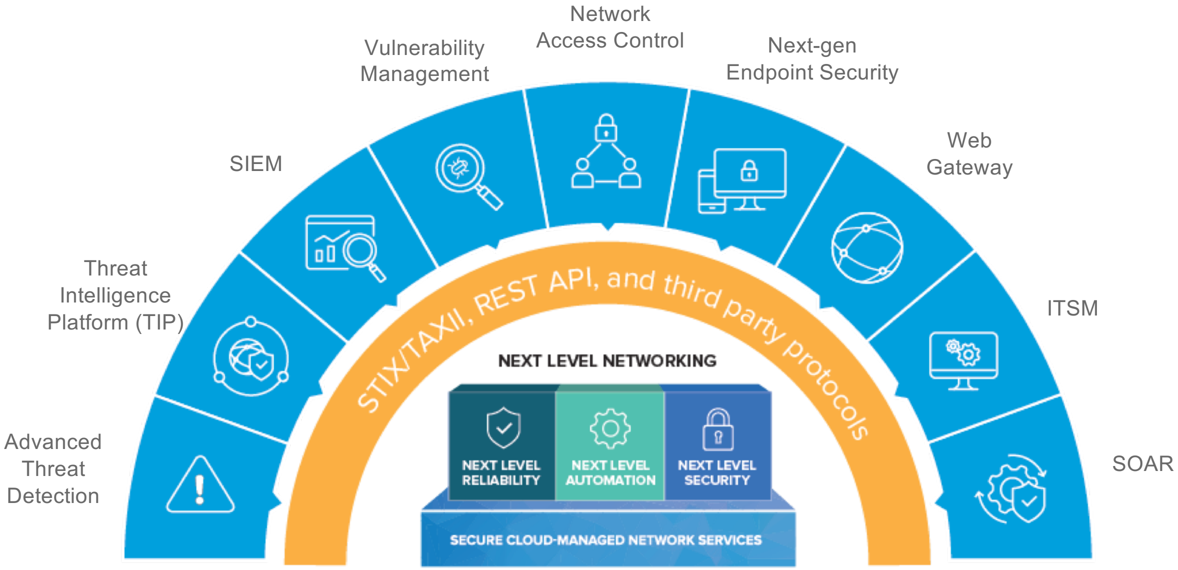
Threat Intelligence (Purpose Built for DNS) + Analytics + Infoblox Cyber Intelligence Unit = Advanced Threat Detection

- Behavioral Models - Machine learning based analytics
  - DNS Data Exfiltration
  - DGA, Fast Flux, Whitelist
  - Fileless Malware, Zero-day
- High accuracy IOCs
  - Extensive IOC collection network
  - Reverse engineering, hunting
  - High accuracy scoring algorithms
- DNS Attack Signatures
  - Secure the name service from protocol attack
  - Protect against protocol misconfiguration



Combined DDI, Threat Intel and Context to Power SOAR Platforms

Enriched data and integrations that can be relied upon to build automation


Network Access Control
Vulnerability Management
Next-gen Endpoint Security
SIEM
Web Gateway
Threat Intelligence Platform (TIP)
ITSM
Advanced Threat Detection
SOAR
STIX/TAXII, REST API, and third party protocols
NEXT LEVEL NETWORKING
NEXT LEVEL RELIABILITY
NEXT LEVEL AUTOMATION
NEXT LEVEL SECURITY
SECURE CLOUD-MANAGED NETWORK SERVICES

Prioritize 100s of alerts | Automate incident response | Reduce cost of human touch/error

DNS

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

DHCP

Device Audit Trail and Fingerprinting

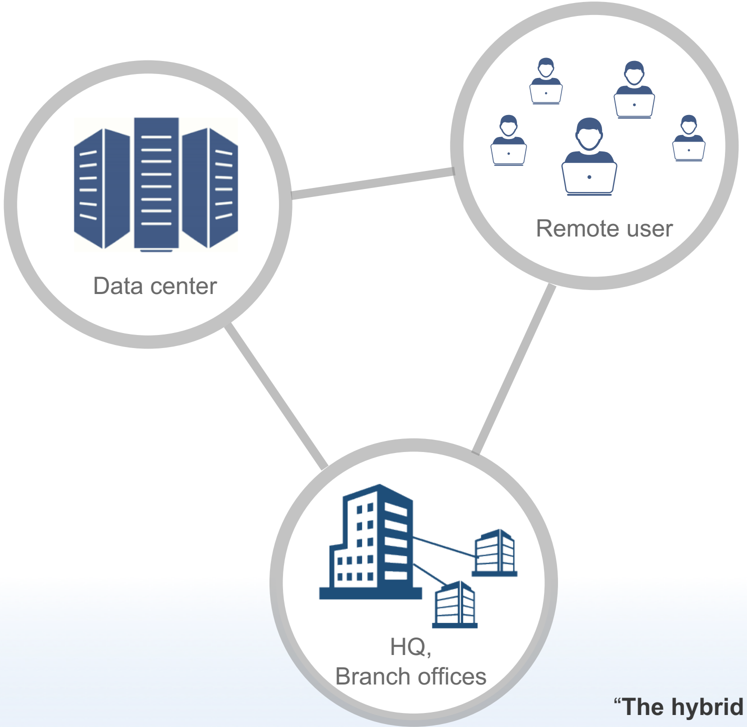
- Device info, MAC, lease history

IPAM

Application and Business Context

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

Hybrid Model: Works Wherever You are Deployed



- Scale from the cloud
- Full integration with on-premises ecosystem
- Resiliency and redundancy

“**The hybrid cloud will be used more regularly.** Organizations looking to exercise the advantages of the cloud without giving up proximity to data and security will invoke the hybrid cloud.” - Comport Technology Solutions

ROI: Reducing Cost of Existing Tech Stack

60x

reduction in traffic sent to NGFWs

3x

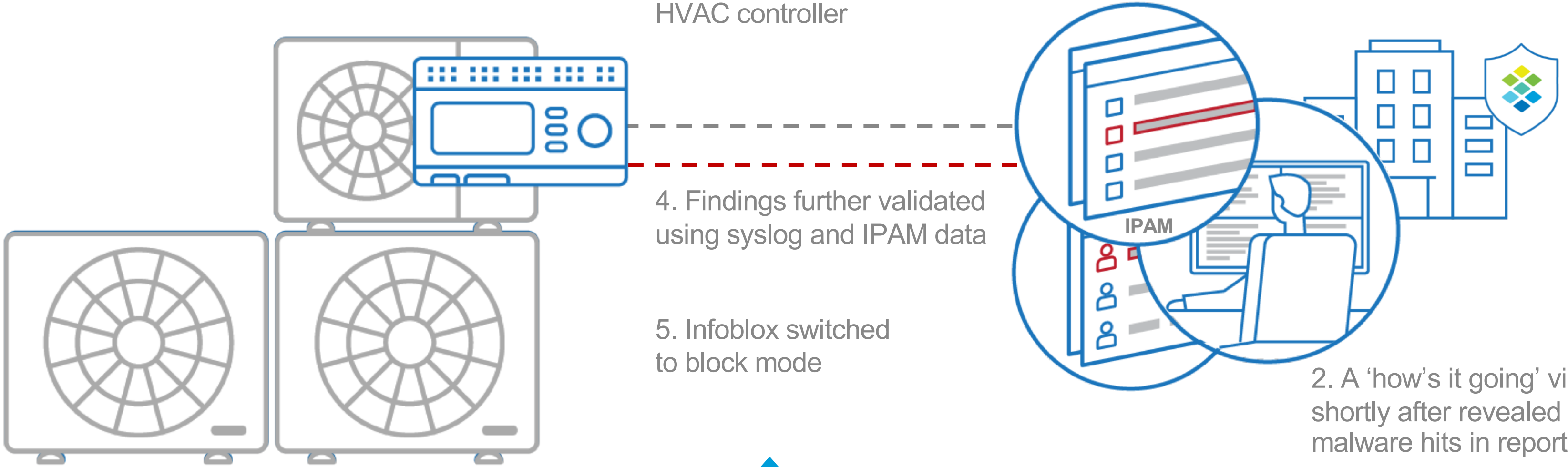
more productivity from threat analysts

2/3

reduction in threat response time

Based on real customer data

Customer story: A consumer appliance manufacturer detects infected HVAC



1. Appliance manufacturer added DNS security in log-only mode

2. A 'how's it going' visit shortly after revealed several malware hits in reports

3. SECOPS team identified the top infected device as an HVAC controller

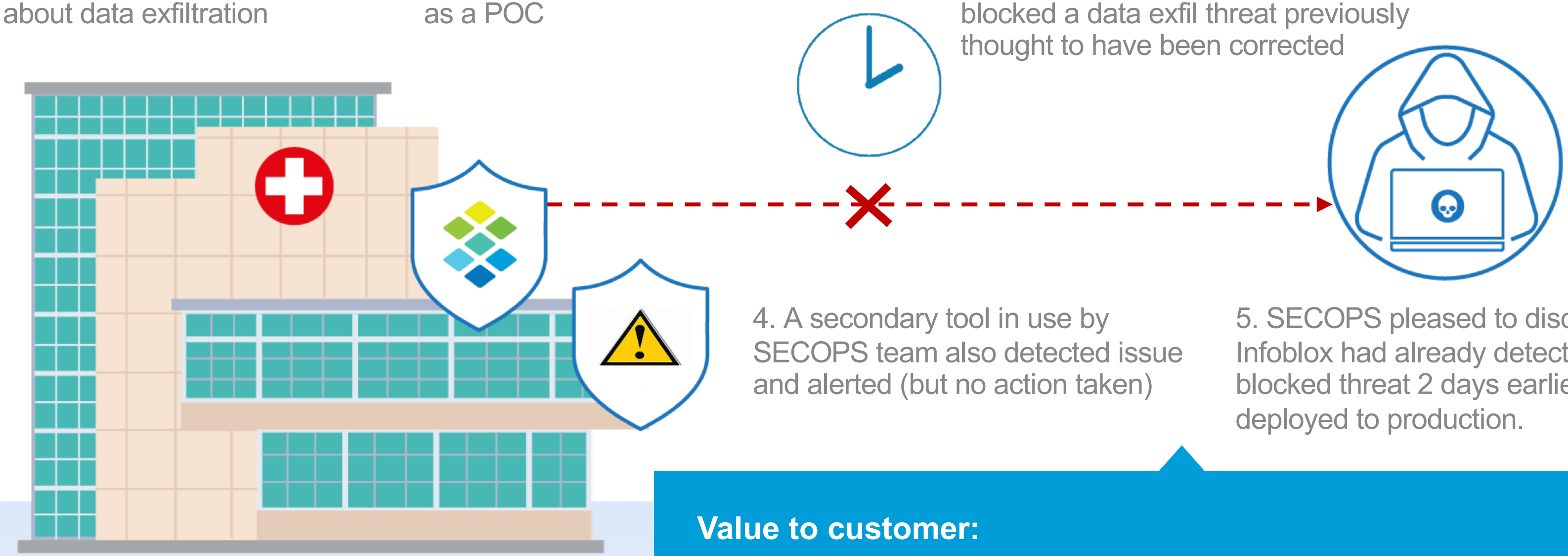
4. Findings further validated using syslog and IPAM data

5. Infoblox switched to block mode

Value to customer:

- Ability to quickly identify and prioritize what client IP is most concerning and act in **real-time** to block the threats
- Leverage IPAM data and syslog for **discovery/investigation**
- Allow security team to see threat before causing further damage

Customer story: A US Children's Hospital Protects Patient Data



1. Hospital highly concerned about data exfiltration

2. Infoblox implemented as a POC

3. Within 24 hrs, Infoblox detected and blocked a data exfil threat previously thought to have been corrected

4. A secondary tool in use by SECOPS team also detected issue and alerted (but no action taken)

5. SECOPS pleased to discover Infoblox had already detected and blocked threat 2 days earlier. Infoblox deployed to production.

Value to customer:

- **Ease of deployment:** Ability to seamlessly enhance existing DDI infrastructure with security
- **Data Protection:** Ability to detect and block data exfil in real time
- **Brand protection:** Help protect the Hospitals name, reputation