White paper

BLUECAT

Nine reasons to unify your DDI

Strategic advantages for modernizing your DNS, DHCP, and IP address management

Table of contents

Executive summary

Managing DNS, DHCP, and IP address management (together known as DDI) has become increasingly complex and critical in today's enterprise environments. Legacy DDI approaches can introduce numerous challenges, including system fragmentation, security gaps, and error-prone and time-consuming manual processes that result in network outages.

Unified DDI addresses these challenges by offering centralized management, automation, and enhanced visibility, security, and resiliency of your core network services. Adopting a Unified DDI solution helps enterprises embrace cloud adoption and modernize and secure their network infrastructure.

This paper explores nine reasons to consider adopting a Unified DDI solution. They include:

1. **Cost optimization:** Reduce engineering costs, optimize infrastructure, and eliminate DNS-related outages to achieve a rapid return on investment.
2. **Risk reduction**: Protect critical infrastructure with automation, standardized workflows, and centralized security policies.
3. **Digital transformation enablement:** Accelerate innovation with DevOps integration, automated workflows, and infrastructure agility.
4. **Complete visibility and control:** Get real-time insights into DDI usage through a single source of truth.
5. **Process automation**: Simplify operations by automating routine tasks and enabling self-service capabilities.
6. **Infrastructure reliability:** Ensure continuous operations with high availability and flexible architectures.
7. **Security by design:** Enhance protection with policy-driven access controls, audit trails, and reduced attack surfaces.
8. **Cloud integration:** Manage hybrid and multicloud environments efficiently with real-time visibility and intelligent DNS routing.
9. **Scalability and agility:** Seamlessly expand and adapt DDI services to meet evolving business needs.

Unified DDI is foundational for organizations seeking to enhance operational efficiency, improve security, and embrace modern IT initiatives like cloud adoption and DevOps. BlueCat offers two distinct approaches to Unified DDI, whether you want to overlay management capabilities onto existing infrastructure or implement a complete DDI platform. With BlueCat's DDI solutions, you can transform your core network operations and unlock new opportunities for growth.

The challenges and costs of legacy DDI

Legacy approaches to managing DDI are characterized by fragmented systems that often evolved organically. The result is a hodgepodge of manual processes that create significant operational challenges and leave DDI susceptible to security gaps. Without a modern approach to DDI, the complexity of core network services will continue to increase as networks grow, expand across clouds, and are adapted to meet new security challenges.

Challenges of a legacy approach to DDI

Fragmented systems

The fragmented nature of legacy DDI environments prevents IT administrators from having a single source of truth for their namespaces and IP address ranges. In a recent Enterprise Management Associates (EMA) survey, more than a quarter of respondents identified having too many management tools and fragmentation as their biggest challenge to network operations success.[1]

The fragments of legacy DDI are often characterized by:

Distributed management

- Multiple DNS and DHCP servers managed independently across locations
- Siloed IP address tracking spreadsheets
- Separate tools, technologies, and vendors for different environments
- Manual cross-reference requirements before making any changes

Technical debt

- Legacy systems with limited capabilities
- Inconsistent configurations across services
- Undocumented dependencies
- Growing maintenance overhead

Operational inefficiencies

- Duplicate data entry requirements
- Manual validation processes
- Limited automation capabilities
- A high risk of human error

Manual processes

Manual processes introduce risk, both to IT and the organization. These risks include time-intensive operations, resource drains that take skilled network admins away from new projects, and the prevalence of errors attributed to one-off updates across a fragmented infrastructure.

Time-intensive operations

- Average time for DNS changes: one to two days[2]
- Average time for DHCP scope configuration: four to eight hours[2]
- IP address allocation may take hours per request due to spreadsheet-based tracking
- Manual scripting and configuration updates can take days to weeks

Resource drain

- Full-time staff dedicated to routine tasks, reducing focus on innovation
- Extended maintenance windows
- Delayed project implementation
- Troubleshooting challenges: 39% of time spent troubleshooting the network[1]

Error prevalence

- 60% of network outages are caused by human error[2]
- Average time to detect configuration mistakes: four hours[2]
- Resolution time for DNS conflicts is extensive in multicloud environments
- IP address conflicts occurring weekly

Security gaps

Legacy environments beholden to the fragmented systems and manual processes described above are rife with security gaps. These include:

Reactive posture

- DNS or DHCP systems are attractive attack vectors with a large surface area
- DNS data used for data exfiltration
- Reactive patch management
- Scattered log collection

Visibility challenges

- Unmanaged active DNS zones
- Untracked IP address usage
- Shadow IT DNS services
- Rogue DHCP servers

Control limitations

- Inconsistent access controls
- Limited audit capabilities
- Weak change management
- Poor policy enforcement

The cost of legacy approaches to DDI

Considering the challenges introduced by legacy DDI, it's no surprise that many network teams haven't been able to modernize and unify their DDI infrastructure. But both the direct and indirect costs of maintaining your DDI status quo are steep.

Resource inefficiency

With fragmentation and manual processes, routine DDI tasks require duplicate efforts, manual cross-checking, extra approval layers, and inefficient troubleshooting. And that's just to make simple additions, changes, and deletions across DNS and IP address records.

Direct costs and business impact

Legacy DDI systems can frequently cause downtime. According to EMA research, the average enterprise loses $12,900 per minute from IT outages,[3] with lost revenue and productivity behind these costs. And it's not just outages driving costs—emergency change implementations, common in a

fractured and manual environment, add to costs and complexity and can cause further downtime.

While the bottom line is critical, issues with legacy DDI can also damage brand reputation, decrease customer satisfaction, and violate service-level agreements with partners.

Compliance issues

With all its challenges, legacy DDI approaches can also lead to compliance issues, whether from audit failure, documentation gaps, violations of regulatory requirements, or failure to enforce policy. Non-compliance further damages reputation, leading to fines and penalties, and requires significant effort to remediate.

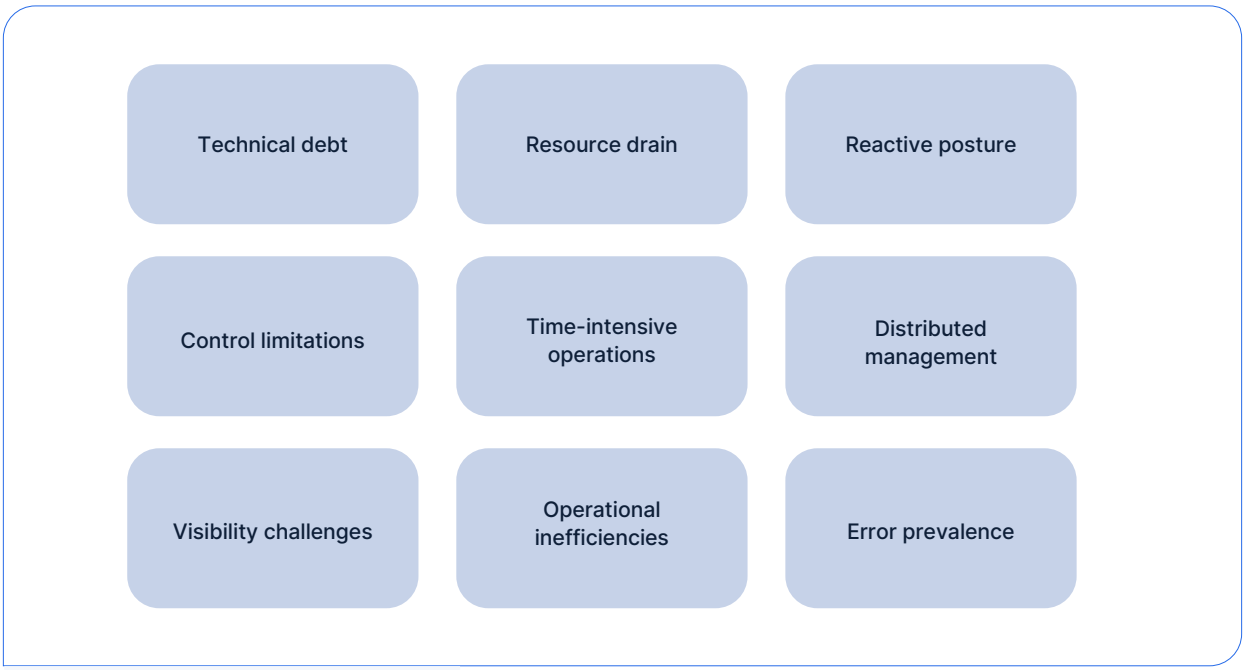

Figure 1. The challenges of legacy DDI

What is Unified DDI?

Unified DDI consolidates, automates, and streamlines the core services that connect devices, applications, and people around your network—on-premises and across any cloud. But Unified DDI provides more than just the foundational building blocks and core services for digital infrastructure and applications. It also facilitates accurate and authoritative capacity planning, policy enforcement with deterministic boundaries, and risk reduction by creating an umbrella of operational rigor and seamless security.

Core capabilities of a Unified DDI platform

A Unified DDI platform is characterized by several intrinsic capabilities, including centralized control, intelligent automation, security by design, and cloud-ready architecture. Organizations that adopt Unified DDI see numerous benefits, including:

Centralized control

- A single management interface for all DDI services
- Automated synchronization across environments
- Real-time visibility into all network resources

- Comprehensive audit and compliance tracking

Intelligent automation

- Self-service resource provisioning
- Policy-driven workflows
- Open API architecture
- Integration with existing tools and platforms

Security by design

- Centralized policy enforcement
- Threat detection and prevention
- DNS security monitoring
- Role-based access controls

Cloud-ready architecture

- Native multicloud integration
- Hybrid environment support
- Automated cloud resource discovery
- Intelligent DNS resolution

Benefits to your business

The resulting business impact of adopting a Unified DDI platform is well-documented. Organizations that transform their legacy DDI footprint to a Unified DDI platform typically experience improvements in operational excellence, enhanced security, accelerated cloud adoption, and financial benefits that boost the bottom line.

Operational excellence

- Reduction in manual tasks
- Faster service delivery
- Zero IP conflicts
- Complete resource visibility

Enhanced security

- Faster threat detection
- Automated policy enforcement
- Real-time security monitoring
- Simplified compliance

Cloud acceleration

- Seamless cloud adoption
- Optimized application performance
- Reduced cloud complexity
- Future-ready infrastructure

Financial returns

- Rapid return on investment
- Reduction in engineering time
- Smaller infrastructure footprint
- Accelerated business processes

The integrated approach offered by Unified DDI ensures organizations can adapt to changing business requirements while maintaining control, security, and reliability across their entire network infrastructure. Now that we understand Unified DDI, we'll explore nine key reasons why progressive IT organizations should adopt it.

Transformation in action

Before Unified DDI	After Unified DDI
Manual DNS changes: 48 hours	Automated DNS changes: 15 minutes
Weekly IP conflicts	Zero IP conflicts
Limited cloud visibility	Complete cloud visibility
Fragmented security	Integrated security

Nine reasons to adopt Unified DDI

In the previous section, we explored some of the key capabilities of a Unified DDI platform and the benefits and business impacts associated with adopting it. Now, let's consider some of the expected outcomes when implementing Unified DDI from business, operational, and technical viewpoints.

Business-focused reasons

1. Cost optimization: Rapid returns on DDI investment

Organizations often hesitate to invest in Unified DDI, viewing their existing do-it-yourself (DIY) approach as "free." However, EMA research reveals that the actual cost of legacy DIY approaches to DDI is substantial and often hidden. A fragmented DIY approach consumes valuable engineering time, requires excessive infrastructure, and leads to costly outages.

Unified DDI delivers rapid and substantial financial returns. EMA's analysis of large enterprises shows an average return of $1.5 million in additional economic benefits within the first year.[4] This comes through multiple vectors: reduced engineering costs, infrastructure optimization (one customer reduced their server count from 150 to 30, saving $840,000 annually[4]), and elimination of DNS-related outages. The investment typically pays for itself within three months, with customers reporting a return on investment in their annual subscription within 2.25 months.[4]

Beyond direct cost savings, Unified DDI enables better resource utilization. Engineers freed from routine DDI tasks can focus on strategic initiatives like cloud transformation, security enhancement, and automation projects. Infrastructure consolidation reduces hardware costs and power, cooling, and maintenance expenses. Finally, automating routine tasks through self-service portals and workflow automation reduces operational overhead while improving service delivery speed.

2. Risk reduction: Protecting critical infrastructure

DDI infrastructure has become an attractive target for malicious actors while growing more complex to secure and maintain. Legacy approaches create significant risk through fragmented security controls, limited visibility, and manual processes prone to error. According to industry research, only 31% of DDI managers report complete confidence in their DNS security.[1] The stakes are high: The average cost of a single data breach has reached $4.88 million,[5] making risk reduction a critical business imperative.

Unified DDI substantially reduces risk across multiple dimensions. At the operational level, automation and standardized workflows eliminate the human errors that cause most outages. Centralized policy

enforcement and role-based access controls ensure consistent security practices, while comprehensive audit trails enable rapid incident response. Through automated validation and change management, organizations report a 75% reduction in configuration errors and a 90% improvement in compliance reporting efficiency.[4] Real-time threat detection and automated response capabilities enable organizations to identify and block threats 80% faster than traditional approaches.[1]

Beyond security improvements, Unified DDI reduces business risk through enhanced reliability and compliance capabilities. Automated failover prevents service outages, while multi-primary DNS ensures business continuity even during network disruptions. Built-in compliance controls and reporting streamline audit processes, reducing the risk of regulatory violations. Organizations using Unified DDI report complete elimination of DNS-related outages and significant improvements in their security posture.

3. Digital transformation enablement: Accelerating innovation

Legacy DDI infrastructure often becomes a bottleneck for digital transformation initiatives. As organizations adopt cloud services, modernize applications, and embrace DevOps practices, their legacy DDI systems can't keep pace. Manual processes that take hours to complete block critical business initiatives, while fragmented systems create barriers to automation and cloud adoption. EMA research shows that organizations spend over a third of their time troubleshooting network issues rather than driving innovation.[4] At the same time, cloud teams need help managing hundreds or thousands of daily DNS changes in dynamic environments.

Unified DDI accelerates digital transformation by providing the foundation for modern IT initiatives. Organizations can integrate DDI into their DevOps pipelines through open API architecture and automated workflows, enabling rapid service delivery and continuous deployment. Cloud teams gain real-time visibility and control across hybrid environments with automated discovery and synchronization of cloud resources. The impact is substantial: Organizations report a nearly 93% reduction in cloud DNS management time, 90% faster service delivery, and elimination of manual cloud resource tracking.[4]

Most importantly, Unified DDI enables innovation by freeing teams from routine tasks and providing the infrastructure agility needed for rapid experimentation. Teams can provision resources in minutes rather than days, test new services without risk of DNS conflicts, and scale operations seamlessly across clouds. Complete automation of cloud resource management frees organizations to focus on strategic initiatives rather than infrastructure management.

Operational reasons

4. Complete visibility and control: Establishing a single source of truth

Many organizations lack holistic visibility of their managed footprint, especially as networks expand across data centers, remote sites, and multiple clouds. This limited visibility leads to IP conflicts, shadow IT DNS services, and untracked cloud resources—creating significant operational and security risks. Legacy approaches using spreadsheets and fragmented tools leave teams blind to substantial portions of their infrastructure, with some organizations managing over 100,000 IP addresses through manual tracking.[5]

Unified DDI transforms visibility challenges through comprehensive resource tracking and centralized management. Organizations gain real-time insight into all DNS zones, DHCP scopes, and IP space usage across their entire infrastructure. The impact is significant: Organizations report 100% visibility into cloud resources, complete elimination of IP conflicts, and 75% faster problem resolution.[4] One health care technology company automated the discovery and tracking of over 1,500 daily cloud DNS changes, achieving complete visibility across their hybrid environment and radically reducing engineering time spent on cloud DNS management.[4]

Beyond basic tracking, Unified DDI provides actionable intelligence for capacity planning, security monitoring, and resource optimization. Teams can proactively identify potential issues, optimize resource utilization, and maintain compliance through comprehensive audit trails. This enhanced visibility allows organizations to reduce mean time to resolution of IT problems while improving capacity planning and management across their entire network footprint.

5. Process automation: Transforming service delivery

The time demands of manual DDI processes create significant operational bottlenecks. Network teams spend an average of 30% of their time on routine DDI tasks,[1] with basic DNS changes taking 24 to 48 hours to implement.[6] Manual validation, multiple approval layers, and cross-checking requirements further slow operations—a single DNS record change can consume two hours of engineering time gathering data and updating servers.[4] This heavy reliance on manual processes delays service delivery and increases risk, with nearly two-thirds of network outages attributed to human error.[2]

Unified DDI revolutionizes service delivery through comprehensive process automation. Organizations dramatically reduce operational overhead by implementing automated workflows and self-service capabilities while improving accuracy. The impact is substantial: Organizations report reducing DNS change implementation time from hours to minutes, with an 86.8% reduction in engineering time spent on DDI operations.[4] One health care technology company managing 300 to 400 weekly DNS changes reduced their implementation time from two hours to 10 minutes while eliminating manual validation steps.[4]

The benefits of automation extend beyond time savings. Standardized workflows enable consistent policy enforcement, reduce errors, and free skilled engineers for strategic initiatives. Integration capabilities allow DDI automation to connect with existing tools and platforms, enabling end-to-end service delivery automation. Organizations that leverage Unified DDI automation report accelerated service delivery, improved capacity planning, and significantly reduced operational costs.[4] This transformation enables IT teams to focus on innovation and strategic projects rather than routine DDI maintenance.

6. Infrastructure reliability: Ensuring continuous operations

Infrastructure reliability has become a critical business imperative as network outages directly impact revenue and productivity. Many organizations experience two or more DDI-related outages monthly, with each incident lasting three to four hours.[4] This impact is compounded in distributed environments, where network issues can isolate locations and halt local operations.

Unified DDI transforms reliability through advanced architectures like multi-primary DNS and automated failover capabilities. Instead of relying on rigid primary-secondary relationships, organizations can implement flexible architectures that maintain both local autonomy and global consistency. The results are compelling: Organizations report eliminating DNS-related outages, with one Fortune 500 transportation company saving $1.2 million annually in avoided downtime.[4] Unified DDI enables 99.999% service availability through intelligent architecture and automated recovery while reducing infrastructure complexity.[1]

Beyond basic high availability, Unified DDI enhances reliability through architectural optimization and automated management. Organizations can consolidate infrastructure without compromising reliability. Automated health monitoring, predictive analytics, and self-healing capabilities prevent outages before they occur. This comprehensive approach to reliability allows organizations to maintain continuous operations across distributed environments while reducing operational overhead and infrastructure costs.

7. Security by design: Protecting core network services

DNS infrastructure has become an increasingly attractive target for cyberattacks, yet legacy DDI approaches leave organizations vulnerable. Fragmented security controls, limited visibility, and manual processes create security gaps that attackers can exploit. Organizations without unified security controls struggle to detect and prevent threats targeting core network services.

Unified DDI transforms security through a comprehensive, built-in approach that spans detection, prevention, and response. By implementing centralized policy enforcement, real-time threat detection, and automated response capabilities, organizations can identify and block threats faster than with traditional approaches.[4] The impact extends beyond basic security—Unified DDI enables automated compliance controls, reducing audit preparation time by 75% while ensuring consistent policy enforcement across all environments.[4] One health care technology company achieved complete visibility of DNS traffic and automated blocking of malicious domains, reducing security incident response time by 75%.[4]

Unified DDI also creates a foundation for zero-trust security initiatives. Organizations can implement least-privilege access while maintaining operational efficiency through granular access controls, comprehensive audit trails, and automated policy enforcement. This integrated approach to security has allowed organizations to reduce their attack surface by eliminating shadow IT DNS services, automating security updates, and maintaining consistent security controls across hybrid environments. The result is a more robust security posture that protects critical infrastructure while enabling business agility.

Furthermore, core services like DNS and DHCP can often be an all-or-nothing approach with administrative permissions, resulting in ongoing friction around change management. With fine-grained role-based access control, teams can be given the permissions required to complete their tasks more quickly without waiting for service tickets in busy queues. Core teams become more agile by delegating responsibility for various zones, records, and prefixes tasks.

8. Cloud integration: Enabling cloud-first initiatives

Legacy DDI becomes a significant bottleneck for cloud adoption, with organizations struggling to manage DNS across multiple clouds while maintaining visibility and control. The challenge is substantial: Enterprises manage hundreds or thousands of DNS changes daily in cloud environments, while different teams maintain opaque virtual networks and disjointed DNS routing. This complexity creates significant operational overhead.

Unified DDI transforms cloud operations through automated discovery, intelligent resolution, and centralized management across hybrid environments. Organizations achieve real-time visibility and control of cloud resources, with automated synchronization eliminating manual tracking requirements. Customers report a dramatic reduction in cloud DNS management time, complete elimination of zone conflicts, and automated discovery of cloud resources.[4]

Beyond basic cloud management, Unified DDI enables sophisticated hybrid cloud architectures through intelligent DNS resolution and automated policy enforcement. Organizations can optimize DNS routing across clouds, automatically resolve naming conflicts, and maintain consistent security policies across all environments. This comprehensive approach to cloud integration has enabled organizations to accelerate cloud adoption, reduce cloud networking, and achieve consistent operations across hybrid environments. The result is a cloud transformation foundation that ensures agility and control.

9. API programmability: Enabling network automation at scale

The lack of comprehensive APIs impedes automation and integration in legacy DDI environments. Network teams spend countless hours on manual tasks because they can't programmatically interface with their DDI infrastructure. This limitation becomes particularly acute in DevOps environments, where 43% of organizations identify API integration as critical for network automation success.[1] Organizations struggle to integrate DDI into their broader automation initiatives without robust API capabilities.

Unified DDI transforms automation possibilities through comprehensive API capabilities that enable integration with existing tools and platforms. Organizations can automate end-to-end workflows, integrate with continuous integration and continuous delivery pipelines, and enable self-service provisioning through API-driven operations. The results are compelling: Organizations substantially reduce time spent on DDI operations and can automate nearly all their cloud DNS management tasks. One Fortune 500 company reduced their network provisioning time from four hours to just minutes by implementing API-driven automation workflows.[9]

Beyond basic automation, API programmability enables sophisticated integration scenarios that transform organizations' infrastructure management. Teams can integrate DDI with security tools for automated threat response, connect with IT service management platforms for streamlined workflows, and enable infrastructure-as-code practices. This comprehensive API approach has allowed organizations to reduce mean time to resolution by over 31%,[1] accelerate service delivery, and achieve true DDI automation at scale. Most importantly, robust APIs future-proof DDI investments by ensuring organizations can adapt to new tools and technologies as they emerge.

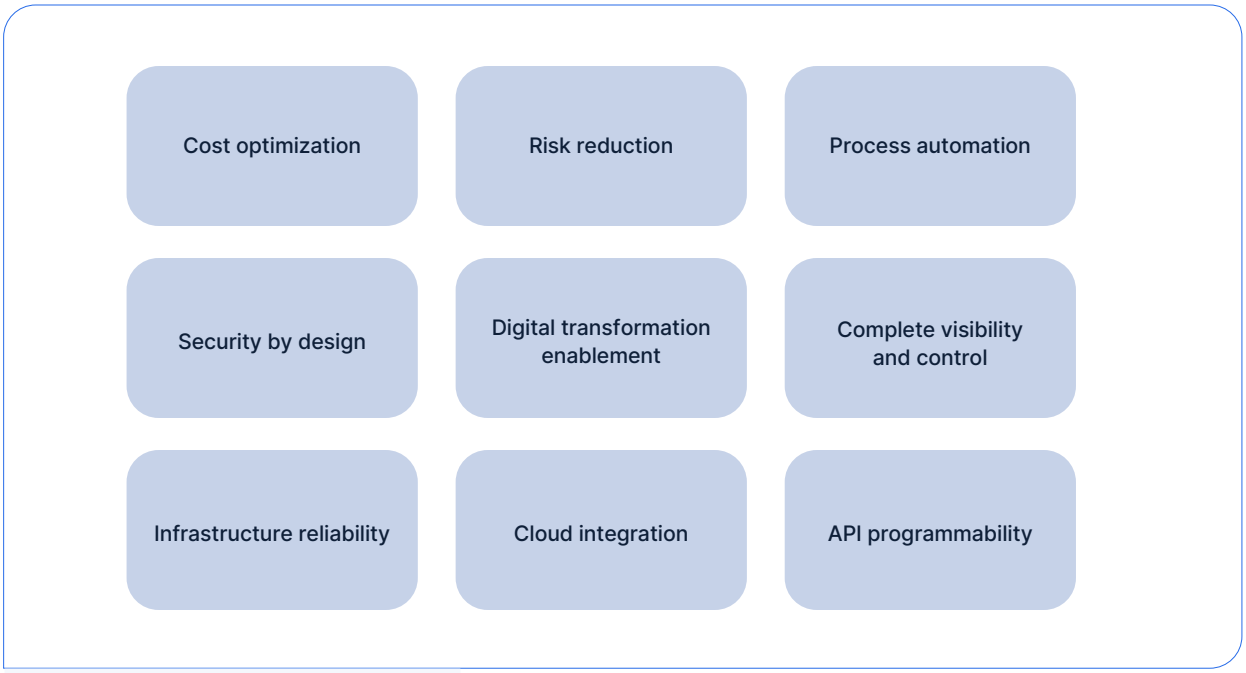

Figure 2. Nine reasons to unify your DDI

BlueCat's Unified DDI offerings

BlueCat offers two distinct approaches to Unified DDI. Whether you're looking to overlay management capabilities onto existing infrastructure or implement a complete DDI platform, BlueCat has a solution aligned with your business objectives.

BlueCat Micetro: Unified DDI orchestration

BlueCat Micetro provides a non-disruptive path to Unified DDI by orchestrating your existing DNS, DHCP, and IP address management infrastructure through a centralized management overlay. Organizations can benefit immediately while maintaining their current DDI investments.

With Micetro, you can modernize your network and gain visibility with a DDI overlay that's easy to implement and use—no matter how complex your cloud and on-premises network architecture is or who touches it. It makes provisioning, access, and control faster and more secure. DDI orchestration with Micetro unifies, visualizes, and automates core network services from a single source of truth—so you get more transparency, self-service, and control with fewer conflicts and outages.

Micetro's key value proposition:

- Rapid time-to-value with no infrastructure changes required
- Unified visibility and control across existing DDI infrastructure
- Progressive modernization path that preserves existing investments

Micetro is ideal for organizations that need to:

- Gain immediate control over fragmented DDI infrastructure
- Maintain existing DDI investments while modernizing
- Address urgent visibility and control challenges
- Start their DDI transformation journey incrementally

BlueCat Integrity: An enterprise DDI platform

BlueCat Integrity delivers a comprehensive, enterprise-grade DDI platform that offers complete control over your DDI infrastructure with built-in automation, security, and cloud integration capabilities.

As the Unified DDI platform for enterprises, Integrity includes three components:

- **BlueCat Address Manager** becomes your IP address management (IPAM) tool and acts as the main DNS and DHCP management platform (cluster or single node).
- **BlueCat DNS/DHCP Servers (BDDSes)** are single instances or clusters that provide authoritative DNS and/or DHCP services (including optional additional plugins and functionality).
- **Cloud Discovery & Visibility** is a container deployed either on premises or in a public cloud to discover and watch for changes that are then streamed back to Address Manager (which means your IPAM is always up to date).

Each instance type is flexible and can be deployed in multiple forms, either physical or virtual. BDDSes selectively provide DNS and/or DHCP services depending on your requirements, architecture, and footprint.

Integrity's key value proposition:

- Complete DDI platform with native automation capabilities
- Advanced security features and cloud integration
- Linear scalability for enterprise growth

Integrity is ideal for organizations that need to:

- Build a foundation for network automation and cloud initiatives
- Implement comprehensive security and compliance controls
- Scale DDI services across large enterprise environments
- Replace aging or inadequate DDI infrastructure

Platform comparison

Capability area	Micetro	Integrity
Deployment model	DDI management overlay	Integrated DDI platform
Implementation timeline	Usually shorter	Usually longer
Infrastructure impact	Non-disruptive	Transformative
Existing DDI integration	Preserves current infrastructure	Replaces existing infrastructure
Automation capabilities	Orchestration of existing systems	Native automation engine
Cloud integration	Native cloud integration	Native cloud integration

Complement Unified DDI with additional products

Based on your network environment and level of cloud adoption, BlueCat's core Unified DDI platforms can be complemented by other products that deliver enhanced benefits.

BlueCat Edge

BlueCat Edge extends intelligent and secure DNS resolution services to a specific site, set of users, or cloud service edges. Edge provides an intelligent layer of control to address threats, solve namespace collisions, and optimize query response latency based on organizational policies.

BlueCat Gateway

With BlueCat Gateway, you can unlock automated end-to-end workflows and seamless integration with third-party tools like ServiceNow and Terraform. Gateway uses an API with a set of Python classes for integrating third-party solutions with Integrity or Edge. Users can create custom integrations and plugins that automate DDI-related tasks and streamline network operations, from common self-service forms to complex workflows.

BlueCat Infrastructure Assurance

BlueCat Infrastructure Assurance proactively alerts BlueCat Integrity enterprise customers to issues and provides remediation steps that network operations teams can use to resolve problems before they cause significant damage. With our domain expertise codified into Infrastructure Assurance, the platform knows what to look for, analyzing your DDI environment to ensure it is healthy.

BlueCat's Unified DDI in action

To demonstrate a Unified DDI environment, we'll use some of BlueCat's scalable, secure, and flexible DDI components as our basic building blocks. In this simple scenario, a multisite network faces challenges typical of a legacy approach to DDI.

Multisite networks relying on legacy DDI often face fragmented management, lack of visibility into resources, inconsistent configurations across sites, and susceptibility to human error. These challenges lead to frequent outages, inefficiencies in resource utilization, and difficulty scaling operations.

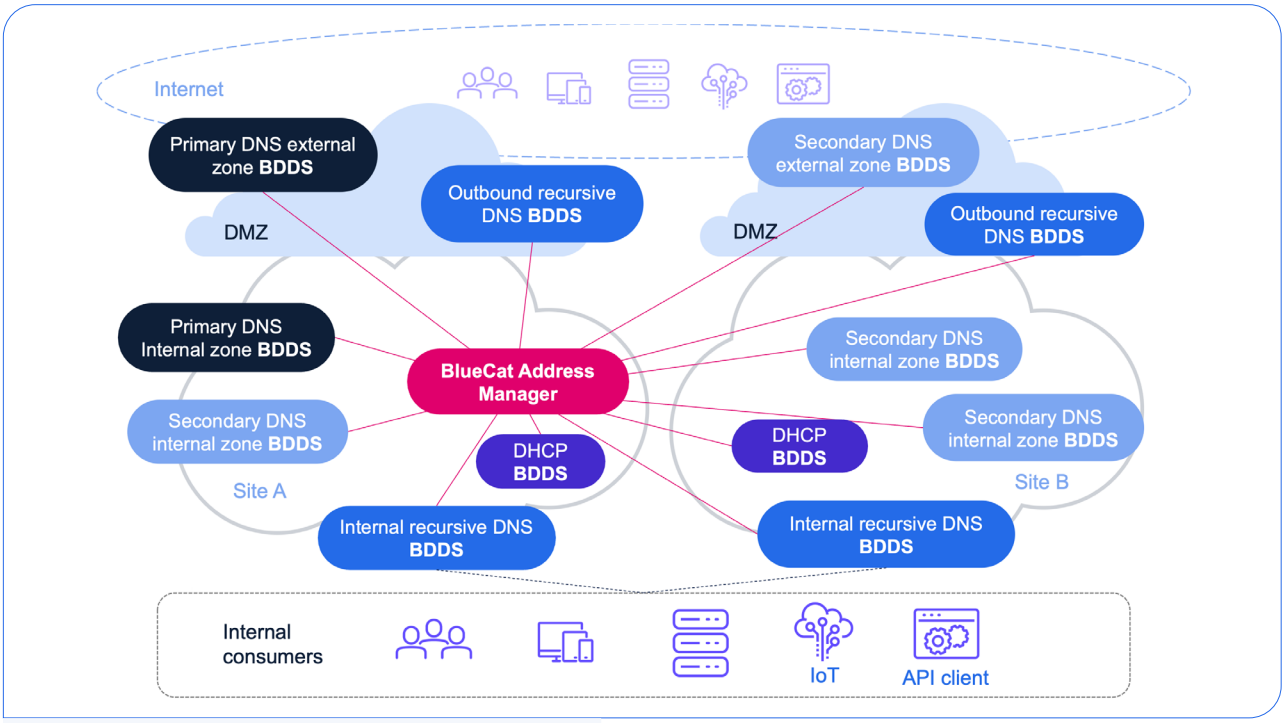

Figure 3. Unifying DDI in a multisite topology using BlueCat Integrity

This example implements an Integrity solution across a multisite environment, unifying DDI and allowing new sites to be easily added by deploying the same blueprint for DHCP and DNS services. The result is a highly scalable, resilient, and secure Unified DDI environment. Specific benefits include:

- Gaining a holistic view of all internal and external zones, DHCP scopes, and tracking or allocation of IP prefixes
- Ensuring sites and services keep functioning even during outages
- Boosting confidence around completeness and authority for IP allocation or design, netblock ownership, DHCP scope allocations, and capacity management

The outcomes of deploying BlueCat's Unified DDI solution in this example are:

Cost optimization: Reduced engineering costs, optimized infrastructure, and elimination of DNS-related outages for rapid return on investment.

Risk reduction: Minimized human error and security risks through automation, centralized policies, role-based access controls, and audit trails.

Digital transformation enablement: Accelerated innovation by integrating DDI into DevOps pipelines and automated resource provisioning.

Complete visibility and control: Single source of truth and real-time insights into DNS, DHCP, and IP usage for efficient tracking and planning.

Process automation: Automated workflows to reduce overhead, improve accuracy, and enhance service delivery.

Infrastructure reliability: Assurance of continuous operations with high availability, failover capabilities, and architectural flexibility.

Security by design: Critical services are protected with granular access controls, DNS policy enforcement, and reduced attack surfaces.

Full DNS and DHCP visibility can benefit your growing IT environment, giving your operations and security teams the upper hand. Unified DDI offers a clear foundation, simplifying multisite development and enhancement without fear or friction.

A strategic transformation with Unified DDI

The transition from legacy to Unified DDI is more than just a technical upgrade—it's a strategic transformation that directly impacts business outcomes. Organizations that adopt Unified DDI realize significant improvements in operations, service delivery, and security.

Unified DDI provides the foundation needed for digital transformation and other business initiatives. Whether accelerating cloud adoption, enhancing security, or automating IT processes, Unified DDI provides the automation, visibility, and control required by modern enterprises. BlueCat's solutions offer flexibility and choice, allowing organizations to choose the path to Unified DDI that best matches their business objectives and transformation timeline.

Footnotes

[1] McGillicuddy, S. (2024). *Network Management Megatrends 2024: Skills Gaps, Hybrid and Multi-Cloud, SASE, and AI-Driven Operations*. Enterprise Management Associates. https://bluecatnetworks.com/wp-content/uploads/2024/08/network-management-mega-trends-2024.pdf

[2] McGillicuddy, S. (2021). *A House Divided: Dysfunctional Relationships Between Network and Cloud Teams Put Cloud Strategies at Risk*. Enterprise Management Associates. https://bluecatnetworks.com/cloud-networking-dysfunction/

[3] O'Connell, V. (2022). *The modern IT outage: costs, cases, and "cures". Enterprise Management Associates*. https://www.enterprisemanagement.com/research/asset.php/4230/The-modern-IT-outage:-costs,-causes,-and-"cures"

[4] McGillicuddy, S. (2023). *From DIY DDI to BlueCat: Customers Earn ROI Within Three Months. Enterprise Management Associates*. https://bluecatnetworks.com/wp-content/uploads/2023/11/From-DIY-DDI-to-BlueCat_Customers-Earn-ROI-Within-Three-Months.pdf

[5] IBM Security. (2024). *Cost of a Data Breach Report 2024*. IBM. https://www.ibm.com/reports/data-breach

[6] McGillicuddy, S. (2023) *DDI Directions: DNS, DHCP, and IP Address Management Strategies for the Multi-Cloud Era*. Enterprise Management Associates. https://bluecatnetworks.com/ema-ddi-directions-report/)

BlueCat helps enterprises achieve their network modernization objectives by delivering innovative products and services that enable networking, security, and DevOps teams to deliver change-ready networks with improved flexibility, automation, resiliency, and security.

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

bluecat.com

Next steps

Find out if **BlueCat Integrity** or **BlueCat Micetro** can help unify your DDI.

Learn more