IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Prepared for:

BLUECAT™

DDI Maturity Drives Multi-Cloud Automation and Security

September 2022 EMA Research Report

By Shamus McGillicuddy, Vice President of Research

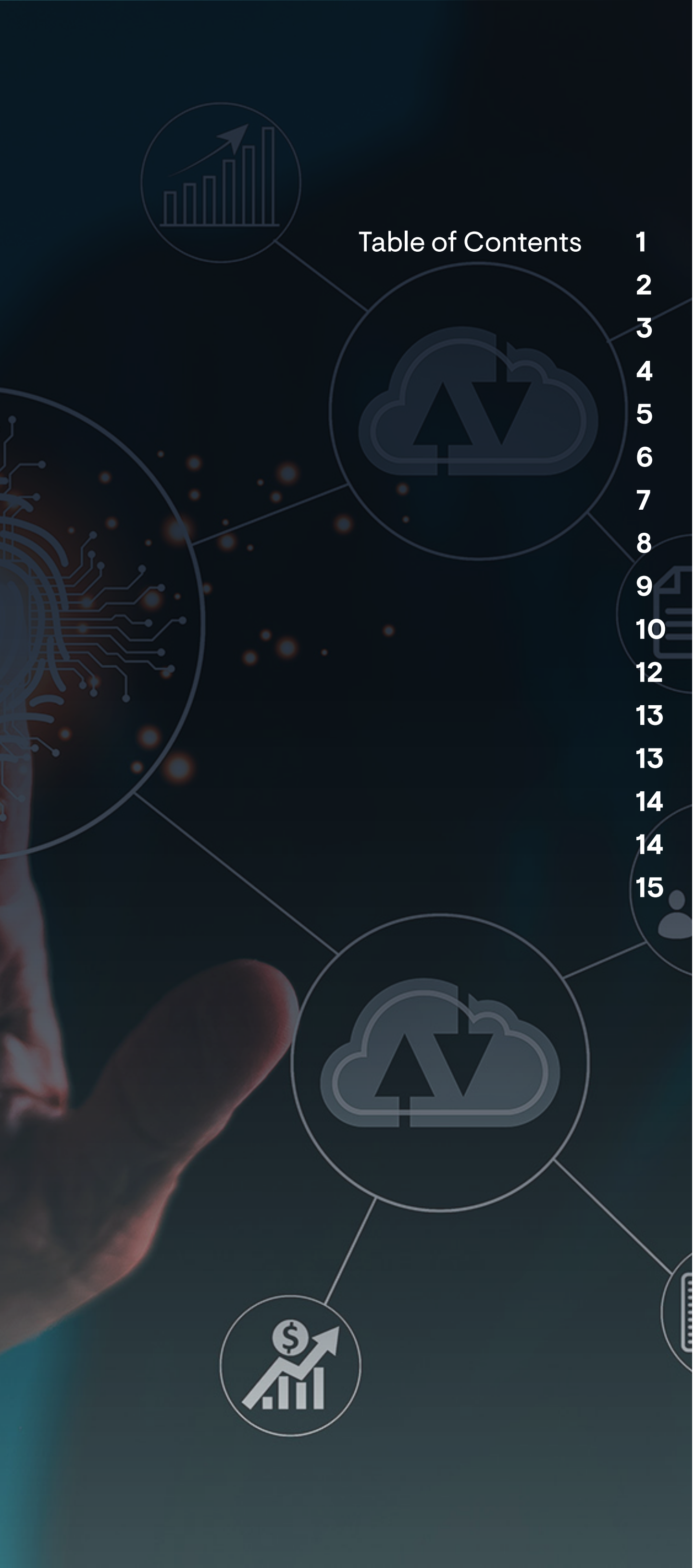

Table of Contents

Executive Summary

This research report explores the state of DDI (DNS, DHCP, and IP address management) maturity in enterprises. It examines the drivers of DDI maturity, and the best practices and challenges associated with the technology. Based on a survey of 227 IT professionals, EMA prepared this research for BlueCat, a provider of DDI solutions.

Why DDI Matters

DDI is an acronym that denotes the infrastructure and tools that provide the core services that enable network communications. It comprises DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), and IPAM (IP address management). DDI services are essential to routing traffic and establishing network connections.

In its interactions with IT organizations, EMA has determined that enterprises vary widely in their approach to DDI services. While commercial vendors offer full-stack solutions for these core network services, many IT organizations elect to take a less integrated approach. Some even rely on do-it-yourself (DIY) approaches using spreadsheets and open-source software.

This research explores the state of DDI maturity in enterprises today. EMA surveyed 227 IT professionals from medium and large enterprises across North America and the United Kingdom about the state of their DDI services. Nearly 67% of respondents were responsible for procuring, implementing, and/or managing DDI services on their networks. The rest provided executive leadership to the teams responsible for DDI services.

Solution Requirements

What are companies looking for in a DDI solution? **Figure 1** reveals the most critical requirements that companies have for DDI. Security functionality is the top priority. Examples of DNS functionality include support for secure DNS protocols, like DNSSEC. Some DDI vendors also offer advanced, protective capabilities like a DNS firewall, which filters and blocks malicious DNS activity. Organizations that use public cloud services were more interested in security functionality.

Cloud support is the secondary priority. This involves the ability to manage IP address space in cloud environments and the ability to deploy and manage DNS services for cloud applications and networks.

Ease of use, scalability, resiliency, and compliance are the other top requirements. Scalability is a higher priority for more mature organizations. A network engineer with a Fortune 500 aerospace and defense company explained to EMA how security functionality and resiliency overlap on his list of top priorities. “We need resiliency overall, and resiliency when it comes to denial of service attacks. We’ve had our share of attacks, especially on our external services. We need rich functionality for DDoS prevention and for self-repair.”

Ease of use was also a priority for a senior network engineer with a Fortune 500 company. “We need good role-based views into IPs and DNS. We also want RegEx search so we can find and sort things quickly for making network changes in a new warehouse, for instance.” This same engineer also pointed to the importance of integrations and scalable, comprehensive APIs, as well as strong customer support.

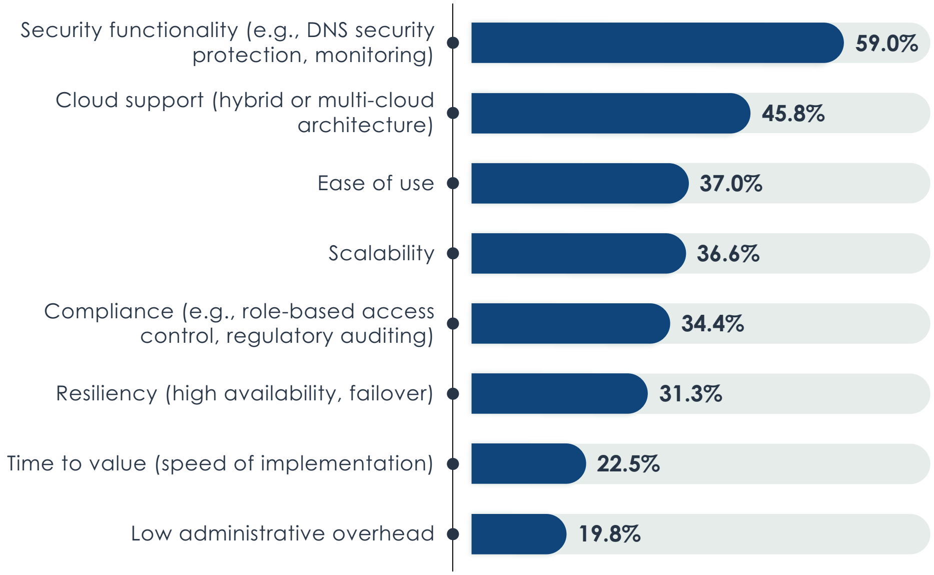

Figure 1. Most critical requirements for DDI solutions

Sample Size = 227, Valid Cases = 227, Total Mentions = 650

DDI Maturity

A Maturity Model

There are three states of maturity.

Stage 1 DIY. A DIY approach to DDI is the least mature strategy. It relies on spreadsheets or open-source software for IP address management and free or open-source software for DNS and DHCP servers. Some DIY organizations might also use commercial DNS solutions from cloud providers or content delivery network (CDN) providers, especially for external DNS services. Overall, DNS services in a DIY organization are fractured, with no central authority for domain name resolution. DIY solutions don't scale, particularly because they rely on manual administration. They are also error-prone and they are insecure, given their lack of role-based access controls.

"We had an unstable and difficult-to-manage legacy environment that was based on OpenDNS," said a network engineer with a Fortune 500 aerospace and defense company. "It was garbage."

"We had an unstable and difficult-to-manage legacy environment that was based on OpenDNS," said a network engineer with a Fortune 500 aerospace and defense company. "It was garbage. It was not centrally located. We had no single pane of glass view. It was all command-line. It was unstable and difficult to manage. Now, we have a [full-stack] DDI solution with centralized address management and DNS. It's reliable, scalable, and it just works, even with increased loads from external DNS attacks."

Stage 2 IPAM Overlay. This moderate maturity stage involves the use of a commercial IPAM tool that integrates with one or more third-party DNS services. IPAM establishes an overlay across the DNS servers. IPAM becomes the control plane for DNS, managing and monitoring changes and coordinating them with IP address space management. This approach is more secure and scalable than Stage 1, but there remain some challenges. For instance, third-party DNS services can present a security risk. Many IPAM overlay users rely on Microsoft DNS, a free service bundled with Active Directory. EMA found that 71% of IPAM overlay users who reported a technical issue with Microsoft DNS ended up experiencing a security breach as a result of that issue.

Furthermore, IPAM overlays may lack a unified approach to orchestrating and automating all third-party DNS services that an organization uses. An overlay may also struggle to extend third-party integrations to all the DNS services included in the overlay. For instance, due to limitations in an API, the overlay may fail to implement a change in a third-party DNS service requested via a ServiceNow ticket.

71% of IPAM overlay users who reported a technical issue with Microsoft DNS ended up experiencing a security breach as a result of that issue.

Stage 3 Full-Stack, DDI Management Platform. A full-stack DDI management platform is the most mature approach to the technology. It involves a fully integrated solution from a single vendor. This approach typically offers the best scalability, control, and security. Automation tends to work consistently across all layers of the DDI stack. This level of maturity can also consolidate costs since a single vendor bundles multiple technologies. Some organizations may find it difficult to reach Stage 3 because the overall IT infrastructure is decentralized, with no central authority responsible for architectural decisions. For instance, 56% of research respondents reported that their companies had adopted cloud services without the involvement of the IT organization. This so-called shadow IT activity virtually guarantees the persistence of third-party DNS services, which are usually native to the organization's chosen cloud provider.

A senior network engineer with a very large North American university that uses a full-stack DDI management platform explained to EMA why his network continues to use third-party DNS services. "We are very decentralized. We are the ISP for other units [who maintain their own DNS services]. We give them an internet connection and we offer DDI services, but those units don't have to use them. Even in our centralized organization, there is a data center team and a network team. The data center team uses their own IP address management system, but they use our DNS."

The State of DDI Maturity

Figure 2 reveals the state of DDI maturity. Only 3.5% of organizations in this survey take an immature DIY approach. EMA believes that DIY strategies are more prevalent in the broader IT market than indicated here. EMA specifically sought DDI subject matter experts within upper midmarket and large enterprises, where network complexity and scale drive a bias in favor of DDI maturity. Small and medium businesses are not included in this research. SMBs have less network complexity and are more likely to adopt immature DDI strategies.

Nearly 32% of respondent companies are at Stage 2 maturity, using a commercial IPAM solution that integrates third-party DNS services into an overlay. The majority, nearly 65%, are at Stage 3, using a full-stack DDI management platform. EMA suspects that Stage 2 maturity is more common and Stage 3 maturity is less common. Members of network engineering teams in the survey were more likely to report Stage 2 maturity, while people who worked in a CIO's office were more likely to report Stage 3 maturity. Network engineering teams are usually the true subject matter experts on DDI. The CIO's office has an awareness gap about the impact of third-party DNS persistence in their organizations.

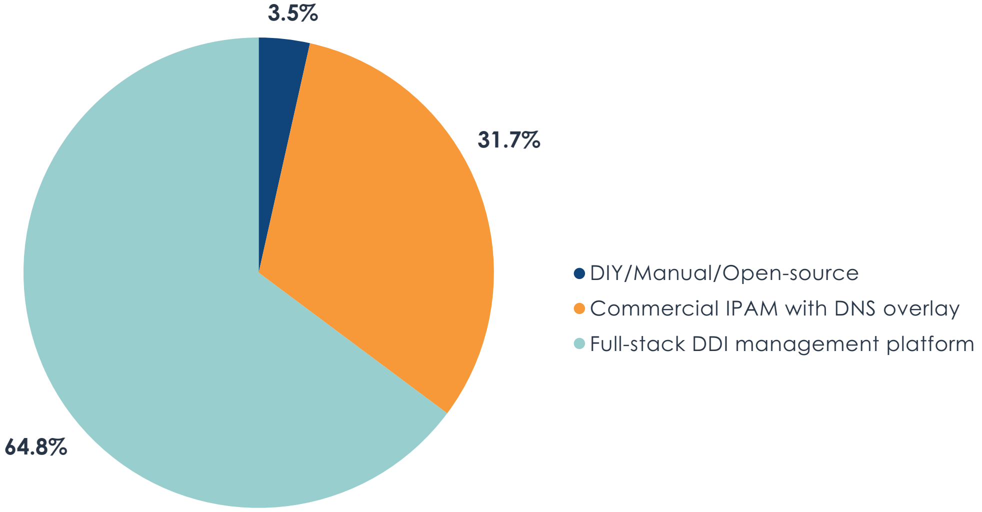

Figure 2. The state of DDI maturity

Sample Size = 227

DNS Diversity

Figure 3 reveals the types of DNS solutions that Stage 1 and Stage 2 organizations use. DIY organizations rely very heavily on free and bundled solutions, like Microsoft DNS. At Stage 2 maturity, organizations are using the native DNS services of their commercial DDI vendor, but they are also relying very heavily on cloud provider and CDN provider services. Neither group is a significant user of open-source DNS software, like BIND or OpenDNS.

The research found that enterprises struggle to manage both Microsoft DNS and open-source DNS. Users of both technologies identified security risk and operational complexity as their top two challenges.

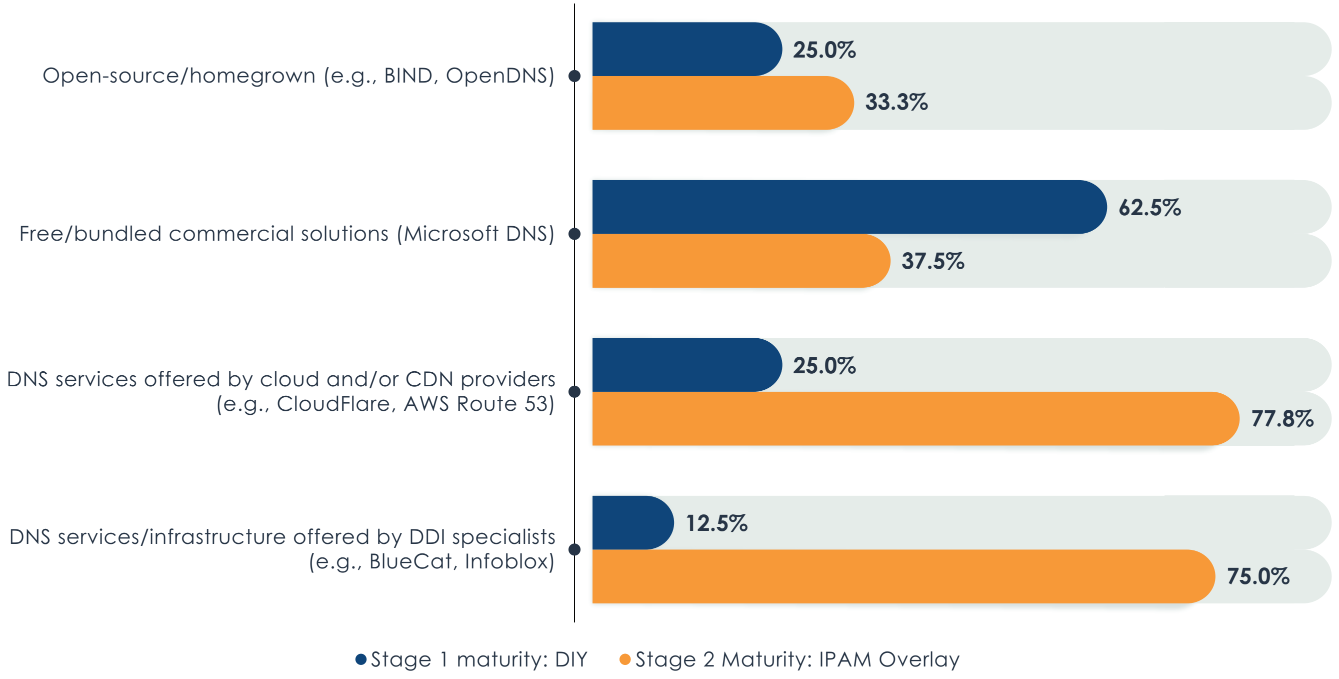

Figure 3. DNS services used by Stage 1 and Stage 2 organizations

Sample Size = 80, Valid Cases = 80, Total Mentions = 171

Benefits of DDI Maturity

52% of organizations cited network complexity as one of their biggest challenges to DDI management. A mature approach to DDI is essential to overcoming this complexity.

Enterprise networks are complex by nature. A large network will have multiple IP address schemas and multiple internal and external DNS services driven by network architecture, geography, business structure, and more. In fact, 52% of organizations cited network complexity as one of their biggest challenges to DDI management. A mature approach to DDI is essential to overcoming this complexity and enabling the business for digital transformation.

Enabling Cloud, Automation, and IoT

Public cloud and network/IT automation are the technology initiatives most responsible for driving of DDI maturity. **Figure 4** reveals that most organizations cited all as factors that led to their investment of time or money in DDI technology. The migration of applications to the cloud adds complexity because the network team loses centralized control over DDI services. A mature DDI solution with cloud support, especially support for multiple cloud providers, can help the network team retake control.

Network and IT automation initiatives usually aim to improve operational efficiency and compliance, neither of which are achievable without DDI services. For instance, when an automation tool instantiates a new virtual machine in a data center or a cloud environment, it will need to assign that server an IP address and domain name. Integration with a mature DDI solution facilitates more effective automation.

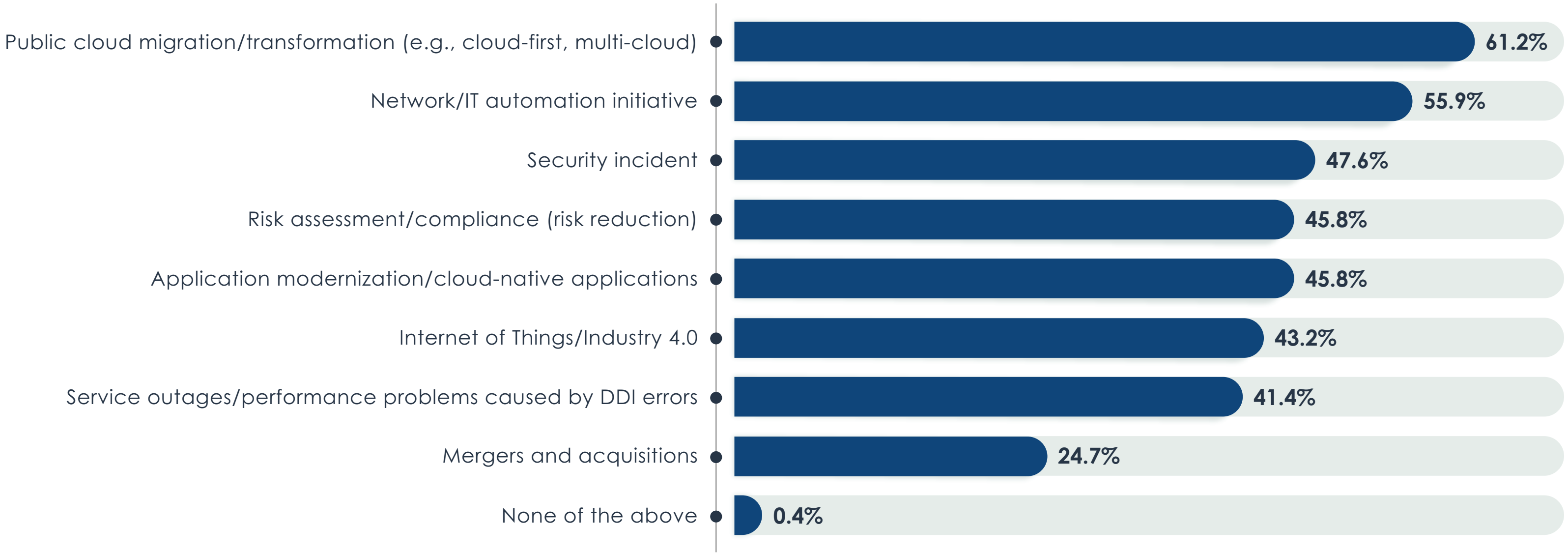

Figure 4. Factors that have driven an investment of time and/or money in DDI technology

Sample Size = 227, Valid Cases = 227, Total Mentions = 831

"We wanted to create network automation," said a senior network engineer with a Fortune 500 retail company. "We had too many things we were doing manually with our small staff. We were spending an hour a day just doing DNS entries. Now, we have ServiceNow integration. You can open a DNS ticket and it automatically generates a DNS request and a DNS update [in our DDI management platform]. We are trying to automate more mundane tasks in DDI so our engineering team can focus on more important things."

Most other drivers of maturity detailed in Figure 4 are secondary. However, research respondents who told EMA that they are the most successful with DDI technology were more likely to single out another important driver: the Internet of Things (58.7%). Many industries are connecting sensors, cameras, and other wireless devices for their business operations in the growing IoT ecosystem. These endpoints often have no individual user associated, so identity can't be relied upon for access control. IP address management can serve as an important foundation of IoT network segmentation.

The Transition From DIY to Commercial Solutions

A key inflection point for DDI maturity is the shift from DIY to commercial, enterprise-grade technology. EMA's research revealed four key drivers of this shift.

Security Requirements

First, 63.5% of research participants cited security requirements as their motivation for maturing their approach to DDI by investing in a commercial product. Commercial DDI products offer robust administrative security capabilities, such as role-based access control. Moreover, DNS services have become a popular target for malicious activity. DDI vendors are increasingly adding security features and additional security products to address this trend. In fact, 77.5% of research participants reported that they are using a DNS security solution, such as DNS firewall or DNS DDoS protection.

"We need to make DNS more secure. We don't have a DNS security solution yet. We're looking at buying it if we have the budget," said a senior network engineer with a Fortune 500 retail company.

63.5% of research participants cited security requirements as their motivation for maturing their approach to DDI by investing in a commercial product.

Cloud Transformation

Nearly 51% of respondents cited cloud complexity as a trigger for commercial DDI investment. As a network engineer with a Fortune 500 aerospace and defense company told EMA, "We'd like increased cloud integration. We've been resisting the cloud, but we can't anymore. Our organization is starting to trust it, so we need to include the cloud in DDI moving forward."

The cloud fractures IP address space and DNS services. With a commercial solution, infrastructure teams can reassert control of core network services in the cloud and reduce complexity. There are several ways that a DDI solution can reduce cloud complexity. EMA's research identified four top priorities.

- Multi-cloud support is essential. Most enterprises today use at least two cloud providers. A DDI product must be able to control core network services across multiple environments.
- Cloud-based DDI management must be fully integrated with on-premises DDI management to ensure a unified approach to network architecture.
- A DDI solution should be capable of monitoring and alerting on malicious activity.
- The solution must provide end-to-end visibility of DNS resolution paths so network teams can ensure that DNS queries and responses are routed as efficiently as possible, especially as applications are delivered from multiple cloud regions.

Operational Efficiency

More than 48% cited operational efficiency as a trigger for matured, commercial DDI investment. Network engineering expertise is in short supply today. IT organizations need their engineers to spend less time on manual tasks. They cannot rely on a spreadsheet for assigning and tracking IP address space. All processes related to core network services must be streamlined and automated as much as possible. DIY solutions are not up to the task.

87% of research participants currently integrate their DDI solutions with an IT service management platform, like ServiceNow.

ITOM Integrations

Finally, 47% of organizations invest in commercial DDI solutions because they need effective integrations with other IT operations management (ITOM) solutions. This facilitates the two-way exchange of data and information between systems, and it also enables collaboration, automation, and efficiency. In fact, nearly 87% of research participants currently integrate their DDI solutions with an IT service management platform, like ServiceNow. They do this primarily to increase security, simplify reporting, address compliance requirements, and automate change tickets. More mature users of DDI make reporting and ticket management higher priorities for this integration.

"We currently integrate one way with ServiceNow," said a senior network engineer with a very large North American university. "Someone on the ServiceNow team can log in and grab what they need from our DDI solution. We would like to do two-way integration so that our DDI solution can open and close tickets automatically. This would allow ServiceNow to provide an audit trail of things like DNS changes."

More than 55% of organizations also integrate DDI with a security monitoring solution. Other integration priorities include network automation (40.5%), network performance management (37%), and network change and configuration management (33.5%).

How to Succeed with DDI

Dump DIY Solutions

The first step to have a successful approach to core network services is to adopt commercial products. A homegrown DIY approach simply won't cut it in today's digital world. Moreover, IT organizations must strive for the most mature solution that they can adopt. A DDI management platform that controls DNS, DHCP, and IP address space across all networks is the best approach. However, organizations may find that an IPAM overlay is the best solution if they lack the ability to consolidate disparate DNS services that the core network team has no control over.

Avoid Common Pitfalls

Organizations should also watch out for potential business challenges. EMA's research found that more than 52% of organizations struggle with budget. People outside the networking world don't often understand the importance of DDI solutions, so winning budget support from upper management can be a challenge. Network engineers must explain how critical it is to do DDI right, from an operation persecutive and also a security perspective.

"People don't understand why [DDI] can be so expensive. Senior leadership is disconnected from understanding how intricate our DNS is until we depict it in a PowerPoint network drawing, showing all the servers across our international data centers," said a network engineer with a Fortune 500 aerospace and defense company.

Network complexity is a pitfall for more than 52% of organizations. Today's networks extend across multiple disparate platforms, including multi-cloud, software-defined WAN, software-defined data center networks, network virtualization, and the Internet of Things, all driving more complexity. A DDI solution should be integrated with the various systems that manage these environments to reduce complexity.

A senior network engineer with a Fortune 500 retail company pointed to network complexity as an issue when implementing a DDI solution. "The biggest challenge we have is architecting DDI correctly in the first place, pre-provisioning IP address schema and having ways to organize it well. That challenge isn't with the DDI platform, but with how we're going to organize it and use the platform."

More than 42% of organizations lack personnel with DDI expertise. In fact, separate EMA research found that only 12.5% of enterprises believe it's particularly easy to hire and retain skilled networking personnel. Their number-one complaint about today's IT labor pool is a lack of advanced skills. Network teams are primarily struggling to hire people who understand network security and network automation, two key components of DDI administration. EMA research found that IT organizations respond by hiring smart people with a good foundation of basic technical skills and training them up. DDI vendors can help with training.

42% of organizations lack personnel with DDI expertise.

Align Technical Teams with IT Management

EMA found several examples in which executive IT management and technical experts had very different perspectives on the state of DDI in their organizations. For instance, CIOs reported higher levels of overall DDI maturity than the DDI subject matter experts. CIOs who misunderstand the true state of DDI maturity will be less supportive of investments to improve it.

"You don't realize how much you need DDI until it's not there and everyone screams and pulls their hair out," said a senior network engineer with a large North American university.

Check out previous research conducted by BlueCat and EMA. "A House Divided: Dysfunctional Relationships Between Network and Cloud Teams Put Cloud Strategies at Risk."

https://bluecatnetworks.com/resources_doc/report/ema-house-divided-report.pdf

EMA suspects that CIOs also misunderstand what DDI maturity truly is. Although CIOs were more likely to report that they have a full-stack DDI management platform, they were also more likely than subject matter experts to report use of Microsoft DNS. Furthermore, executives were less aware than members of IT or cloud architecture groups to recognize the risks of using Microsoft DNS, such as DNS replication issues, change control problems, outdated DNS records, operational complexity, and security risk. Engineers need to educate IT leadership.

"One thing that inhibits us from investing in DDI is just the difficulty of trying to explain to upper management why we need the product," said a senior network engineer with a Fortune 500 retail company.

Focus on Cloud Support and Integration

As this research iterated several times, network teams should also design their DDI environment with multi-cloud in mind. Look for vendors that can support a wide variety of cloud providers consistently.

Finally, design with integration in mind. Security monitoring and off-the-shelf integration with IT service management should be priorities. In many cases, custom integrations with these solutions may be better.

This report has offered some tips on how one can modernize and mature DDI core network services. There is no excuse to rely on homegrown and open-source technology any longer. Today's business environment demands better. EMA recommends that all organizations evaluate the effectiveness of their DDI solutions today and look for ways to modernize and mature what they have.

About BlueCat

BlueCat is the Adaptive DNS™ company. The company's mission is to help the world's largest organizations deliver reliable and secure network access from any location. To do this, BlueCat re-imagined DNS. The result – Adaptive DNS™ – is a dynamic, open, secure, scalable, and automated DDI management platform that supports the most challenging digital transformation initiatives, like adoption of hybrid cloud and rapid application development. The company is headquartered in Toronto and New York and has additional offices throughout the world, including Germany, the United Kingdom, Japan, and Singapore. Learn more at **bluecat.com**.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com You can also follow EMA on Twitter or LinkedIn

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 www.enterprisemanagement.com 4209.083022