efficient iP®

Solution Paper

Modernizing DNS with SOLIDserver™ for Resilient, Secure, and High-Performance Hybrid Multicloud Environments

How Intelligent DNS Architecture and Automation Drive Business Continuity, Security, and Operational Efficiency

Core SOLIDserver™ Platform Capabilities:

- **Unified Multi-Vendor Overlay:** A single control plane across on-premises, cloud, and hybrid DNS environments eliminating silos, reducing configuration drift, and restoring operational visibility at scale
- **Automation-First Architecture:** API-driven, zero-touch provisioning that reduces manual errors and integrates seamlessly into CI/CD and DevOps pipelines
- **Built-in Network Source of Truth (NSoT)**: DDI-enabled extended NSoT with IPAM at its core unlocking scalable automation and enforcing governance across distributed environments
- **Engineered Resilience:** Automated SmartArchitecture™ deployments and high-availability and performance capacity ensuring continuous DNS uptime
- **Intelligent Traffic Management:** Dynamic traffic steering with Edge DNS GSLB to optimize application performance and availability
- **Security by Design:** Built-in threat protection, detection, and response preserving DNS service continuity, even during extreme attacks

efficientip.com

Why DNS Modernization Is Now a Business Imperative

DNS has evolved far beyond basic name resolution. It now operates as a strategic control plane that underpins application availability, user experience, and overall security posture. Yet most organizations are managing it with architectures designed for a simpler era: before hybrid cloud, before DevOps at scale, and before AI-driven threats. The result is a widening gap between what modern digital operations demand and what legacy DNS can deliver. These systems lack the scalability, automation, and governance required for hybrid and multicloud environments, creating operational silos and increasing risk exposure.

Recent IDC findings highlight how legacy DNS introduces significant business risks across three fronts:

- **Multicloud Complexity and Tooling Fragmentation:** Hybrid cloud adoption means every provider brings its own DNS services, APIs, and operational models. IDC data shows that most enterprises run several cloud DNS platforms in parallel. This fragmentation leads to configuration drift, overlapping private zones, and inconsistent policy enforcement. Without a centralized overlay, IT teams operate across disconnected systems, creating blind spots that increase the likelihood of routing errors, degraded performance, and service disruptions.
- **Organizational Friction and the IT Skills Gap:** Tooling fragmentation is compounded by fragmented ownership. With networking, cloud, and security teams each managing their own DNS domains, coordination becomes a bottleneck. IDC data reinforces this: only **28% of EMEA enterprises have fully integrated security and networking teams** (2025 data), **with 20% citing lack of operational skills as a core challenge**. As a result, organizations rely heavily on manual processes, slowing modernization efforts, increasing the risk of human error, and creating bottlenecks for DevOps and automation initiatives.
- **The AI-Driven Threat Landscape and Data Silos:** Organizations that treat DNS as passive infrastructure are operating without one of their most effective security controls. Threat actors now use AI to generate credible malicious domains and dynamically evade detection, making DNS hijacking, data exfiltration, and DDoS campaigns faster and harder to catch. When DNS telemetry is fragmented across logging silos, teams lose the visibility needed to correlate signals and respond before damage is done.

The Cost of Legacy DNS

The operational friction IDC identifies doesn't stay in IT. It cascades directly to the bottom line. Maintaining legacy DNS is no longer a technical compromise; it is an active, compounding business risk.

When foundational infrastructure such as DNS fails to scale with modern demands, the consequences cascade across the organization:

- **Delayed Time-to-Market:** Manual DNS provisioning generates friction at every stage of deployment. Without API-driven automation, network teams become a bottleneck that stalls DevOps pipelines, delays critical application rollouts, and slows the pace of innovation.
- **Escalating Operational Costs (OpEx):** Manual management of DNS across spreadsheets and fragmented cloud interfaces consumes valuable engineering resources. The absence of centralized control increases configuration drift and operational overhead, limiting the ability of IT teams to focus on strategic initiatives.
- **Financial and Reputational Damage from Breaches:** Legacy DNS systems often lack built-in security and visibility. This makes them more vulnerable to attacks such as DNS hijacking, data exfiltration, and DDoS. A successful breach carries consequences well beyond the technical response: regulatory fines, customer churn, and lasting brand damage.
- **Lost Revenue from Poor User Experiences:** DNS is the first step in every digital interaction. Inefficient routing and high latency directly impact application performance. For digital businesses, even small delays can result in reduced engagement, abandoned transactions, and lost revenue.
- **The Ultimate Cost ➔ Service Outages:** Over time, configuration drift, manual errors, and unresolved vulnerabilities increase the likelihood of outages. When DNS fails, applications become inaccessible. Productivity halts. Revenue stops.

Every DNS failure is a business failure that impacts revenue, reputation, and customer trust.

Introducing EfficientIP SOLIDserver™: A Unified Approach to DNS Modernization

IDC is clear about what modern DNS must deliver: security by design, resilient and scalable architecture, centralized orchestration, operational simplicity, and full-stack visibility.

Meeting these needs, especially across hybrid and multicloud environments, demands more than incremental upgrades. It requires a fundamental shift toward a unified, automated, and centrally governed DNS architecture.

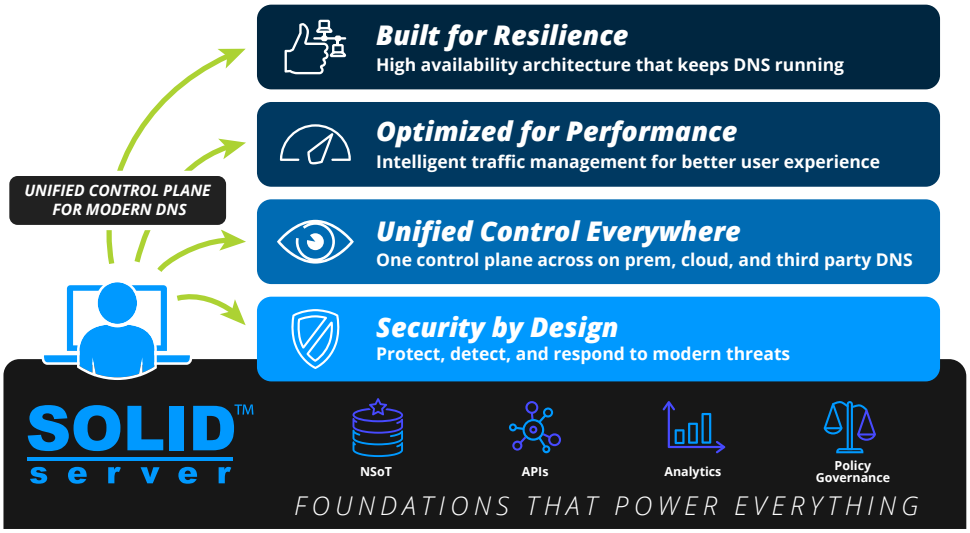
Recognized as a DDI leader for hybrid and multicloud environments, EfficientIP enables this transformation. Through the SOLIDserver platform, EfficientIP delivers integrated DNS, DHCP, and IPAM (DDI) services that directly align with IDC's blueprint for modernization. The platform is purpose-built to reduce complexity, improve resilience, and strengthen security across distributed environments. It is structured around four key pillars:

- **Resilient and Scalable Architecture:** Engineered for high availability, SOLIDserver supports geographic distribution and automated failover mechanisms to ensure continuous service delivery. Built-in Service Virtual IP (VIP) and IP Anycast DNS access enhance availability and mitigate DDoS impact, while automated deployment of hidden primary (stealth) DNS architectures protects sensitive infrastructure from public exposure.
- **Centralized Orchestration & Operational Simplicity:** SOLIDserver provides a unified control plane for seamless overlay management across multi-vendor and multicloud DNS environments. By centralizing control across heterogeneous infrastructures, organizations can standardize lifecycle management, ensure consistent policies, significantly reduce manual processes, and eliminate configuration drift, thus improving both operational efficiency and governance.

EfficientIP transforms DNS into a unified control layer for hybrid and multicloud infrastructure.

- **Data, Visibility, and Automation:** As an API-first platform, SOLIDserver centralizes comprehensive and up-to-date data in a Network Source of Truth - with IPAM at its core - to create an authoritative inventory that enables deep integration across the IT ecosystem and API-driven automation for CI/CD pipelines. It also delivers comprehensive DNS observability and exports actionable telemetry to SIEM and SOAR platforms, accelerating threat detection and enabling faster, coordinated response.
- **Security by Design:** EfficientIP elevates DNS to the network's first line of defense. The platform enforces strict separation of authoritative and recursive roles, natively supports DNSSEC and advanced encryption (DoH/DoT), and integrates seamlessly into Zero Trust frameworks, thus ensuring data integrity and reducing the attack surface.

EfficientIP SOLIDserver Capabilities



SOLIDserver unified control plane for resilience, performance, control, and security

Architectural High Availability and Resilience

According to IDC, modern DNS should be designed around centralized orchestration and clear role separation, so that recovery follows a defined architectural pattern instead of manual rebuilding under pressure. SOLIDserver SmartArchitecture™ supports this approach by automating proven DNS deployment patterns such as

- Primary-Secondary: at least one primary and one secondary servers
- Stealth: one hidden-primary plus secondary servers, with one used as pseudo-primary
- Multi-Primary: two or more primary servers authoritative for the same zone
- Farm: primary and secondary servers potentially behind a load balancer

where organizations have to manage DNS across Microsoft, free and Open Source Software (such as BIND, NSD or Unbound), and cloud-based DNS services, along with AWS Route 53, Google Cloud DNS, and Azure DNS as typical examples.

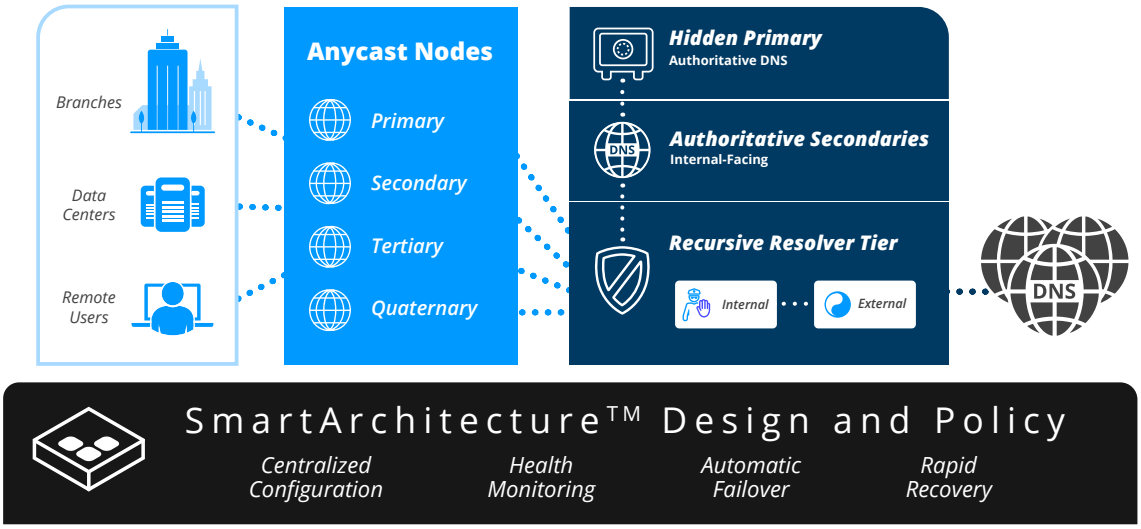
By standardizing these architectures through policy-driven templates, **SOLIDserver SmartArchitecture™** reduces manual configuration effort, limits drift, and helps customers implement resilience as part of the design rather than as an operational afterthought.

This availability-oriented model continues after go-live through centralized DNS configuration management and multi-vendor disaster recovery. If a managed DNS server fails, **SOLIDserver** can rapidly reapply the saved configuration to a replacement system, reducing downtime and restoring service in a controlled way. For DNS service continuity, **SOLIDserver** also supports VIP-based failover, allowing a standby node to take over the shared service IP transparently if the active node becomes unavailable. In addition, **SmartArchitecture** supports flexible evolution of the DNS design over time, helping organizations adapt high-availability architectures to changing requirements without disruptive manual rework.

For highly-available DNS recursive services, a simple and easy-to-implement approach is to use a Service VIP. This provides clients with a single, consistent connection point to the DNS service, instead of requiring them to connect directly to the physical IP address of a specific appliance. In addition, to provide even more service continuity and scalability, the use of IP Anycast DNS access strengthens geographic resilience by directing traffic to the nearest available node.

For externally exposed authoritative DNS, stealth SmartArchitecture helps reduce attack surface by keeping the hidden primary out of public NS records.

In that sense, resilience is engineered directly into the DNS architecture through centralized control, secure role allocation, and repeatable recovery.

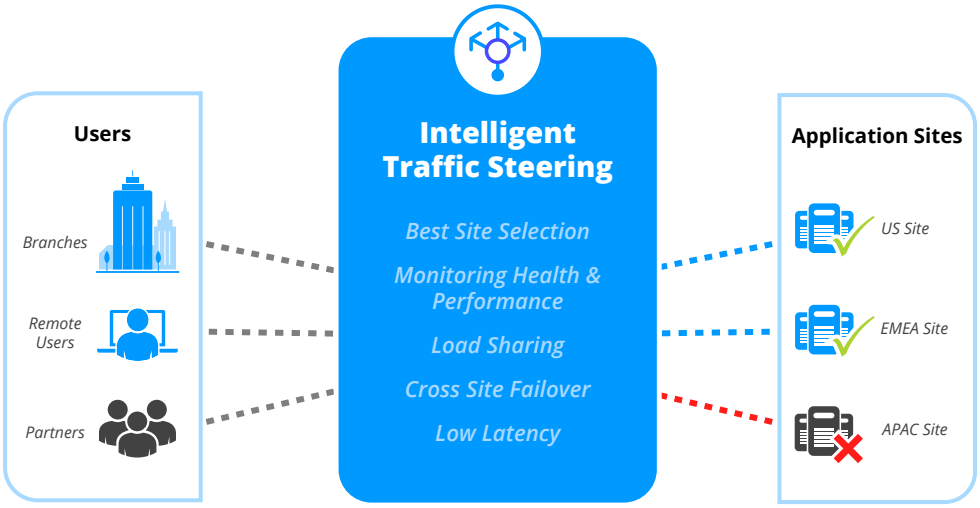


SOLIDserver SmartArchitecture for High Availability and Resilience

Performance Optimization and Traffic Management

IDC highlights that DNS performance has a direct influence on digital experience, application responsiveness, and service continuity. **SOLIDserver** addresses this through DNS-based traffic management capabilities, including edge DNS Global Server Load Balancing (DNS **GSLB**), which allow organizations to steer users across sites and regions toward the closest or best-performing application endpoint. This supports intelligent traffic steering and cross-site continuity when an application stack or regional service becomes unavailable. Rather than treating DNS as a passive lookup function, **SOLIDserver** turns it into an active control point for improving application delivery and availability in distributed hybrid and multicloud environments.

Beyond query resolution performance, edge DNS **GSLB** extends **SOLIDserver** with DNS-based application traffic control across distributed environments. It supports disaster-recovery planning by predefining primary and backup application nodes behind the same FQDN and enabling manual, orchestrated, or automatic switchover to a backup site when needed. It also improves multi-data center traffic distribution by steering users toward the most appropriate application endpoint based on health checks, latency, and service availability as seen from the edge of the network, closer to the user. This allows organizations not only to improve user experience, but also to simplify cross-site failover, increase datacenter agility, and make DNS an active part of service continuity and traffic-routing strategy.



SOLIDserver Intelligent Application Traffic Management

Performance optimization also depends on visibility. IDC stresses that DNS observability must cover not only infrastructure status but also latency, service continuity behavior, and end-user impact. **DDI Observability Center** complements **SOLIDserver** by providing cloud-based analytics and near-real-time visibility into DNS performance, traffic behavior, errors, and service health across distributed environments. This helps NetOps and NOC teams detect bottlenecks faster, validate policy changes, and improve resolution quality over time. From a business perspective, DNS performance is more than a technical measure and directly shapes application experience and service reliability.

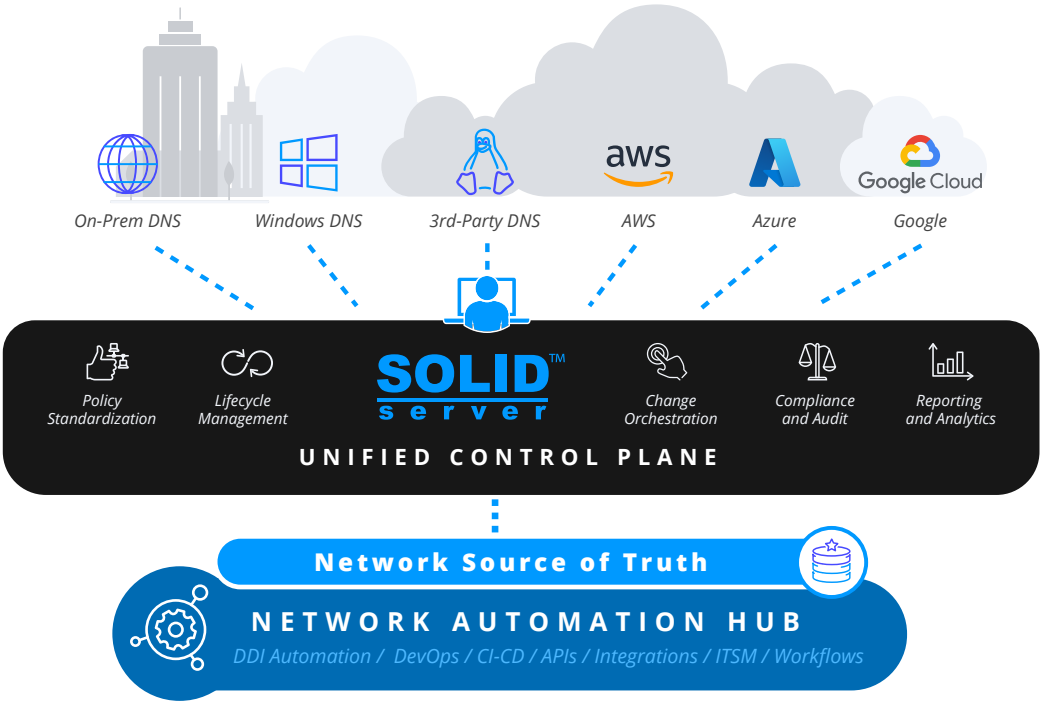
Unified Control Across Hybrid and Multi-Cloud DNS

To reduce tooling fragmentation, inconsistent governance, and operational silos, organizations need centralized, overlay-based approach for DNS management across hybrid and multicloud environments. **SOLIDserver** is well aligned with that requirement through its unified multi-vendor DNS overlay management across on-premises, Microsoft, Open Source, and cloud-based DNS environments, including providers such as AWS Route 53, Google Cloud DNS, and Azure DNS.

This allows enterprises to preserve existing investments while applying consistent governance, visibility, and operational control across heterogeneous DNS estates. As DNS complexity grows across platforms and teams, this unified control plane becomes essential to reducing fragmentation, change risk, and policy inconsistency.

In addition, modern DNS should be anchored in a Network Source of Truth (**NSoT**) and embedded in automated workflows. **SOLIDserver** enables this through its API-first platform model and by integrating DNS, DHCP, and IPAM data into a centralized, authoritative inventory that drives visibility, governance, and automation.

With built-in asset discovery across environments, organizations can continuously align intended state and operational state while integrating DNS into **DevOps** pipelines and broader IT processes. As a result, DNS is no longer a siloed infrastructure service. With **SOLIDserver**, it becomes a governed, policy-driven control layer enabling visibility, compliance, and automation across hybrid and multicloud DNS environments.



SOLIDserver unified control plane for multi-vendor DNS overlay management, visibility, governance, and automation

Advanced Security & Threat Mitigation

As emphasized by IDC, DNS security must be built-in from the beginning. **SOLIDserver** supports this principle through architectural role separation, stealth DNS designs, **DNSSEC**, and **Hybrid DNS Service**, helping customers strengthen integrity, reduce exposure, and avoid the risks of overly uniform DNS environments.

On top of that foundation, **DNS Guardian** adds centralized DNS security policies and **Client Query Filtering**, enabling highly granular DNS controls based on client identity, IP address, MAC address, tags, domains, and actions. This supports segmentation and **Zero-Trust** enforcement directly at the DNS layer, which aligns closely with IDC's recommendation to treat DNS as a control point rather than a background utility.

DNS Threat Pulse further enhances protection through a real-time, AI-driven threat intelligence feed that analyzes multi-source domain data to identify malicious, suspicious, and emerging threats. This enables organizations to proactively block threats such as malware, DGA, phishing, DNS tunneling, and unauthorized encrypted DNS activity before they cause harm.

For detection and continuity under attack, **DNS Guardian** uses **DNS Transaction Inspection** and **User Behavioral Analysis** to identify tunneling, data exfiltration, phantom domains, random subdomain attacks, and other low-noise threats in real time. **Rescue Mode** helps maintain DNS continuity during recursive saturation or attack conditions, while **DNS Blast** provides high-performance caching at up to 17 million queries per second to absorb extreme query loads and preserve service availability. **DNS Intelligence Center** adds contextual investigation and faster adaptive response. Together, **SOLIDserver**, **DNS Guardian**, **DNS Blast**, **DNS Threat Pulse** and **DNS Intelligence Center** support the outcomes IDC sees as essential for modern DNS security, namely preserving DNS service continuity while improving visibility, control, and threat response.

Deliver Measurable Business Outcomes with EfficientIP SOLIDserver

The case for DNS modernization is not theoretical. Modernizing DNS with EfficientIP SOLIDserver transforms network infrastructure from a reactive cost center into a strategic enabler of business agility, resilience, and security.

Organizations that have deployed EfficientIP SOLIDserver report measurable improvements across operations, security posture, and financial performance, outcomes that extend well beyond IT.

Operational Impact: Accelerate MTTR and Unlock Agility

Legacy and manual processes drain expensive IT resources, introduce delays, and increase the risk of human error.

With centralized visibility and API-driven automation, EfficientIP streamlines DNS operations, reduces configuration errors, and accelerates incident response. This unified approach significantly improves Mean Time to Resolution (MTTR) and enables faster, more agile service delivery.

MetaX (Technology Sector): 80% Faster, Zero Configuration Errors: By replacing manual Microsoft DNS management with EfficientIP's integrated DDI platform and Edge DNS GSLB, MetaX cut administrative workload by **80%**. This shift eliminated configuration errors and delivered measurable improvements in application availability and business resilience.

Société Générale (Financial Services): 10x Faster. Sub-Minute RTO: To accelerate DevOps delivery, Société Générale automated its private cloud infrastructure using SOLIDserver DNS and APIs. As a result:

- API response times improved **5x**
- DNS propagation accelerated **10x**
- Recovery Time Objective (RTO) dropped from **2 hours to under 1 minute**

Security Impact: Ensure Service Continuity Under Attack

DNS is the most consistently exploited layer in enterprise infrastructure and among the least defended. EfficientIP addresses this directly. With built-in behavioral threat detection, Client Query Filtering (CQF), and adaptive countermeasures including Rescue Mode, the SOLIDserver platform identifies threats earlier in the attack lifecycle and maintains DNS service continuity even under large-scale or sophisticated DDoS conditions, without requiring bolt-on security tooling.

Roland-Garros - French Tennis Federation (FFT): 4–6x Faster Resolution. DNS as the First Line of Defense: During two weeks of Grand Slam competition, the FFT wanted to guarantee connectivity for 40 global TV stations, 2,000+ journalists, and 1,200 VIPs while managing thousands of unmanaged devices bringing unknown threats onto the network. By deploying DNS Blast and DNS Guardian, the FFT transformed DNS into an active defense layer: monitoring real-time traffic for volumetric attacks, cache poisoning, and data exfiltration, while absorbing extreme query loads up to **17M QPS**. DNS resolution times improved by **up to 6x at peak**, guaranteeing 100% service continuity across the entire tournament.

Financial Impact: Lower Costs and Protect Revenue

Automation reduces operational overhead and frees engineering teams to focus on higher-value work.

At the same time, improved DNS performance directly enhances application responsiveness that helps prevent revenue loss, customer churn, and reputational damage associated with outages or degraded user experiences.

FusionNet (ISP): 300% Faster Responses. Zero Outages: After deploying high-performance SOLIDserver DNS, FusionNet improved subscriber request response rates by over **300%**. DNS-related outages were eliminated, resulting in improved user experience and reduced customer churn.

From infrastructure efficiency to business resilience, DNS modernization with EfficientIP delivers measurable outcomes.

Why EfficientIP for DNS Modernization

Achieving these operational, security, and financial outcomes requires more than recognizing the need for change; it requires the right architectural approach.

When evaluating how to modernize critical network infrastructure, technical leaders face a choice: cobble together disparate cloud-native tools, rely on brittle manual workarounds, or adopt a purpose-built platform designed for hybrid and multicloud environments.

EfficientIP's SOLIDserver addresses the realities of modern IT and provides distinct advantages over alternative approaches:

Capability	Alternative Approach	EfficientIP Advantage
Unified DDI vs. fragmented tools	Disconnected DNS and DHCP point solutions and spreadsheet-based IPAM create operational blind spots and increase the risk of configuration errors.	SOLIDserver **unifies** DNS, DHCP, and IPAM (DDI) into a single management framework delivering **end-to-end visibility**, consistent configuration, and **centralized control** across the entire network.
Multi-Vendor Overlay Control vs. Cloud-Native Silos	Native DNS services from individual cloud providers introduce vendor lock-in and inconsistent policy enforcement across environments.	SOLIDserver provides a **unified, multi-vendor overlay** control plane that enables **operational consistency** and **governance** across on-premises, AWS Route 53, Google Cloud DNS and Azure DNS environments, without introducing vendor lock-in or sacrificing operational flexibility.
Built-in Security vs. Bolt-on Complexity	Retrofitting legacy DNS with external security tools increases architectural complexity and introduces latency.	EfficientIP embeds security directly into the DNS layer, delivering **native protection** without added complexity through hybrid DNS engines, built-in DNSSEC compliance, and **automated threat detection and mitigation**.
Automation-First Architecture vs. Manual Scripting	Manual configurations and ad hoc scripts are difficult to scale and prone to human error.	SOLIDserver's **API-first**, automation-driven architecture, leveraging **SmartArchitecture**, eliminates configuration drift, reduces provisioning errors, and integrates seamlessly into CI/CD pipelines **accelerating IT operations** and **removing manual processes** from the critical path.
Proven Resilience at Scale vs. Brittle Infrastructure	Traditional, fragmented DNS infrastructure struggles under high query volumes and volumetric attacks, increasing the risk of outages.	SOLIDserver is engineered for resilience at scale. With advanced Anycast capabilities and high-performance caching that can handle up to **17 million queries per second (QPS)**, the platform ensures **continuous service availability**, even under extreme conditions.

Not all DNS solutions are built for hybrid, multicloud reality; EfficientIP is.

From Legacy Liability to Strategic Foundation

The case for DNS modernization is no longer a future consideration. Across every dimension this paper has examined, from operational efficiency and security posture to resilience and business continuity, the evidence points to a single, urgent conclusion: fragmented, legacy DNS infrastructure is a liability that compounds over time, and the cost of deferring action is no longer theoretical.

EfficientIP is the partner for this modernization.

The **SOLIDserver** platform gives technical leaders a direct path to modernizing their network foundation, built around the three imperatives IDC identifies as non-negotiable for hybrid and multicloud environments:

- **Performance & Resilience by Design:** SOLIDserver ensures high-performing, always-on DNS services through SmartArchitecture™, intelligent application traffic management, and IP Anycast to ensure continuous service availability.
- **Centralization and Automation:** A single, multi-vendor control plane that eliminates tooling fragmentation and delivers complete visibility, while enabling API-driven, zero-touch provisioning that replaces error-prone manual processes and integrates natively into agile DevOps workflows.
- **Security-First Architecture:** DNS elevated from a passive utility to an active first line of defense, with built-in threat detection and uncompromised service continuity.

Purpose-built for this architectural reality, SOLIDserver does not patch around the limitations of legacy DNS; it unifies disjointed systems under a single, automated, secure, and resilient control plane.

The organizations best positioned for what comes next are not waiting for the next outage or breach to make the case internally. They are acting now.

Start Your DNS Modernization Journey

- See the SOLIDserver overlay architecture in action

Request a Live Demo

- Assess your DNS maturity and define your modernization roadmap

Schedule a Consultation

efficient iP®

REV: C-260325

As one of the world's fastest growing DDI vendors, EfficientIP helps organizations drive business efficiency through agile, secure and reliable network infrastructures. Our unified management framework for DNS-DHCP-IPAM (DDI) and network configurations ensures end-to-end visibility, consistency control and advanced automation. Additionally, our unique 360° DNS security solution protects data confidentiality and application access from anywhere at any time. Companies rely on us to help control the risks and reduce the complexity of challenges they face with modern key IT initiatives such as cloud applications, virtualization, and mobility. Institutions across a variety of industries and government sectors worldwide rely on our offerings to assure business continuity, reduce operating costs and increase the management efficiency of their network and security teams.

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