# **Gaining Visibility & Control**

Automation is driving new efficiencies across today's networks.Unfortunately, this wave has not yet reached most core network infrastructure services. Most back-end systems like DNS, DHCP, and IPAM are still largely managed through manual processes.

It's like yelling, 'there's a fire in our town' but not knowing which house it is. I can't send a fire truck to every house and check it. And I can't just dump water on the entire town.
Security Analyst, Healthcare Provider

# The Solution - Cisco Umbrella & BlueCat DNS Edge

To stay ahead of network threats and provide continuous delivery of mission-critical services, network operations and security teams need to work smarter. With 60% of network traffic flowing through internal DNS, and attacks using DNS continuing to rise, teams must gain better visibility into east/west network traffic and uncover threats faster to avoid business disruption.

# Gain Visibility & Control Across Internal & External DNS Traffic

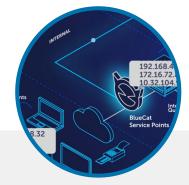
BlueCat DNS Edge with Cisco Umbrella expands the boundaries of network defenses providing unprecedented visibility into all network traffic. The solution enables customers to strengthen security and network defenses by reducing complexity, expediting response times, optimizing security investments and improving the effectiveness of security operations teams.

### **Eliminate Blind Spots**

Network operations and security teams are challenged with correlating endpoint threats that move laterally within the network. These teams must quickly look back at the DNS attribution chain for suspicious endpoint activity connecting North-South and East-West traffic. Together BlueCat DNS Edge and Cisco Umbrella provide rich DNS data to answer the most critical questions in network security: Who, What, When, and Why.

### **How It Works**

Using BlueCat DNS Edge, customers deploy a lightweight, cloud-managed DNS servicer (or "service point") at the edge of the network. As a client-facing solution, BlueCat DNS Edge serves as the first-hop for DNS query resolution for endpoints. It logs every DNS request, from every endpoint, and applies policies based on any number of criteria.



### **Benefits**



#### Improved Network Performance

Reduce network congestion using DNS Edge as both a caching and forwarding server.



Secure Access To Critical Internal Resources Apply security policies to stop attacks and prevent the spread of malware.



#### Prevent Outages & Downtime

Enable faster remediation with real-time analytics and forensics of DNS traffic.



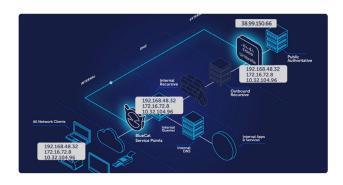
#### Improved Customer Experience

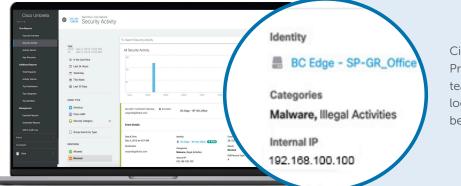
Accelerate application performance and reliability for hybrid environments.

# Simple To Deploy, Easy To Manage

- Apply Cisco's powerful threat detection and content filtering capabilities to any end point on the network, protecting them from malware, bad domains and other threats.
- See the source of every outbound DNS query down to the individual endpoint IP address, providing greater context and allowing for more granular security policies.
- See every outbound DNS query including those resolved by caching servers inside the network. This provides more context into the scope of a threat, and can help identify and remediate cache poisoning techniques.
- See every internal "East-West" query including those that never go through the Cisco Umbrella cloud security platform. This speeds remediation and helps identify 'patient zero' in any cyber attack.
- Apply policies to internal "East-West" traffic in order to lock down critical internal services and intellectual property.

BlueCat DNS Edge service points sit at the network edge, capturing all DNS queries and source IP addresses and passes them directly to Cisco Umbrella for policy management.





Cisco Umbrella's industry leading Threat Protection provides threat alerts to security teams. Quickly triangulate the endpoint by looking back at the attribution chain shared between BlueCat DNS Edge and Cisco Umbrella.

With BlueCat DNS Edge, investigate the lateral movement of suspect endpoints by capturing all internal DNS queries and apply internal policies.

192.168.100.100     easyridegolfcars.com.     10.000     www.sec.ex	
SOURCE IP     QUERY NAME     NAME       192.168.100.100     easyridegolfcars.com     Image: Comparison of the comparison of	
SOURCE IP     QUERY NAME     NAME       192.168.100.100     easyridegolfcars.com     Image: Comparison of the comparison of	
Number     Numer     Numer     Numer <th></th>	
Number     Numer     Numer     Numer <td></td>	
192.168.100.100     easyridegolfcars.com.     192.168.100.100     finance.acmecorp.com     Notestantian	
192.168.100.100     easyridegolfcars.com.     under state     addition of the state     addition of	Vonto
192,168.100,100     finance.acmecorp.com     Normation     Control to the state of the	i leck 🔺
92.168.100.100     finance.acmecorp.com     Harden accumecorp.com     Har	tieck 🔺
192.168.100.100     finance.acmecorp.com     10.277     40.44 minute     10.46 mi	lieck 🔺
102.168.100.100     engineering.acmecorp.     100.101     Access acmecorp.	tinck 🗛
92.168.100.100     engineering.acmecorp     output     output <td>int A</td>	int A
.92.168.100.100     engineering.acmecorp     .01.07     state     .02.07     <	Airch A
92.168.100.100     dev.acmecorp.com     90.100     000000000000000000000000000000000000	Nere
92.168.100.100     dev.acmecorp.com     1000000000000000000000000000000000000	Mary
92.168.100.100     customers.acmecorp.com     000000000000000000000000000000000000	Nare
92.168.100.100     customers.acmecorp.com     000000000000000000000000000000000000	kieck 🗛
22.168.100.100     customers.acmecore     customers.a	Flock 🔺
1068.100.100     sales.acmecorp.cf     101220     Market Market Street St	liect 🔺
168.100.100     sales.acmecorp.cf     for the same sector of the same sector o	eleck 🗛 🚽
168.100.100     sales.acmecorp. Construction     optimizer     opti	Field A
100.100.100 legal.acmeco	Hart A
100.100 legal.acmeco	Hert A
100.1000 J [10,007] (2000 J [10,000]) (2000 J [1	lint A
100.1000 J Lot 2017 2024 http://www.sec.edu/actives/activ	tieck 🗛
	tiest 🔺
	tieck 🔺
	ilace 🔺

#### **United States Headquarters**

156 W. 56th Street, 3rd Floor New York, New York 10019 +1.817.796.8370 | 1.833.BLUECAT

#### Canada Headquarters

4100 Yonge St. 3rd Floor, Toronto, ON, M2P 2B5 +1.416.646.8400 | 1-866-895-6931

### **Next Steps**

Get in touch with a BlueCat representative to future proof your network.

Visit <u>bluecatnetworks.</u> <u>com/contact-us/</u>

### bluecatnetworks.com