
BLOX FEST
Infoblox

Craig Sanderson

Senior Director, Product Management (Security)

Insight Driven Networks Create Enterprise Value

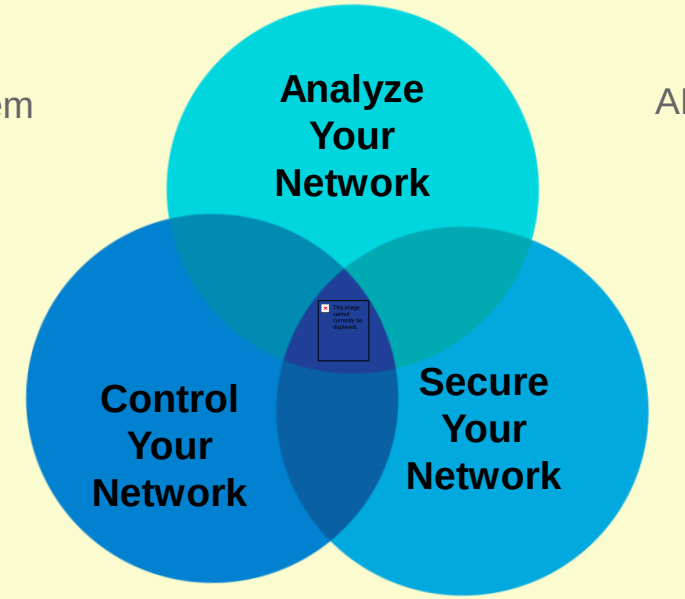
Next Generation Data Center | **Security and Compliance** | **Digital Economy**

Noise

Actionable Network Intelligence Platform

Eco-system

APIs



Authoritative Distributed Database

Business Outcomes

- Customer Experience
- Risk Management
- Operational Efficiency
- Visibility

On Premise | Hybrid | Cloud

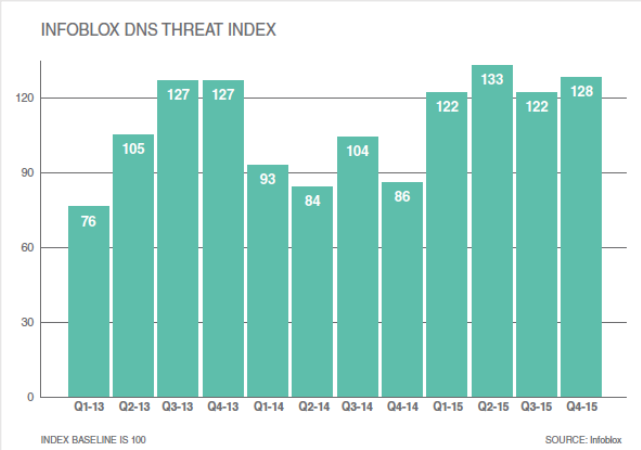
BLOX FEST

Security Landscape

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

DNS Threat Index

The threat index reached a record high in Q1 2016 to 137—surpassing the previous record high of 133 set in Q2 2015.



DNS – The Hacker's Control Plane

91% of malware—relies on DNS for command and control

431M

New unique pieces of malware in 2015[2]

#1

Malware C&C is #1 responsible vector for Crimeware[3]

DNS-based Data Exfiltration

"Multigrain" PoS malware exfiltrates card data over DNS

46%

Of large businesses have experienced DNS exfiltration[1]

>$3.8M

The average cost of a single data theft occurrence[2]

Threat Intelligence Data Sharing

Cybersecurity Information Sharing Act of 2015

The Automated Indicator Sharing (AIS) initiative

The Security Silo – Industry Analyst

"Silos between network, edge, endpoint, and data security systems and processes can restrict an organization's ability to prevent, detect, and respond to advanced threats…"

BLOX FEST

Infoblox Security Vision

Deliver Industry Leading DNS Security Solutions

- Protect DNS
- Break the Malware Control Plane

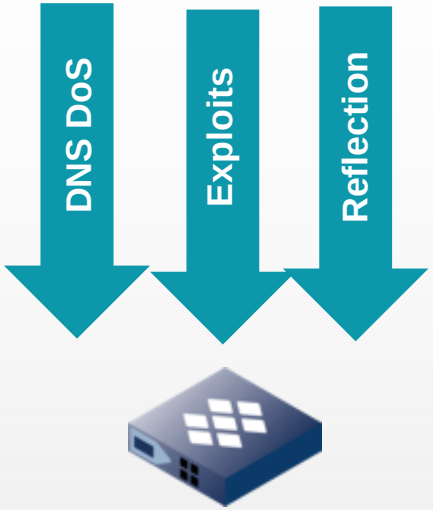
Become the Threat Data and Intelligence control plane for security deployments

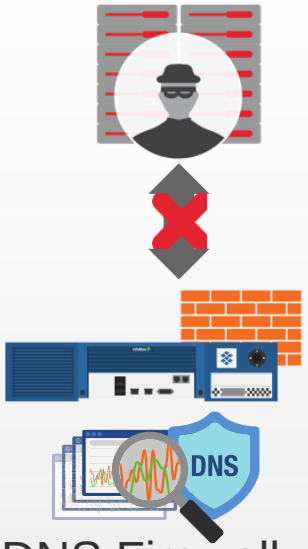
- Deliver a Threat Intellligence Data Exchange
- Break the Security Deployment Siloes

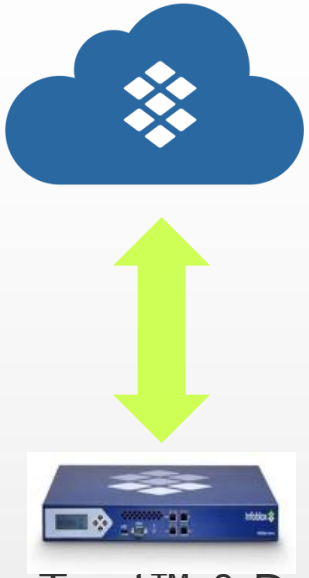
Security Strategy

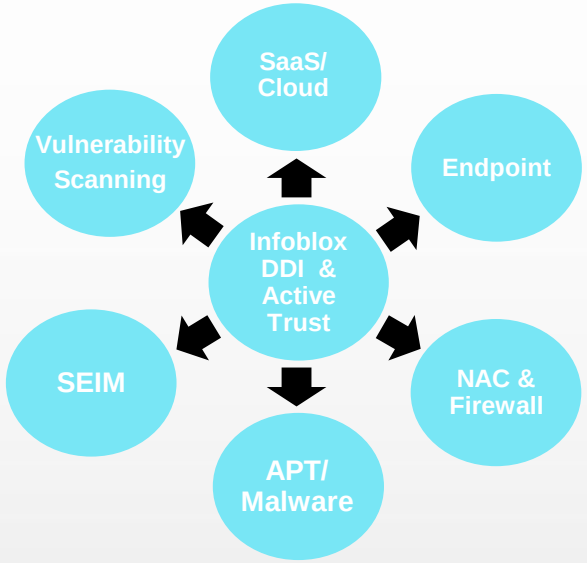
Solution Strategy

Secure DNS	Breaking the Malware Control Plane	Threat Intel Data Exchange	Security Control & Data Plane









Product Strategy

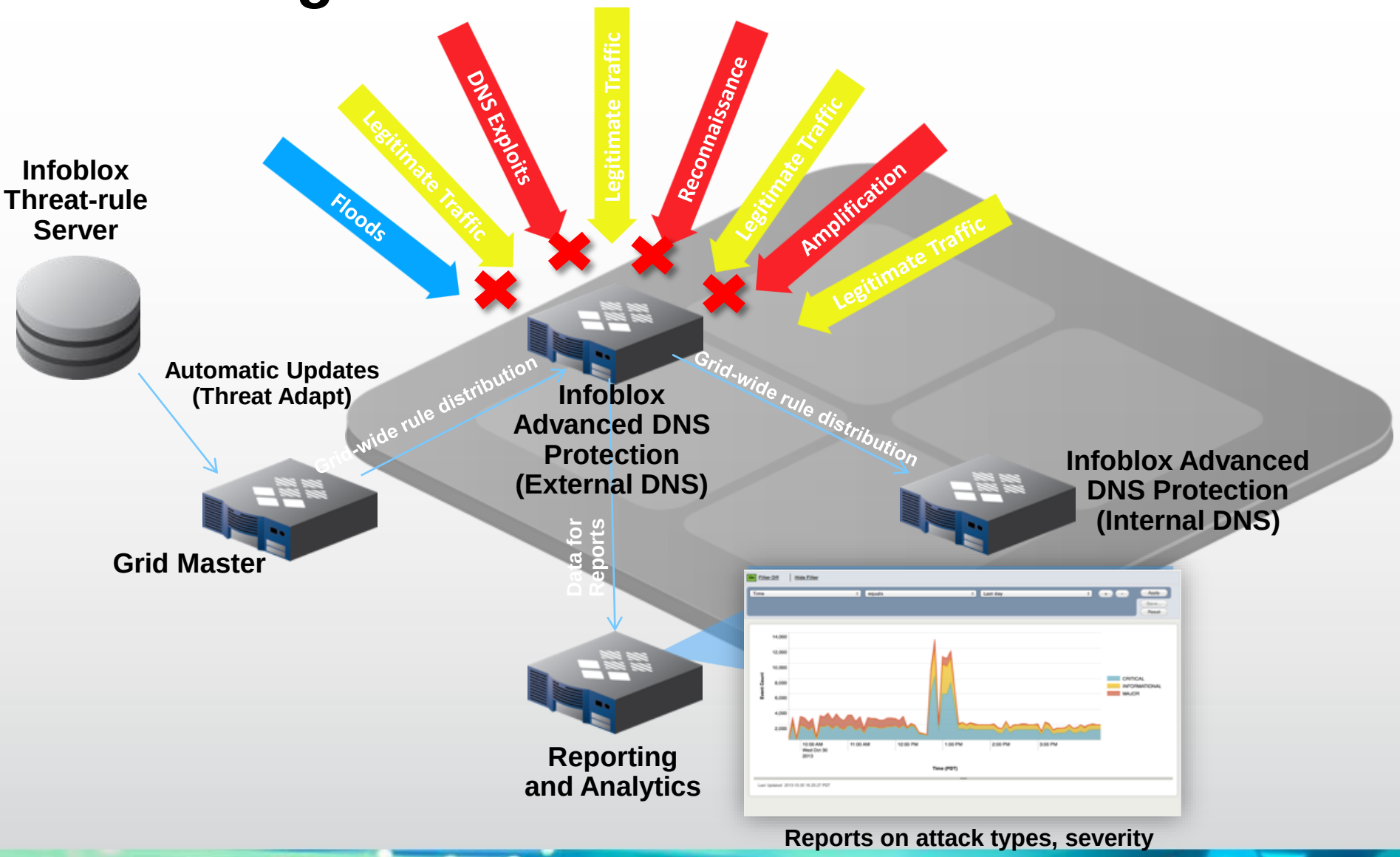
Advanced DNS Protection (DDoS)	DNS Firewall Threat Insight	ActiveTrust™ & Dossier	Secure Data Exchange Ecosystem API's

Technology Strategy

- Ecosystem
- Analytics
- Threat Intelligence
- Data Sharing

Secure DNS: Infoblox Advanced DNS Protection

Protecting critical DNS services

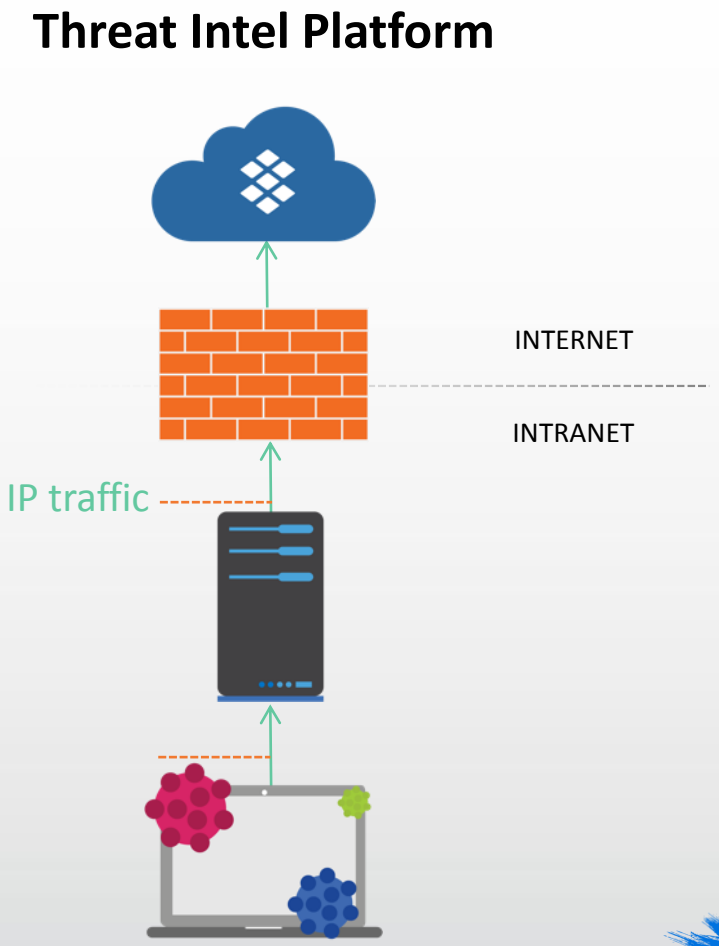


- Hardened OS
- Dedicated platforms designed to withstand DDOS attacks
- Signatures to detect and block exploitation of vulnerabilities

Breaking the Malware Control Plane

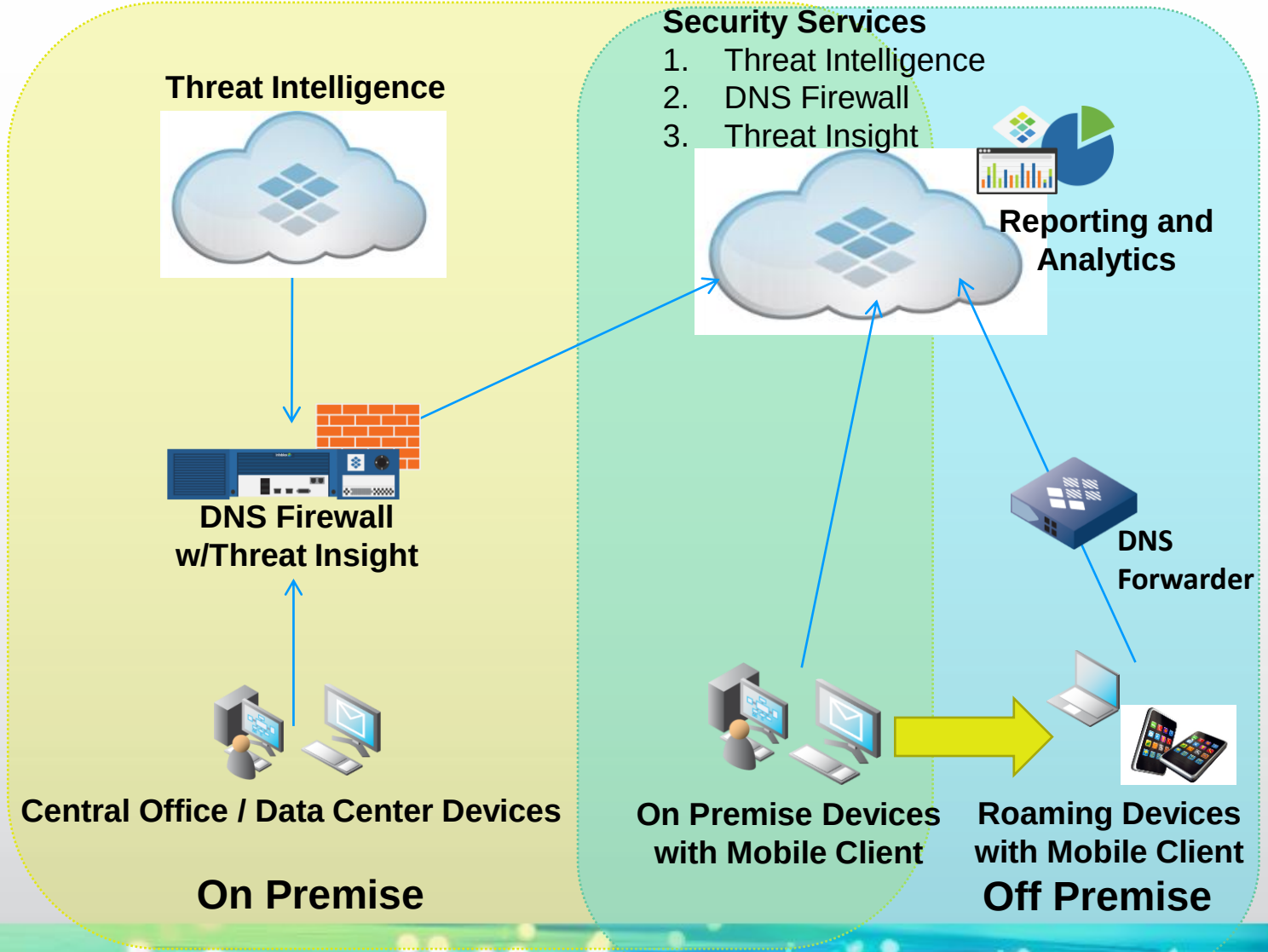
Malware & Data Exfiltration

- Malware containment and control
  - DNS Firewall: Ubiquitous visibility and blocking
  - Adding high quality Threat Intelligence
  - Offer additional 3rd party Threat data
  - Dossier: Threat intelligence research tool to accelerate incident analysis
  - Endpoint containment via ecosystem partnerships
  - Open APIs enabling 3rd party devices to block using DDI infrastructure
- Threat Insight – Streaming analytics
  - Data Exfiltration detection and prevention
  - Blocks known and custom exfiltration tools



Extending Protection Outside the Enterprise

DNS Firewall as-a-service



DNS Firewall

- Deploy on premise, private/public cloud, Internet

Unified Reporting and Analytics

- Unified view for on and off-premise users and devices for internal and external applications
- Pinpoint exact device, switch and port for malware
- 10+ ecosystem integrations with leading security vendors

Threat Intelligence

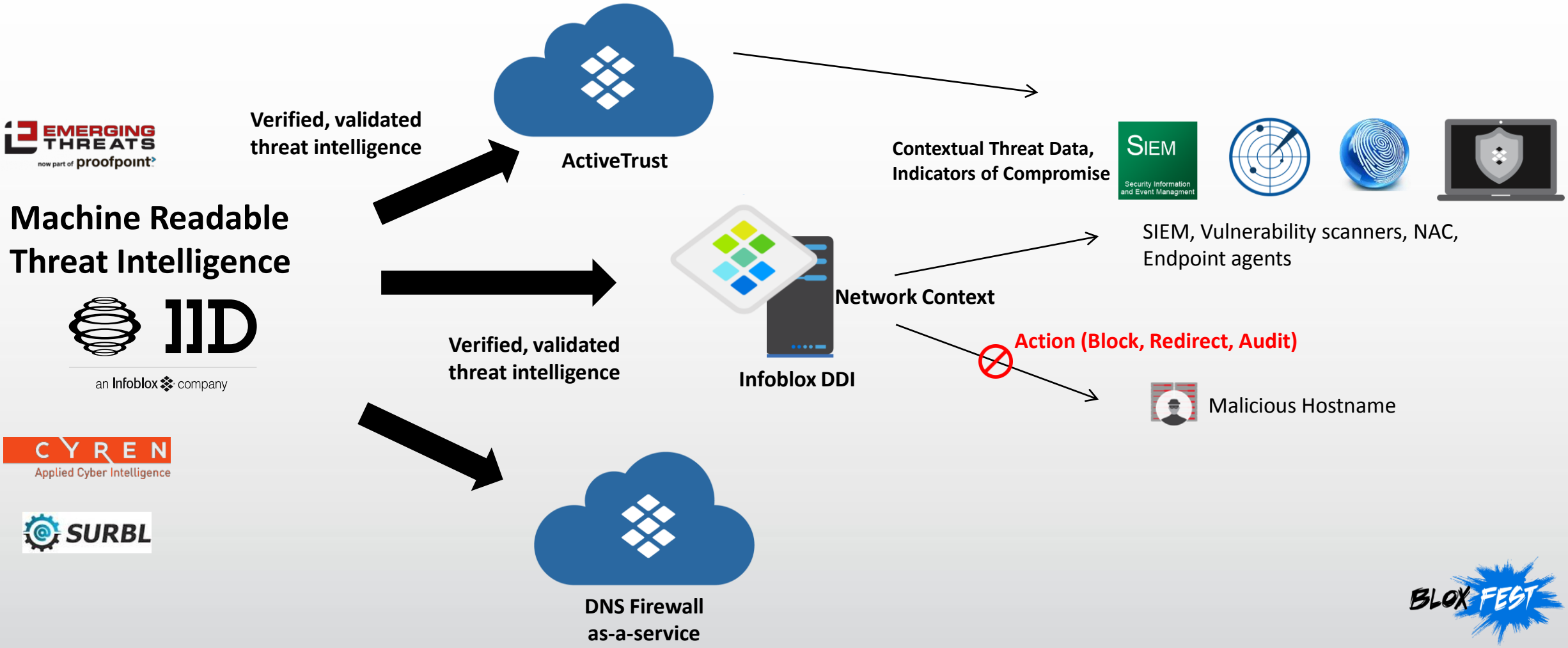
- Leverage investment across all deployments

Advanced Threat Analytics

- Data exfiltration prevention
- Malware containment and control

BLOX FEST

Threat Intel Data Exchange - Ecosystem



Context Driven Threat Intelligence Driving Operational Efficiency

Network Context and Control

Infoblox CONTROL YOUR NETWORK

- Ubiquitous Tier-1 network control points
- Unique network position to provide device information and metadata
- DNS audit trail of system and user activity

Collective Threat Intelligence

IID

- Verified and accurate MRTI
- Distills data from thousands of sources, processes and services that IID offers
- Federated platform for threat data sharing

Context-Aware Security

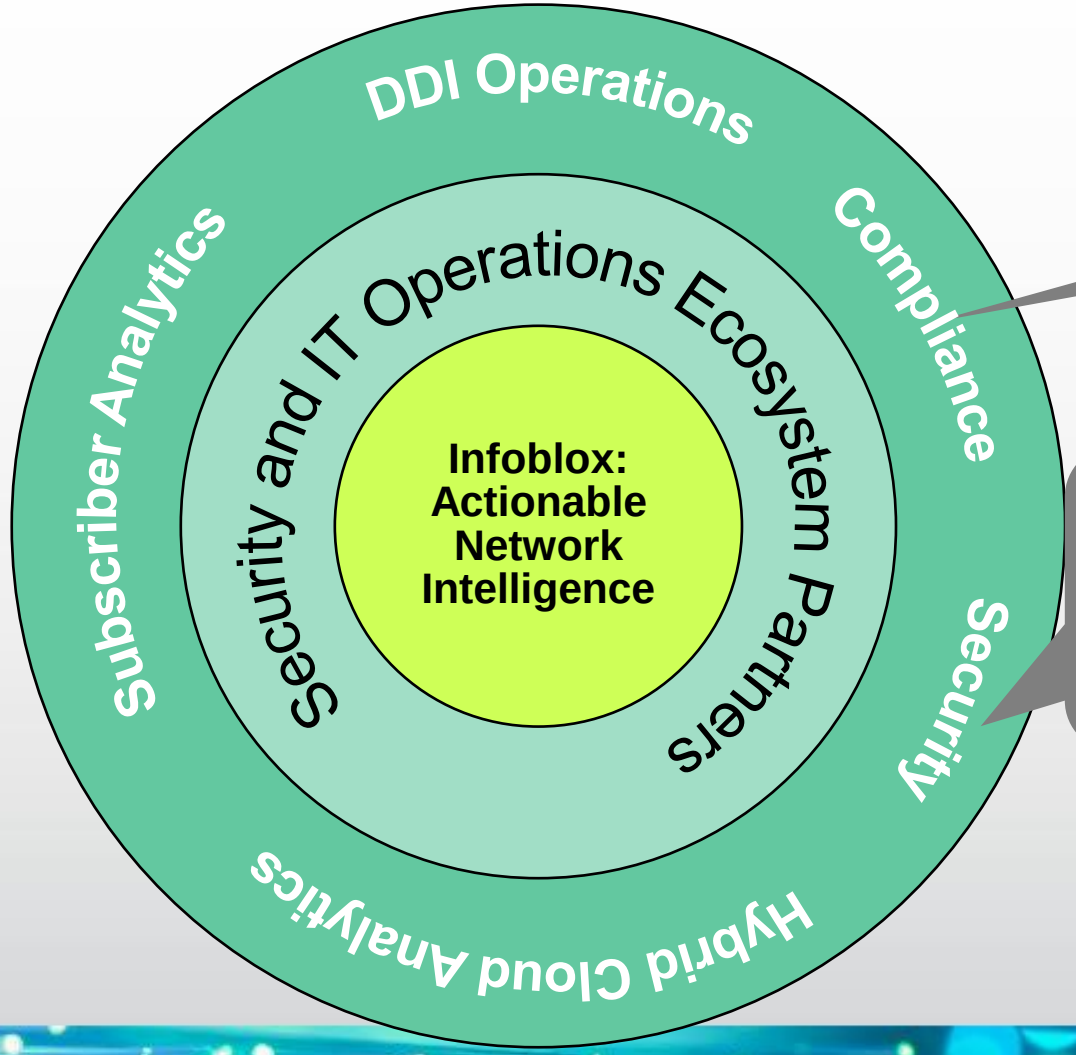
- **Prioritize** response to threats based on enterprise context and risk
- **Protect** by instantly blocking malicious activity on both on-premise and off-premise devices; share threat data with ecosystem for additional action
- **Predict** threats using ecosystem, vertical and geo data

BLOX FEST

Security Analytics Strategy

Leveraging Threat Intelligence, DDI and 3rd party data to provide

- New and Deeper insights into threats
- Automation of analysis and compliance to save time and accelerate response



What's on my network?
Are devices compliant to policy?
Are admins compliant to policy?

Which devices are infected & how?
How do I prioritize security events and eval risk?
How do I auto-gather data to do incident response?

DDI & DNS Security: A Control & Data Plane for Security Deployments

DNS Security

Breaking the malware control plane

DDI Data

Security Operations Efficiency

Ecosystem & Data Exchange

Real time Threat Intelligence exchange between diverse security platforms

Enforcement & Mitigation

Pervasive mitigation and enforcement

Infoblox Data: 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 <u>important</u> 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.

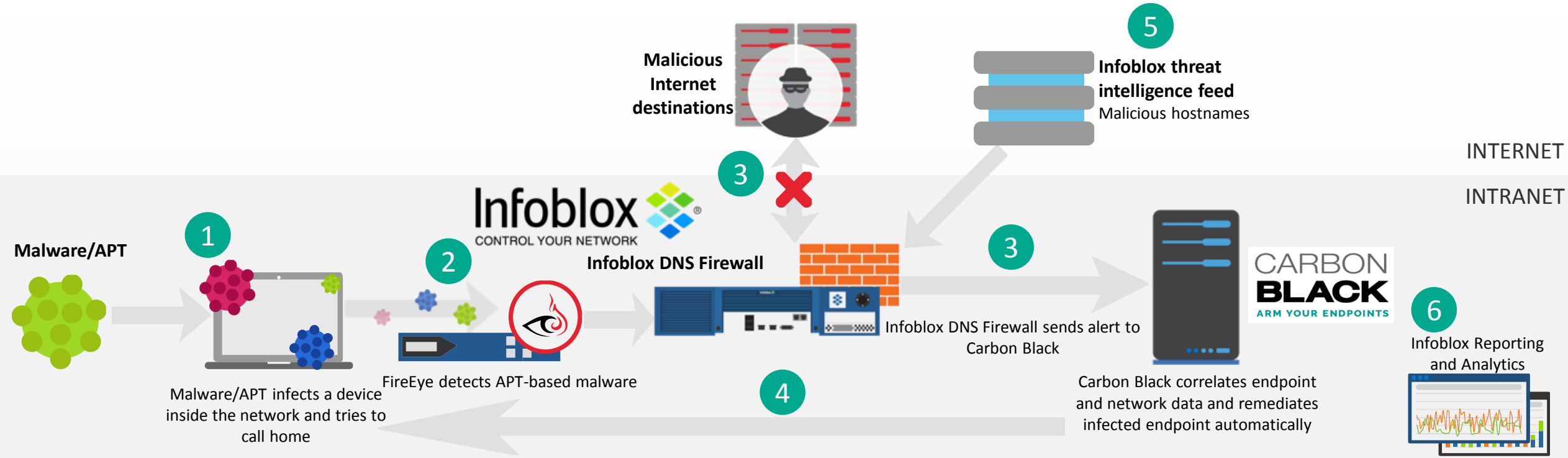
DNS query data provides a “client-centric” record of activity

- 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

Breaking the Security Silo

Infoblox, FireEye and Carbon Black



1 An infected device brought into the office.

2 FireEye detects the APT-based malware communication to malicious domain destination, and shares this information with DNS Firewall.

3 Infoblox DNS Firewall blocks endpoint DNS query and sends alert to Carbon Black.

4 Carbon Black correlates its own endpoint data and network data from Infoblox and remediates infected endpoint.

5 An update will occur every 2 hours (or more often for significant threat).

6 **Pinpoint.** Infoblox Reporting and Analytics lists DNS Firewall action as well as the:

- User name
- Device IP address
- Device MAC address
- Device type (DHCP fingerprint)
- Device host name
- Device lease history

Summary

- Infoblox is committed to provide best in class security to both protect DNS and break the malware control plane.
- Infoblox DDI platforms as the control and data plane for network security
  - Busting the silo’s through open API integration
  - A platform for real time data exchange and Threat Intelligence
  - Leveraging the inherently valuable DDI data to improve security operations and efficiency


BLOX FEST