efficient iP®

The Ultimate Guide to Modernizing DDI

How to **simplify**, **secure** and **automate** DNS, DHCP and IPAM across hybrid and multi-cloud environments

Executive summary

DNS, DHCP and IP address management sit at the foundation of every digital interaction.

They determine how users, devices, applications and services find one another and connect. Yet in many enterprises, these essential services remain fragmented across legacy appliances, spreadsheets, open-source tools, Microsoft infrastructure and multiple cloud platforms.

That fragmentation creates more than an operational inconvenience. It limits visibility, slows service delivery, increases security risk and makes it harder to maintain resilience across increasingly distributed environments.

Modernizing DDI is therefore not simply a network infrastructure upgrade. It is an opportunity to establish a more reliable source of truth, automate repetitive work, improve security and support faster digital transformation.

Enterprise Management Associates evaluated 12 DDI products from 10 vendors for its 2025 EMA Radar for DDI. The research identified security, scalability, performance, integrated DDI, ease of use, multi-cloud support and resiliency among the most important platform requirements. It also found that end-to-end ecosystem automation, comprehensive network source of truth capabilities, improved network and cloud discovery, and AI/ML-driven insights are leading customer priorities for the next two years.

This guide explains:

- Why traditional approaches to DDI are becoming unsustainable
- What a modern DDI platform should deliver
- How to evaluate potential solutions
- How to build the business case for modernization
- How to reduce migration risk
- What to ask before selecting a vendor

1. Why DDI modernization matters

DDI combines three foundational network services:

Domain Name System (DNS) translates names into the IP addresses that users, applications and devices need to connect. It is a critical service: without functioning DNS, users and applications cannot reach the services they depend on, and business operations can quickly come to a halt.

Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses and network settings to devices.

IP address management (IPAM) provides the system of record for planning, assigning, tracking and governing address space.

These services are tightly connected, but many organizations still manage them through separate tools, processes and teams.

Common environments include:

- Microsoft DNS and DHCP
- Cloud-native DNS services
- Legacy DDI appliances
- Open-source servers
- Spreadsheets and homegrown databases
- Different tools across business units or regions

Each technology may perform an individual function adequately. The problem is the absence of a unified operational model.

As infrastructure expands across data centers, branch locations, public clouds, edge environments and remote users, fragmented DDI makes it difficult to answer fundamental questions:

- What is connected to the network?
- Which IP addresses are available or in use?
- Who made a DNS or DHCP change?
- Are cloud and on-premises records synchronized?
- Which services depend on a particular address or DNS record?
- Is an unauthorized DNS or DHCP service operating in the environment?
- Is the DNS protected against the growing volume and sophistication of cyberattacks?
- Can the organization recover quickly from a DNS failure?

EMA notes that spreadsheets and open-source approaches are less scalable, resilient, manageable and secure for enterprises with complex networks. Its research connects mature, vendor-supported DDI with improved network resilience, IT productivity, security, user experience and service delivery.

2. Signs that your DDI environment needs modernization

Not every organization needs to replace its DDI platform immediately. However, certain **symptoms indicate that current tools and processes are no longer keeping pace.**

Changes depend on manual intervention

Routine requests for DNS records, subnets or IP addresses move through tickets and spreadsheets. Engineers repeatedly perform work that should be policy-driven and automated.

There is no trusted source of network data

Different teams maintain different records. IPAM, cloud inventories, configuration tools and spreadsheets disagree about what exists and how it is configured.

Cloud adoption has fragmented visibility

Cloud teams create DNS zones, virtual networks and address ranges without consistent synchronization with enterprise DDI.

Troubleshooting takes too long

Teams must search multiple consoles, logs and spreadsheets to understand an outage, address conflict or failed service dependency.

DNS and DHCP changes create unnecessary risk

Changes are applied manually with inconsistent approval, testing, rollback and audit procedures.

Legacy infrastructure is difficult to scale

In some environments, adding capacity can involve licensing changes, additional appliances, lengthy planning or significant professional services.

DNS resilience depends on manual recovery

DNS continuity depends on manual failover or rebuilding, making recovery during failures, outages or attacks slow and inconsistent.

Security teams lack DNS context

DNS activity is not analyzed for attacks or integrated with SIEM, SOAR, endpoint or incident-response workflows.

The platform cannot support automation initiatives

APIs expose only limited functionality, documentation is weak or integrations require custom development.

When several of these conditions exist, the cost of maintaining the status quo may be greater than the perceived risk of modernization.

3. The seven requirements of modern DDI

Requirement 1: Unified DNS, DHCP and IPAM management

A modern platform should provide centralized control over DNS, DHCP and IP address data, while supporting the reality that enterprises often operate multiple vendors and service types.

The objective is not necessarily to replace every existing DNS or DHCP service on day one. A modern DDI platform should be able to manage native services and provide overlay management and control for selected third-party infrastructure.

Look for:

- A consistent data model across DNS, DHCP and IPAM
- Centralized policy and administration
- Synchronization across services
- Support for native and third-party DNS and DHCP
- Consistent audit trails
- Delegated administration with role-based access

EMA ranks full integration of DNS, DHCP and IPAM among the leading platform requirements identified by DDI stakeholders.

Requirement 2: Hybrid and multi-cloud visibility

Cloud adoption often creates new operational silos.

Cloud teams may use Amazon Route 53, Azure DNS, Google Cloud DNS and cloud-native address management independently from the network team. This creates overlapping address space, stale records and inconsistent controls.

A modern DDI platform should help teams discover, reconcile and govern network resources across:

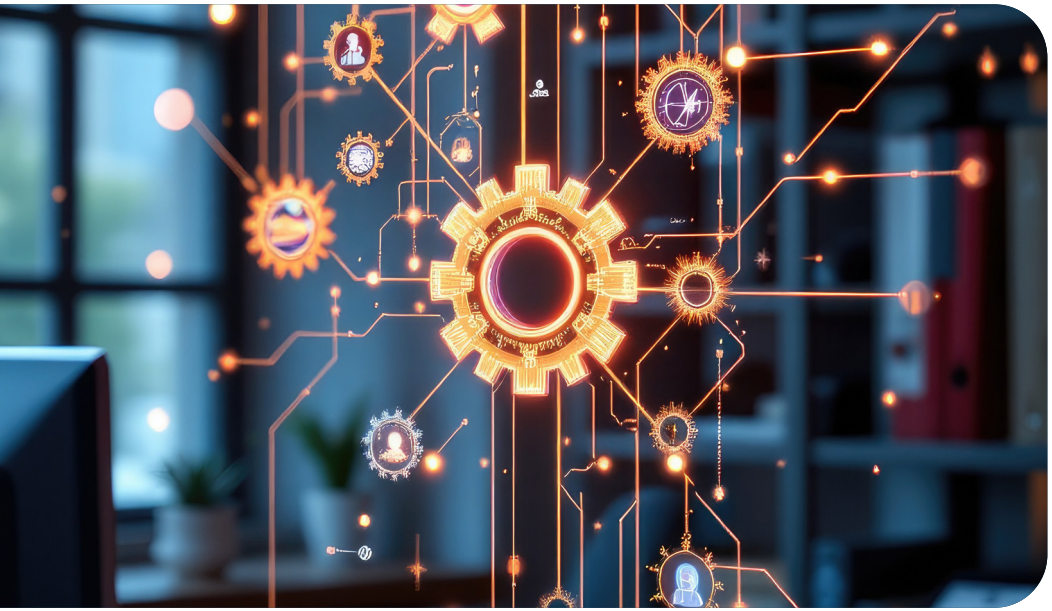
- Data centers
- Private clouds
- AWS
- Microsoft Azure
- Google Cloud
- Branch offices
- Edge infrastructure
- Remote environments

The platform should provide a consistent inventory without forcing every team to abandon the tools native to its environment.

Ask whether the platform can:

- Discover cloud IP space and DNS services
- Discover and reconcile cloud IP address space with enterprise IPAM
- Identify overlapping address ranges
- Track ownership and business context
- Manage or govern cloud DNS services
- Support multiple cloud accounts and subscriptions
- Detect unauthorized or unmanaged resources

EMA identifies multi-cloud support as a major DDI platform requirement and network and cloud discovery as a top automation and roadmap priority.



Requirement 3: Policy-driven workflow automation

The value of modern DDI extends well beyond eliminating spreadsheets.

Automation should allow infrastructure teams to define policies once and apply them consistently across routine activities.

High-value workflows include:

- Network and cloud discovery
- DNS and DHCP deployment
- IP address allocation
- DNS record creation
- Subnet and VLAN provisioning
- Address synchronization
- IP address reclamation
- Compliance enforcement
- Failure and conflict alerts
- Approval and rollback processes
- Security policy definition and enforcement

Automation should not mean losing control. Effective platforms combine automation with governance, role-based approval and complete auditability.

EMA found that network and cloud discovery, DNS and DHCP configuration and IP address allocation are among the highest-priority workflows for DDI automation.

Requirement 4: A network source of truth

Traditional IPAM is centered on address-space planning and control.. A modern network source of truth extends that foundation by DDI data to the broader network context, objects, and relationships.

Depending on the organization, this may include:

- IP addresses
- Subnets
- DNS records
- DHCP leases
- VLANs and VXLANs
- VRFs
- Devices
- Users
- Applications
- Cloud resources
- Network objects
- Ownership and location
- Relationships and dependencies

A network source of truth becomes strategically valuable when other systems can trust and act on its data.

Potential consumers include:

- IT service management
- Network automation
- Cloud orchestration
- Security platforms
- Configuration management
- Observability tools
- Self-service portals
- AI assistants and agents

EMA identifies comprehensive network source-of-truth capabilities as one of the top priorities that DDI buyers want vendors to advance.

Requirement 5: Open APIs and ecosystem integration

DDI operates across network, cloud, security and IT operations. It should not become another closed system.

Modern platforms need well-documented APIs that expose meaningful data and functionality rather than a limited subset of administrative tasks.

Common integration requirements include:

- ITSM platforms
- Network automation tools
- Cloud orchestration
- SIEM and SOAR
- Security monitoring
- Configuration management
- Observability systems
- CI/CD pipelines
- Self-service portals

EMA found that automation and orchestration and security and compliance enforcement are the two leading use cases for DDI APIs.

During evaluation, ask vendors to demonstrate an actual workflow through the API. Do not rely solely on a statement that the product is “API-first.”

Requirement 6: Built-in resilience and DNS security

DNS is both a critical service for digital connectivity and a strategic security control point. If DNS is disrupted, users, applications and devices may be unable to reach the services they depend on, even when the rest of the infrastructure remains operational. A modern DDI platform must therefore keep DNS available during failures and attacks, support rapid recovery, and detect and respond to malicious DNS activity.

Modern platforms should provide:

- **Reliable operations** - Centralized, policy-driven management across the lifecycle
- **Always-on resilience** - Continuity during failures, attacks and recovery
- **Scalable growth** - Expand capacity without multiplying operational complexity
- **High-performance DNS** - Ensure fast, reliable service under any demand
- **Ecosystem automation** - Connect DNS with cloud and security workflows
- **Built-in DNS security** - Detect, enforce and respond at resolution

Security was the top general platform requirement identified by EMA respondents. EMA also found that organizations with a stronger focus on DDI security tend to report greater overall success with their DDI strategy.

Requirement 7: Scalable and cost-efficient architecture

License price alone does not determine cost.

The true cost of DDI includes:

- Deployment time
- Appliance requirements
- Professional services
- Administrative effort
- Upgrade complexity
- Support and maintenance
- Downtime risk
- Migration effort
- Integration development
- Future expansion

A lower-priced product may become expensive if it requires significant manual administration. A premium product may deliver better value if it reduces operating effort and scales more efficiently.

A scalable DDI architecture should support growth in DNS and DHCP services, IP address data, infrastructure and policies without requiring proportional increases in appliances, administrative effort or operational complexity.

EMA evaluates DDI value by combining product strength with cost efficiency, including deployment and administration. This is a more useful model than comparing software prices in isolation.

4. Building the business case

A strong DDI modernization business case should connect technical limitations to measurable operational and business outcomes.

Reduce administrative effort

Estimate the time teams spend on:

- DNS and DHCP tickets
- Manual address allocation and changes
- Spreadsheet reconciliation
- Troubleshooting address or DNS conflicts
- Audit preparation
- Cloud resource discovery
- Policy enforcement
- Patches/ Upgrades/ Backups
- Threat investigation and incident response
- Disaster and cyberattack recovery

Then identify which activities could be eliminated or automated.

Accelerate service delivery

Measure how long it takes to:

- Provision a subnet
- Create a DNS record
- onboard a new application
- connect a new branch
- allocate cloud address space
- deploy DNS or DHCP capacity
- Automatically detect and mitigate DNS threats

Modernization should reduce waiting time and handoffs.

Improve resilience

Document:

- DNS-related incidents
- configuration errors
- outages caused by manual changes
- recovery time
- systems without high availability
- inconsistent failover procedures

Reduce security exposure

Evaluate:

- unmanaged DNS services
- weak administrative controls
- incomplete audit trails
- lack of DNSSEC
- Inability to define and enforce granular DNS security policies
- limited DNS threat visibility
- Limited ability to detect malicious DNS activity
- Lack of automated mitigation and DNS service continuity during attacks
- inability to integrate DNS events with the SOC
- lack of protective dns compliance

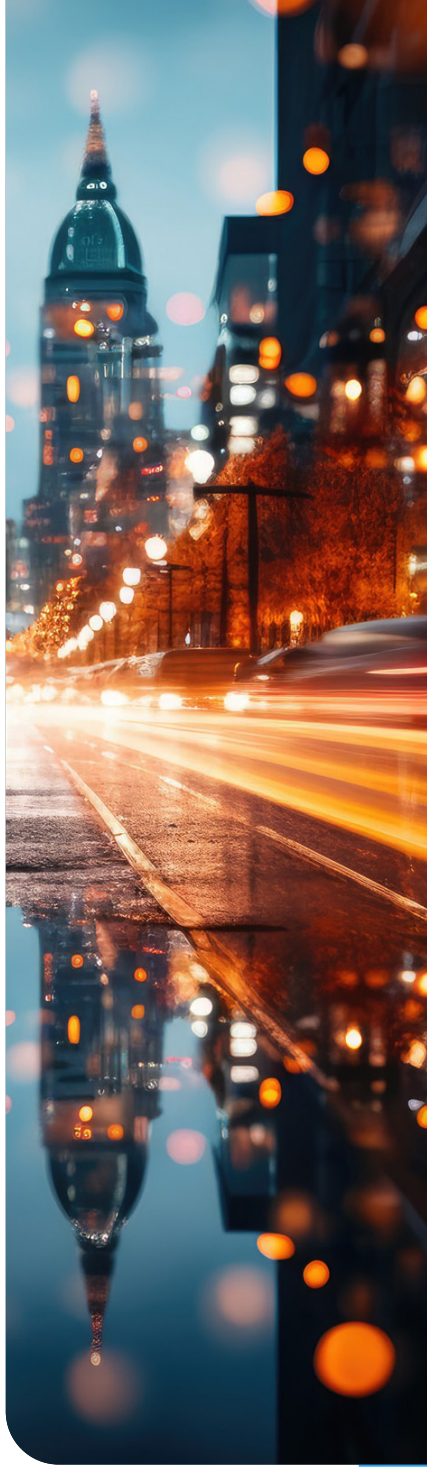
Consolidate tools and infrastructure

Identify overlapping spending on:

- point products
- legacy appliances
- open-source support
- homegrown tools
- professional services
- cloud management utilities

Avoid false precision

Do not claim savings that cannot be documented. Establish current baselines, identify plausible improvements and validate assumptions through a controlled proof of concept.



5. A practical modernization roadmap

Phase 1: Discover and baseline

Create a complete inventory of:

- DNS and DHCP servers
- IPAM tools and spreadsheets
- address blocks and subnets
- DNS zones and records
- cloud environments
- integrations
- owners and administrators
- dependencies
- security policies
- unsupported or obsolete systems

Identify data quality issues before migration.

Phase 2: Define the target operating model

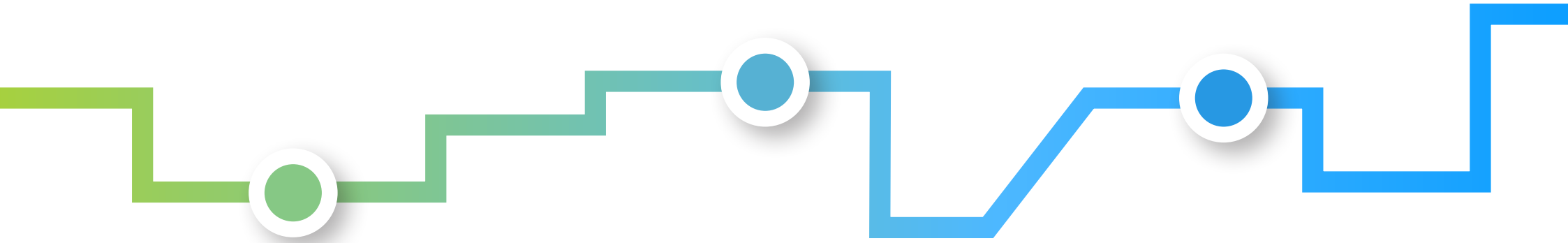
Decide:

- Which services will be replaced
- Which services will remain under overlay management
- Which teams will own DDI
- What can be automated
- What approval controls are required
- How cloud teams will participate
- Which systems will consume DDI data
- How security operations will use DNS telemetry

Phase 3: Design the architecture

Define:

- Availability requirements
- Geographic placement
- Capacity and scalability
- Cloud connectivity
- Security controls
- Disaster recovery
- Upgrade strategy
- Logging and monitoring
- Ecosystem connectivity



Phase 4: Prove the critical workflows

The proof of concept should test real use cases, not generic demonstrations.

Examples:

- Import existing IP data
- Discover cloud resources
- Create a DNS record through an ITSM workflow
- Allocate a subnet through an API
- Simulate a service failure
- Roll back a configuration change
- Apply delegated administration
- Integrate DNS events with security monitoring
- Assess DNS security risk based on your own traffic

Phase 5: Migrate in stages

A phased migration reduces risk by validating data, workflows, and operational readiness before critical services are moved.

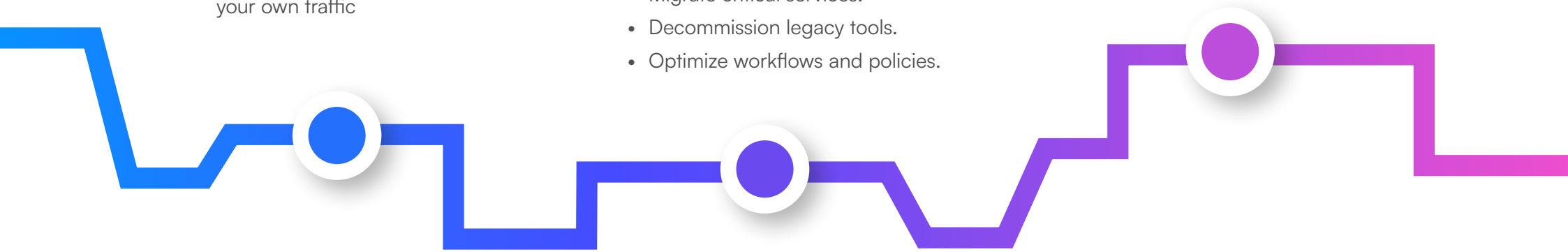
Proposed sequence:

- Establish the network source of truth.
- Import and reconcile data.
- Deploy visibility and overlay management of DNS and DHCP services.
- Migrate noncritical DNS and DHCP services.
- Validate performance and operations.
- Migrate critical services.
- Decommission legacy tools.
- Optimize workflows and policies.

Phase 6: Measure and improve

Track:

- Ticket reduction
- Provisioning time
- Address utilization
- Change failure rate
- Mean time to resolution
- Unmanaged asset discovery
- DNS availability and performance
- Security detections
- Policy compliance
- Adoption of automated workflows



6. How to evaluate DDI vendors

EMA evaluated vendors across five broad dimensions:

- Deployment and administration
- Cost advantage
- Architecture and integration
- Functionality
- Vendor strength

These provide a useful starting point for an enterprise evaluation framework.

Deployment and administration

Evaluate:

- Proof-of-concept options
- Typical deployment time
- Professional-services requirements
- Deployment flexibility
- Upgrade and rollback procedures
- Administrative overhead
- Support response commitments
- Training and documentation

Cost and licensing

Evaluate:

- Subscription structure
- Appliance costs
- Support and maintenance
- Expansion costs
- Cloud licensing
- Cost of nonproduction environments
- License portability
- Contract flexibility

Architecture and integration

Evaluate:

- Scale-out architecture
- IPAM scalability
- DNS and DHCP performance
- High availability
- APIs
- Standard integrations
- Hybrid and multi-cloud support

Functionality

Evaluate:

- Discovery
- IPAM
- DNS
- DHCP
- Reporting
- Cloud management
- Security
- Workflow automation
- Source-of-truth capabilities
- Multi-vendor management

Vendor strength

Evaluate:

- Product vision
- Roadmap
- R&D investment
- Financial stability
- Support capabilities
- Channel ecosystem
- Customer references
- Migration experience

7. Independent validation of EfficientIP

EMA named EfficientIP a 2025 Value Leader, a designation based on the balance of product strength and cost efficiency.

EMA rated EfficientIP outstanding in:

- Deployment time
- Maintenance and support costs
- Scale-out architecture
- IPAM scalability
- DNS scalability
- APIs
- IP address management functionality

It rated EfficientIP strong in areas including administration overhead, customer support, resiliency, network discovery, reporting and visualization, DNS and DHCP functionality, security, vision and strategy.

EMA highlighted EfficientIP's outstanding IPAM functionality, one of the best approaches to establishing a network source-of-truth among pure DDI vendors, customizable reporting and visibility, and a highly scalable architecture.

Third-party recognition should not replace a buyer's own assessment. Organizations should evaluate the platform against their architecture, workflows, security requirements and migration priorities.

8. Final takeaways

DDI modernization is not about replacing one set of DNS and DHCP servers with another.

It is about creating a more unified operating model for the network.

A modern DDI strategy should help the organization:

- Establish a trusted source of network data
- Automate repetitive work
- Support hybrid and multi-cloud environments
- Improve network and application resilience
- Strengthen DNS security
- Integrate network data with broader IT workflows
- Scale without multiplying operational complexity

The right platform should deliver immediate operational value while providing a foundation for future automation, AI and digital infrastructure initiatives.

Read the full EMA report

Reach out to EfficientIP

to assess your **DDI modernization readiness**.

Identify gaps in visibility, automation, resilience, cloud management and DNS security.

efficient iP®

EfficientIP is a global leader in network automation and security, specializing in DNS, DHCP, and IP Address Management (DDI), with over 20 years of expertise. Its 360° DNS Security serves as a first line of defense, enabling teams to protect, detect, and respond to threats. Powered by advanced and AI-patented technologies, its DNS Threat Intelligence platform transforms billions of DNS queries into actionable insights, helping teams detect threats earlier and respond faster.

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752