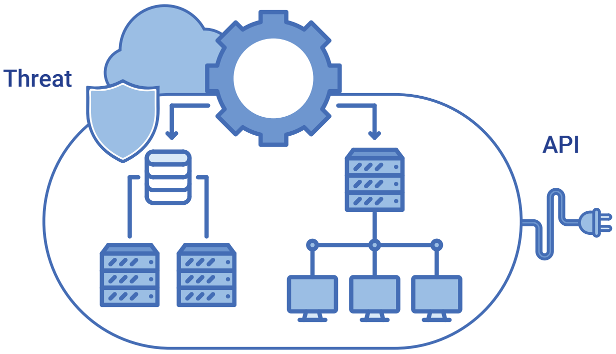
Table of Contents

Delivering a Single Source of Truth

With devices and applications multiplying exponentially, networking teams are forced to maintain complex infrastructures as they integrate new hybrid and multi-cloud platforms, security tools, SDN, IoT, and more. For most organizations, DNS, DHCP, and IP address management (DDI) services seem invisible until they malfunction. However, DDI solutions provide a single source of truth, simplify management, improve business resilience, and enable automation and DevOps practices. To enable business growth networking teams operating agile environments and cloud infrastructure, a DDI platform that works at the speed of business is needed.

The Solution – BlueCat Integrity

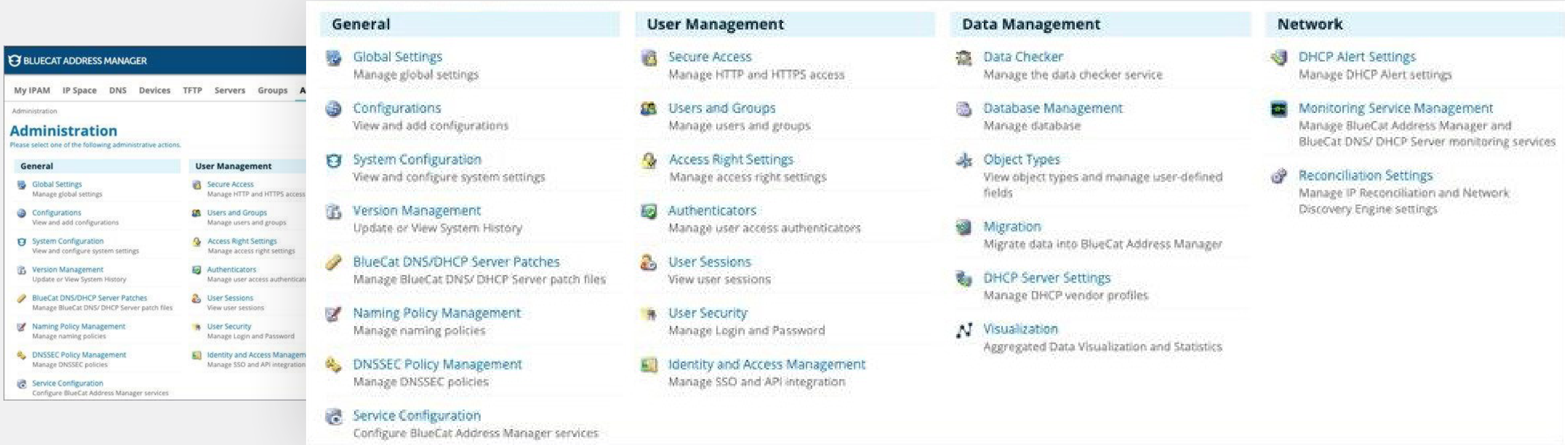


You need your DNS to enable your business and customer transactions and BlueCat can help you make it fast, resilient, and secure. Whether you need to centralize control of core DDI services, accelerate application performance, deliver networking for branch offices, or to integrate with hybrid and multi-cloud environments, we have you covered.

BlueCat Integrity provides an intelligent DDI platform designed to eliminate complexity, automate provisioning, accelerate application deployment, and ensures business resilience.

Benefits

- Unifies disparate DNS, DHCP, and IPAM (DDI) solutions into a single source of truth
- Reduces network administration costs by 80%
- Moves with compute workloads across physical and hybrid environments
- Integrates everywhere to provide universal DNS access
- Drives speed and efficiency by eliminating manual errors through smart automation
- Delivers uncompromising DNS visibility and control to protect against cyber threats



BLUECAT ADDRESS MANAGER

My IPAM | IP Space | DNS | Devices | TFTP | Servers | Groups

Administration

Administration

Please select one of the following administrative actions.

General

- Global Settings — Manage global settings
- Configurations — View and add configurations
- System Configuration — View and configure system settings
- Version Management — Update or View System History
- BlueCat DNS/DHCP Server Patches — Manage BlueCat DNS/ DHCP Server patch files
- Naming Policy Management — Manage naming policies
- DNSSEC Policy Management — Manage DNSSEC policies
- Service Configuration — Configure BlueCat Address Manager services

User Management

- Secure Access — Manage HTTP and HTTPS access
- Users and Groups — Manage users and groups
- Access Right Settings — Manage access right settings
- Authenticators — Manage user access authenticators
- User Sessions — View user sessions
- User Security — Manage Login and Password
- Identity and Access Management — Manage SSO and API integration

Data Management

- Data Checker — Manage the data checker service
- Database Management — Manage database
- Object Types — View object types and manage user-defined fields
- Migration — Migrate data into BlueCat Address Manager
- DHCP Server Settings — Manage DHCP vendor profiles
- Visualization — Aggregated Data Visualization and Statistics

Network

- DHCP Alert Settings — Manage DHCP Alert settings
- Monitoring Service Management — Manage BlueCat Address Manager and BlueCat DNS/ DHCP Server monitoring services
- Reconciliation Settings — Manage IP Reconciliation and Network Discovery Engine settings

Features

DNS

BlueCat feature-rich Recursive and Authoritative DNS solutions can be deployed for any environment delivering a responsive and reliable network that manages unwanted traffic, rapidly enables core services, and speeds application performance and availability.

DHCP

Our Dynamic Host Configuration Protocol (DHCP) solution offers built-in security, high availability, a scalable architecture, and dual-stack support. We help you make the most of limited IPv4 space and manage dual-stacked IPv4 and IPv6 environments

IPAM

Our IP Address Management (IPAM) offering provides an authoritative source of intelligence and insight into the relationship between the devices, users, and IP addresses on your network, using built-in IP modeling tools and network templates for simplified management.

Full-Featured APIs

BlueCat enables an automated environment through a robust library of APIs that facilitate continuous updates, improve threat detection, and policy enforcement by providing instant access for users and applications. Our API-first approach works with any environment and optimizes existing IT investments.

High Availability

Our solutions deliver highly available DDI services across the enterprise, with the flexibility to deploy in high-throughput, centralized architectures, or fully distributed environments. DNS and DHCP failover ensure that IPv4 and IPv6 retain the highest standards of service uptime.

Threat Protection

BlueCat threat protection integrated security intelligence helps cybersecurity teams rapidly identify and stop threats before they can reach business-critical applications or data. Your DNS data is enriched with crowdsourced data and backed by an elite group of threat analysts and security researchers.

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

bluecatnetworks.com

Next Steps

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

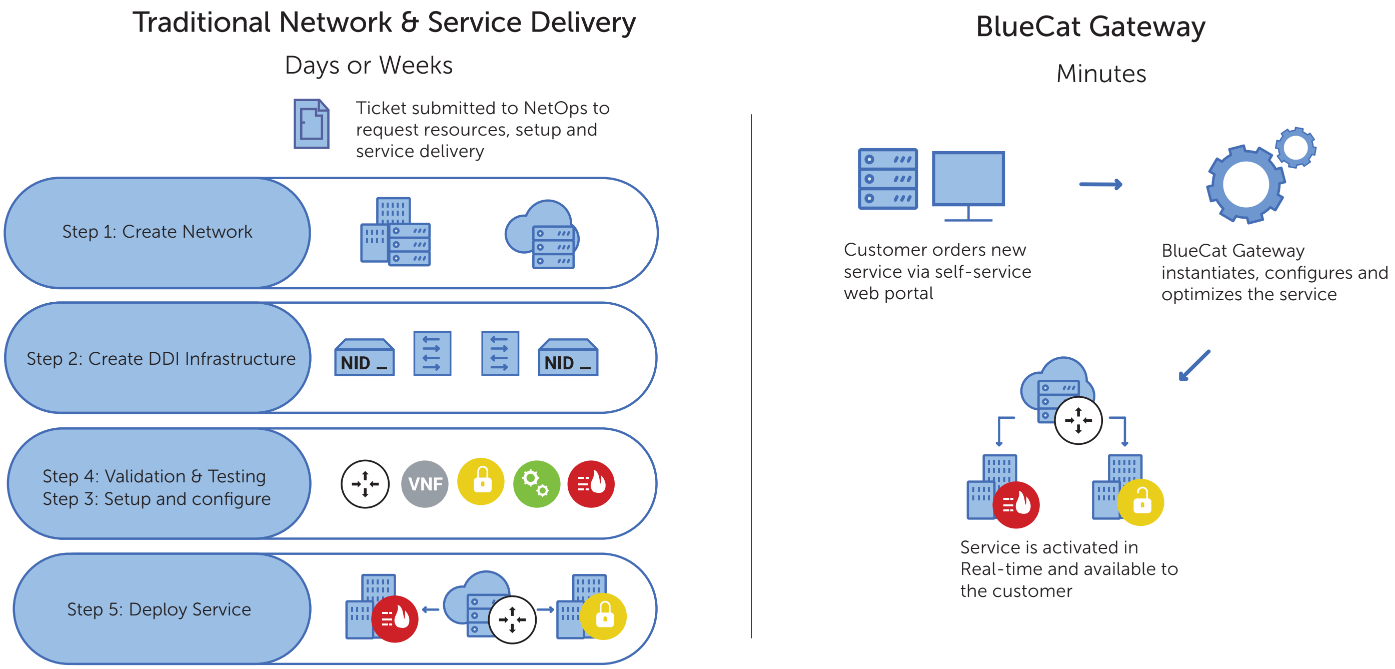
Visit bluecatnetworks.com/contact-us/

Scale Network Automation

Today, there is an exponential rise in the number of devices, users, and applications connecting to the network. To meet these demands, networks are getting more complex. Yet up to 95 percent of network changes are still performed manually, resulting in operational costs 2 to 3 times higher than the cost of the network itself. Network automation plays an essential role in accelerating the deployment process, and simplifying day-to-day operations and maintenance needed for a responsive and resilient network.

The Solution – BlueCat Gateway

BlueCat Gateway allows you to automate and transform mission critical business requirements into DNS, DDI, DHCP and IPAM workflows, plugins, and applications, and enables the rapid development of turn-key integrations with existing technology investments. Using zero-touch automation frees IT teams from time-consuming, error-prone, and repetitive network configuration and provisioning tasks so they can focus on the innovation your business needs. With everyday network tasks and functions automated and repetitive processes controlled and managed automatically, network service availability and application performance improves.



Traditional Network & Service Delivery

Days or Weeks

Ticket submitted to NetOps to request resources, setup and service delivery

Step 1: Create Network

Step 2: Create DDI Infrastructure

Step 4: Validation & Testing
Step 3: Setup and configure

Step 5: Deploy Service

BlueCat Gateway

Minutes

Customer orders new service via self-service web portal

BlueCat Gateway instantiates, configures and optimizes the service

Service is activated in Real-time and available to the customer

Benefits:

- Allows you to rapidly innovate new services
- Accelerates time to revenue
- Enables the rapid change and adoption of new technologies
- Eliminates manual errors and increases business continuity
- Reduces network administration costs by up to 80%
- Cuts implementation times via community-powered GitHub resources

Features

Adaptive Applications & Plugins

BlueCat Gateway leverages a robust library of Adaptive Plugins and Applications that facilitates continuous updates, improves threat detection and policy enforcement, and provides instant access for users and applications. Our Adaptive Plugins and Applications work with any environment and helps to optimize existing IT investments.

Integrations include:

- Networking: Cisco, VMware, Microsoft, Nutanix, OpenStack, ServiceNow, Ansible, and more
- Cloud: AWS, Azure, Google Cloud Platform*
- Security: Palo Alto, Cisco, Splunk, IBM, Archsight, Crowdstrike, and more

Why Adaptive Plugins & Applications

Capabilities	BlueCat Adaptive Plugins	Adaptive Applications
Licensed as subscription		✓
Out-of-the-box configurable		✓
Full roadmap		✓
Tested & Certified	✓	✓
Fully supported	✓	✓
Included with Gateway Support	✓	
Customizable by PS	✓	
Updated as required	✓	

Self-Service

Gateway provides self-service capabilities to end users by automating IT service requests via built-in web forms. So, whether users need device registration and onboarding or configuration and permissions management, BlueCat Gateway empowers IT to instantly meet the broadest range of unique end user requirements.

Workflow Management

BlueCat Gateway allows organizations to build, verify, and validate modules in a test environment and then easily promote them to a production. This modular approach simplifies change and workflow management via an intuitive interface that eliminates the need to train users on complex technical processes while preventing them from making costly mistakes.

Configuration and Provisioning

BlueCat Gateway automates the DNS services necessary to provision and deallocate cloud and on-premise resources, enabling IT to respond faster to user requests. Automated cloud provisioning reduces bottlenecks in delivering cloud services that all too often result in shadow IT, minimizing security risks and excessive costs that IT is unable to manage.

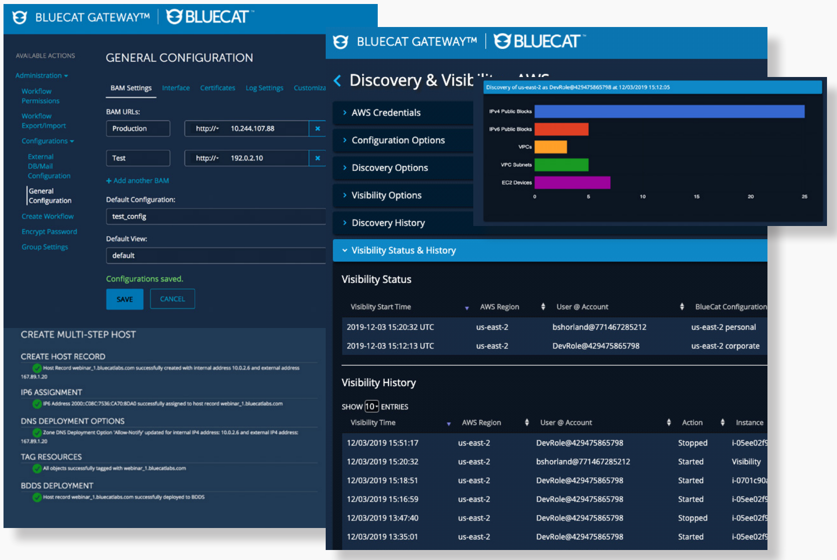
BlueCat Labs Community-Powered Plug-Ins and Workflows

BlueCat Gateway integrates seamlessly with BlueCat Labs, our community-powered GitHub repository. Here you'll find a wide range of tools including production-ready certified workflows, examples, and unique community-contributed solutions to make your network more efficient, eliminate errors and downtime, and integrate DNS into the network management solutions you use every day.

Cloud Discovery and Visibility

BlueCat Gateway helps IT automate the provisioning of diverse cloud and network resources quickly and reliably, providing end-to-end service visibility and discovery to multiple clouds and cloud providers from any location, whenever they need it.

Supported Clouds: AWS



GENERAL CONFIGURATION

BAM URLs:

Production	http:// 10.244.107.88
Test	http:// 192.0.2.10

Default Configuration: test_config

Default View: default

Configurations saved.

CREATE MULTI-STEP HOST

CREATE HOST RECORD

✓ Host Record webinar_1.bluecatlabs.com successfully created with internal address 10.0.2.6 and external address 167.89.1.20

IP6 ASSIGNMENT

✓ IP6 Address 2000::C08C:7536:CA70:8DA0 successfully assigned to host record webinar_1.bluecatlabs.com

DNS DEPLOYMENT OPTIONS

✓ Zone DNS Deployment Option 'Allow-Notify' updated for internal IP4 address: 10.0.2.6 and external IP4 address: 167.89.1.20

TAG RESOURCES

✓ All objects successfully tagged with webinar_1.bluecatlabs.com

BDDS DEPLOYMENT

✓ Host record webinar_1.bluecatlabs.com successfully deployed to BDDS

Discovery & Visib

Discovery of us-east-2 as DevRole@429475865798 at 12/03/2019 15:12:05

Visibility Status

Visiblity Start Time	AWS Region	User @ Account	BlueCat Configuration
2019-12-03 15:20:32 UTC	us-east-2	bshorland@771467285212	us-east-2 personal
2019-12-03 15:12:13 UTC	us-east-2	DevRole@429475865798	us-east-2 corporate

Visibility History

SHOW 10 ENTRIES

Visibility Time	AWS Region	User @ Account	Action	Instance
12/03/2019 15:51:17	us-east-2	DevRole@429475865798	Stopped	i-05ee02f9
12/03/2019 15:20:32	us-east-2	bshorland@771467285212	Started	Visibility
12/03/2019 15:18:51	us-east-2	DevRole@429475865798	Started	i-0701c90
12/03/2019 15:16:59	us-east-2	DevRole@429475865798	Started	i-05ee02f9
12/03/2019 13:47:40	us-east-2	DevRole@429475865798	Stopped	i-05ee02f9
12/03/2019 13:35:01	us-east-2	DevRole@429475865798	Started	i-05ee02f9

* coming 2020

About BlueCat Infrastructure Assurance

BlueCat Infrastructure Assurance is a proactive network monitoring and automation solution. Customers use BlueCat Infrastructure Assurance to gain deep visibility into their DNS, DHCP, and IP address management (together known as DDI) infrastructure. It automates repetitive network tasks such as ongoing maintenance and high availability validation steps. Out of the box, this solution knows how to collect the most relevant data from DDI infrastructure components and analyzes it according to known best practices.

How does BlueCat Infrastructure Assurance work?

BlueCat Infrastructure Assurance uses SSH and SNMP protocols to connect and run collection scripts on BlueCat Address Manager (BAM) and BlueCat DNS/DHCP servers (BDDSes) using CLI commands or SNMP MIB files. These scripts run continually and undergo continuous analysis. BlueCat Infrastructure Assurance notifies users of potential issues before they become bigger problems, along with actionable remediation steps.

Key capabilities

Device health monitoring and detection

BlueCat Infrastructure Assurance continuously analyzes metrics to track device health and posture. It proactively notifies users before problems occur, avoiding outages. Use cases include:

- High availability verifications: Ensure configuration across DNS/DHCP clusters is correct and constistent, and ensure clusters are operational.
- External services: Monitor critical services for dynamic updates.
- Best practices: Get recommendations for vendor-specific best practices and golden configuration conformance to avoid outages.

Management tools to reduce risk

BlueCat Infrastructure Assurance offers a variety of tools for effective operational management that reduces risk. With these tools, users can:

- Visually track critical metrics over time and correlate issues to time of discovery for more effective trouble-shooting.
- Build and schedule custom reports for devices not conforming to best practices or that are non-compliant.
- Utilize role-based access control to restrict access and read-only privileges for certain users.
- Segregate information with granular device permissions, restricting users' views to their respective purviews.

Support informed by user data

BlueCat Infrastructure Assurance's cloud-based analytics service contains production data collected from its users to provide proactive customer support. The data includes issues identified in user environments, scripts executed, and metrics collected.

Integration with APIs and applications

BlueCat Infrasturcture Assurance improves efficiency for IT teams through integration of email, syslog, APIs, and SNMP traps. Furthermore, users can:

- Carry out commands using APIs to retrieve information from or to BlueCat Infrastructure Assurance.
- Centralize authentication with Active Directory via LDAP, RADIUS, or SAML 2.0.
- Integrate with ticketing systems such as ServiceNow.
- Integrate with monitoring solutions such as Solarwinds Network Performance Monitor or BigPanda.
- Integrate with data visualization tools such as Grafana or Tableau.

System requirements

The sizing of BlueCat Infrastructure Assurance is critical to its overall stability and performance. Various sizes are available for different deployment scenarios. The requirements listed below are for up to 1,000 devices and are minimal recommendations. Please reach out to your BlueCat representative with questions.

Device Count	1-30	31-100	101-300	301-1,000
Server	• 8 vCPU Xeon or i7 • 8 GB RAM • 180 GB HD (3000 IOPS)	• 16 vCPU Xeon or i7 • 16 GB RAM • 180 GB HD (3000 IOPS)	• 32 vCPU Xeon or i7 • 64 GB RAM • 400 GB HD (6000 IOPS)	• 64 vCPU Xeon or i7 • 96 GB RAM • 400 GB HD (8000 IOPS)
Browser	• Internet Explorer 11 • Chrome • Edge	• Internet Explorer 11 • Chrome • Edge	• Internet Explorer 11 • Chrome • Edge	• Internet Explorer 11 • Chrome • Edge

Supported devices

BlueCat Address Manager	• BAM 1000/3000/5000/6000/7000 • XMB • Virtual appliance or virtual instance in AWS or Azure • Running 9.4 or later
BlueCat DHCP/DNS Servers	• BDDS 20/25/45/50/60/75/120 • XMB • Virtual appliance or virtual instance in AWS or Azure • Running 9.4 or later

Canada Headquarters

4100 Yonge St. 3rd Floor, Toronto, ON, M2P 2B5
1-416-646-8400 | 1-866-895-6931

US Headquarters

156 W. 56th St. 3rd Floor, New York, NY, 10019
1-866-895-6931

Next steps

Reach out to a BlueCat representative to future-proof your network.

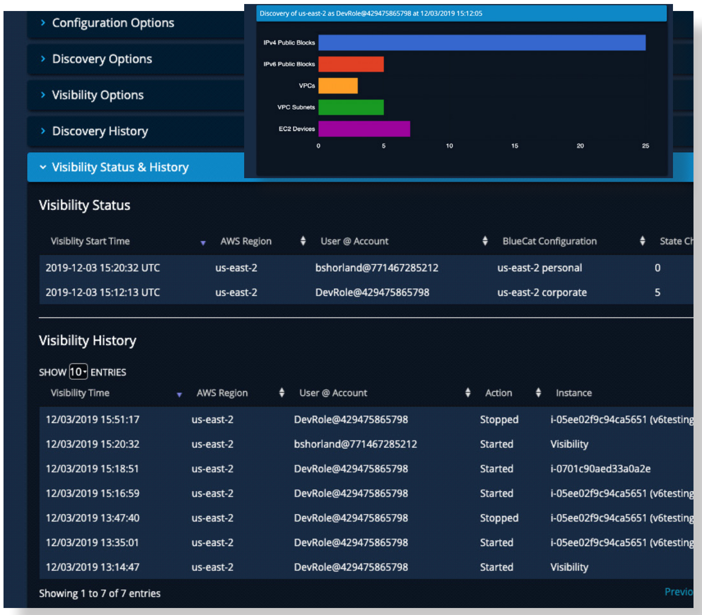
Connect with us

Siloed Environments & Lack of Visibility

Being in the cloud means moving fast. Cloud and DevOps teams are constantly standing up new compute, tearing it down, and moving workloads. To work at the speed of business DevOps teams need multi-cloud environments to deliver what they want, when they want it, and how they need it. When this happens, the complexity of managing essential DDI services and the need for automation can prevent you from realizing the full potential of the cloud. Unfortunately for most businesses, cloud network management has resulted in siloed solutions that fail to interoperate across the on-prem, virtual and multi-cloud environments. To succeed you need a DDI platform that simplifies the management of core networking services, integrates with everything and provides visibility and control for any environment.

The Solution: BlueCat Cloud Discovery & Visibility

Cloud Discovery & Visibility from BlueCat provides exactly that. The solution simplifies the management of core services regardless of the environment. It fuels growth and provides complete visibility and control of cloud assets from a single-pane-of-glass. Manage virtual and cloud workloads or provision and deprovision DNS and IP addresses all in real-time. Eliminate errors, misconfigurations, and delays resulting from old processes and manual effort, while optimizing the performance of your multi-cloud environment with BlueCat Cloud & Discovery.



Visibility Status

Visiblity Start Time	AWS Region	User @ Account	BlueCat Configuration	State Ch
2019-12-03 15:20:32 UTC	us-east-2	bshorland@771467285212	us-east-2 personal	0
2019-12-03 15:12:13 UTC	us-east-2	DevRole@429475865798	us-east-2 corporate	5

Visibility History

Visibility Time	AWS Region	User @ Account	Action	Instance
12/03/2019 15:51:17	us-east-2	DevRole@429475865798	Stopped	i-05ee02f9c94ca5651 (v6testing
12/03/2019 15:20:32	us-east-2	bshorland@771467285212	Started	Visibility
12/03/2019 15:18:51	us-east-2	DevRole@429475865798	Started	i-0701c90aed33a0a2e
12/03/2019 15:16:59	us-east-2	DevRole@429475865798	Started	i-05ee02f9c94ca5651 (v6testing
12/03/2019 13:47:40	us-east-2	DevRole@429475865798	Stopped	i-05ee02f9c94ca5651 (v6testing
12/03/2019 13:35:01	us-east-2	DevRole@429475865798	Started	i-05ee02f9c94ca5651 (v6testing
12/03/2019 13:14:47	us-east-2	DevRole@429475865798	Started	Visibility

Showing 1 to 7 of 7 entries

Benefits

Smart Discovery - Extends visibility from the datacenter to the cloud through automated discovery, inventory, and continuous synchronization of cloud-based IP and DNS configurations.

Rapid Response - Reduces time to remediate problems and shortens investigations by automating the reconciliation of IP addresses and DNS records.

Scalability & Performance - Centralizes DDI management and reduces the problems network and cloud teams encounter when using disparate tools, data sources, and terminology.

Current State

- IP Configuration is not centralized
- DNS records are manually created/modified
- Existing DDI solution has no visibility
- Blind spots exist and cause outages
- Deploying compute requires manual configuration/tracking

Adaptive DNS - Cloud Discovery & Visibility

- IP Configuration centrally managed
- DNS records are automatically updated
- Complete visibility for cloud and on-prem
- Blind spots and IP conflicts are eliminated
- IP assignment and DNS changes are simplified and continuously updated

Features

Environment agnostic

Single-pane of glass command and control for on- prem, virtual, multi-cloud and private cloud environments.

API-first approach

Accelerates application delivery with an easy to use RESTful API to fully automate configuration and deployment for dev, test, and production environments.

DevOps-ready Integrations

Integrates seamlessly with native DNS and IP configuration services offered by cloud providers.

Customizable

Tailor cloud workflows to meet your defined business requirements and share with the broader BlueCat Labs community.

Continuous updates

Automated discovery and real-time synchronization ensures up-to-date visibility and awareness of host and/or record changes, additions, or deletions.

Security

Accelerates incident investigation and remediation by logging and centralizing a single source of truth of all host and record additions, changes, and deletions.

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

bluecatnetworks.com

Next Steps

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

Visit bluecatnetworks.com/contact-us/

Cloud resolution that delivers consistency

As network teams adopt hybrid cloud and private DNS-supported services, they must provide the most optimal resolution path to different zones across virtual networks. Traditionally, admins manually create an avalanche of conditional forwarders to help private endpoints access resources. Unfortunately, without automated zone discovery, admins cannot keep up because manual forwarders can't adapt to the resolution needs of private endpoints. Fortunately, a cloud-native and agnostic solution restores order by simplifying zone discovery and namespace management to tame complexity and improve service delivery.

The Solution - BlueCat Cloud Resolver

BlueCat Cloud Resolver is the first cloud-native DNS resolver that provides immediate resolution to and across any private virtual network. Once placed in a region, it becomes cloud-aware, discovering all DNS zones and creating a single BlueCat Edge namespace for any endpoint in the data center or cloud to resolve queries. The solution is also cloud-agnostic, allowing network teams to embrace any combination of private cloud vendors without getting buried in DNS forwarding rules.

Benefits

Easy Deployment

Rapidly deploy a cloud resolver to any region using popular automation tools like Terraform.

Cloud-Native

Optimized to live in any cloud and scale up or down based on workloads.

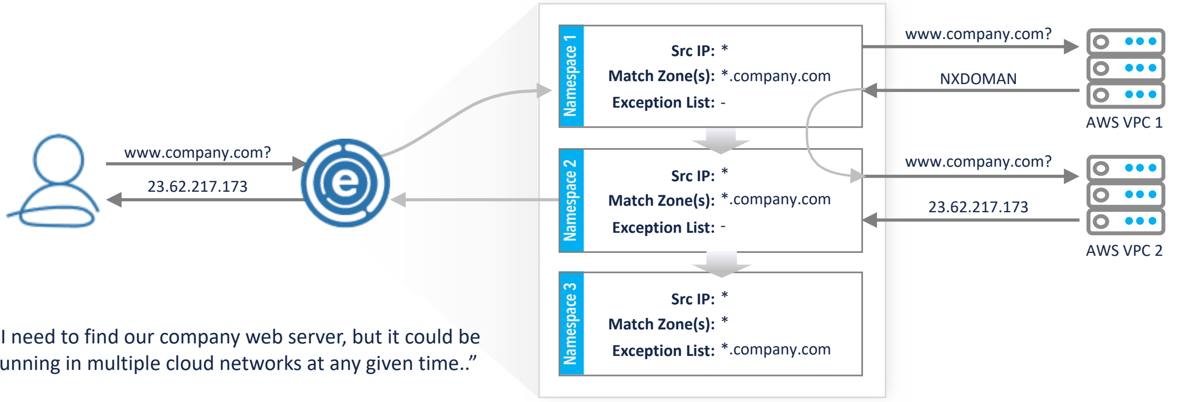
Cloud Aware

Discover all zones instantly with a direct path to resolution, even in any segmented or restricted private virtual network.

Cloud Agnostic

Perfect private endpoint resolution into AWS, Azure, and GCP without juggling multiple interfaces and DNS resolution frameworks.

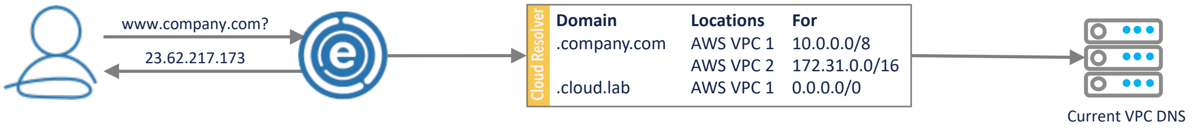
Traditional Namespaces vs. Cloud Resolver for any cloud environment



Namespace	Src IP:	Match Zone(s):	Exception List:
Namespace 1	*	*.company.com	-
Namespace 2	*	*.company.com	-
Namespace 3	*	*	*.company.com

Manual Configuration
No Dynamic Changes
Limited # of Paths
Sequential Querying

"I need to find our company web server, but it could be running in multiple cloud networks at any given time.."



Domain	Locations	For
.company.com	AWS VPC 1	10.0.0.0/8
	AWS VPC 2	172.31.0.0/16
.cloud.lab	AWS VPC 1	0.0.0.0/0

Self-Configuration
Watch & Adapt to Changes
Unlimited Paths
Single Query for Results

Features

DNS resolution

Resolution for all queries made to the cloud namespace for discovered zones using any available connector.

Comprehensive discovery

Continuous role-based discovery of all DNS-related cloud information.

Auto-configuration

based on discovered cloud resources, Cloud Resolver configures Edge namespaces to direct appropriate queries to Cloud Resolver for resolution.

Cloud Native Deployment

Cloud Resolver is easily deployed using automation tools such as Terraform.

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

bluecatnetworks.com

Next Steps

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

Visit bluecatnetworks.com/contact-us/

About BlueCat Edge

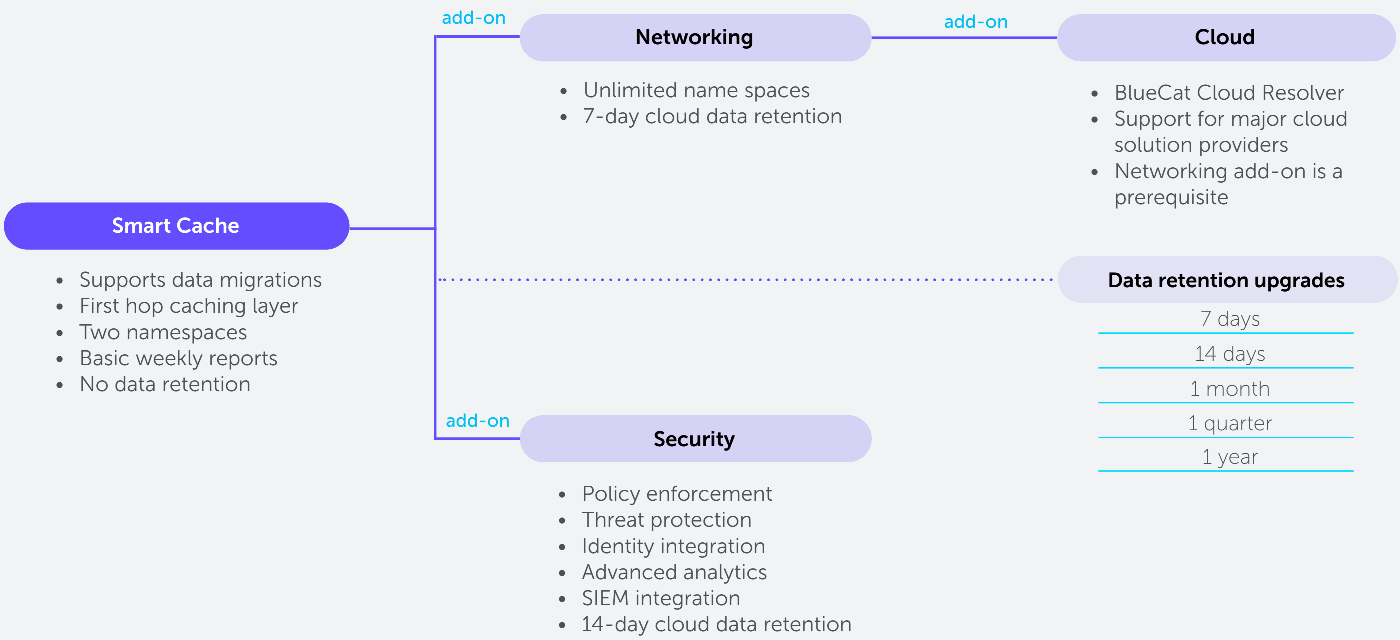
BlueCat Edge is our intelligent DNS resolver and caching layer that provides unprecedented visibility and control over DNS traffic. You can quickly and easily deploy Edge in any hybrid cloud environment. As the first hop of any DNS query, Edge intelligently directs DNS traffic, tames conditional forwarding rules, blocks malicious DNS queries, and helps monitor and collect all DNS query and response data for diagnostics and investigations.

Benefits

- **Networking:** Intelligently optimize DNS to increase resolution performance and reliability, all with complete visibility and control at the first hop of any DNS query.
- **Branch:** Deploy secure, self-reliant, and compliant DNS and DHCP services, as well as cloud IP address management, at multiple brick-and-mortar locations, using existing networking infrastructure.
- **Cloud:** Extend provider-agnostic DNS discovery and resolution for resources across multicloud environments, accelerating the development of critical applications and services.
- **Security:** Provide another layer of intelligence and protection that security teams can use to enhance the overall security stack and protect enterprises from DNS-based attacks.

Standard Edge offering

BlueCat's standard Edge offering starts with a package called Smart Cache, which provides an intelligent caching layer that supports data migrations and includes two namespaces and basic weekly reporting. Unlock advanced capabilities by activating add-ons on top of Smart Cache for security, networking, and cloud. Data retention options of lengths up to one year are also available. Pricing varies based on the number of active IP addresses in use.



Smart Cache

- Supports data migrations
- First hop caching layer
- Two namespaces
- Basic weekly reports
- No data retention

add-on

Networking

- Unlimited name spaces
- 7-day cloud data retention

add-on

Cloud

- BlueCat Cloud Resolver
- Support for major cloud solution providers
- Networking add-on is a prerequisite

Data retention upgrades

7 days

14 days

1 month

1 quarter

1 year

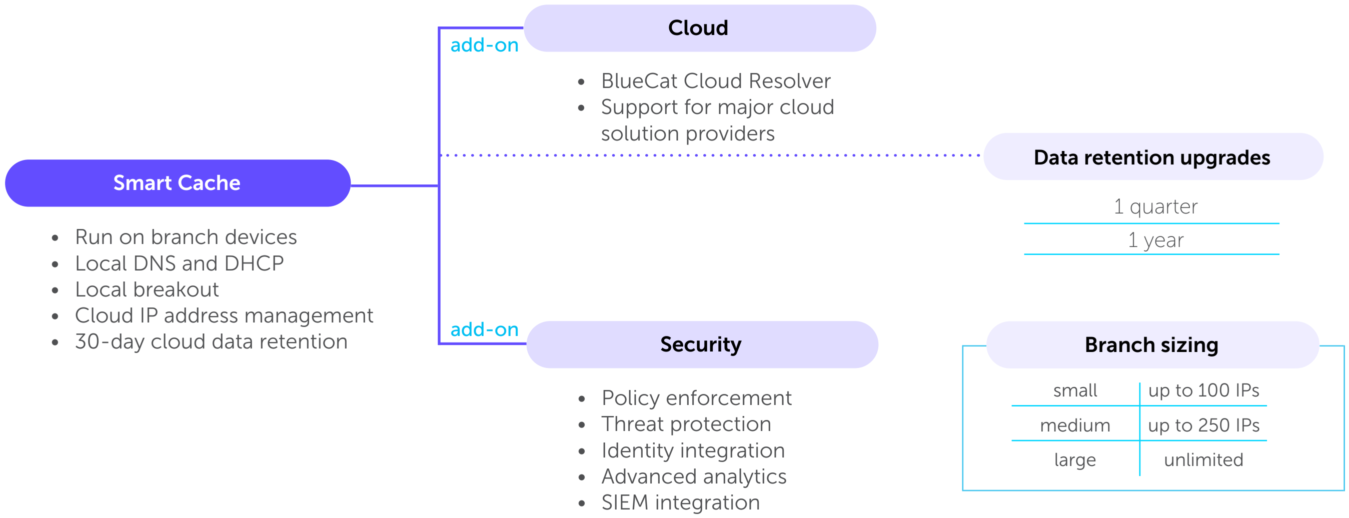
add-on

Security

- Policy enforcement
- Threat protection
- Identity integration
- Advanced analytics
- SIEM integration
- 14-day cloud data retention

Branch DDI

For deployment at multiple branch locations, the Branch DDI (DNS, DHCP, and IP address management) version of BlueCat Edge offers a similar framework, with the starter package, Smart Cache, and add-ons for security and cloud. Branch DDI includes 30-day data retention, with options to extend for one quarter or one year. Pricing varies based on the number of remotely connected IP addresses.



Smart Cache

- Run on branch devices
- Local DNS and DHCP
- Local breakout
- Cloud IP address management
- 30-day cloud data retention

add-on

Cloud

- BlueCat Cloud Resolver
- Support for major cloud solution providers

add-on

Security

- Policy enforcement
- Threat protection
- Identity integration
- Advanced analytics
- SIEM integration

Data retention upgrades

1 quarter

1 year

Branch sizing

small	up to 100 IPs
medium	up to 250 IPs
large	unlimited

Frequently asked questions

What is included in Smart Cache?

Smart Cache includes basic production environments, standard weekly reports, and two namespaces to support most data migrations. One namespace is used for internal queries and the other for external queries, dramatically reducing the amount of recursion and authoritative DNS query activity.

How will my cloud team benefit from Edge?

As cloud networks become more complex—with multiple clouds, regions, and private virtual networks—the compounding effect on manual forwarding rules becomes unmanageable. BlueCat Cloud Resolver, Edge's cloud add-on, tames cloud DNS by simplifying zone discovery and conditional forwarding rule management.

How will my security team benefit from Edge?

DNS query and response data offers a trove of intelligence for security teams, resulting in:

- Improved visibility of devices and traffic;
- Identification of attack sources, their source IPs, and user identities;
- Discovery of unsecured entry points on the network used during an attack; and
- Faster threat hunting during a security incident.

Can I still benefit from Edge even if my organization does not use the cloud?

Most organizations already use a variety of cloud-based applications (e.g., Microsoft 365, Salesforce). Edge conforms to the same security and compliance requirements as these applications. However, for some cases of strict cloud constraints, there are options available for on-premises configurations. Contact your BlueCat sales representative for more information.

Next Steps

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

bluecatnetworks.com/contact-us/

Migrations that meet risk & time criteria

With the demand for more a more resilient and scalable network, networks teams need to migrate to a purpose built DDI platform. Traditionally, migrations are very difficult to plan and execute, often due to constant legacy DNS data changes that get missed and are not reflected in the new system. Without a way to build in redundancy and migrate DNS in real time, IT teams risk major service disruptions due to incomplete or rushed cut-over migrations.

The Solution - Edge Enabled Migrations

BlueCat Edge Enabled Migrations simplifies migration from legacy systems using Edge's intelligent forwarding and Adaptive plugins while mitigating downtime risk. It does this by applying a hierarchy to namespaces, prioritizing the legacy system for DNS resolution, while it automatically captures and adds DNS data to BlueCat Address manager. Once the migration of DHCP data into the BlueCat environment is complete, admins can reverse the namespace hierarchy, making the legacy system a redundant check for any failed query before a final-cutover.

Benefits

Reduce Risk
Use intelligent forwarding with new and legacy systems to ensure every query is answered

Configuration Flexibility
Leverage BlueCat Edge to reorder namespace hierarchy at any migration stage

Real-time Automation
Use BlueCat Edge to capture and store DNS queries to facilitate seamless migrations

Seamless integration
Enhance IT migration strategy with BlueCat's proven methodologies & tools

Features

Namespace Order: Initially order all Sites in BlueCat Edge to forward queries to the legacy DNS system, followed by BlueCat Adaptive DNS.

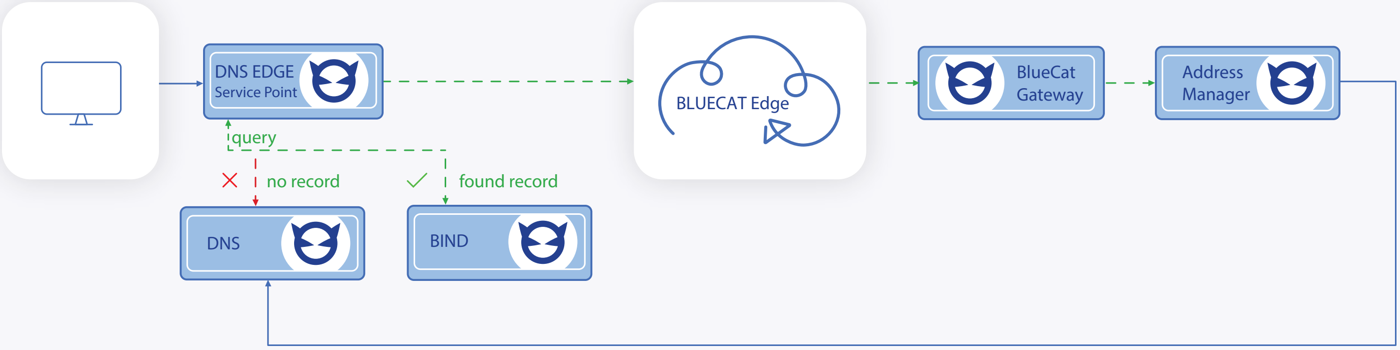
Record migration: add queried records and authoritative responses to Address Manager, as responses are provided by the legacy DNS system.

Reverse Namespace Order: As DHCP Networks are migrated from legacy devices to BlueCat Adaptive DNS, the corresponding Site in BlueCat Edge is modified so that BlueCat is the first Namespace and top priority for DNS response, followed by legacy DNS.

DDNS Updates: ensure that the legacy DHCP server only updates the legacy DNS server, and the BlueCat DHCP server only updates the BlueCat DNS server.

Zone Exclusion and Record Exclusion: Sets of DNS Zones and Records can be excluded from BlueCat Adaptive DNS by manually entering them, or uploading a CSV in the Stealth Migration UI.

IP Exclusion: DNS records associated with certain IP addresses and Ranges can be excluded from being added to BlueCat Address Manager by manually entering the IP addresses, or uploading a CSV in the Stealth Migration UI.



United States Headquarters
1000 Texan Trail, Suite #105, Grapevine, Texas 76051
+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

bluecatnetworks.com

Next Steps

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

Visit bluecatnetworks.com/contact-us/

About BlueCat Infrastructure Assurance

BlueCat Infrastructure Assurance provides network and security automation that offers a deep level of visibility. BlueCat Infrastructure Assurance provides production-ready automation elements, continuously curated from vetted, community-sourced experience, to auto-triage issues in your network and security infrastructure. It automates repetitive tasks such as ongoing maintenance and high availability validation steps. Out of the box, it knows how to collect the most relevant data from your security or network infrastructure components and analyzes it according to known best practices.

How does BlueCat Infrastructure Assurance work?

BlueCat Infrastructure Assurance uses SSH, HTTPS, and SNMP protocols to connect and run collection scripts on network and network security devices using API calls, CLI commands, SNMP MIB, logs, or configuration files. These scripts run continually and undergo continuous analysis. BlueCat Infrastructure Assurance notifies users of potential issues, identifies the potential cause of the problem without human intervention, and provides diagnostic results along with actionable remediation steps.

Key capabilities

Auto-detection

BlueCat Infrastructure Assurance continuously analyzes device metrics to track device health posture, proactively notify users before problems occur (e.g., connection counts approaching the device limit), and avoid outages. Use cases include:

- **High availability verifications:** Ensure consistent configuration across clusters, and that redundant links and paths are both operational and correctly configured.
- **External services:** Monitor critical services for log service, identity awareness, authentication and authorization service, dynamic policies, or dynamic content updates with the latest threat intelligence.
- **Best practices:** Get recommendations for vendor-specific best practices and gold configuration conformance to avoid outages.
- **Security risks:** Enforce compliance with a defined set of internal or external policies and identify device vulnerabilities that matter.

Auto-triage

Upon BlueCat Infrastructure Assurance's detection of an issue, you can autonomously or manually run CLI commands and API queries according to best practices. BlueCat Infrastructure Assurance analyzes data to determine the cause of the problem, without any human intervention. Analysis results are presented visually in workflow diagrams, along with recommended resolution steps.

Automated configuration backup

With BlueCat Infrastructure Assurance, you can schedule daily, weekly, or monthly device backup to prepare for cases of device failure. This capability is supported for selected Check Point, Palo Alto Networks, Juniper Networks, Broadcom Symantec (formerly Blue Coat), F5, and Fortinet firewalls (check with your sales representative for details).

Operations management

BlueCat Infrastructure Assurance offers a variety of tools to accelerate troubleshooting, including:

- Visual tracking of critical metrics over time, allowing for correlating issues and timeframes for effective troubleshooting
- Custom report building and scheduling for devices that are not conforming to best practices, non-compliant, or harbor security risks
- Role-based access control to restrict access and read-only access privileges to certain users
- Granular device permissions to allow segregation of information between users, restricting their view to their respective purview
- Audit log to look back at changes and user activities

Integration

With BlueCat Infrastructure Assurance, you can improve the efficiency of IT teams through integration of email, syslog, APIs, and SNMP traps. Furthermore, users can:

- Carry out commands using APIs to retrieve information from or to post information to BlueCat Infrastructure Assurance
- Centralize authentication with Active Directory via Lightweight Directory Access Protocol (LDAP), RADIUS, or Security Assertion Markup Language (SAML) 2.0
- Integrate with ticketing systems such as ServiceNow
- Integrate with monitoring solutions such as Solarwinds Network Performance Monitor or BigPanda
- Integrate with data visualization tools such as Grafana or Tableau

Benchmark infrastructure

BlueCat Infrastructure Assurance's cloud-based analytics service contains production data collected from its users to provide proactive customer support. The data includes issues identified in user environments, scripts executed, and metrics collected.

System requirements

The sizing of BlueCat Infrastructure Assurance is critical to its overall stability and performance. Various sizes are available for different deployment scenarios. The requirements listed below are for up to 1,000 devices and are minimal recommendations. Please reach out to your BlueCat representative with questions.

Device count	Server	Browser
1-30	▪ 8 vCPU Xeon or i7 ▪ 8 GB RAM ▪ 180 GB HD (3000 IOPS)	▪ Chrome ▪ Edge
31-100	▪ 16 vCPU Xeon or i7 ▪ 16 GB RAM ▪ 180 GB HD (3000 IOPS)	
101-300	▪ 32 vCPU Xeon or i7 ▪ 64 GB RAM ▪ 400 GB HD (6000 IOPS)	

301-1,000	▪ 64 vCPU Xeon or i7 ▪ 96 GB RAM ▪ 400 GB HD (8000 IOPS)	

Supported devices

BlueCat	**BlueCat Address Manager (BAM):** ▪ BAM 1000/3000/5000/6000/7000 ▪ Virtual appliances running VMware Hyper-V or KVM ▪ Virtual cloud instances running in AWS, Azure, or Google Cloud ▪ Running 9.4 or later
	BlueCat DNS/DHCP Server (BDDS): ▪ BDDS 20/25/45/50/60/75/120 ▪ XMB ▪ Virtual appliances running VMware Hyper-V or KVM ▪ Virtual cloud instances running in AWS, Azure, or Google Cloud ▪ Running 9.4 or later
Broadcom Symantec (formerly Blue Coat)	**Hardware: ProxySG** ▪ Physical: SG S200, SG S400, SG S500 (physical ProxySG appliance) ▪ Virtual: SG-VA Alteon VA, Alteon VADC ▪ **Software:** ProxySG SGOS 6.5 and later ▪ **Content Analysis series:** CAS S200-A1, CAS S400-A1, CAS S400-A2, CAS S400-A3, CAS S400-A4, CAS S500-A1 ▪ Running CAS 2.3.5.1
Check Point	**Hardware (support includes open server deployments):** ▪ **Quantum Security Gateway appliances:** 700, 900, 1200R, 1550, 1590, 2200, 3100, 3200, 3600, 4200, 4400, 4600, 4800, 5100, 5200, 5400, 5600, 5800, 5900, 6200, 6500, 6600, 6800, 6900, 12200, 12400, 12600, 13500, 13800, 15400, 15600, 16000, 21400, 21600, 21700, 21800, 23500, 23800, 23900, 26000, 41000, 44000, 61000, 64000 ▪ **Quantum Lightspeed appliances:** QLS250, QLS450, QLS650, QLS800 ▪ **IPSO (Nokia) appliances:** IP150, IP290, IP390, IP560, IP690, IP1280, IP1220, IP2255 ▪ **Quantum Smart-1 security management appliances:** 405, 410, 625, 5050, 5150
	Software: ▪ **Gaia** R80 -> R81.20 ▪ **Scalable Platform:** R76.40SP -> R81.10SP ▪ **IPSO:** R70 and later ▪ **Embedded Gaia:** R75.20 and later ▪ **CloudGuard Network Security:** R80 -> R81.20 ▪ **Maestro** R80.20SP -> R81.10SP ▪ **Multi-Domain Security Management (Provider-1)** R80 -> R81.20
Cisco	▪ **ASA 5500 Series:** 5505, 5510, 5512, 5515, 5520, 5525, 5540, 5545, 5550, 5555 ▪ **ASA 5500-X Series:** 5506-X, 5506W-X, 5506H-X, 5508-X, 5516-X, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X ▪ **ASAv:** Running ASA 9.x

F5	▪ **BIG-IP:** 5200v, 5250v, i5800, 7200v, 7250v/7255v, i7800, 10200v-F/10350v-N/10350v, i10800, i2250v ▪ **VIPRION**: 2200/D114, 2400/F100, 4400/J100, 4480/J102, 4800/S100 ▪ **BIG-IP Virtual Edition (VE):** ▪ Running TMOS 11.6 or later; ▪ Software modules supported: Load Traffic Manager (LTM)
FireEye	▪ **NX series:** NX-VM, NX-900, NX-1400, NX-1500, NX-2400, NX-2500, NX-2550, NX-3500, NX-4420, NX-4500, NX-5500, NX-6500, NX-7400, NX-7420, NX-7550, NX-9450, NX-10450, NX-10000 ▪ Running wMPS 8.2.0
Fortinet	▪ **FortiGate:** 100E, 200E, 300D, 300E, 500D, 500E, 600D, 800D, 1000D, 1200D, 1500D, 2000E, 2500E, 3000D, 3100D, 3200D, 3700D, 3960E, 3980E ▪ **FortiGate-VM and FortiOS** (minimum 4GB RAM) ▪ Running 6.4.x and 7.0.x
Gigamon	▪ **GigaVUE visibility appliances (TA Series and HC series):** GigaVUE-TA10, GigaVUE-TA40, GigaVUE-TA100, GigaVUE-TA200, GigaVUE-HC1, GigaVUE-HC2, GigaVUE-HC3 ▪ Running GigaVUE-OS 4.7.01
Juniper Networks	▪ **SRX Series:** SRX100, SRX110, SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, SRX345, SRX650, SRX1400, SRX1500, SRX3400, SRX3600, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX ▪ **Software:** Junos 12.1X46 and later
Palo Alto Networks	**Hardware (support includes open server deployments):** ▪ **Next-Generation Firewalls:** PA-200, PA-220, PA-500, PA-800, PA-820, PA-2000, PA-3000, PA-3200, PA-4000, PA-5000, PA-5200, PA-7000 ▪ **VM-Series Virtual Next-Generation Firewalls:** VM-50, VM-100, VM-200, VM-300, VM-500, VM-700, VM-1000HV ▪ **Panorama:** M100 and M-500 ▪ **Software:** PAN-OS <= 11.0
Radware	**Hardware: Radware Alteon** ▪ Physical: Alteon 5K, 6K, 8K series (both in Standalone and VX Mode) ▪ Virtual: Alteon VA, Alteon VADC ▪ **Software:** Alteon OS 29.0 and later
Zscaler	**Zscaler App Connector** ▪ Running on RedHat 7.x or 8.x

Corporate Headquarters

4100 Yonge St. 3rd Floor, Toronto, ON, M2P 2B5
1-416-646-8400 | 1-866-895-6931

bluecat.com

Next steps

Reach out to a BlueCat representative to schedule a demo.

Request a live demo

Intuitive and easy orchestration for DDI

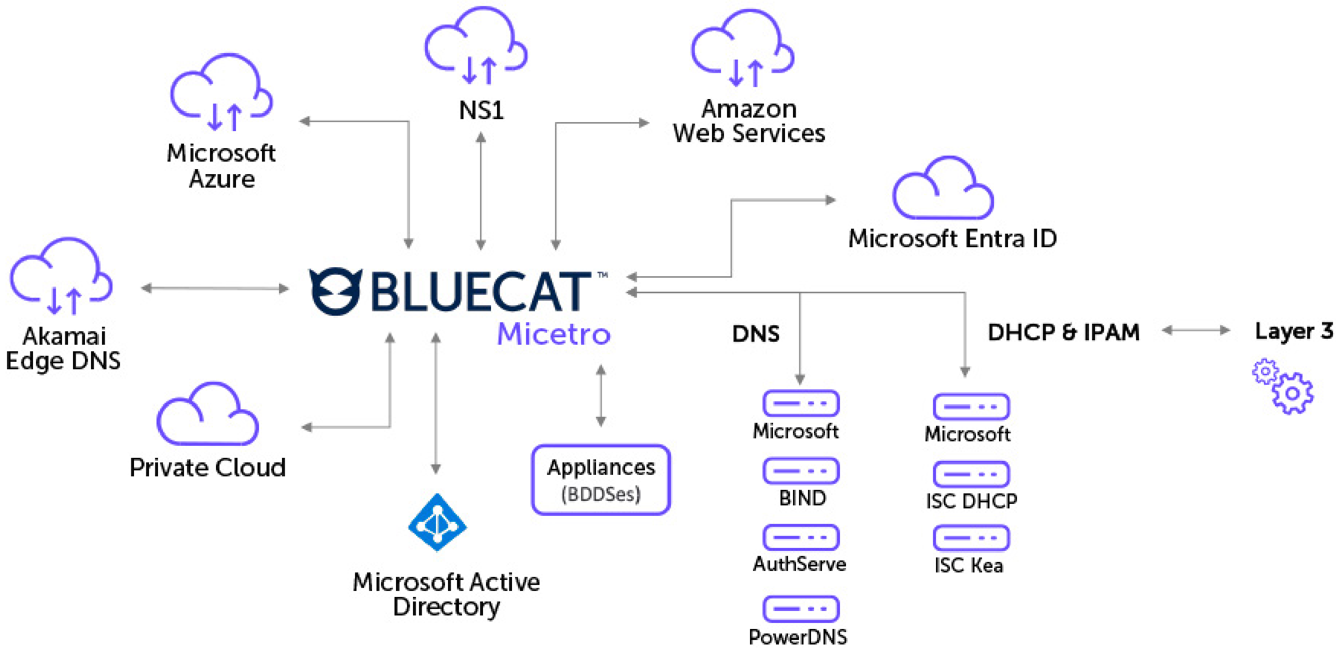
From the access edge to the core and beyond, your users, customers, and agents rely on DNS, DHCP, and IP address management (together known as DDI) solutions to get where they're going on the network. But DDI information viewed in DNS, DHCP, or IP address management (IPAM) silos won't give you the information you need to make informed decisions, validate network status, or create whole-picture audit trails quickly. Your network and systems are not static. They grow and change with your services, users, and applications. A good overlay solution meets you where you are and helps you get where you want to go.

The solution: BlueCat Micetro

Micetro is an easy and intuitive DDI orchestration solution. Like an orchestra maestro, it conducts your existing DNS and DHCP services using an overlay architecture.

You can rapidly embrace enhanced workflows and a range of out-of-the-box integrations without any disruption to existing services or architectures. By preserving institutional knowledge and expertise, Micetro results in a faster time to value compared to other DDI solutions.

Deployed in any on-premises, hybrid, or multicloud network environment, Micetro acts as a non-disruptive overlay that unifies server management under a single graphical user interface and API. By centralizing and contextualizing your DNS, DHCP, and IPAM, you can make decisions based on the big picture that only an overlay DDI solution provides.



Benefits

- **Ease of installation – Forget proof of concepts, which take weeks**
  Install Micetro on a virtual machine on-premises or in the cloud, or on a bare metal server, in less than an hour. Available as a free trial.
- **Ease of migration – Stop forklift upgrades**
  No need to change your existing environment if you're running Microsoft DNS, ISC DHCP, Kea DHCP, AWS Route 53, or Azure DNS.
- **Reduced learning curves – Standardize in a multi-vendor environment**
  Standardize your DDI on premises and in the cloud to reduce the need for acquiring new skill sets to do the same tasks.
- **Effortless management – Tame agent sprawl for DNS and DHCP environments**
  Eliminate the need for multiple agents on Microsoft DNS/DHCP servers with a single proxy agent for your entire environment, simplifying installations and maintenance.
- **Granular access control – Tailored permissions for precise management**
  Assign permissions to specific objects like DHCP scopes and DNS zones, mitigating unnecessary access or changes to Microsoft DNS domain controllers that can affect network uptime.
- **Enhanced insights – Comprehensive integration for data-driven decisions**
  Improve visibility, planning, and management with supported and integrated Active Directory forests and dy namic IPvX allocation methods for Microsoft DNS and Kea DHCP.
- **Secure access – Compliant security across environments**
  Seamlessly use single sign-on (SSO) and multi-factor authentication (MFA) to manage access to integrated hybrid cloud systems and meet internal security requirements.

Features

- **Bring order to your IPAM**
  Gain a complete overview of your network and prevent downtime caused by IP conflicts and misconfiguration with powerful IPAM tools.
- **Improve DNS management**
  DNS is the nerve center of your sophisticated and complex enterprise network, and Micetro helps you run it smoothly with better DNS management.
- **Boost DHCP performance and reliability**
  Facilitate uninterrupted connectivity in any network environment and provide DHCP management for a wide range of servers within a single user interface.
- **Manage DDI across hybrid and multicloud environments**
  Move toward more efficient DDI with consolidated views, secure monitoring of hybrid and multicloud net work services, and integrated management of all network spaces across platforms.
- **Defend against DDoS with xDNS redundancy**
  xDNS redundancy reduces the risk of exposure due to single points of DNS failure, and enhances the successful mitigation of DDoS and other harmful DNS attacks.
- **Work smarter with DNS workflows**
  Gain greater control and transparency over changes within your DNS infrastructure through an efficient queue of requests and approvals for DNS tasks.
- **Make better decisions with data-driven reporting**
  Track available assets, spot trends, discover vulnerabilities, and benefit from collecting and filtering data.
- **Micetro-managed BlueCat appliances**
  Network appliances are a key component in many enterprise networks. Micetro can manage dedicated physical or virtual appliances for BlueCat DNS/DHCP servers (BDDSes).

Next steps

The best way to find out if Micetro is for you is to try it for yourself.

Download free trial

Bridging the Multi-System Divide

With users located worldwide, organizations must provide highly available access to distributed applications and services. Network teams often use complex solutions such as custom integrations, third-party Global Server Load Balancing (GSLB) solutions, or duplicate data to direct users to the nearest accessible server.

Fortunately, there is an integrated solution that allows you to easily configure and update DNS for globally distributed applications without complex, expensive GSLB solutions.

The Solution - BlueCat Global Server Selector

Your DDI investment must be purpose-built to deliver different answers for different networks, based on the health of any application cluster. BlueCat Global Server Selector (GSS) provides easy configuration and automatic updates to DNS for highly available access to distributed applications and services. With an easy to use interface, admins can configure DNS to direct users to the nearest accessible server.

Benefits

Simplified administration

Meet complex problems with simple solutions and eliminate GSLB workarounds.

Improve SLAs

Ensure highly available access for users. DNS is updated to direct users to healthy application servers.

Centralized control

Configuration is built into the core of Adaptive DNS. Easily configure and update conditional DNS responses using a simple UI launched from BlueCat Address Manager.

Seamless integration

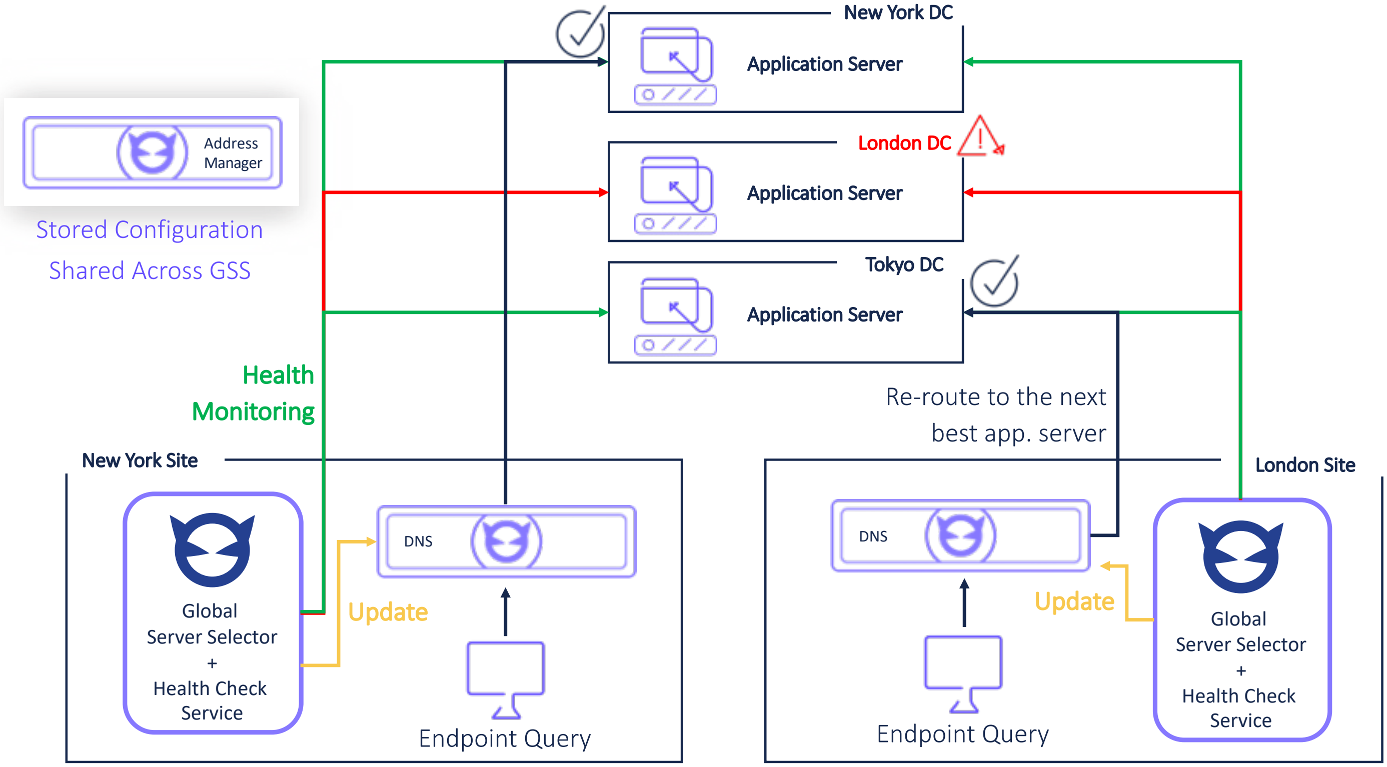
Keep a pulse on server health. Use APIs to update DNS and integrate with existing health monitoring applications.

Features

Multi-answer configuration
Give different DNS responses to clients behind Network Address Translation (NAT).

Health Check Integration
Update DNS in real-time when a server is down, using REST APIs or the built-in health check service.

Search Order
Direct endpoints to the best application servers for their location, based on server availability.



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

bluecatnetworks.com

Next Steps

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

Visit bluecatnetworks.com/contact-us/