Purpose: To arm Cisco Umbrella sellers and account teams with a differentiated DNS security solution to effectively compete and win against InfoBlox.

Value of integration:

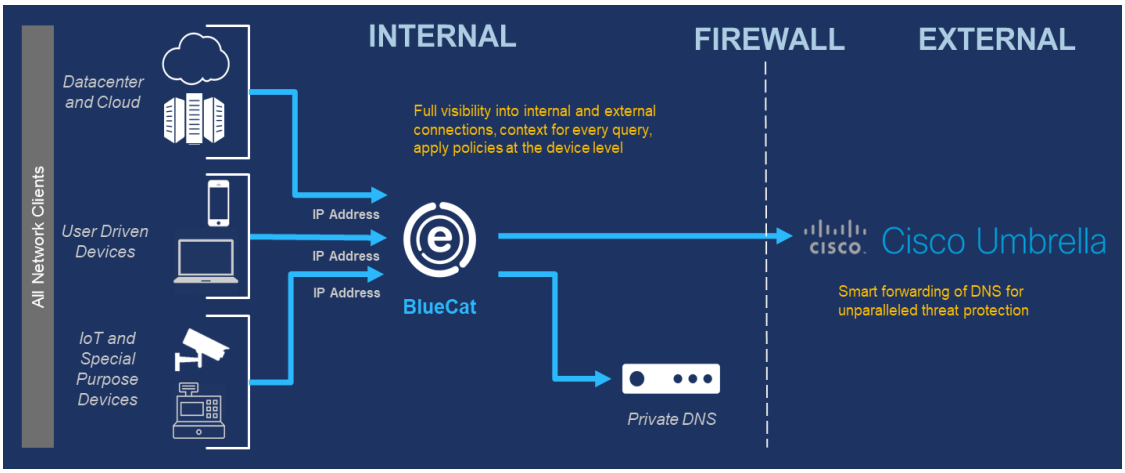
- **Visibility:** Allows Cisco Umbrella users to see the IP address and device information that are protected by Umbrella, providing additional security context and details
- **Policy Enforcement:** Using IP information, security operations teams can now deploy more granular security policies, improving the end user experience and enforcing more sophisticated forms of least privileged access.
- **East-West Visibility and Control**: Users can now see and control all East-West traffic on their network. Since up to 60% of network traffic is internal, users now have unprecedented visibility and policy enforcement, including black-listing, white-listing and securing IoT devices.
- **Optimization:** BlueCat's compatibility with Cisco ISE, Cisco ISRs, Active Directory, and other core network management elements, ensures consistent delivery of policies across internal and external access points.
- **Unifies core DDI** infrastructure capabilities with Cisco Umbrella to detect and stop threats faster everywhere, both on and off-network.

Elevator Pitch:
The Cisco Umbrella integration with BlueCat fortifies network defenses, providing visibility and context into all internal and external traffic to find threats faster and prevent downtime. The joint solution enables security and networking teams to keep end point users safely connected to data center, cloud and internet services without adding complexity and operational cost and risk.

Cisco Umbrella	**BlueCat DNS Edge**
Cisco Umbrella is a secure internet gateway that provides the first line of defense against threats on the internet wherever users go. And because it's built into the foundation of the internet and delivered from the cloud, Umbrella is the simplest security product to deploy and delivers powerful, effective protection.	DNS Edge provides an intelligent DNS layer inside your network as the first-hop for all internal devices, users and applications. It arms you with an early warning system that provides granular visibility and control over DNS traffic, allowing you to set smart policies to actively monitor, steer DNS traffic, and block threats.

An integration with BlueCat delivers these benefits:

- **Find threats faster** through rapid correlation of external threat data with source IP
- **Visibility and control** over internal, "east-west" queries (around 60% of network traffic)
- **Reduce network costs** and optimize SD-WAN performance by eliminating data center backhauls
- **Improve customer experience** with fast, easy deployment – no matter what DDI solution is in place



Who is BlueCat:

BlueCat is the Adaptive DNS™ company. We help the world's largest organizations thrive on network complexity, from the edge to the core. Unfortunately, most DNS solutions like Microsoft and BIND are outdated, error-prone and manually configured, which means more work, higher risk, spiraling costs and stifled innovation. So BlueCat re-imagined boring, old DNS. The result – Adaptive DNS™ – is a dynamic, open, secure, scalable, and automated resource that supports the most challenging digital transformation initiatives, like:

- Cloud migration and the challenge of orchestration in hybrid environments.
- Massive increase in apps, services & devices
- Evolving network security threats
- Critical demand for network availability
- Lack of network visibility and control
- Soul-crushing manual network configuration

How to recognize an opportunity:

- Customer is unhappy with Infoblox due to cost, service etc.
- Customer has security/compliance requirements for tracking connected east-west DNS traffic.
- Need visibility of internal and external traffic and shared security event information and context for improved decision making.
- Difficulty logging DNS data into SIEMs.
- Need to rapidly detect and block DNS-based attacks and data exfiltration.
- Need to accelerate incident response and threat investigation and threat hunting efforts.

Qualifying Questions:

1) How are you currently logging DNS data into your SIEM?
2) Can you correlate the DNS response data to a source IP in real time?
3) How do you currently get visibility into east-west traffic and apply security policies when a threat is discovered?
4) How do you allow users to stand up compute on demand, if so, how do you enforce security policies?
5) How do you manage and provide visibility into the DNS environment supporting Cloud?

Why BlueCat wins over InfoBlox in DDI:

- **White-glove Customer Service** is the bridge between our technology and your business. These bridges create partnerships, not transactions. That's why BlueCat is the #1 highest rated network automation vendor on Gartner's peer reviews. With core infrastructure technology, like DNS, the best customer service is needed to ensure network resilience at all times.
- **Flexible Architecture** that scales with customer's growth without expensive upgrades and add-ons that might require re-architecting their DNS deployment at random thresholds and tiers. Infoblox is more box-centric, while BlueCat is focused on what works for the customers, ultimately leading to lower cost of ownership.
- **Automation, Integration and Extensibility** focused to accelerate service delivery with other enterprise systems, DevOps processes and hybrid-environment migrations.

Overcoming Objections:
Objection: Doesn't Infoblox offer a fully integrated solution so that I am only dealing with one solution?
Response: Having a single solution is important and one we have heard from many organizations. That's why our joint solution is fully integrated enabling you to make faster decisions when it comes to stopping cyberthreats. It capitalizes on the strengths of both Cisco and BlueCat to deliver complete visibility across the entire IT estate. Integrated threat intelligence provides critical insight and context and makes identifying and responding to both internal and external threats more effective, ensuring you take the right action the first time.

Objection: I have no budget for this project.
Response: Have you had a DNS/DHCP outage recently? If so, how much would an outage cost your organization? Recent trends show outages costing companies millions of dollars and reputational damage and we have seen in many instances the cost savings when implementing our solution saving valuable time and money for already strapped IT teams and allowing them to re-invest in other areas.

Objection: I already have a security solution place and don't need it.
Response: I hear that often in discussions with many of the organizations I speak with. If you don't mind me asking, how do your current solutions effectively monitor for east-west traffic to determine if the traffic is legitimate or malicious? And what actions do you take in the event the traffic is indeed malicious and how do you prevent it from happening in the future?

How to engage:
To engage with the BlueCat team, email Alejo Calaoagan at acalaoag@cisco.com. For SE assistance with an account, contact Thomas Wood or Mark Murtagh.

Cisco Advantage:
Cisco's commitment to fostering integration between its own best-of-breed security products and third-party point solutions is almost unparalleled in the enterprise security industry. With CIsco Umbrella you get a solution that works with your existing stack and local intelligence, so you can enrich incident response data and easily extend protection to devices and locations beyond your perimeter.

The **Cisco Cloud Security** ecosystem also expands with more integrations from *BlueCat, Cisco ACI and Cisco DNA*. These integrations not only help organizations manage, prioritize, and mitigate IOCs, but they also provide mechanisms to automate several threat lifecycle workflows, effectively improving both mean time to detect and respond to threats, as well overall SOC efficacy.