
BLOX FEST
Infoblox

Building a Bridge to Security, The Infoblox Cybersecurity Ecosystem and API

Utpal “U.J.” Desai
Senior Product Line Manager, Infoblox

Ricardo Lafosse
CISO, Cook County Government

Agenda For This Session

1. Security Teams and Their Challenges
2. Infoblox Security Ecosystem
3. How Cook County Leverages Infoblox
4. Q/A

Infoblox Customer, Insurance Company

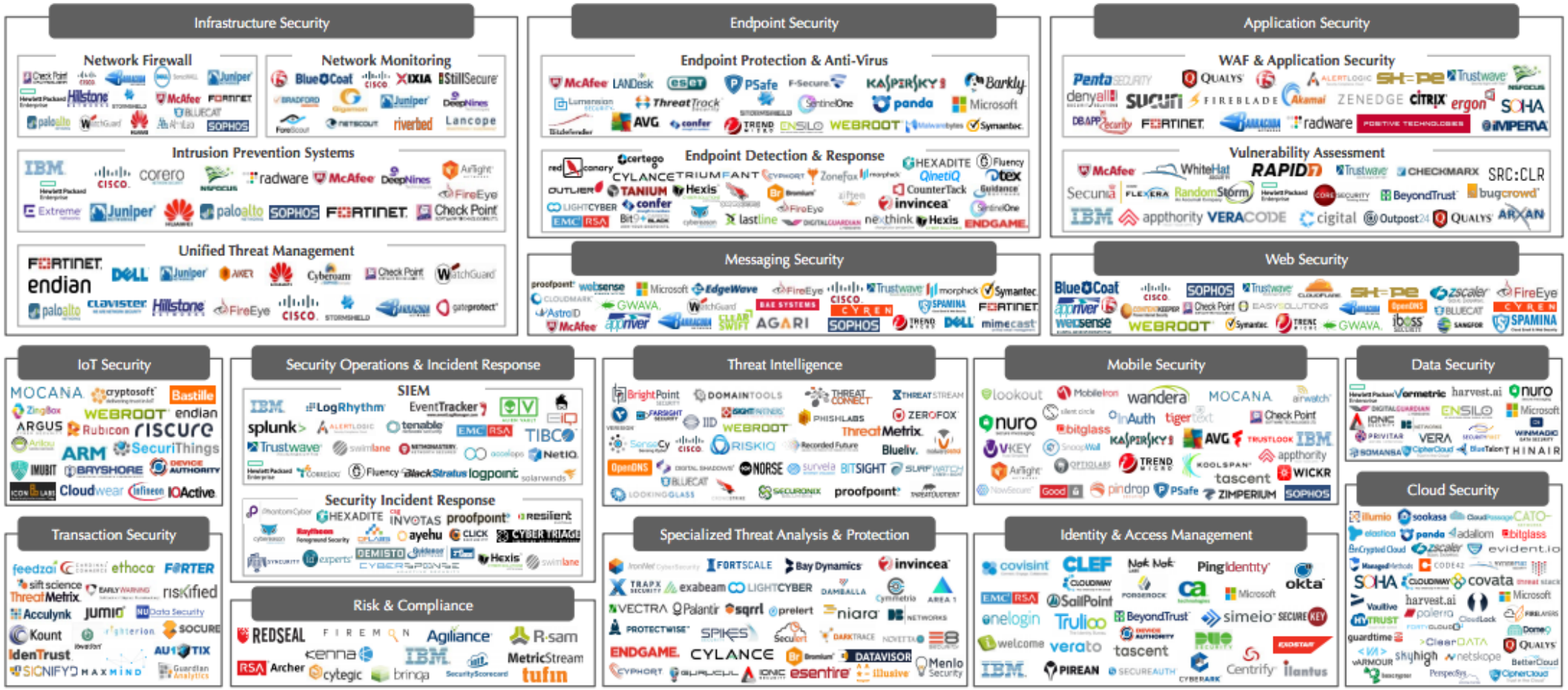
“There are so many processes and tools that could benefit leveraging Infoblox data for security. I probably can't name them all.”

Security Landscape

Infrastructure Security	IoT Security	Mobile Security
Endpoint Security	Transaction Security	Identity and Access Management
Application Security	Incident Response	Data Security
Messaging Security	Risk and Compliance	Cloud Security
Web Security	Threat Intelligence	Threat Analysis and Protection

The **cyber security market** is estimated to grow to $170 billion (USD) by 2020, at a Compound Annual Growth Rate (CAGR) of 9.8 percent from 2015 to 2020

Welcome to the Jungle



Source: Momentum Partners.

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	Staffing

Challenge – The Big Disconnect in IT

Network and Security – Separate teams with different priorities

NETWORK TEAM	SECURITY TEAM
High Availability	Risk Mitigation
Network Infrastructure: routers, APs, switches, etc	Security Infrastructure: firewalls, endpoints, sandboxing, etc
Network Logging and Monitoring	Security Logging and Monitoring (SIEM)

The problems this causes:

- Wastes resources for security and audit/compliance
- Makes IHR process more difficult
- Extends time to remediation of incidents

Gartner's View: The Security / Network Disconnect

Gartner

G00296530

Best Practices for Detecting and Mitigating Advanced Threats, 2016 Update

Published: 29 March 2016

Analyst(s): Lawrence Pingree, Neil MacDonald, Peter Firstbrook

Information security, network and communications practitioners must implement specific best practices to prevent, detect and mitigate advanced threats. These practitioners should leverage both existing and emerging security technologies in their security architectures.

Key Challenges

- Most organizations rely on low overhead prevention techniques, such as firewall and antivirus solutions, and intrusion prevention. However, these tools are insufficient, and breach data shows that detection and IR must be improved.
- Attackers continue to use social engineering and social networks to target sensitive roles or individuals within an organization to target data.
- Attackers reside undetected for months, often moving laterally within environments. New attack surfaces — for example, IaaS, SaaS and IoT — remain challenges and do not yet benefit from the more proven practices used for traditional technologies.
- Silos between network, edge, endpoint and data security systems and processes can restrict an organization's ability to prevent, detect and respond to advanced attacks.

Recommendations

- Perform an ongoing business impact and threat assessment analysis with business leaders to categorize threats, users and digital assets into high-, medium- and low-priority classifications to enable faster alert response on high-impact threats, events and critical assets.
- Think strategically throughout your security program, keep up to date with evolving threats, proactively thwart social engineering techniques and pay greater attention to all security layers — avoid stagnation of your technology controls.
- Uplift your perimeter, endpoint and network-based security controls to match the latest threats.

"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…"

Key Challenge:
Silos between systems and processes

https://www.gartner.com/doc/3266630/best-practices-detecting-mitigating-advanced

BLOX FEST

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

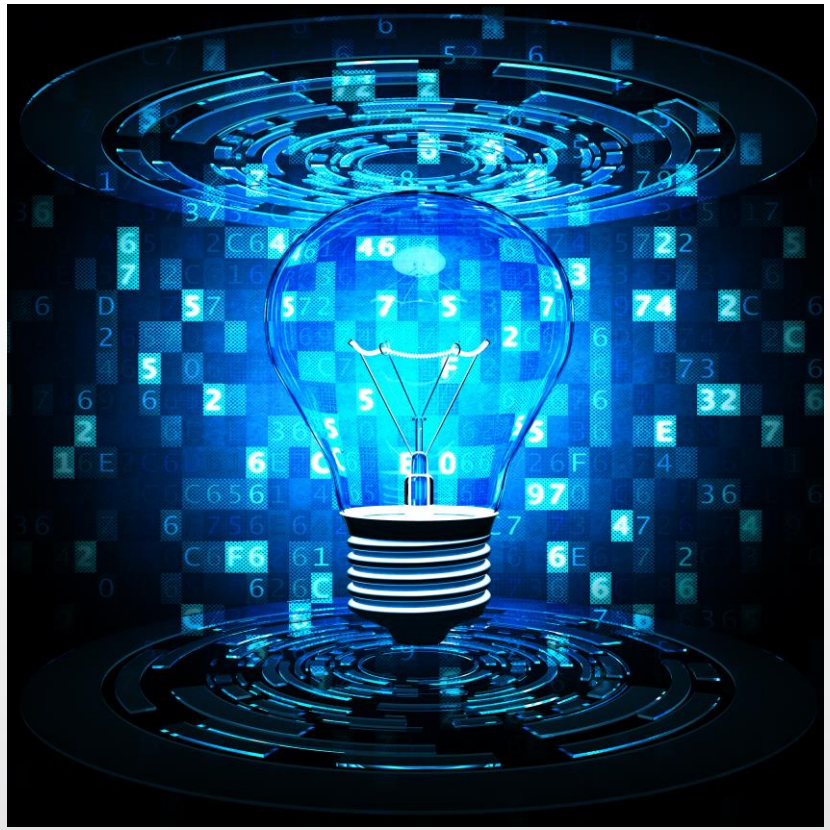
- Focus on improving efficacy (No. 1 Buying Criteria).
- Focus on delivering suite or bundled solutions.
- Continue to leverage cross-product integration efforts to utilize context information and automated response capabilities.
- Providers in segments with decreased demand should increase marketing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

BLOX FEST

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



BLOX FEST

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

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

BLOX FEST

Our Security Ecosystem – Where Infoblox Fits

Ecosystem Integration Examples

Cook County Wiki

- Cook County is the 2nd largest county in the US
- Has more than 5 million residents
- A few key services include
  - Public Safety
  - Property Tax
  - Courts System
  - Hospitals
- More than 50,000 active IP addresses

http://www.cookcountyil.gov/wp-content/uploads/2014/12/seal_color_300dpi_6in-half.jpg

BLOX FEST

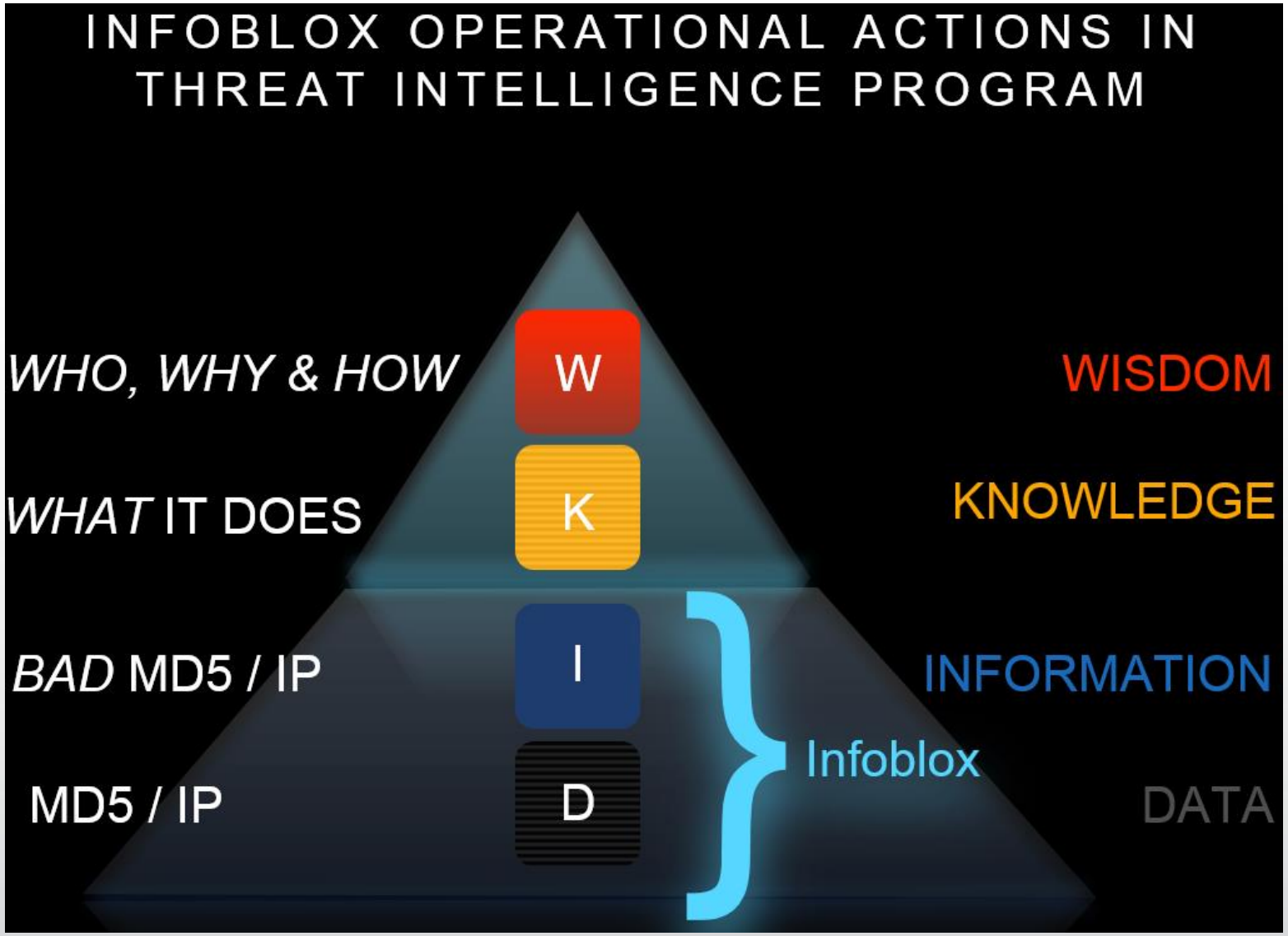
Why Infoblox

- A record of authority that actually works
  - IPAM
  - DNS
  - DHCP
- Open ecosystem
  - Open standards (e.g. RPZ)
- Security visibility

http://www.ew.com/sites/default/files/styles/tout_image_612x380/public/i/2014/12/10/Eye-of-Sauron.jpg?itok=QB7ehKYf

BLOX FEST

Why Infoblox

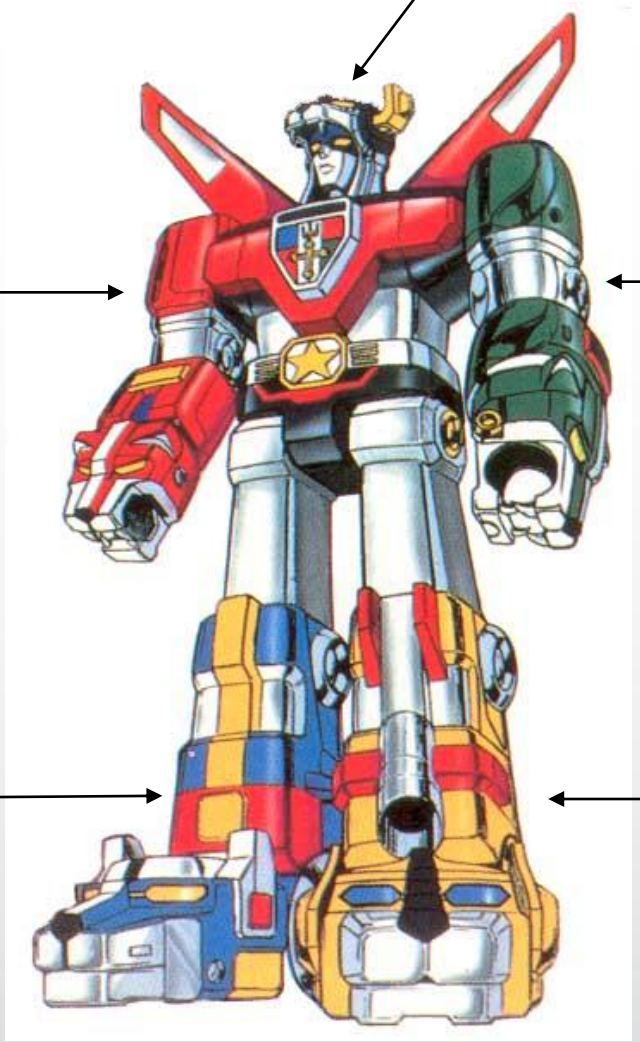


Key Integrations

Infoblox
CONTROL YOUR NETWORK

FireEye

RAPID7



ANOMALI

intel Security

https://camo.githubusercontent.com/09d4e9d8264ac54629d8de5a46f8ff338f3b4629/68747470733a2f2f7261772e6769746875622e636f6d2f7a6174732f566f6c74726f6e2f6d617374722f566f74726f6e2e6a7067

BLOX FEST

FireEye Integration

- This is not a threat feed!
- Pulls feeds from FireEye appliances
- Real time blocking on all DNS firewall enabled devices

FireEye Integration

FireEye sends alerts to the grid from evil internet

Query to malicious site is blocked

Grid updates all member RPZs with FireEye data

Data sent to SIEM

Anomali Integration

- This is a threat feed!
- Provides real time updates of malicious information
  - IP
  - MD5
  - Domains
  - Etc
- Current integration is an automated blacklist
- New integration is a direct RPZ
  - Requires 7.2 of higher NIOS

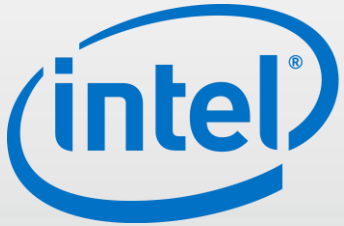
Anomali Integration

Query to malicious site/IP is blocked

ANOMALI

Anomali updates blacklist on a set interval

Grid updates all member DNS blacklist



Data sent to SIEM

Rapid7 Integration

- Vulnerability Management
- Provides real time continuous monitoring
  - Identify new devices
- Feed into Cisco ISE or HP Aruba workflows

KEY GOAL: Identify new devices on the network and perform vulnerability scan to identify risk

Rapid7 Integration

DHCP members send lease information to Rapid7

New DHCP host

RAPID7

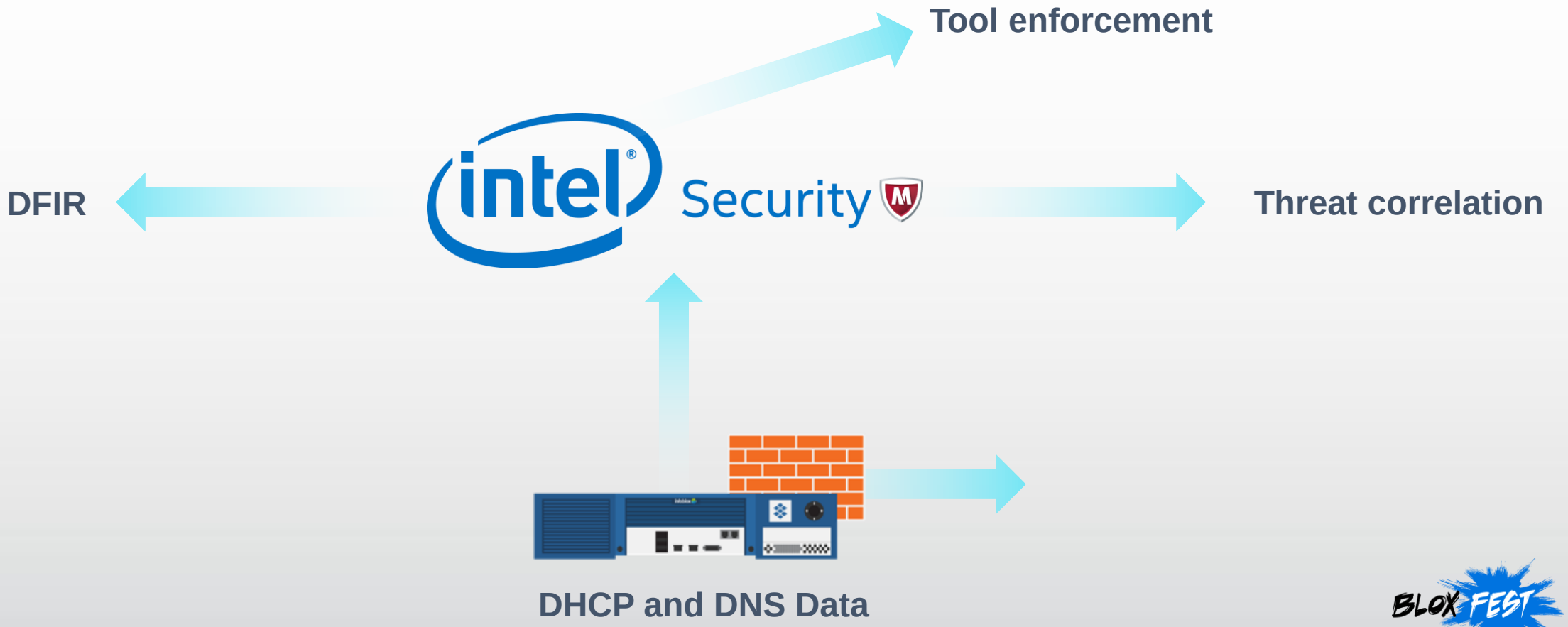
Enforcement workflow

Data sent to SIEM

Intel Security Integration

- Threat analytics and alerting
- Provides real time alerts
- Correlate DHCP/DNS data against malicious feeds
- DFIR

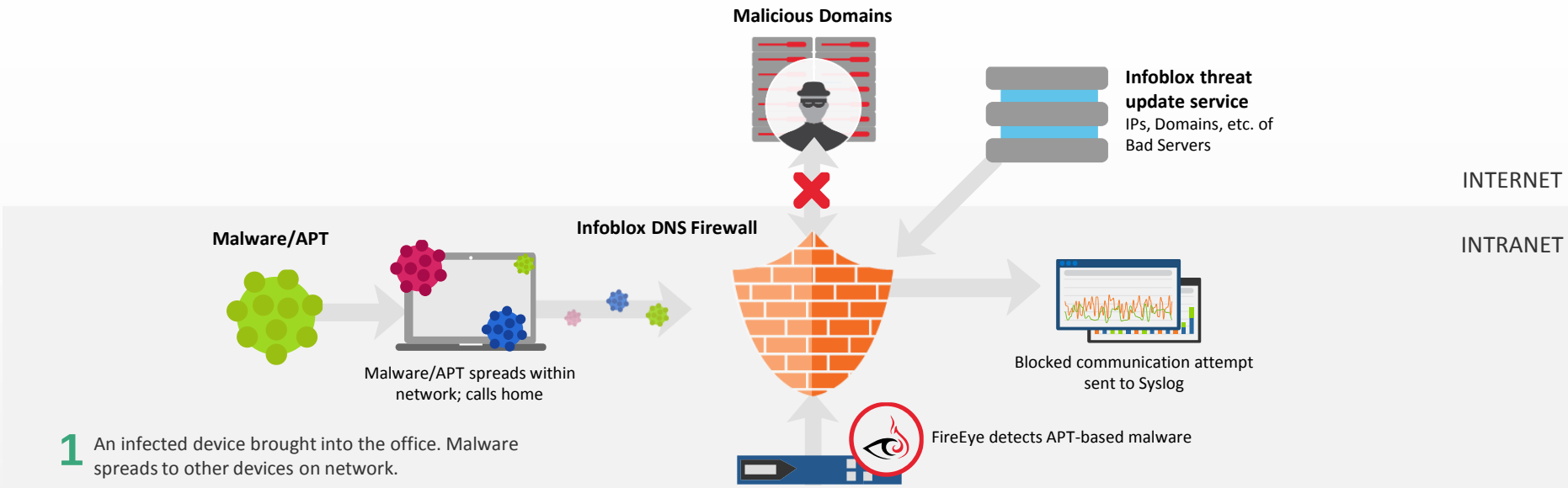
Intel Security Integration



Summary

- Open ecosystem
- Security visibility
- Cost effective enforcement
- Data enrichment for SIEM

Advanced Threat Detection



1 An infected device brought into the office. Malware spreads to other devices on network.

2 Malware makes a DNS query to find "home" (botnet / C&C). DNS Firewall looks at the DNS response and takes admin-defined action (disallows communication to malware site or redirects traffic to a landing page or "walled garden" site).

3 **Pinpoint.** Infoblox Reporting 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

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

5 Additional threat intelligence from sources outside Infoblox can also be used by DNS Firewall (e.g. FireEye)

BLOX FEST

End-Point Security

Infoblox sends alert to Carbon Black

CARBON BLACK

Infoblox identifies domain associated with data exfiltration and blocks connection

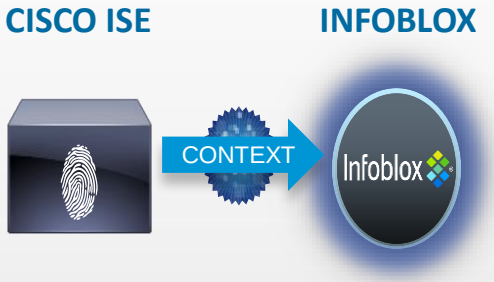
Infected endpoint attempts data exfiltration

- Carbon Black correlates endpoint, network data and remediates infected endpoint automatically
- Kills endpoint process, preserves evidence
- Updates security policy [kill process] on all endpoints

BLOX FEST

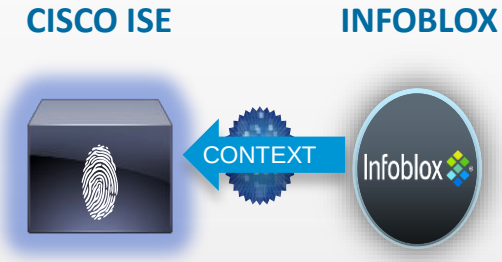
Cisco ISE pxGrid Integration

1 Cisco Provides Network Context to Infoblox



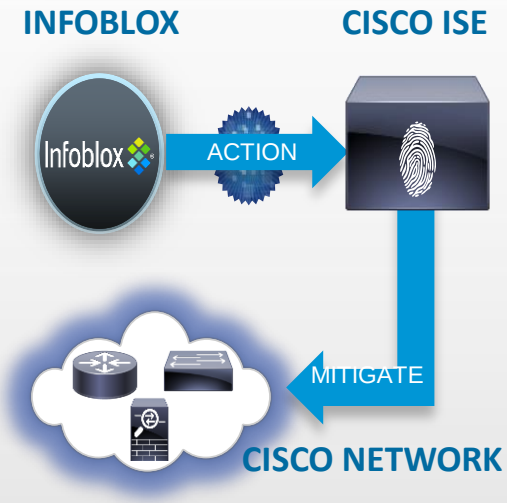
Cisco Shares User/Device & Network Context with Infoblox

2 Use Infoblox DHCP & IPAM Context for Cisco Network Policy

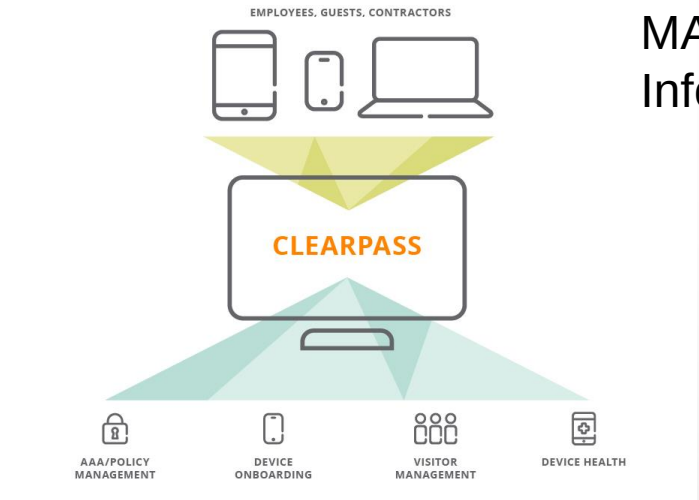


Cisco Receives Context from Infoblox to Make Better Network Access Policy

3 Infoblox Secure DNS events into the Cisco Network for Remediation

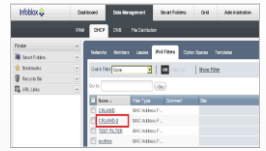


HP/Aruba ClearPass Exchange Integration



ClearPass acts as a single point of policy control across all wired, wireless and remote infrastructure for a global organization.

ClearPass Exchange sends Username to MAC Address mapping information to Infoblox's MAC Address Filters

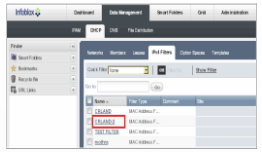


Infoblox
CONTROL YOUR NETWORK

Infoblox appliances will only provide a DHCP IP address to device that is listed in the MAC filter. This prevents unauthorized devices from connecting to internal wired/wireless networks.

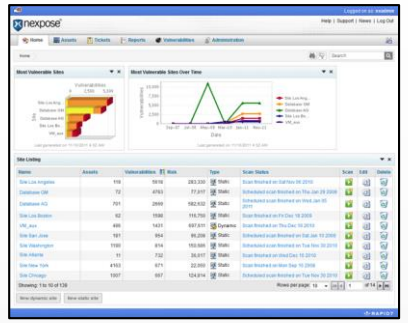
BLOX FEST

Vulnerability Scanning Integration



Infoblox
CONTROL YOUR NETWORK

Infoblox authoritative IPAM



RAPID7 nexpose

Scan new devices as soon as they join the network

BLOX FEST

Infoblox DDI, NAC and Vulnerability Scanner Integration

1 Infoblox issues a new DHCP lease

2 Notify ISE of the new DHCP lease

Cisco ISE

3 ISE requests device scan

4 Reports vulnerability risk, updates status to ISE

5 ISE quarantines device based on the risk score

Our Security Ecosystem – Expanding Aggressively

BLOX FEST

Final Thoughts

- Customers don’t need yet more security solutions. They need to use what they have better
- Infoblox is making significant efforts:
  - To make our data available to the security team
  - To drive our vendor ecosystem via open APIs and out-of-box integrations
    - More integrations to come with the release of NIOS 7.4!
  - To offer focused solutions for DNS security
  - To provide flexibility for virtualization and cloud transitions

Q/A

http://vignette1.wikia.nocookie.net/unofficial-nerdcubed/images/d/d7/Tardis.jpg/revision/latest?cb=20130702013111

BLOX FEST