

# Modernizing DNS Infrastructure for Hybrid and Multicloud: From Background Plumbing to Strategic Control



Bruno Teyton  
Associate Vice President  
Network Infrastructure and Services, IDC



Romain Fouchereau  
Senior Research Manager  
European Security, IDC

Modernizing DNS infrastructure is no longer optional; it is a business imperative. However, modernization must balance incremental evolution with targeted architectural resets where required.

# Modernizing DNS Infrastructure for Hybrid and Multicloud: From Background Plumbing to Strategic Control

April 2026

**Written by:** Bruno Teyton, Associate Vice President, Network Infrastructure and Services; Romain Fouchereau, Senior Research Manager, European Security

## Introduction

Organizations worldwide operate in increasingly distributed, hybrid, and multicloud environments that often span traditional IT and operational domains. Rapid growth in cloud adoption, remote access, connected assets, generative AI (GenAI) use, and digital services has significantly increased reliance on core network services.

DNS has evolved far beyond basic name resolution. It is now a strategic control point that directly impacts application availability and user experience, security enforcement and threat detection, and overall service continuity and operational resilience. However, many legacy and organically grown DNS architectures were not designed to support today's demands for scale, elasticity, automation, and high query-per-second (QPS) workloads.

Modernizing DNS infrastructure is no longer optional; it is a business imperative. It reduces operational complexity while improving resilience, visibility, performance, and security across hybrid and multicloud environments to drive business outcomes.

## AT A GLANCE

### WHAT'S IMPORTANT

- » DNS modernization is critical for resilience, performance, and security in hybrid and multicloud environments.
- » Legacy DNS architectures require an architectural overhaul and centralized governance.

### KEY TAKEAWAYS

- » Security must be built into DNS design and operations from the start.
- » Architecture, performance, and management require clear role separation and centralized orchestration for reliability and scalability.
- » Hybrid and multicloud architectures require the centralized orchestration of DNS services with overlay-based multivendor DNS management.
- » Data, observability, and automation enable unified visibility and rapid response.

However, one size does not fit all. DNS modernization must balance incremental evolution with targeted architectural resets where required. Optimization alone cannot resolve every constraint, and some legacy design assumptions must be reconsidered to support modern requirements for scale, automation, unified hybrid and multicloud, and resilience. In heterogeneous environments, centralized overlay management of multivendor DNS services is essential to reduce complexity, ensure consistent operations, and maintain full visibility. Organizations must make deliberate architectural trade-offs between operational simplicity and functional flexibility, guided by workload characteristics, risk tolerance, and velocity requirements.

Finally, security must be foundational and built in by design rather than added as an afterthought. It should actively shape DNS architecture decisions, including namespace design, resolver placement, separation of authoritative and recursive roles, data residency, and operating models. Only then can DNS function as a meaningful first line of defense rather than a passive transport layer.

### ***How DNS trends affect networking operations***

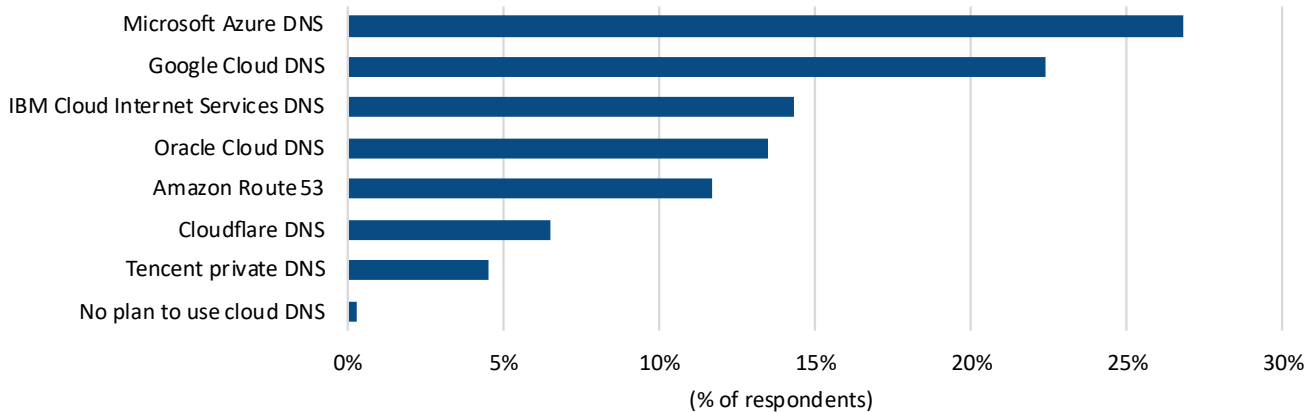
As DNS evolves to support hybrid and multicloud architectures, it increasingly acts as the glue between clouds and between cloud and on-premises environments. According to IDC's *Q2 2025 Cloud Pulse Survey*, 90% of organizations that have moved to the cloud have implemented hybrid cloud (data/workload integration in private and public clouds); 84% report multicloud adoption using two or more public cloud providers. This shift introduces new operational and governance challenges.

Organizations must address the following aspects:

- » **Tooling fragmentation:** Each cloud provider and platform introduces its own DNS services, APIs, and operational models. IDC data indicates that enterprises frequently use multiple cloud DNS services in parallel, increasing operational fragmentation and the need for centralized governance across heterogeneous environments (see Figure 1).
- » **Change management challenges:** DNS changes must propagate accurately and consistently across multiple environments to prevent configuration drift and service disruption.
- » **Namespace complexity:** Overlapping private zones and split-horizon resolution across parallel environments require centralized, tenant-aware management to maintain resolution integrity and prevent naming conflicts.
- » **Security risks:** Multiple control planes and identity systems increase exposure and reduce visibility.

Figure 1: **Adoption of cloud-native DNS services across providers**

Q Which cloud DNS service(s) does your organization currently use or plan to use?



Source: IDC's *IaaS Network Security Services Survey*, 2024 (n = 1,003)

Today, many organizations operate federated DNS models in which separate teams manage different DNS systems across environments. While this approach reflects organizational structure, it can result in weak governance, limited end-to-end visibility, and inconsistent policy enforcement. Without centralized oversight, complexity increases and operational risk grows.

At the same time, DNS is evolving into a foundational control and enablement layer for modern IT architectures. It underpins key technology trends such as GenAI workloads, cloud-native platforms, IPv6 adoption, zero trust architectures, and highly automated, ephemeral environments. Application-driven DNS changes and increasing service dynamism are reshaping automation requirements in terms of performance, openness, and flexibility, necessitating tighter integration with DevOps workflows to support rapid, automated service delivery.

Modern DNS must scale to high query rates, protect sensitive data, and operate efficiently in dynamic infrastructures. As environments become more ephemeral and distributed, dynamic DNS is essential for tracking changes, automating updates, and reducing manual effort while maintaining performance, reliability, and control.

### **Modern DNS infrastructure under security pressure**

Classic DNS attack mechanisms — including cache poisoning, registrar attacks, data exfiltration, hijacking, distributed denial-of-service (DDoS), and domain exploitation — are not disappearing; rather, they are becoming more sophisticated. For instance, in February 2026, Microsoft disclosed an attack that leveraged a new variant of the "ClickFix" technique to deliver malware by exploiting user trust in technical error messages. By running a command that executes a DNS lookup, users allowed attackers to install malware and steal sensitive data. At the same time, new DNS attack vectors are emerging, driven by artificial intelligence. AI is increasingly used to generate highly credible malicious domains, dynamically adjust to evade detection algorithms, and rapidly rotate domains to avoid blacklisting. As a result, the DNS threat landscape is becoming more adaptive, automated, and difficult to contain.

This threat landscape is further compounded by highly complex DNS architectures that often combine legacy appliances, outdated Windows DNS versions, multiple security layers, hybrid DNS deployments, and a myriad of authoritative servers

and recursive resolvers. Consequently, operational complexity increases while visibility remains limited. Misconfiguration risks grow, troubleshooting slows, and the overall impact of DNS failures is amplified — ultimately degrading user experience and business continuity.

Many organizations have adopted DNS encryption mechanisms such as DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT). While these protocols provide meaningful benefits with regard to spoofing protection, confidentiality, and privacy, they also introduce operational challenges. Encryption can complicate troubleshooting and increase performance overhead. If DNS traffic does not terminate on enterprise-owned servers, it reduces visibility into DNS traffic. In such cases, control shifts away from the organization, potentially creating blind spots that enable data exfiltration or denial-of-service scenarios.

A modern DNS strategy must be data-driven, but organizations face significant data-related challenges:

- » **Logging silos:** DNS data is scattered across multiple systems and infrastructures, including cloud DNS platforms, on-premises appliances, and authoritative DNS services, resulting in numerous logging silos. These logs often use different formats, are retained for varying periods, and are managed by separate teams. This fragmentation prevents organizations from achieving a unified view of DNS activity and makes correlation and decision-making more complex.
- » **Normalization and enrichment gaps:** Data quality is critical for effective DNS operations, but normalization and formatting inconsistencies persist. In some cases, logging is incomplete across resolvers, security appliances, and cloud DNS services. Moreover, DNS data is not always enriched with asset inventories, identity systems, or contextual metadata, slowing investigations and delaying incident response.
- » **Exponential telemetry volume:** DNS generates massive volumes of telemetry — sometimes millions of queries per second. Generative AI adoption further amplifies this, as AI-driven applications generate higher query rates. Storing, processing, and analyzing this data requires significant infrastructure investment, and rising volumes can slow response times and reduce detection accuracy.

Beyond technical complexity, organizational factors exacerbate these challenges. According to IDC's *Network and Life-Cycle Services Survey*, only 28% of enterprises in the EMEA region had fully integrated security and networking teams in 2025. As a result, silos persist: Security teams manage DNS firewalls, Active Directory teams manage Windows DNS, and cloud teams oversee cloud DNS environments. This fragmentation leads to inconsistent policies, limited coordination, and slower response times.

Additionally, 20% of respondents cited a lack of skills to adopt new technologies or maintain operations as a key challenge. This skills gap is particularly acute in terms of DNS, where expertise is often concentrated among a small number of engineers. Many organizations lack specialized capabilities in DNS troubleshooting, hybrid DNS ecosystem management across appliances and cloud environments, and deep protocol-level knowledge.

## Core elements of a modern DNS

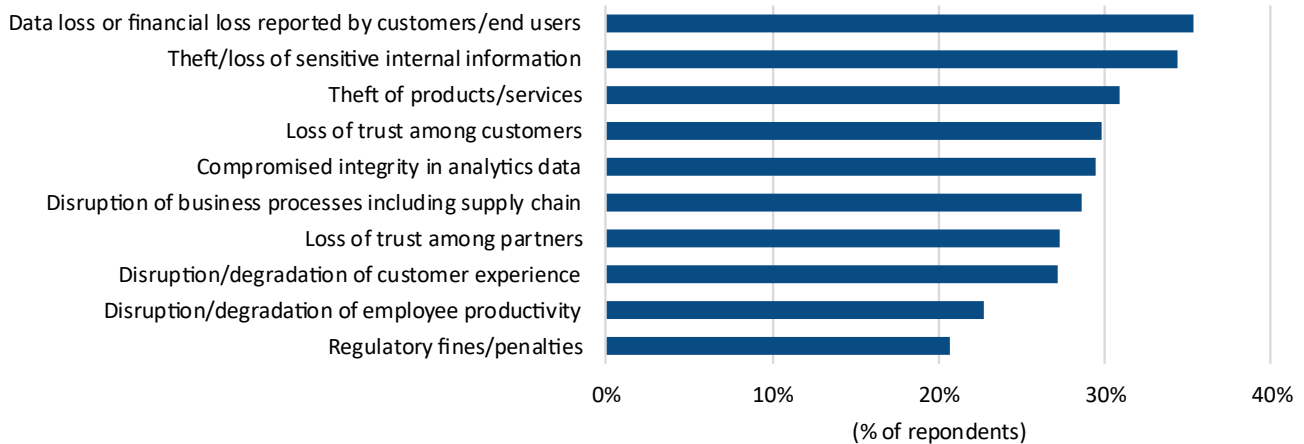
### 1. Security and trust foundations

Security must be built into DNS architecture from the beginning. In hybrid and multicloud environments, DNS cannot rely solely on perimeter defenses. Security considerations should influence DNS design, including data placement, domain

structure, and operational management. As DNS is increasingly a first line of defense, it becomes a critical control point within the network.

Figure 2: **Adoption of cloud-native DNS services across providers**

Q What types of damage to your organization were caused by attacks targeting applications, APIs, and availability in 2024 (including web/API exploits, DDoS, bots, etc.)?



Source: IDC's *Web Application & Availability Protection Buyer Insights, 2025*

Attacks targeting applications and availability have a significant business impact, including financial loss, service disruption, and reputational damage (see Figure 2). Because DNS underpins application access and service continuity, its architecture and security posture directly influence organizational exposure to these risks.

Security and trust in modern DNS architecture requires attention to three key areas:

- » **Namespace isolation:** This requires clear separation between internal and external domains, without overlapping namespaces. In more complex environments, different namespaces can be used to isolate security zones or trust boundaries. Clear separation reduces confusion, limits exposure, and supports consistent policy enforcement.
- » **Integrity and confidentiality:** DNSSEC strengthens integrity by protecting against cache poisoning and spoofing, but it should be part of a broader DNS security approach. The use of encrypted DNS protocols (e.g., DoT and DoH) protects DNS queries from interception in transit, especially in hybrid environments. However, because encryption affects monitoring, resolver behavior, and performance, security policies and tools must be updated to maintain visibility.
- » **Zero trust integration:** DNS modernization is a pillar of zero trust architectures. By limiting name resolution privileges, controlling resolvers, segmenting DNS services, and improving visibility through real-time traffic analysis and telemetry, organizations can enforce granular access control and detect abnormal activity. In this context, DNS becomes an integrated part of the overall security architecture rather than a background service.



## 2. Architecture, performance, and management

- » **Separation of duties:** Separation of authoritative and recursive DNS roles is mandatory to ensure reliability, governance, and security. Organizations must deploy them on distinct servers and segregated networks, governed by different security policies. In particular, recursive resolvers must never be exposed to the public internet, and access should be strictly restricted to authorized devices.
- » **Hidden primary server architecture:** For authoritative DNS servers, organizations should adopt a hidden primary (or stealth master) architecture. In this model, the primary server is not publicly listed in the zone's Name Server records and does not respond to external queries. Instead, it distributes zone data to publicly exposed secondary servers, which handle all client requests. This approach reduces the attack surface of mission-critical DNS infrastructure, enforces a clear separation between control and query roles, and enables maintenance of the primary server without service interruption. It also allows tighter control over zone transfers through access restrictions and authentication mechanisms.
- » **Tiered resolver deployment:** Building on this foundational separation, organizations must also distinguish between client-facing resolvers and those dedicated to controlled internet name resolution.

**Client-facing resolvers:** Sit at the earliest stage of the DNS resolution path; this strategic position enables enforcement of security controls such as filtering, logging, and DNS traffic analysis, strengthening both security posture and operational visibility.

**Internet-dedicated resolvers:** Not directly accessible by clients; they operate in a constrained role focused on controlled external resolution.

- » **Intelligent traffic management:** To improve application availability and user experience and reduce downtime, organizations must implement intelligent traffic management across authoritative and recursive resolvers. Intelligent traffic management enables dynamic traffic steering, load balancing, and failover decisions among geographically distributed sites. At the authoritative level, it steers traffic to the available nodes. At the recursive level, resolvers optimize resolution paths by enforcing segmentation and security policies.
- » **Hybrid and multicloud placement:** In hybrid and multicloud environments, poor DNS placement creates bottlenecks, increases security breaches, and adds complexity in DNS operations, affecting the user experience. To minimize latency, recursive DNS must be deployed close to users (on-prem or by cloud region), while authoritative DNS should be globally distributed. In Kubernetes, DNS should be automated as part of the provisioning and deployment workflow to support rapid scale-out. Clusters rely on in-cluster DNS (e.g., CoreDNS) for service discovery, while external access is exposed via Ingress/Gateway and cloud load balancers, with DNS records managed by controllers (e.g., ExternalDNS).
- » **Active Directory integration:** Within enterprise environments, particular attention must be paid to Active Directory–integrated DNS. Unlike standalone DNS implementations, AD DNS is tightly coupled with authentication and directory services. As a result, weak integration with broader DNS ecosystems — such as cloud DNS platforms, public authoritative DNS services, or conditional forwarders — can result in authentication failures, service outages, security gaps, and complex troubleshooting scenarios. Therefore, effective integration begins with rigorous namespace design and clear alignment between AD DNS, private DNS zones, and cloud DNS architectures. As a core infrastructure component, AD DNS must be strongly protected and never be exposed externally.

- » **Centralized orchestration:** Hybrid and multicloud architectures require centralized orchestration of DNS services via an overlay-based, multi-vendor DNS management approach. Introducing a unified control plane above multiple DNS platforms enables API-driven automation, record synchronization across vendors, and policy standardization. This approach preserves flexibility across heterogeneous environments, reduces vendor lock-in, and simplifies cloud migrations while maintaining consistency and auditability.
- » **Geographic resilience:** For organizations operating across multiple countries and verticals (e.g., ecommerce, financial services, and gaming) or organizations operating critical infrastructure, DNS architecture must also address geographic resilience. In this context, anycast DNS significantly enhances availability and fault tolerance. It simplifies configuration by reducing the number of resolver addresses to be managed, enables automatic failover to improve uptime, and strengthens DDoS resilience by dispersing attack traffic across multiple locations.

### 3. Data, observability, and automation

Full-stack DNS visibility is mandatory. Without end-to-end visibility, DNS becomes blind and difficult to manage. This visibility must span the security layer (threat detection, filtering, anomaly detection), the authoritative and recursive resolution layers, and the control plane, including configuration changes and API activity. However, data consistency and quality present critical challenges in hybrid and multicloud models. DNS data must be standardized through strict naming conventions, regularly assessed for integrity, and continuously cleaned to eliminate unused records.

Because DNS directly affects application availability and user experience, monitoring must extend beyond traditional infrastructure indicators. Observability should align with business and application SLAs, focusing on resolution time, TTL strategy, failover convergence, and end-user latency. DNS performance and security indicators must be assessed together, since resolution anomalies often result in degraded application performance or increased exposure to threats.

At the governance level, fragmentation remains a major operational and security risk. Every DNS record must be documented with a defined life cycle and a clearly defined owner. However, manual life-cycle management is no longer sustainable in fast-changing multicloud environments. Therefore, DNS must be integrated into automation frameworks and CI/CD pipelines for automatic provisioning, change management, and decommissioning.

### Best practices

DNS modernization initiatives must align with business objectives rather than being treated as purely technical upgrades. Accordingly, DNS should be architected by design for resilience, security, performance, and scalability, ensuring strong security and compliance controls and an optimized user experience.

1. **Form a DNS steering committee:** Organizations should establish a cross-functional DNS steering group comprising representatives from networking, IT operations, cloud/platform teams, and security. The group would be responsible for defining standards, approving architectures, and management principles. This ensures alignment between business outcomes and technological evolution while establishing a defined set of measurable KPIs to track progress and business value. These KPIs should combine the following indicators:
  - » **Technical indicators:** Mean time to repair/recover/restore (MTTR), query resolution latency, and change deployment success rates



- » **Business indicators:** Service impact on customer experience, operational efficiency gains, and contribution to digital transformation initiatives
- 2. **Anchor modernization in core principles:** Not all organizations are equal in terms of DNS modernization. Legacy environments may require structural redesigns and governance resets, while cloud-native deployments often need incremental optimization. Regardless of maturity, modernization should follow these core principles:
  - » **Enforce strict role separation:** Separate authoritative and recursive DNS, and internal and external name resolution, to strengthen security and improve operations.
  - » **Centralize management:** Standardize visibility, analytics, and control across heterogeneous, multi-vendor environments via a unified overlay approach, enabling consistent governance in hybrid and multicloud environments.
  - » **Maintain a Network Source of Truth (NSoT):** Maintain a continuously updated and reliable NSoT to ensure DNS reflects the intended infrastructure state.
  - » **Automate with guardrails:** Automate configuration, service discovery, and policy enforcement with embedded guardrails to reduce human error and configuration drift.
  - » **Adopt a DDI platform approach:** Leverage DDI platform capabilities for unified management, IP/DNS consistency, IPAM and built-in NSoT asset data and metadata, integrated DNS security, and intelligent traffic steering (e.g., Anycast routing) across on-premises and cloud deployments.
  - » **Centralize and integrate DNS telemetry:** Feed DNS telemetry into security monitoring (SIEM/SOAR) and operational workflows to enable proactive detection and faster incident response.
  - » **Balance autonomy and control:** Strike the right balance between team autonomy and centralized control, allowing delegated operations within clearly defined governance frameworks to maintain agility without compromising security or consistency.
- 3. **Continuously evaluate:** Organizations must evaluate their DNS capabilities continuously to determine which functions should remain in-house and which should be delegated to external providers. This evaluation should consider the level of specialized expertise required, the operational effort needed to maintain reliability and scalability, and the overall risk profile associated with availability, security, and compliance.
- 4. **Future-proof DNS:** Finally, organizations must maintain a comprehensive, forward-looking view of emerging risks and disruptive technologies that may impact DNS in the medium- to long term, including quantum computing, which could weaken DNSSEC because it relies on public key cryptography. This outlook must also cover operational technology (OT) environments, which are typically fully separated and built on different, resource-constrained components. Adding DNSSEC validation and encrypted DNS can overwhelm simple devices such as sensors. Organizations must plan for OT-specific DNS designs (including isolation where appropriate) and engage vendors on upgrade paths and device capabilities.

## ***Vendor profile: EfficientIP***

EfficientIP is a global provider of DDI-based network automation, security, and observability solutions for enterprises operating distributed, hybrid, and multicloud environments. Its portfolio covering DNS, DHCP, and IP address management serves as a foundation for modern digital infrastructure, simplifying operations while supporting centralized governance, automation, and visibility across heterogeneous environments.

With operations across the Americas, EMEA, and APAC and a partner-led go-to-market model, EfficientIP addresses organizations managing multi-vendor network infrastructures with availability, performance, and security requirements. The company has more than two decades of experience in DNS architecture design and DDI deployment in complex environments.

The core of EfficientIP's portfolio is the SOLIDserver platform, which provides centralized management capabilities for DNS, DHCP, and IP address services across on-premises and public cloud environments. The platform supports DNS analytics and observability, multi-vendor DNS and DHCP management, and API-driven automation for integration with external IT and security workflows.

Security capabilities include Protective DNS functions, DNSSEC support, zero trust, and hybrid DNS technologies. The platform also incorporates network discovery and Network Source of Truth functionality to help organizations align intended and actual network configurations.

For performance and service continuity, EfficientIP provides DNS-based global server load balancing to enable multi-regional application delivery and disaster recovery strategies. Integration with cloud platforms and security ecosystems is supported through APIs and connectors.

Through this portfolio, EfficientIP supports enterprise DNS modernization initiatives, improving operational visibility, automation, and policy consistency across hybrid and multicloud environments.

## ***IDC recommendations and market challenges for EfficientIP***

As DNS modernization becomes more strategic, EfficientIP's success will depend on its ability to translate technical capabilities into measurable business outcomes. Organizations expect evidence of reduced outages, improved resilience, faster incident response, and lower operational risk. Demonstrating this value beyond traditional DNS metrics will be essential to expanding influence at the enterprise level.

Adoption must also extend beyond networking teams. In many organizations, DNS is still managed in siloed structures, limiting visibility and coordination with security and operations functions. Aligning DNS and DDI capabilities with cross-functional workflows, governance models, and shared operational objectives will be critical to unlocking full value.

At the same time, EfficientIP must continue to elevate the role of DNS and DDI in modern IT architectures. As automation, zero trust models, and AI-driven network operations expand, DNS becomes a foundational control and enablement layer. Positioning DNS modernization as a strategic architectural capability, rather than a specialized infrastructure upgrade, will be key to sustaining relevance and growth in hybrid and multicloud environments.

## ***Conclusion: DNS modernization is the foundation of resilient, secure, and high - performance digital operations***

DNS modernization is foundational to resilient, secure, and high-performing digital operations. As organizations operate across increasingly distributed, hybrid, and multicloud environments, DNS has evolved from a background utility into a systemic dependency that underpins availability, security, and performance. Modernizing DNS infrastructure enables enterprises to reduce operational complexity while strengthening their ability to support business-critical applications and digital services at scale.

Modern DNS architectures deliver both strategic and operational advantages. From a resilience perspective, modernization reduces downtime and strengthens service continuity through automation, architectural separation of functions, and robust failover mechanisms. In distributed environments where applications and users are globally dispersed, DNS performance directly affects user experience. Optimized resolution paths, intelligent caching strategies, and traffic steering capabilities contribute to faster application access and consistent performance.

Security considerations are equally central. Embedding mechanisms such as DNSSEC, encryption, segmentation, and enhanced telemetry into DNS workflows improves protection against evolving threats while supporting governance and compliance requirements. As organizations adopt zero trust principles and expand digital ecosystems, DNS serves as an early control point for detecting anomalous activity and enforcing policy boundaries.

Operational efficiency is another key outcome of modernization. Managing heterogeneous, multi-vendor DNS environments through centralized governance and automation reduces manual intervention and configuration drift. Integration with broader IT and security workflows enables DNS to participate in automated change cycles, improving agility while maintaining control. By fully integrating DNS into DevOps and CI/CD pipelines, organizations can automate resource provisioning, ensure consistency across hybrid environments, and accelerate application deployment, further reducing operational overhead and minimizing service disruption.

Looking ahead, a modern DNS foundation positions organizations to support emerging requirements, including AI-driven automation, distributed application architectures, and evolving cryptographic standards. As environments become more dynamic and automated, treating DNS as critical infrastructure rather than background plumbing is essential to meeting both technical and business expectations.

IDC anticipates that demand for scalable, automated, and security-aware DNS capabilities will continue to grow as hybrid and multicloud complexity increases. Vendors that provide centralized governance, automation, and cross-domain visibility are best positioned to address evolving enterprise requirements. In this context, EfficientIP offers a strategic opportunity for organizations seeking to modernize DNS as a unified control layer within distributed digital infrastructures.

## About the Analysts



***Bruno Teyton, Associate Vice President, Network Infrastructure and Services***

Bruno Teyton is Associate Vice President within IDC's enterprise infrastructure global research domain. He leads EMEA Network and Life-Cycle Services research as part of the Network Infrastructure and Services subdomain. Bruno's research covers both network infrastructure (WLAN, SD-WAN, routers, and switches) and associated services (consulting and integration, maintenance, and managed services). It also covers networking for AI, network automation, network modernization across datacenter and campus networks, and new business models such as networking as a service. At the worldwide level, Bruno focuses on optical technologies spanning enterprise and service provider network environments.



***Romain Fouchereau, Senior Research Manager, European Security***

As senior research manager for IDC's European Security group, Romain has a specific focus on network security and the security technologies linked to the extended enterprise, such as IoT, edge, and IT/OT convergence. He closely monitors the development, evolution, and penetration of these technologies and the approaches vendors are taking to stimulate adoption at both the channel and end-user levels.

Romain manages the IDC security appliance market tracker for Europe, which provides market size, vendor share, and forecasts for network security products such as unified threat management (UTM), firewall, IDP, and content management (web and messaging) appliances.

Romain also co-leads the European Future of Operations practice, looking at the shift in operational mindset for European organizations to a market-driven outlook that leverages digital capabilities to build a resilient organization. Romain has a specific interest in the role of security as a business enabler for IT/OT integration strategies.

Romain joined IDC from a manufacturing industry company, where he specialized in market research consultancy. Within this role, he handled go-to-market projects for a variety of products and vendors, focusing on the French and Italian markets.

## MESSAGE FROM THE SPONSOR

Effective DNS modernization is critical to support resilient, secure, and high-performing hybrid and multicloud infrastructures. Overlay-based management of multivendor DNS services allows organizations to maintain consistent governance, visibility, and policy enforcement across hybrid and multicloud infrastructures, while reducing operational complexity and configuration drift. Best practices also include separating authoritative and recursive roles, implementing intelligent traffic management, maintaining a reliable network source of truth, embedding DNS in automated workflows, and integrating DNS telemetry into operational and security processes.

By following these principles, enterprises can improve operational efficiency, accelerate service delivery, future-proof DNS against emerging risks, and strengthen resilience across dynamic IT environments.

For more information on implementing these best practices and exploring DDI-based solutions for hybrid and multicloud DNS modernization, visit [www.efficientip.com](http://www.efficientip.com)



The content in this paper was adapted from existing IDC research published on [www.idc.com](http://www.idc.com).

**IDC Research, Inc.**  
One Beacon Street  
Suite 33100  
Boston, MA 02108, USA  
T 508.872.8200  
F 508.935.4015  
[blogs.idc.com](http://blogs.idc.com)  
[www.idc.com](http://www.idc.com)

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2026 IDC. Reproduction is forbidden unless authorized. All rights reserved. [CCPA](#)