White Paper

The Power of Centralized DDI for Small and Medium-Sized Businesses: Advancing DNS, DHCP, and IPAM to Accelerate Network Transformation

Sponsored by: BlueCat

Brandon Butler
November 2023

IDC OPINION

As organizations across the globe embark on digital transformation initiatives, they increasingly realize the importance of core network services in enabling a range of digital business use cases. Small and medium-sized businesses (SMBs) – those with less than 1,000 employees – face a variety of unique challenges and opportunities related to digital and network transformation.

Core network services such as domain name systems (DNS), Dynamic Host Configuration Protocol (DHCP), and IP address management (IPAM) play a critical role in supporting reliable and efficient network operations and management. A centralized DDI system that orchestrates management across these core network services can enable powerful benefits.

For SMBs, having a DDI system that is tailored to their specific needs is critical. SMBs face unique challenges in accelerating their digital transformation initiatives. They need IT management systems that are simple to use but produce meaningful outcomes. DDI systems designed for SMBs should focus on simplicity of operations, as well as integrations with existing systems, and they should act as a platform that can help SMBs ensure their technology strategy is equivalent – or exceeds – to those of larger enterprises. DDI orchestration solutions customized for SMBs provide a unique opportunity for organizations to accelerate network transformation, simplify operations, and improve automation and security.

DDI systems designed for SMBs should focus on simplicity of operations, as well as integrations with existing systems, and they should act as a platform that can help SMBs ensure their technology strategy is equivalent — or exceeds — to those of larger enterprises.

IN THIS WHITE PAPER

This white paper leverages IDC survey data to explore key trends among SMBs in IT investments and network management, with a specific focus on the opportunity for more integrated management of core network services via DDI orchestration solutions. The white paper analyzes key network management challenges organizations face and describes solutions that can help organizations advance their network transformation via DDI, particularly in the areas of optimizing multicloud, enhancing automation and security, and increasing the resiliency of their networks.

SITUATION OVERVIEW

The State of SMB IT

As small and medium-sized businesses look to digitally transform, they're placing an increased importance on IT. IDC research shows that most SMBs — 59.5% — planned to increase their technology spending in 2023 compared with 2022 levels. In terms of IT spending priorities, SMBs rank automation as a top priority, while video/virtual appointments, connectivity automation, and low-code/no-code app development rounded out the top investment areas. Top IT obstacles in achieving their business goals included security, IT budget size, and talent gaps.

As SMBs look to digitally transform, they increasingly understand the importance of networking and connectivity transformation. Organizations rely more on distributed applications across multiple public clouds thus the network becomes a mission-critical part of SMB operations. Meanwhile, data demands on the network and new digital services are driving organizations to focus more on network operations and management.

Core network services such as DNS, DHCP, and IPAM are important no matter the size of organization. These critical network functions provide the foundational elements of any network architecture. Integrated management of these network services via a DDI orchestration platform enables a range of benefits, from operational efficiency to increased network reliability and resiliency, and fundamentally, a network that can be an enabler of business transformation, rather than a roadblock.

To explore the state of core network services within the SMB market, IDC conducted a survey of 300 United States–based SMB and midmarket companies to gain insights into their use, or potential use, of DDI systems and key criteria they consider in network investment decisions.

Network Challenges for SMBs

Organizations of all sizes today rely on business-critical data and applications that are distributed across a variety of sources, from those being hosted on premises to those hosted in multiple different clouds. For SMBs, leveraging cloud-based resources can be a game changer. Cloud-based infrastructure-as-a-service (IaaS), SaaS, and PaaS offerings allow SMBs to add advanced technology platforms with massive scalability at low up-front costs compared with on-premises offerings that typically require up-front capital and resources.

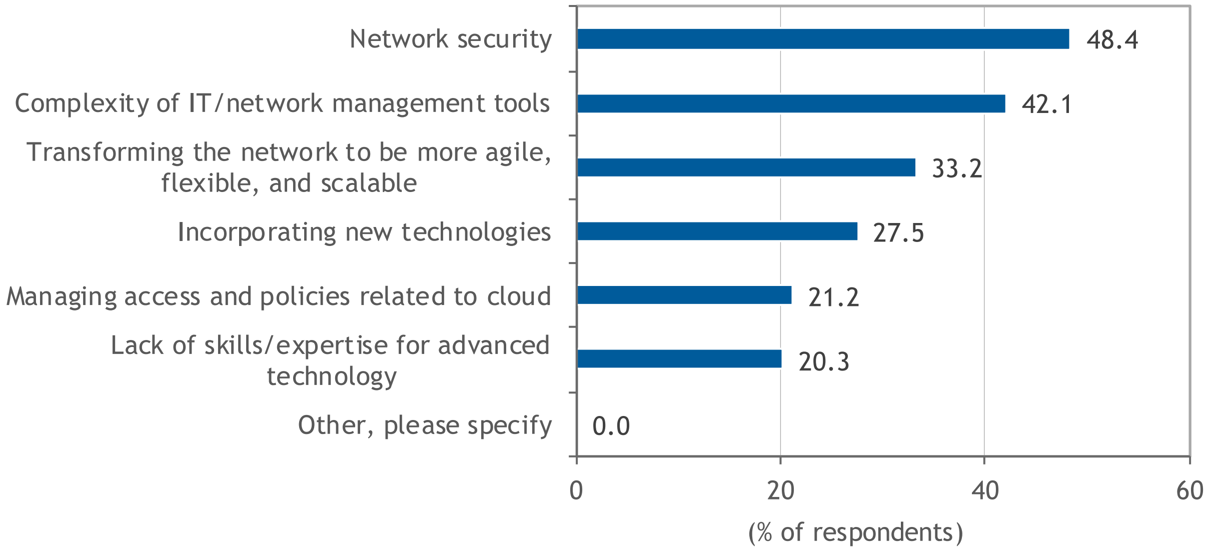
As SMB organizations rely more on cloud-based platforms for their digital business operations, ensuring the secure and effective use of cloud and on-premises infrastructure becomes a critical function of IT teams. Networking platforms can play a critical role in enabling the secure and efficient management of distributed environments. IDC research shows that SMBs are placing an increasing importance on networking in general. An IDC survey asked SMBs what the strategic importance of networking was to their organization today and what they expect it to be in two years. The strategic importance of networking takes into account the overall performance, management and, fundamentally, the ability of the network to meet the needs of the business. In the survey, respondents were asked to rate the strategic importance of the network on a 5-point scale, with 1 representing that the network is not strategically important and 5 representing that the network is strategically important. Results showed that 77% of respondents rated the network as a 4 or 5 in terms of strategic importance today, including 29% who chose a 5.

Yet SMB organizations report having significant challenges in managing their networks (see Figure 1). IDC research data shows that the top network management challenges organizations face today include network security, complexity of IT/network management tools, and transforming the network to be more agile, flexible, and scalable. Other issues cited include incorporating new technologies, managing cloud access and policies, and lacking skills/expertise for advanced technology. SMBs are looking for IT systems that are simple, yet powerful that enable them to be nimble and efficient.

FIGURE 1

Top Network Management Challenges

Q. What are the two most significant network management challenges your organization faces today? (Select up to two responses)



n = 316

Source: IDC's *USA Networking DDI (DNS, DHCP, and IPAM)*, April 2023

DNS, DHCP, and IPAM Challenges

IDC research data shows that SMBs face a series of specific challenges when it comes to core network services. DNS, DHCP, and IPAM are each critical network functions, but they can grow complex as applications become distributed across multiple public clouds, and the number of users and devices connecting to the enterprise network increases. As SMB organizations scale – either in terms of the number of applications used or the distributed nature of the applications – the challenges of DNS, DHCP, and IPAM increase. IDC survey data found that SMBs have unique challenges for each of these three network services.

DNS are used to convert domain names into IP addresses, but DNS can also be used by nefarious actors. Hence, the top-rated response for SMBs related to DNS management challenges was securing the DNS. DNS can also be challenging as an organization's use of hosted applications increases. When using public cloud infrastructure as a service, there can be cloud-specific DNS tools, which can be difficult to centrally manage with internal DNS. The second and third top responses for SMB DNS challenges point to this issue: scaling DNS policies and management across multiple sites and a lack of centralized DNS management across on-premises and cloud platforms. Reliability and redundancy was listed as another top concern for DNS management.

DHCP is a technology that automatically assigns IP addresses to network devices. Automated DHCP is an integral part of efficient network operations, but as the number and variety of devices on a network grows, it can be a challenge to manage. The survey found other top challenges with DHCP, including the process of integrating multiple DHCP servers and end-user performance impacts from inefficient DHCP management. Other top challenges noted by respondents included an inability to offer self-service access for simple changes, such as creating DHCP reservation or release leases, and an inability to monitor the DHCP environment to review lease history, utilization, and concurrent leases.

IPAM is a third core network service that allows for the efficient planning and management of IP address assignments within an organization. For SMB organizations specifically, one of the most common practices is to rely on manual processes for IPAM, namely spreadsheets listing IP address assignments. As the number of IP addresses under management increases, the manual processes become highly inefficient. More than 30% of respondents to the IDC survey noted manual processes for IP address management was a top challenge related to IPAM. Other challenges noted by survey respondents included a lack of a single source of truth in regard to network and IP assignments and difficulty tracking internal versus external IP addresses.

The ability of an automated IPAM to provide information on users, devices, and associated IP addresses creates a powerful single source of truth regarding the network. Combining the discovery and inventory of IP addresses with information from DNS and DHCP, such as historical records of IP address usage, enhances the confidence and context of the IPAM data so that it can be used not just for optimized management but for building a trusted and secure network too.

Taken together, SMBs face significant challenges in managing core network services. Overcoming these challenges is a key avenue to a successful network transformation initiative. DDI platforms represent a key platform for providing centralized and efficient management and orchestration of DNS, DHCP, and IPAM.

While DDI enables a range of benefits for organizations, IDC survey data found that usage of DDI among SMBs is nascent. Overall, more than three-quarters of respondents (77%) were familiar with DDI, but only one in three (33%) SMBs currently use DDI. Another 45% were not using DDI but said they would plan to within the next one to two years.

THE POWER OF DDI FOR SMALL AND MEDIUM-SIZED BUSINESSES

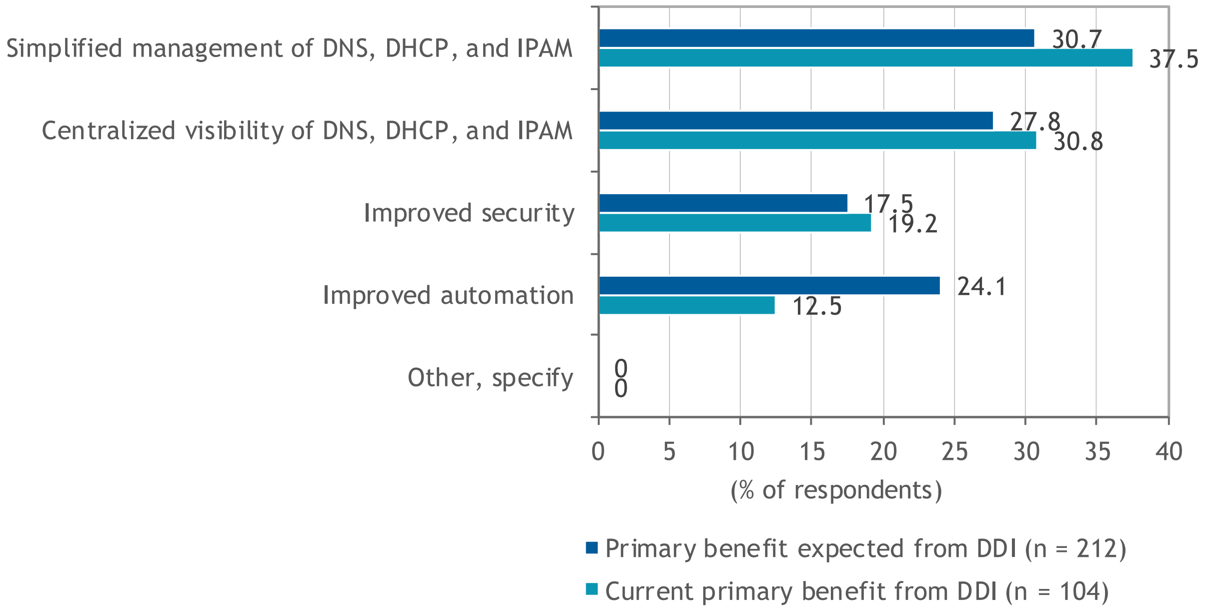
DDI provides a range of benefits for any size organization, but especially SMBs. DDI systems help simplify the design and management of core network services, increase the visibility and control of complex networks, and improve the security of the network. Having a simple, extensible platform that can provide intuitive and automated control over a complex network environment makes DDI systems especially helpful for SMB organizations.

Figure 2 shows the survey results when IDC asked DDI users to identify the primary benefit they get from using DDI. The top response was simplified management of DNS, DHCP, and IPAM, along with centralized visibility of the core network services. Almost 20% of respondents noted that DDI helps improve the security of their core network services too.

FIGURE 2

Top DDI Benefits

Q. What is the primary benefit you get/you would expect to get from using DDI?



n = 316

Source: IDC's *USA Networking DDI (DNS, DHCP, and IPAM),* April 2023

Overall, DDI can help organizations in a variety of ways, including:

- **Simplified management:** Fundamentally, DDI systems provide a point of integration across three core networking technologies that many organizations manage separately. Having a single orchestration system enables organizations to simplify their overall management approach. For SMBs, this can be especially critical given the lean IT staff that many SMB organizations rely on. Making IT more efficient, and specifically ensuring core network services are an enabler – rather than a roadblock to digital businesses – is key.
- **Heightened visibility:** The components of DDI are a powerful set of tools for providing detailed insights and control into what's happening in the network, managing the network efficiently, and preventing security threats. Insights into DNS traffic and IP addresses that are used and unused within an organization as well as what users and devices are connected to the network are all readily available in a centralized DDI orchestration system.
- **Standardized operations:** Enabling IT staff to consolidate management of DDI components into a single platform leads to management efficiencies and simplified architectures. Simplified orchestration systems also reduce the learning curve for IT workers to get advanced core network services even if they don't focus on DDI as a daily task. For SMB organizations that

manage a set of distributed workloads across on-premises and public cloud infrastructure, standardized operations can be an especially important benefit. Instead of having separate systems for on premises and cloud, a DDI system should be able to act as an overlay across these environments to provide centralized management of core network services. For example, the process of adding a DNS record internally on Microsoft or a DNS record in AWS Route 53 can be the same when using an abstracted orchestration layer for DNS.

- **Improved automation and agility:** DDI platforms have an opportunity to not just integrate management of the core networking components but can also enable a more agile management approach via automation of these services too, including via application programming interfaces (APIs). For organizations that may be relying on manual tasks, automation capabilities of DDI can be very powerful. Automation isn't just about agility and speed; another powerful benefit is creating consistent network policies that are more reliable and resilient. Consistency breeds reliability when systems are tried and true, with the added benefit of being easier to manage and troubleshoot.
- **Enhanced security:** Each of the components of DDI are, unfortunately, used as an attack vector for organizations of all sizes. Having standardized architectures and heightened visibility into DNS, DHCP, and IPAM can act as the basis for a robust security platform for organizations.
- **Faster identification and resolution of problems:** A key to fixing a problem quickly is reducing the time to identify it, and then finding a way to resolve it. DDI systems have a unique opportunity to coordinate identification and problem resolution across all three components of the core network services.

DDI for Security

The benefit of enhanced security via DDI is an important one, specifically for SMBs. Each of the components of DDI has a role to play in enforcing a strong security posture for an organization. DNS-level security can help prevent distributed denial of service (DDoS) and other brute-force attacks, as well as other DNS-related security threats, such as cache poisoning by nefarious actors using DNS requests to carry malicious data.

DDI platforms help secure the network in a variety of ways. Perhaps most important is in simplifying network architectures and management. Complexity leads to not just inefficiencies but also vulnerabilities that can be exposed by bad actors. DDI platforms help organizations coordinate the architecture and management of core network services, allowing for simpler management and better integrations with existing security defenses. Even as networks stretch across multiple platforms on premises and in the cloud, a DDI solution can provide centralized control and visibility, which can reduce human error and allow for more clear visibility into what's happening in the network, especially when there is a problem. Security is enhanced by centralized and systemic processes that create simplified architectures and consistency in operations and allow for faster troubleshooting of problems.

Key stat: Two-thirds of respondents to an IDC survey agreed or strongly agreed with the following statement: "Using a DDI platform can help improve the security of my network."

Another survey question asked respondents how much they agree with the following statement: "Using a DDI platform can help improve the security of my network." Two-thirds of respondents agreed (38%) or strongly agreed (28%) with the aforementioned statement. A follow-up question asked in what specific ways DDI platforms help improve security. Top response options included improving the security of distributed users/devices, an ability to identify attacks quickly, and improving security-incident response times.

Technical Benefits of a DDI Solution for SMB Customers

DDI orchestration systems enable a range of technical benefits for SMBs. Specific examples of ways DDI helps improve network operations are:

- **Modernize IPAM:** For many small and midsize organizations, IPAM can be a key point of inefficiency, especially for those organizations that rely on manual processes for IP address assignment and management. Automating IPAM functionality via DDI systems represents a significant step forward in network operations' efficiency and standardization. Automated IPAM via DDI simplified IPAM operations and enables real-time visibility and control of IP infrastructure.
- **Evolve from relying on ISC BIND**: Another common inefficient practice is for organizations to rely on open source tools for components of DDI management, particularly DNS and DHCP. Of respondents to the IDC survey who are not using DDI, 18% said they were using BIND DNS with command-line editors. A DDI system can be a step function increase in DNS and DHCP management compared with open source tools, particularly in the ease of use, centralized management, and granular role-based access controls that can be enabled, for example, at the DNS server, DNS zone, or DNS resource record layers.
- **Enable hybrid and multicloud**: As the footprint of an SMB network expands from on premises across to multiple public IaaS and SaaS cloud platforms, the complexity of the network and core network services can exacerbate. DDI orchestration systems can act as an overlay that provides visibility and control over the entire network footprint, whether on premises or in the cloud. A key to this is having an overlay approach to a DDI system that integrates natively via APIs to cloud and on-premises infrastructure platforms so that, for example, configurations can be migrated, replicated, and scaled across cloud and on-premises platforms. Native support for cloud-based DNS systems like Azure DNS and Amazon Route 53 means SMBs can take advantage of cloud-native tools without lock-in.
- **Get a handle on virtualized environments:** Across on-premises and cloud environments, issues related to visibility, change management, and overlapping IP address spaces can be challenges in virtualized environments. DDI systems provide a centralized platform for insights into and management of dynamic virtualized environments, on premises or in the cloud. A key to this is having robust SOAP and REST APIs and integrations with IT orchestration systems like VMware vRealize.
- **Embrace automation and orchestration**: Specifically for DevOps teams, having automated and integrated DDI can help ensure new applications and services that are built are done so from the ground up with core network components that are scalable and efficient. A simple, yet robust API is key, along with integrations with infrastructure automation tools like Ansible and Terraform. Another key here is having an orchestration system that can integrate with automation solutions that are already in use by the organization. For example, if DevOps teams use Ansible, then they should be able to create Ansible playbooks for DDI so they don't have to learn yet another new tool.
- **Enhance network resiliency:** DDI systems simplify not just the architecture but the management of core network services. A simpler network design and management approach leads to fewer manual errors, increased visibility, and control and, fundamentally, a more resilient network. This is particularly key for DNS, where failover and redundancy are key to uninterrupted operations.

- **Get advanced reporting:** As SMB organizations face increased need for compliance and auditing, DDI systems can provide detailed visibility and integrated reporting across the core network services. This includes detailed tracking, logging, and change management tools.

For SMBs to get the full value from DDI, it's important that they consider a platform that meets their specific needs. Namely, SMB organizations prioritize simplicity of a technology offering, integrations of a technology with existing systems, and the opportunity for a technology investment to provide the maximum value to their organization.

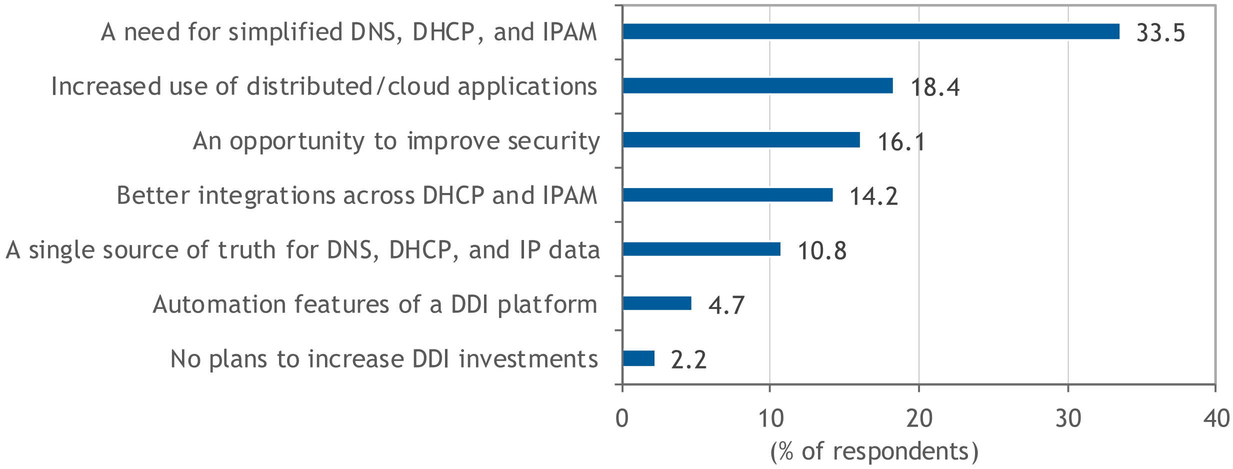
A survey question probed this point further: It asked SMBs to identify what caused their organizations to increase their DDI investments (see Figure 3). The top-rated response was a need for simplified management of DNS, DHCP, and IPAM; the second-rated response was the increased use of distributed/cloud applications; and the third was an opportunity to improve security.

For SMBs to get the full value from DDI, it's important that they consider a platform that meets their specific needs.

FIGURE 3

DDI Investment Drivers

Q. What would cause your organization to increase its DDI investments?



n = 316

Source: IDC's *USA Networking DDI (DNS, DHCP, and IPAM)*, April 2023

CHALLENGES/OPPORTUNITIES

SMBs face a variety of challenges and opportunities as they look to leverage DDI solutions. With the right focus on DDI systems that cater specifically to SMBs, these challenges can be overcome.

Challenges

- **IT expertise**: SMB and midmarket engineers often must have a broader set of skills and wear multiple proverbial hats within the IT organization, especially when compared with dedicated network, security, or cloud operations teams of larger enterprises. DDI platforms for SMBs should be intuitive and simple to deploy and manage by SMB engineers who may not have time to dive deep on DDI. IDC survey data finds that almost a quarter of SMBs were not familiar with the term *DDI.* Hence, it's important for SMBs to understand their specific challenges as they relate to managing their core network services and consider whether centralized management of those systems would be beneficial. If so, then consider a system that's specifically designed for SMBs — one that focuses on simplicity of use, resiliency, visibility, and control.
- **Reliance on legacy methodologies:** As SMB organizations start off very small and grow, their reliance on processes that may have worked when they were a very small organization may become untenable as they become larger. Furthermore, as an organization's network architecture expands to multiple cloud platforms, the management of core network services can become challenging. This expansion in scope of responsibilities of IT, network, security, or DevOps teams can be one of the chief catalysts for pursuing a network transformation initiative. It's key that IT and the core network services specifically are not a roadblock to an organization's growth trajectory.
- **Organizational alignment:** SMBs can also have a challenge in aligning technology investments for core network services such as DDI. With IT generalist teams that may be responsible for multiple roles within the organization, it can be difficult to prioritize investments. Key to overcoming this challenge is having a system that can be used by both generalist, lean IT teams and network, security, and DevOps teams. Having IT and companywide leadership prioritize digital and network transformation initiatives is another key to ensuring organizational alignment.

Opportunities

- **Improved operations:** DDI systems have a unique ability to enable a range of technical and operational benefits. Fundamental to these is an ability to centralize and simplify the management of three core network services that provide the basis of any network architecture. Integrated management of DNS, DHCP, and IPAM can help organizations improve operational efficiency, increase visibility, and control and improve the security of the network.
- **Increased resiliency and agility:** As the reliance on IT and networking services continues to grow, ensuring that core network services are an enabler of business operations, rather than a hinderance, is critical. The benefits enabled by DDI help ensure that the core network services are efficiently managed, enabling resilient network operations in a simple way, even as the complexities of the network increase.
- **Technology as a way to compete upmarket:** Savvy SMBs recognize the potential that investments in technology can play to help the company compete with larger competitors. There's a distinct advantage that technology can enable that allows a smaller organization to be more agile, operationally efficient, and compete — and win — against larger competitors. Investments in DDI systems can be a platform for building technologically advanced processes that allow efficient use of cloud platforms and automation and fundamentally enabling an alignment between technology and the growing business.

CONCLUSION

As SMBs look to digitize, the network — and specifically core network services — can be a bottleneck. The use of multiple cloud platforms, new applications being spun up and down, and a lack of visibility and control over IP address spaces and DNS policies are all common issues that impact the core IT function of SMB organizations. Network transformation is increasingly becoming an accelerant of overall digital transformation. DDI systems that centralize the orchestration of core network services are a key enabler of this transformation effort.

About IDC

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, IT benchmarking and sourcing, 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. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com