White paper

BLUECAT

# Micetro features and capabilities

A comprehensive overview of Micetro's architecture, core modules, and business value

# Table of contents

# Executive summary

## Transforming DDI into an orchestrated, automated service

Today's enterprise networks span data centers, cloud environments, and distributed edge systems. DNS, DHCP, and IP address management (together known as DDI) form the foundation of network connectivity. However, these critical services are often managed in silos, limiting visibility, automation, and governance.

**BlueCat Micetro** is a **vendor-agnostic DDI orchestration platform** that unifies management under a single, API-driven control plane. Acting as a **non-disruptive overlay**, Micetro orchestrates existing Microsoft, BIND, Kea, Cisco Meraki, and cloud-based services without requiring re-architecture or downtime.

Through its modular design, Micetro empowers organizations to:

- Simplify and standardize DDI operations across environments
- Integrate seamlessly with cloud DNS, IP address management (IPAM), and automation frameworks
- Enforce governance through policy-driven workflows and access controls
- Deliver reliable, scalable network services that support digital transformation

This white paper describes all high-level features and capabilities of Micetro 25.2.

# Micetro at-a-glance

| Category | Details |
|---|---|
| **Type** | Modular, software-defined DDI orchestration platform |
| **Deployment** | On-premises, hybrid, and multicloud |
| **Architecture** | API-first, vendor-agnostic overlay |
| **Core functions** | DNS, DHCP, and IPAM |
| **Add-ons** | Workflow, Advanced Reporting, Threat Protection |
| **Cloud integrations** | Included within DNS and IPAM modules |
| **Security** | Role-based access control, on-premises Microsoft Active Directory integration for user and group authentication and authorization, multi-factor authentication (MFA) and single sign-on (Microsoft Entra ID, Okta), full audit logging |
| **Integrations** | Azure, AWS, Akamai, NS1, Cisco, Kea, BIND, Microsoft, PowerDNS, ISC DHCP |
| **Automation APIs** | REST, JSON-RPC, SOAP, event hooks |

# Platform architecture overview

## Unified control across vendors and clouds

### The challenge

Enterprise networks rarely run homogeneous DNS and DHCP. These services may be distributed across Windows Server, BIND, Kea, Cisco Meraki, and multiple cloud providers. Each system has its own management console, API, and data model, making centralized visibility and consistent policy enforcement nearly impossible.

### Micetro's solution

Micetro delivers a unified orchestration layer across all supported DNS, DHCP, and cloud platforms, abstracting vendor-specific differences and providing a single management framework for the entire network. Through Micetro, administrators can view, configure, and synchronize DNS, DHCP, and IPAM data across on-premises and cloud infrastructures in real time.

Micetro communicates directly with DNS and DHCP services through native integrations or lightweight agents. For Microsoft environments, agent-free management uses Windows APIs; Kea and Cisco DHCP are also agent-free, while BIND leverages a dedicated Micetro agent to provide secure command and configuration control. Cloud environments connect via API-level integrations with Azure, AWS, and others.

### The value

- **Single source of truth:** Consolidated DNS and DHCP data across all environments.
- **Operational consistency:** Standardized workflows for multi-vendor systems.
- **Simplified management:** Fewer consoles, fewer tools, less training.
- **Reduced error rates:** Centralized validation and policy enforcement.

Micetro transforms multi-vendor complexity into a single, orchestrated ecosystem—simplifying operations while maintaining native compatibility with all major DNS and DHCP technologies.

## API-first architecture

Micetro is composed of modular components designed for scalability, resilience, and integration.

### Core components

- **Micetro Central:** Orchestration engine for authentication, policy enforcement, and automation.
- **Micetro agents:** Lightweight connectors that securely manage communication with DNS and DHCP services (Microsoft, BIND, Kea, Cisco, etc.).
- **Web application:** Browser-based interface for administration, delegation, and visualization.
- **Data storage:** Embedded SQLite or external SQL (MS SQL, PostgreSQL) for enterprise high-availability deployments.
- **REST API:** Full create, read, update, and delete access to all DDI objects; the foundation of automation and extensibility.
- **Micetro DNS/DHCP Server (MDDS):** BlueCat appliances (physical or virtual) providing DNS and DHCP services.

### Automation and extensibility

Micetro's automation framework is central to its architecture. The REST API, JSON-RPC, and SOAP

endpoints allow complete integration with third-party platforms. Event hooks extend these capabilities by triggering automated actions whenever system changes occur—such as DNS record creation or workflow approval. Administrators can connect these hooks to CI/CD pipelines, IT service management tools, or custom scripts, making Micetro the control layer for network automation.

## Infrastructure-as-code integrations

Micetro integrates with Ansible and Terraform to support infrastructure-as-code workflows. These modules enable automated provisioning and configuration of DNS, DHCP, and IPAM resources within CI/CD pipelines or enterprise orchestration tools. This bridges the gap between traditional network management and modern DevOps practices, ensuring consistency and agility across environments.

## Custom Properties (core platform)

Custom Properties enrich Micetro's DDI data model by adding flexible, user-defined metadata across all object types. Instead of listing every object type, you can focus on their value: They provide business context and actionable insights across DNS, DHCP, and IPAM objects. Administrators can define these fields through the UI or APIs to support dynamic reporting, precise filtering, and automated workflows. This framework turns raw DDI data into meaningful, contextual intelligence that enhances decision-making, operational analytics, and policy enforcement.

## High availability and scalability

- Active or standby clustering for Micetro Central with synchronized databases.
- Stateless web and API services, horizontally scaled behind load balancers.
- Multi-environment support (production, test, delegated) under one deployment.

## Security by design

- Encrypted communications between components.
- Role-based authorization for DNS, DHCP, and IPAM objects.
- MFA and identity federation with Active Directory, Microsoft Entra ID, or Okta.

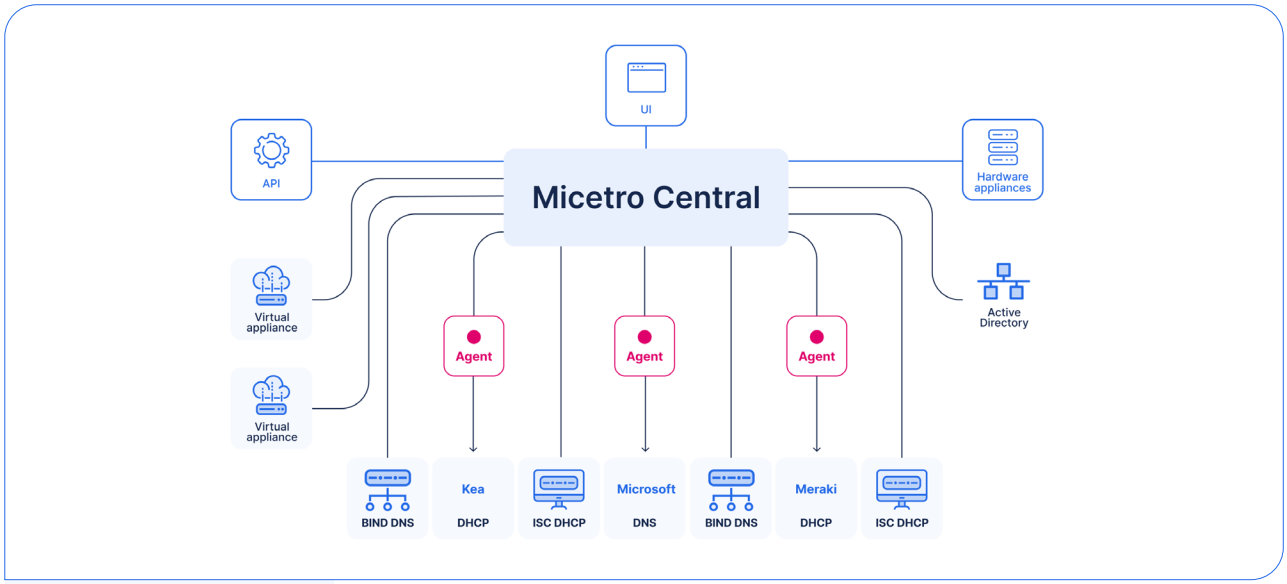


Figure 1. Micetro architecture

# Core functional modules

DNS, DHCP, and IPAM are the foundation of Micetro's core functionality. Together, they deliver unified visibility, control, and automation across the entire DDI ecosystem. This section introduces these tightly integrated components and how they collectively simplify network operations, strengthen governance, and enhance scalability.

## DNS management

### Key capabilities

- Centralized management of DNS zones and records across Microsoft, BIND, Akamai, NS1, AWS, and Azure.
- Support for all zone types, including primary, secondary, stub, forward, and private zones.
- Anycast configuration.
- Cloud-native DNS integrations (AWS Route 53, Azure DNS, NS1, and Akamai Edge DNS).
- DNS cache viewing and management from the web UI.
- Object change history provides a detailed log of all modifications made to any DNS zone or record, including timestamps, user information, actions taken, and user-entered comments.
- xDNS: Micetro's cross-DNS capability groups related zones across multiple platforms into a unified logical service, enabling synchronization and centralized management of DNS architectures spanning multiple environments.
- Custom properties: Extend the power of DNS management with object-level metadata across DNS services, zones, and records. Use custom attributes to tag and search for records based on owner, business unit, or environment.

### Value to customers

- Unified visibility of all DNS records and zones.
- Streamlined cross-platform and cross-cloud zone migration via a zone migration wizard.
- Eliminate configuration drift through synchronized updates.
- Simplified auditing and troubleshooting of DNS changes.
- Consistent configuration management through xDNS and metadata tagging.

## IPAM and DHCP services

### Key capabilities

- Central repository of address spaces—IPv4 and IPv6—with synchronized DNS and DHCP context.
- Manage DHCP services across Microsoft, Kea, ISC, Cisco Meraki, and MDDS servers within IPAM workflows.
- Hierarchical view of networks, subnets, and containers.
- Integration with Active Directory sites and services for mapping and discovery of Active Directory forests, sites, and subnets.
- Automated subnet allocation, merging, and discovery via ICMP or SNMP.
- Object change history provides a detailed log of all modifications to DHCP scopes, networks, and IP addresses, including timestamps, user information, actions taken, and user-entered comments.
- Custom properties: User-defined fields available across all object types, including DHCP services,

networks, IP addresses, devices, interfaces, requests, cloud networks, and cloud account subscriptions.

### Local discovery and SNMP profiles

Micetro enhances visibility with discovery capabilities using SNMP profiles. Administrators can configure SNMP to poll routers and switches, automatically discovering connected subnets, devices, and utilization metrics. This keeps IPAM synchronized with live infrastructure and provides deep insight into device state, interface mapping, and address usage.

### Value to customers

- Unified DDI management with DHCP integrated directly into IPAM workflows.
- Full situational awareness across hybrid environments.
- Intelligent capacity planning and utilization tracking.
- Context-rich visibility through metadata and SNMP-driven discovery.

## Active Directory integration

Micetro natively integrates with Active Directory for both authentication and infrastructure mapping, providing a seamless link between network identity and infrastructure data. This integration allows administrators to manage user access and directory structures directly within Micetro, while automatically aligning DNS, DHCP, and IP address data with Active Directory sites and organizational units—creating a unified, policy-driven view of enterprise networks that enhances security, accuracy, and operational efficiency.

### Authentication integration

- Supports single sign-on (SSO) via Microsoft Entra ID.
- Allows domain-based user and group management.
- Maps Active Directory roles and permissions directly to Micetro roles.
- Optionally integrates with LDAP and RADIUS for hybrid environments.

### Active Directory sites and subnets

Micetro synchronizes subnets and forests directly from Active Directory, automatically correlating IP ranges with corresponding sites. Administrators can view, manage, and modify subnet associations within Micetro's IPAM interface. Changes propagate bi-directionally to maintain parity with Active Directory.

### Value to customers

- Streamlined authentication and role management.
- Centralized control of DNS and DHCP in Microsoft environments.
- Automated subnet and site correlation for hybrid Active Directory deployments.

## MDDS appliances

Micetro seamlessly manages MDDS appliances, extending DDI orchestration into purpose-built, high-performance service nodes. MDDS appliances tightly integrate with Micetro Central to provide consistent, scalable DNS and DHCP services across distributed environments.

### Key capabilities

- Unified management and monitoring from the Micetro web application.
- Supports authoritative and caching DNS and DHCP services.
- Configuration and updates are managed directly from Micetro Central.
- Anycast support with Border Gateway Protocol and Open Shortest Path First routing for highly available DNS.
- Dedicated management interfaces to separate control and data planes.
- Appliance-level logging, monitoring, and lifecycle operations from a central console.
- Appliances are available in a variety of physical configurations or as virtual appliances.

### Value to customers

- Simplifies DDI infrastructure deployment with pre-configured, hardened service nodes.
- Ensures consistent DNS and DHCP performance across on-premises and edge locations.
- Reduces administrative overhead by centralizing updates and improving visibility.
- Improves resilience and scalability with integrated Anycast and high availability options.

## Cloud and hybrid integration

Micetro provides unified management for on-premises and cloud DDI resources through direct API integration with major cloud platforms. Enterprises can manage Azure, AWS, Akamai, NS1, and Cisco Meraki services from a single interface without duplicating data.

### Supported integrations

- **Azure DNS and IPAM:** Manage private or public DNS zones, synchronize virtual networks, and monitor IP utilization across subscriptions.
- **AWS Route 53:** Full management of virtual private clouds, subnets, hosted zones, and DNS records across multiple accounts.
- **Cisco Meraki:** Synchronize subnets and IP relays for visibility and orchestrate DHCP changes.
- **Akamai Edge DNS and NS1:** Integrate external DNS providers for global zone management.

### Use cases

- Migrate DNS zones to the cloud while maintaining central control.
- Centrally manage IP space across hybrid environments.
- Track IP usage and DNS configurations in real time.
- Simplify governance with a unified management framework.

### Value to customers

Micetro bridges operational gaps between data centers and modern cloud networks. By synchronizing DNS and IPAM data, organizations achieve hybrid visibility, consistent policies, and centralized control of DNS, DHCP, and IPAM across providers.

## Security and access control

Micetro is built with enterprise-grade security and compliance at its core. Every transaction and configuration change is authenticated, logged, and auditable, with Micetro acting as the single point of

control and security for all orchestrated systems. By centrally enforcing policies, authentication, and access across integrated DNS, DHCP, and IPAM platforms, Micetro ensures consistent governance, minimizes risk, and provides complete visibility into every administrative action across the network.

### Key security features

- Role-based access control (RBAC) for granular delegation.
- Multi-factor authentication and SSO (Microsoft Entra ID and Okta) via Active Directory.
- LDAP and RADIUS authentication for directory integration.
- Full audit history with immutable logs.
- Encrypted communication between all Micetro components.

### Enhanced RBAC

Micetro's RBAC model provides fine-grained, hierarchical control over who can view, modify, or administer DNS, DHCP, and IPAM objects within Micetro itself. All access decisions are enforced centrally in Micetro, ensuring that users can only perform authorized actions through the Micetro UI and APIs.

Rather than modifying native permissions on managed platforms such as Windows DNS, Windows DHCP, BIND, or Kea, Micetro acts as a unified access governance layer across these disparate systems. This allows organizations to define and maintain consistent access policies in one place, without the complexity of configuring and maintaining permissions independently for each underlying service.

Prior to Micetro, enforcing consistent access controls across multiple DNS and DHCP platforms was time-consuming and difficult to sustain at scale. With Micetro, administrators gain a centralized, secure, and scalable control plane for DDI access—simplifying delegation, improving auditability, and reducing the risk of unauthorized changes.

### Value to customers

These enhanced RBAC features ensure compliance with internal and external security frameworks, reduce operational complexity, and enable secure delegation of responsibilities. Micetro simplifies enterprise-grade access control while ensuring full accountability for every action taken on managed systems.

## Availability and disaster recovery

Building on Micetro's automation and orchestration foundation, its availability and disaster recovery capabilities ensure that these automated network operations remain resilient and uninterrupted.

Micetro is built for continuous service delivery and resilience. It incorporates multiple features and tools to ensure data integrity, uptime, and operational continuity across all DDI services.

### Micetro high availability

Micetro Central supports active-standby clustering with synchronized databases, enabling failover without disruption. The web application and API layers are stateless, allowing load-balanced, horizontally scaled deployment for regional redundancy.

### xDNS for service resilience

Micetro's xDNS capability not only unifies management across DNS platforms but also enhances availability through distributed zone synchronization. Administrators can maintain live, consistent copies of zones across multiple providers and environments, minimizing single points of failure.

### Backup and restore

Micetro includes built-in backup and restore capabilities for all configurations and data stores. Database backups can be automated and scheduled, ensuring rapid recovery from data loss, corruption, or disaster events.

### DNS zone migration wizard

The zone migration wizard simplifies transferring DNS zones between servers or providers—whether for load balancing, platform replacement, or recovery purposes. It ensures consistency and minimal downtime during zone migration operations.

### DHCP scope migration and recovery

Micetro provides a robust DHCP scope migration tool that supports seamless migration between servers and platforms. This includes the ability to migrate scopes from offline or unreachable servers, preserving configurations and lease history to restore service rapidly after hardware or network failures.

### Value to customers

- Ensures high availability and fast recovery for all DDI services.
- Reduces downtime through built-in clustering and synchronization.
- Simplifies disaster recovery with automated backup and restore.
- Streamlines migration workflows for DNS and DHCP services.
- Provides a single control plane for resilient, distributed DDI environments.

# Advanced modules (licensed add-ons)

Beyond the core DDI modules, Micetro offers several advanced modules that enhance the platform's capabilities. These modules include Workflow, Advanced Reporting, and Threat Protection.

## Workflow module: Governed change control

Micetro's Workflow module introduces governance to DNS operations by providing a structured approval system for record changes. Users submit DNS change requests, which are automatically routed for review and approval. This enforces policy and maintains accountability in distributed teams.

### Highlights

- Configurable multi-step approval chains.
- Integration with tagging and automation scripts.
- Full audit log of requested, approved, and rejected changes.
- Integration with IT service management tools (e.g., ServiceNow, Jira).

### Value to customers

- Reduces misconfiguration risk and downtime.
- Enforces compliance and operational accountability.
- Enables safe delegation without losing centralized control.

## Advanced Reporting module: Operational insight and auditing

The Advanced Reporting module transforms raw DDI data into meaningful analytics. Administrators can design, schedule, and export reports covering DNS records, DHCP leases, IP usage, and historical changes.

### Highlights

- Customizable report definitions and filters.
- Scheduled delivery in CSV, TSV, or Excel.
- Historical and trend-based utilization analysis.
- Role-based access to reporting data.

### Value to customers

- Unified visibility across hybrid DDI infrastructure.
- Simplified compliance and audit readiness.
- Faster troubleshooting and data-driven capacity planning.

## Threat Protection module: Real-time threat intelligence

The Threat Protection add-on provides malicious DNS activity detection, integrated with MDDS. Threat Protection surfaces risky queries or behaviors on managed resolvers to block or alert, aiding incident response for customers seeking DNS-based threat protection.

### Highlights

- Advanced, real-time threat intelligence
- Automatic protection against malicious domains
- Exclusively integrated with MDDS

### Value to customers

- Strengthen DNS security posture.
- No complex setup or external integrations.
- Protect everything connected to your network from resolving to known threat domains.

# Implementation

BlueCat Micetro unifies DNS, DHCP, and IPAM into an orchestrated, policy-driven service that simplifies complex hybrid networks. Its modular, API-first architecture enables full automation, governance, and scalability—empowering IT teams to operate with agility, precision, and confidence.

Micetro's overlay model allows enterprises to modernize their DDI environment without downtime. Existing DNS and DHCP servers remain in place and are managed directly through Micetro's orchestration layer.

This approach provides a seamless bridge between current operations and future modernization and is easily implemented with no disruption to existing systems.

## Implementation approach

1. Integrate existing infrastructure under a unified management plane.
2. Automate routine DNS and DHCP operations with workflows and APIs.
3. Introduce policy-driven governance and reporting.
4. Optionally migrate services to modern platforms or BlueCat appliances at your own pace.

## Strategic outcomes

- Accelerated network automation via REST, Ansible, and Terraform integrations.
- Improved service reliability through centralized policy and workflow controls.
- Enhanced governance with role-based permissions and approval-based changes.
- Reduced operational costs by automating repetitive DDI tasks.
- Simplified hybrid cloud management with unified visibility and control.

BlueCat's Intelligent Network Operations (NetOps) solutions provide the analytics and intelligence needed to enable, optimize, and secure the network to achieve business goals. With an Intelligent NetOps suite, organizations can more easily change and modernize the network as business requirements demand.

**Headquarters**
4100 Yonge St. 3rd Floor, Toronto, ON, M2P 2B5
Phone: 1-416-646-8400 I 1-866-895-6931

bluecat.com

### Next steps

See Micetro for yourself and learn how you can get centralized visibility and control across your network in just minutes.

Get a free demo



WP-Micetro-03-17-2026