IDC ANALYZE THE FUTURE

DNS, it’s role in Digital Transformation and in the NOC and SOC

Infoblox Security & Cloud Roadshow 2019

Digital Transformation (DX) Defined

The application of 3rd Platform and related technologies to fundamentally improve all aspects of society. For business this means:

TRANSFORM…

New sources of innovation and creativity to enhance experiences and improve financial performance. Simply modernizing the technology underpinning existing systems is not transformation.

…DECISION MAKING…

Using information to create an evidence based culture. Companies should plan on doubling the productivity of their knowledge workers by using information more effectively.

…WITH TECHNOLOGY

Digital transformation is not to be confused with digital technologies, however, it does use 3rd Platform technologies such as Cloud, mobility, Big Data, and social as well as Innovation Accelerators including IoT, robotics, and 3D printing.

What's the Damage?

Business Operations

- Lost Data
- Halted Operations
- Stolen IP
- Unrecoverable Assets

Business Costs

Average Cost of a breach $3.62 million

Average cost of a record $141

–IBM

Ransomware Costs in the Billions?

–Fedex/TNT Estimated $300 million

- Downtime per hour
- Reputation Harm
- Legal Costs
- Regulatory Fines

CHANGES IN FIVE YEARS — THEN

1. Best-of-breed security point products protected assets behind a stateful firewall.
2. Cybersecurity is a repetitive and manual process.
3. Role- and rule-based defenses, and known malware and blacklists.
4. Security, IT, and Operational Technology have distinct functions within organizations.
5. Cyber defense is necessarily reactive (needs alerts, vulnerability scans, etc. to prompt activities).
6. Point products compete within silos against other point products.

Cybersecurity Now (and Evolving)

1. Each point (application/device) is its own version of truth and must be treated as its own perimeter.

2. Moving toward automation and orchestration.

3. UEBA and heuristics play an important supporting role in cybersecurity.

4. Still some segmentation—however, IT/security/OT inform and bleed into each other. *Foreshadow: This will matter in the DNS discussion.*

5. Hopefully, there is a degree of proactivity in cybersecurity (predictive analytics/prevents bad behavior).

6. All solutions in evidence (best-of-breed, platforms, managed/co-managed, and professional services).

SOC Concerns in Cybersecurity

New Security Considerations

- Public and Private Clouds
- Internet of Things
- Mobile
- Contractors affecting Line of Business
- Attention to DevOps — NEW

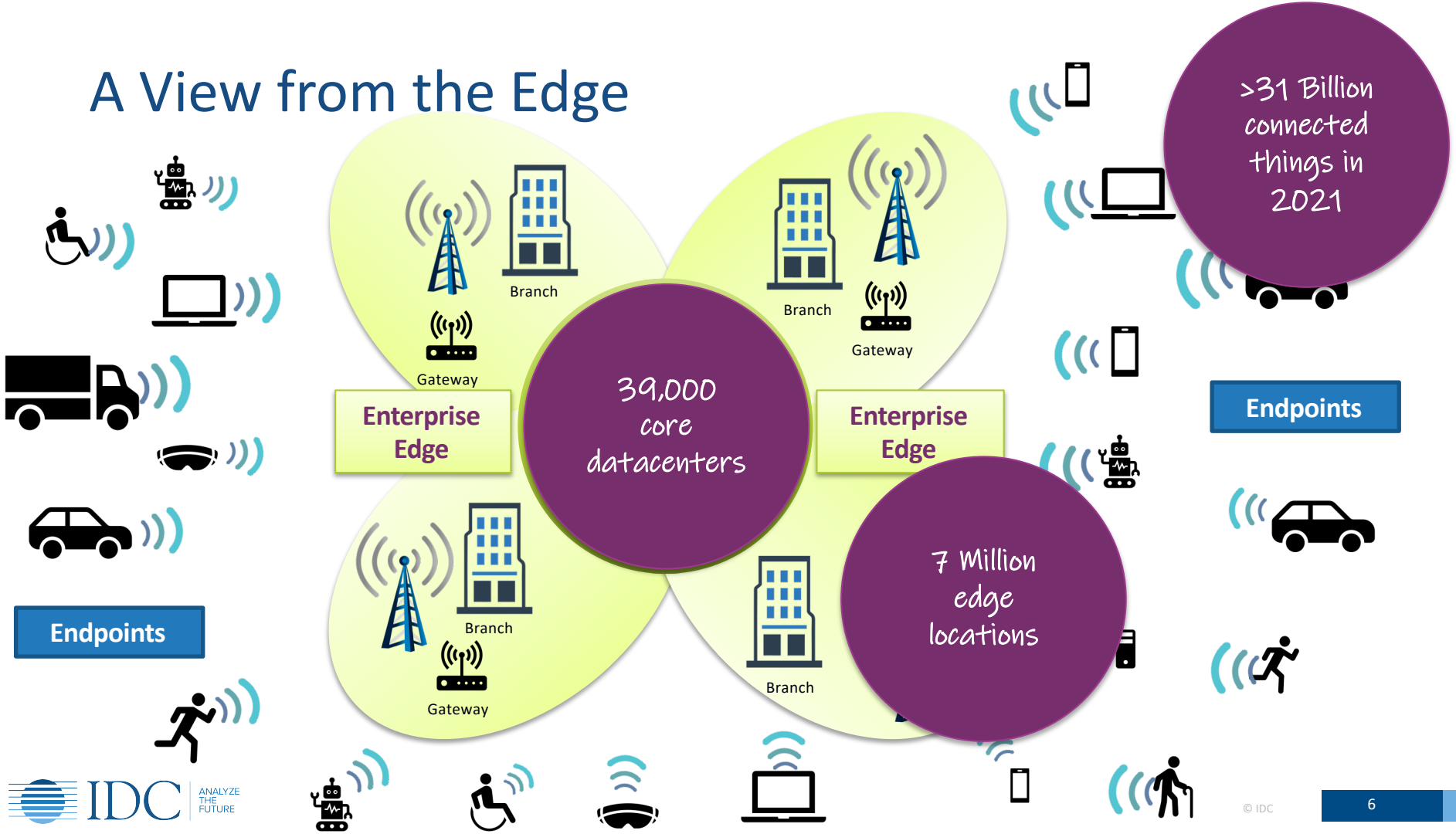
Public Cloud in Cybersecurity

- Cloud-based SaaS
- Popular applications hosted and accessed
- One security flaw, one to many
- Threat Intelligence-as-a-service — NEW

Incident Detection *AND* Response

- Encrypted Traffic — NEW
- Vendors taking on more of the IDR stack
- Automated response and orchestration — NEW
- Transitioning security events into operations — NEW

A View from the Edge



Gaps in Conventional Cybersecurity

1. If a network event *appears* legitimate, security tools are often hamstrung to find anomalies
2. Trouble detecting threats from either side of the perimeter
3. Cybersecurity tools require bandwidth or static high performance computations; could be more agile or adaptive

Areas for Future Innovation

- **Convergence and Hyperconvergence.** Platforms such as SD-WAN and cloud-managed networking provide opportunities to efficiently converge enterprise networking and communications functions. Network access (wired/wireless) convergence will grow in importance as well. As IT becomes leaner and IoT deployments become more prevalent, enterprise interest in hyper-converged edge IT is poised to grow.

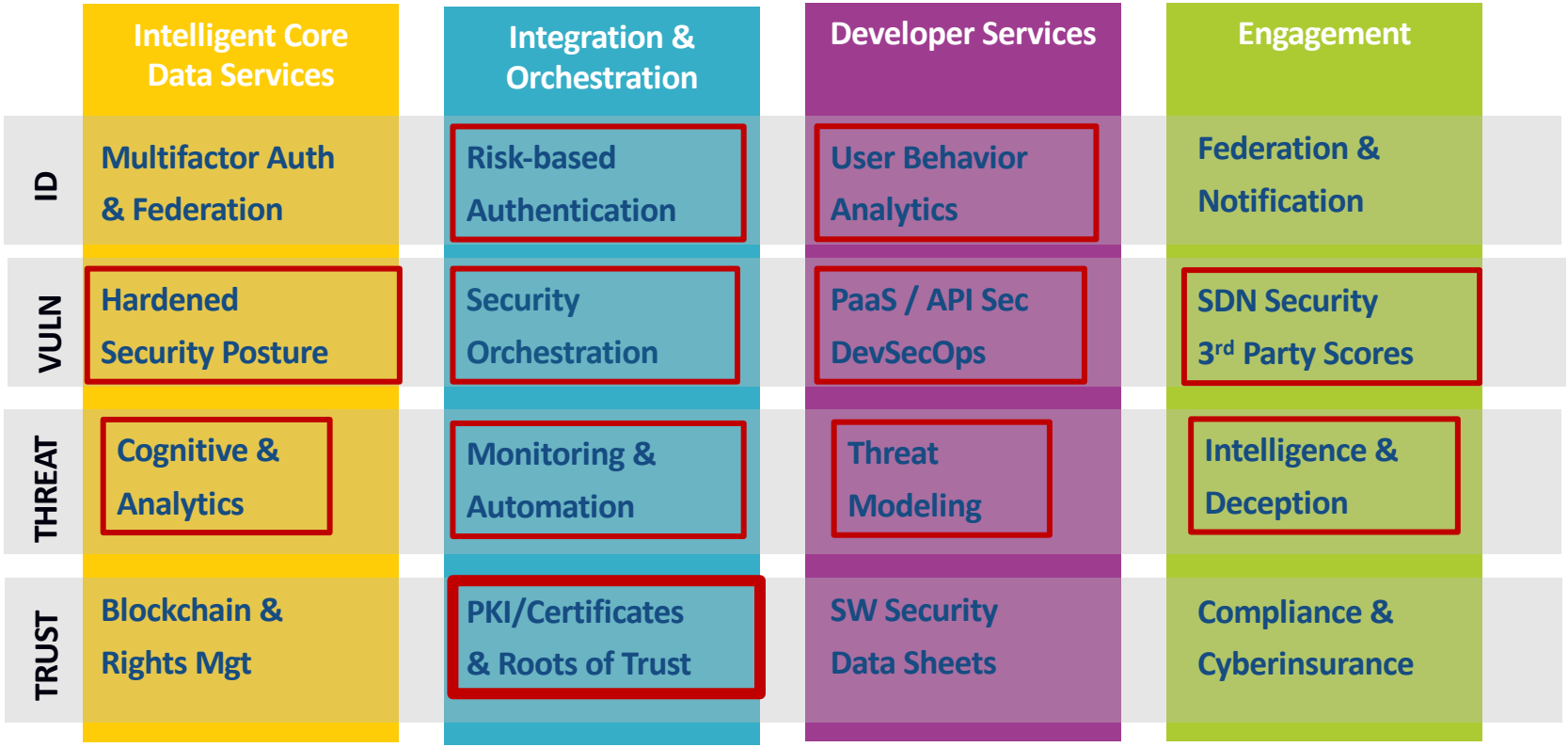
- **Advanced automation platforms.** As the complexity of networks continues to increase, enterprises have an appetite for management platforms that provide detailed levels of visibility and advanced automation, which IDC refers to as Intent Based Networking. Vendors have an opportunity to leverage machine learning and artificial intelligence tools to creating self-driving networks.

- **Cloud-managed delivery models.** While cloud-managed networking continues to grow, there are some limitations (e.g. regulatory) to it becoming ubiquitous. However, many organizations would like to leverage the benefits of cloud to deliver network and communication functions/services - an area that will provide opportunity for network infrastructure suppliers to innovate.

Infoblox for Cybersecurity

- Infoblox has multiple approaches to monitor and investigate domain name service (DNS), dynamic host configuration protocol (DHCP), and IP addresses (IP); the combination of services is called DDI, and it is powerful.
- Infoblox ActiveTrust Cloud can be used like a Web filter because it looks for malicious sites, top-level domains (TLD) keywords, and categories. ActiveTrust serves as a cloud-based recursive DNS server, and does not require a physical appliance or proxy. Protection/detection is centrally managed and can be applied across an organization.
- Heuristics applied to The session itself may yield useful information; an endpoint beaconing is different than a legitimate Web or email session.
- By cataloging DHCP communications, Infoblox can build a profile of what a device is.
- In various platforms, Infoblox provides more than just a topographical representation between internal devices. The topography includes where devices are connected by VLAN which can be utilized in incident detection and response.

Manage Shared IT Resource Risk



Places where DDI have direct influence

Security Automation

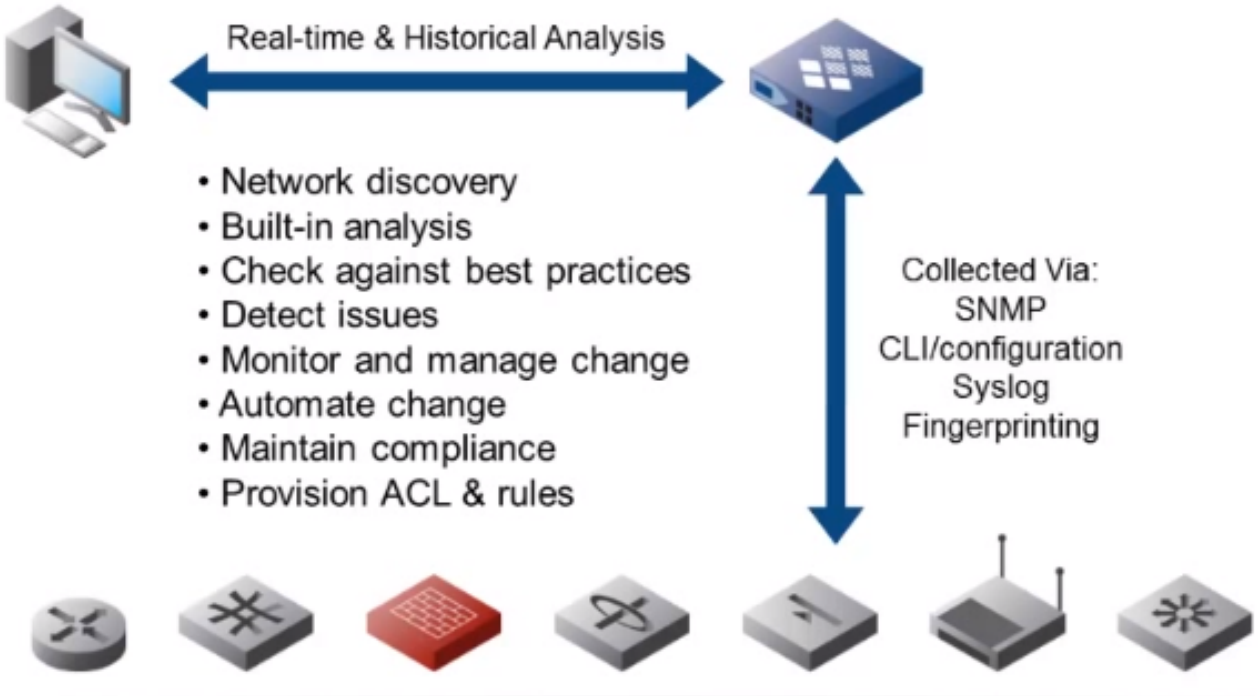
- Security automation and analytics are poised to change the way we “do” security.
- Security-at-scale for automation is a necessary ingredient to any security program.
- Machine learning must be used to evaluate security controls for threat and attack detection.
- The data used for security analytics can also be aggregated and used to measure the efficacy of a security program.

INFOBLOX Cybersecurity Automation and Orchestration

(various products)

- An important facet of Infoblox Microsoft IPAM service is the integration of Active Directory with IP addresses. A NOC/SOC administrator keeps context in investigations constant and can apply DNS firewall or RPZ policies based upon user groups.
- Adding heuristics to DNS log data helps tremendously when investigating alerts (one example, isolating a malware signature to cross reference against TLDs or external threat intelligence need not be a manual process).
- For network automation, the change manager includes automatic change detection, job flow and control, saved historical configurations, and configuration search.
- Reporting is handled by a mouse-click.

Infoblox Network Automation Overview



NOC? NOC? Who's There?
Network (DDI) to find Indicators of Compromise

- Entropy analysis is in important security inspection capability—the adversary can be jamming data in the host field or in the label field.
- Be it ever so humble…the Change Management feature in Infoblox DDI may see small changes in traffic patterns, DNS queries, etc., over time that may not have been detected.
- An underappreciated idea is if the adversary understands that there is a discontinuity between the NOC and SOC, it is easier to tease out an attack vector.
- Port activity and end-user/network device connectivity are useful to determine if more capacity is needed or if there are specific bottlenecks. But suspicious Port activity is also an IOC.
- Dashboard viewpoints include Replies Trends, Daily Query Rate, Top Client activity (by query, by domain), and Top SERVFAIL errors. To monitor DHCP, the client sees message rate trend, and v4 utilization statistics.

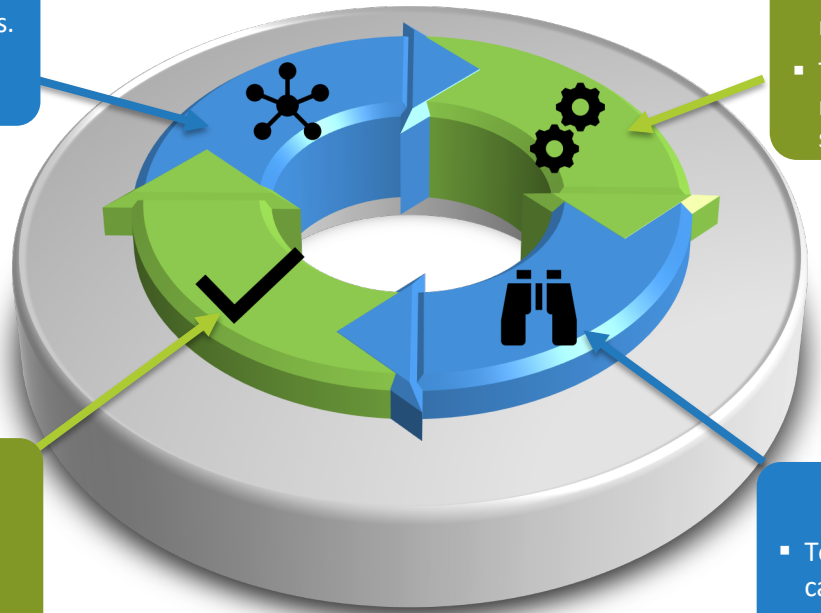
NOC Focus—Facilitating Networks

Policy

- Optional use of BIND for RPZ, embedded compliance rules, and misconfigurations.
- DNS firewall (prevent, sinkhole)

Automation

- Using DNS routing to determine nearest POP server (uptime)
- Triggered job capabilities like bare metal provisioning, and rogue DHCP server isolation.



Verification/Assurance

- Identify end users through Active Directory
- Protection against specific DNS attacks (DNS reflection for example)

Visibility

- Topography of the network is a central capability.
- DHCP protocols used to identify devices.

Forced Multipliers in Infoblox Platforms

Cloud Integration

DNS is protocol agnostic

Extensible

Consolidation of servers (central management)

External Threat Intelligence**

RPZ can be used as a firewall

Understand Malware

Change Monitor

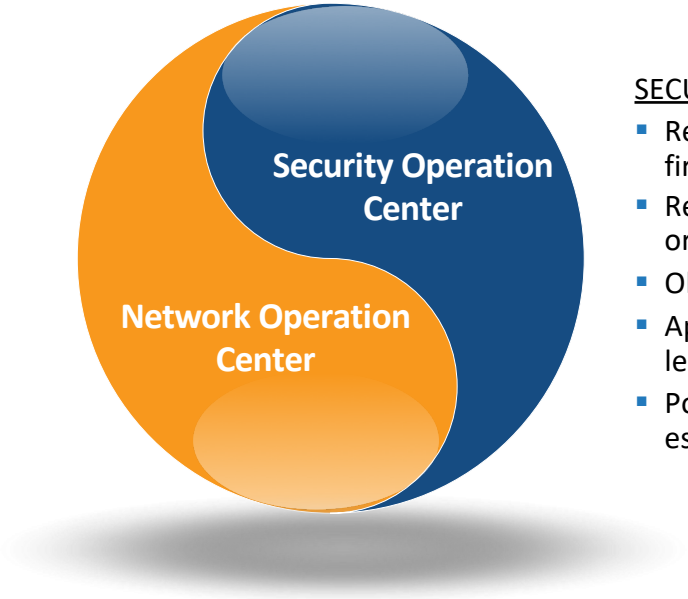
NOC/SOC visibility

IDC ANALYZE THE FUTURE

Where DNS management and monitoring enhance NOC and SOC practices

NETWORK OPERATIONS

- Load balancing (*Note: availability is security related)*
- Management internal servers/subnets
- Consolidate and centralize DDI (and other extensions as well)
- dnstap for visibility into socket type, socket protocol, query port, query address, timestamp.
- See http://dnstap.info
- Pre-check server health before routing traffic (SNMP, HTTP/S, and round trip delay).



SECURITY OPERATIONS

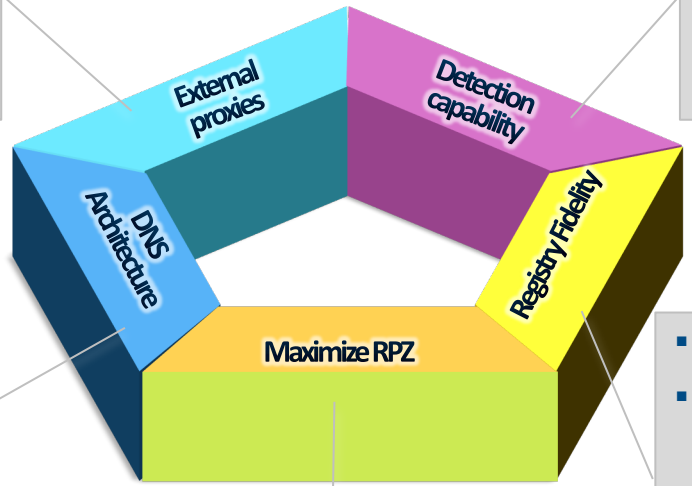
- Response Policy Zones (functional as firewalls, can be customized)
- Reconciliation (check for changes in original DNS registry)
- Obfuscation (CNAME)
- Apply heuristics and machine learning to new DNS sites
- Possible detection of privilege escalation

The Big Scary Stats about DNS-related Attacks

- A 2018 survey estimates the average DNS attack cost global businesses $715,000 per attack; a+57% YoY.
- The same survey shows that the average business was attacked 7 times in a year on average.
- According to a 2018 survey sponsored by Infoblox, 33% of organizations suffered data theft via DNS.
- Over 48% of DDoS attacks use multiple attack vectors (malware strains).
- According to the Arbor Networks 13th Annual Worldwide Infrastructure Security Report, April 2018, service providers were attack targets—87% suffered a DDoS attack, and 15% were victims of route hijacking.
- According to the same report, DNS is the largest reflection/amplification attack tactic.

DNS Best Practices

- When working with cloud-providers make sure they have local proxies.
- GeoDNS approach for response time, load balance.
- DNS resolution goes out the same path as the Internet traffic.



- Real-time monitoring
- Contextual aware DNS traffic analysis
- Behavioral threat detection

- Only Internet forwarders should be able to access the Internet
- Limit the number of devices that can initiate a DNS query
- Establish a local DNS server
- Update root hints to refresh DNS servers with latest information.

- Monitor security practices of registries and registrars
- Find a mechanism to monitor changes in your registries

- Leverage open-standard BIND.
- Customize RPZ policies (i.e. compliance, PII, etc.).
- Continually update RPZ against known malicious sites.

Adapting defenses to match future networks

The traffic itself is changing

More than half of the traffic on the Internet is encrypted—this percentage will only rise as browsers insist on safer point-to-point protocols.

Manual processes in the NOC/SOC are through

…although it's been said many times many ways. Contextual awareness toward investigating alerts has to be readily available to analysts. NOC and SOC alerts have to be refined to a single alert[1].

Use everything

Machine learning, smartly developed algorithms, and high-performance computing allow for multiple NOC/SOC vantage points—feel free to use them all.

Cleanliness is godliness

Intelligent traffic management includes de-duplication. If multiple NetFlow are reduced at the source; the mean-time-to-detect a threat is greatly reduced.

Analytics at the source

Applying analytics at the point of traffic processing is preferable to product aggregation and interpretation.

[1] Consider professional/managed services to fill in tools gaps or manpower shortages.

Conclusion—It's a Wrap

- The first step when an end user attempts to access the Web is to access the cache of known good IP addresses in the DNS cache resolver. If this step is compromised in anyway; the options for disruption or exfiltration that the adversary gains are limitless.
- DNSSEC is not a 'like-to-have' capability, it is more like a 'need-to-have.' DNS security directly affects the end user, the health of the network, and the overall security posture of business and network applications.
- The problems that Infoblox appliances and cloud-based services solve are intuitive; the Microsoft IPAM service and Infoblox DDI helps consolidate NOC/SOC procedures.
- DNS visibility is another quiver in the arsenal of security operations becoming more valuable as encrypted communications become the norm and not the exception.