Infoblox

eBook

THE DDI BUYER'S GUIDE

Finding the right core networking solution for today's challenging IT environment

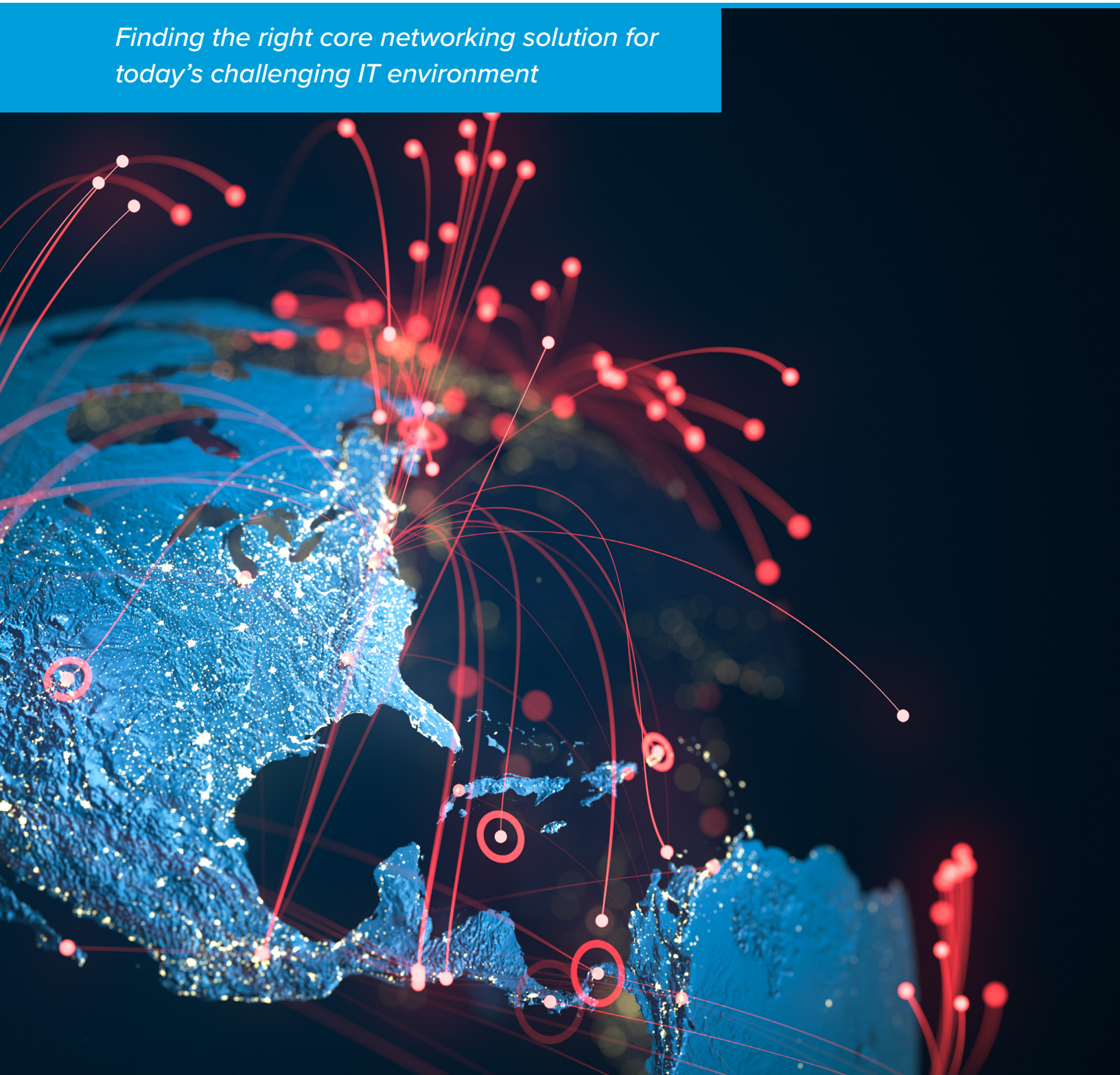

Table of Contents

Introduction: The New Normal

Recent world events—especially the COVID-19 epidemic and the subsequent global adoption work from anywhere (WFA)—have made network reliability and visibility more important than ever. This massive disruption has highlighted a fact that was becoming abundantly clear even before the pandemic hit—that achieving network reliability and visibility depends on the core network services that make all modern networking possible: DNS, DHCP and IP address management (DDI). According to a Dimensional Research 2019 study, almost every business suffers network interruptions. Three-fourths of them experience these several times a year. For many organizations, these network disruptions can be traced to out-of-date and inadequate DDI services.

This eBook provides an overview of modern DDI services, why they matter and the requirements needed in this new era of distributed networking where working from home has become the "new normal." We'll look at the market forces in play. We'll also explore key details of DDI services and upgrades that can set organizations on the best course not just for digital transformation but also for providing every remote worker and location with the fast, reliable networking experiences that DDI services make possible.

We Are in the Middle of a Big Shift

2020 saw a 10-fold surge in remote workers because of the pandemic. This trend is likely to have long-lasting effects. Global Workplace Analytics estimates that 30 percent of the U.S. workforce will be working from home or outside of the office multiple days per week by the end of 2021.

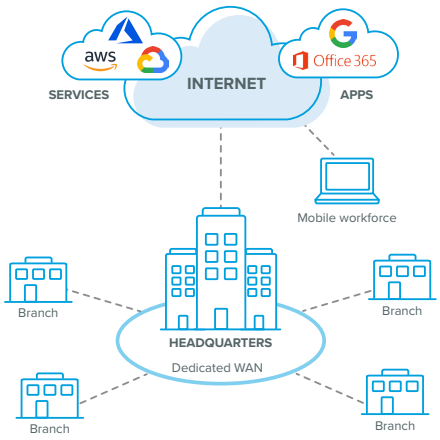

Figure 1: Traditional network architecture

In the new WFA normal, businesses are finding it exceptionally challenging to achieve visibility and control while balancing productivity and security requirements. Among the biggest challenges that organizations are facing:

- **Legacy solutions are insufficient**
  - Partial endpoint visibility for remote workers
  - Absence of networking solutions that are closer to endpoint

- **IT departments are under pressure to shift priorities fast**
  - Lack of automation and endpoint network compliance for scalable and secured networks
  - Need for improved network readiness for the next wave of Internet of Things (IoT), software-defined networking (SDN) and bring your own device (BYOD)
- **Endpoints lack full protection**
  - The biggest concern, with rising threats: DNS security
  - Inadequate intrusion protection and detection (IPS/IDS) that can analyze only known threats and not the new ones

As every sector rolls up its sleeves to handle the new normal, network resilience and endpoint visibility have drawn the most attention in the business world, heightening the need for reliable core network services.

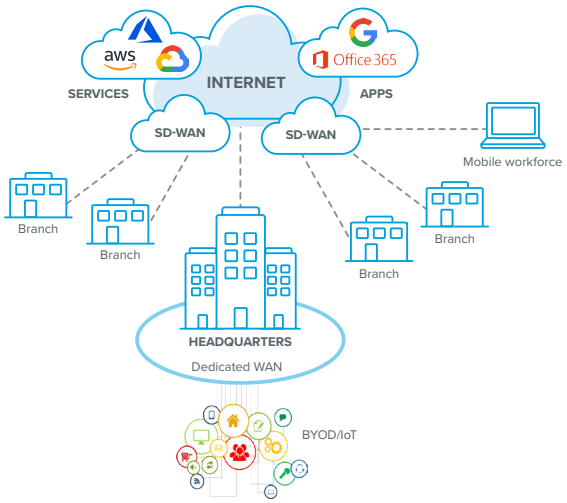

Figure 2: Modern architecture

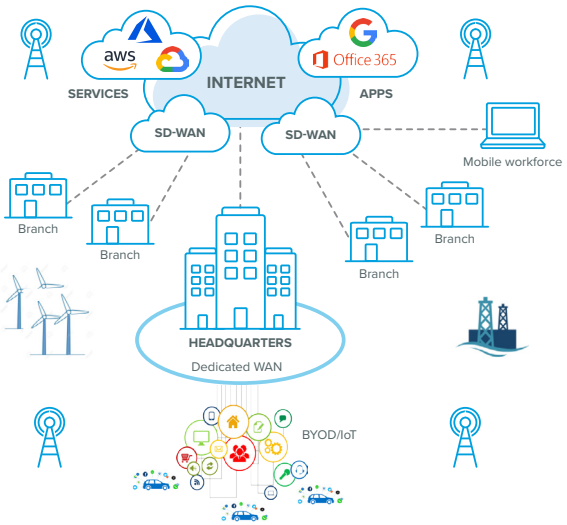

Figure 3: Today's reality for the borderless enterprise

Endpoint Visibility for the Distributed Workforce Is Now More Crucial Than Ever

In the enterprise, the once well-defined headquarters security perimeter has given way to a borderless edge as users access cloud applications directly from everywhere (see Figures 1 - 3 above). Further, branch offices and remote users also connect directly to the Internet without the full protection of the corporate security stack. The lack of adequate endpoint safeguards can turn devices in homes and branch locations into potential security vulnerabilities on the network.

Learn How to Secure Remote Workers in the Age of Teleworking

IT teams are realizing that core networking services are more important than ever for organizations that expect to not just survive but also thrive in this new era. For many, this is prompting renewed scrutiny of existing resources and a move toward modern DDI services.

The Heart of Networking: Core Network Services

DNS, DHCP and IP address management (collectively known as DDI) play a central role in every network interaction. Here's a brief look at each component.

DDI – FOUNDATIONAL SECURITY ARCHITECTURE

- DDI enables an adaptive security architecture
- Lowest Common Denominator to Maximize RoI
  - DNS is the fouincation of every network conversation
  - DHCP is the foundation of network access
  - IPAM database is the authoritative source of all network-connected assets

DDI provides inside-out security: Protect from the date center to the network edge & everything in between.

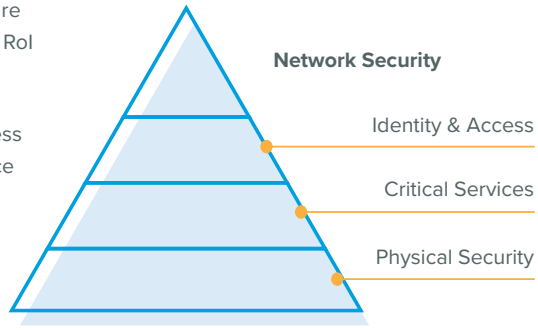

Figure 4: DDI foundational security

DNS (Domain Name System)

The Domain Name System is the starting point for all network interactions. A hierarchical naming system, DNS is built on a distributed database for computers, services or any resource connected to the Internet or a private network. Most importantly, it translates domain names meaningful to humans into the numerical identifiers associated with networking equipment to locate and address these devices worldwide. It is the first component of DDI services that came into the networking world when IP allocations were mostly manual and tracked on spreadsheets.

DHCP (Dynamic Host Configuration Protocol)

As the IT infrastructure expanded and the Internet exploded, IP allocation became dynamic. This gave birth to DHCP and the first IP address management tools. DHCP is used to dynamically assign IP addresses to endpoints. It enables IT teams to more easily keep track of networks, ranges, names and hardware address mappings.

IPAM (Internet Protocol Address Management)

IPAM (IP address management) is the administration of DNS and DHCP, which are the network services that assign and resolve IP addresses to machines in a TCP/IP network. Simply put, IPAM is a means of planning, tracking and managing the IP address space used in a network. Most commonly, tools such as DNS and DHCP are used in tandem to perform this task, although true IPAM will glue these services together so that each is aware of changes in the other.

Visibility, Automation and Control: The Three-Step Framework for Unbeatable DDI Services

Now that we've covered DDI basics—they're the Internet Protocols governing how devices and endpoints connect to web destinations and applications—let's consider their potential as business differentiators. Modern organizations are taking every possible step to enhance their networking capabilities, and many are focusing on DDI services as the best way to do that. At a higher level, organizations can evaluate the goals for DDI services with a three-step framework. Visibility is the first step of this framework. To get better, faster and more efficient DDI services, automation and control are the other two strategic steps.

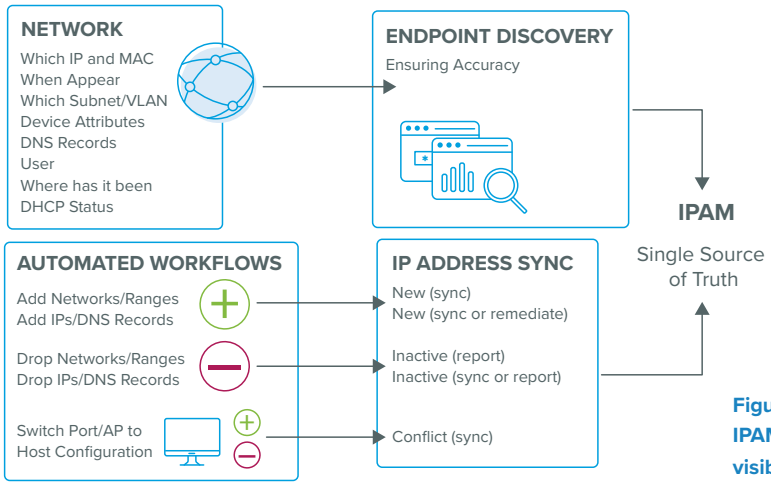

Figure 5: Authoritative IPAM discovery and visibility

Discovery and Visibility

In the new normal WFA era, networking and security teams need endpoint discovery into their widely distributed workforces and the devices these workers use. DDI services provide that visibility. They can do so because of their unique position at the heart of every network interaction. DNS, DHCP and IP address management contain a wealth of data about devices, including where they reside on the network, what they connect to, whether they've been infected with malware and more. As a result, a robust DDI architecture makes it easier not only to monitor IT operations but also to understand key performance indicators. Tasks such as understanding application latency are possible only if the DDI architecture allows such assessments. The impact of better visibility isn't limited to network operations; the security aspect of the business is equally empowered. Bottom line: You need to be able to discover devices and network activity to enforce policy and report on and secure distributed environments. Today's advanced DDI solutions in general, and DHCP fingerprinting in particular, provide an easy way to gain this information and control.

Better visibility from DDI services offers:

- 360-degree visibility into key network assets, including devices, endpoints and switch ports
- DNS query assessment and access to performance history
- Timely threat detection and monitoring for crucial services
- Automatic discovery of rogue, non-compliant or misconfigured devices

Though the need for visibility through DDI became more urgent with the surge in WFA, the impact and benefits of achieving foundational visibility in DDI architecture are long-lasting. As remote workers rely increasingly on personal devices—not just laptops and phones but also home routers and Wi-Fi hot spots—IT administrators are being challenged with dynamic network device detection and control. Legacy approaches to DHCP, or workarounds such as mobile device management, simply can't deliver the kind of clear visibility necessary in new normal environments.

Automation

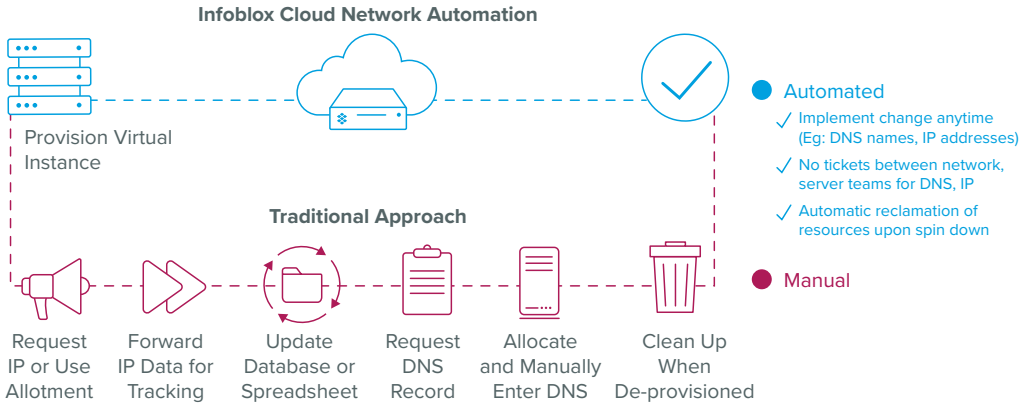

Figure 6: The Power of Cloud Network Automation; network automation accuracy and efficiency

Engineering teams dedicate a disproportionate share of resources and time to maintaining routine activities, such as assigning IP addresses, creating and managing subnets and reporting and auditing device connection history. Again, much of this work has been managed on spreadsheets or other cumbersome, error-prone methods. Automated DDI helps in cutting through these routine tasks and enabling a more efficient workflow with fewer resources. Having automated DDI in place is especially crucial for small and mid-level organizations where the dependency on a limited number of engineering staff can lead to increases workflow interruption.

Immediate benefits of automation for core networking services include:

- Scalable core networking capabilities
- Robust user/IP mapping
- Access to Microsoft Active Directory sites services
- Improved efficiency due to reduction in supervision for routine tasks
- Reduction of errors introduced through manual intervention

Control

Well-designed DDI services simplify networking for widely distributed branch locations by enabling centralized management of the entire DDI implementation. They not only give networking teams greater control over their networks, but they also help business leaders in staying on top of their network performance and IT health. The best DDI platforms enable organizations to:

- Centrally control network assets whether they are on site, in the data center or in the cloud
- Use DDI data to bridge tool and departmental silos
- Centrally manage DNS, DHCP and IP address provisioning from a common console
- Implement compliance with greater confidence and ease

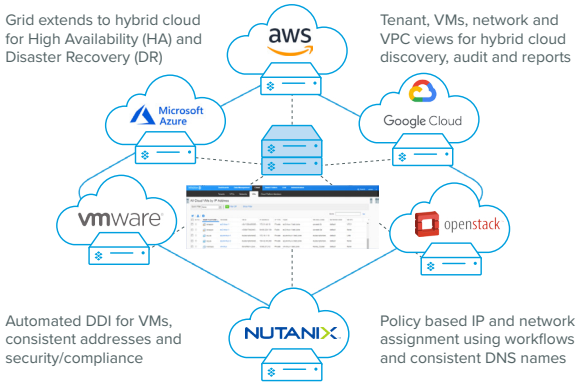

Figure 7: Single Control Plane

DDI Essentials: Critical Capabilities to Consider

Visibility, automation and control are the key attributes—the framework and the overarching goals—that organizations need to keep in mind as they seek to optimize and secure their networks for new WFH realities. But what are the specific underlying elements and capabilities that will enable them to achieve these ends? Here's a closer look at the DDI essentials to consider for a robust networking infrastructure.

Centralized Authoritative IPAM Database

Traditionally, IPAM was tracked using spreadsheets and often separate tools and systems. But as network complexity has grown, so has the demand for ways to consolidate IPAM information. A centralized and authoritative IPAM database acts as a single source of truth for all the network-connected assets within the organization. It empowers IT teams with network discovery and optimum use of resources. Advanced IPAM solutions include this single-source of truth capability, which plays a key role in network optimization.

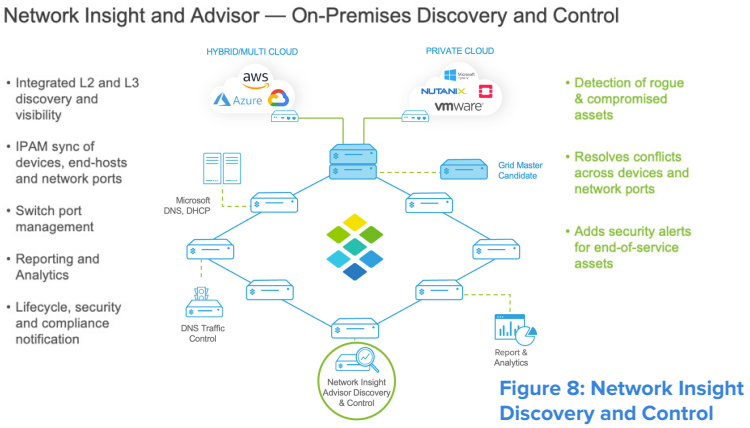

Figure 8: Network Insight Discovery and Control

- **Get detailed visibility across the network**
  Discover all layer-2 and layer-3 devices, end hosts, connectivity, switch port and VLAN data.

- **Improve operational efficiency**
  Automate controls from a single UI to improve workflow cadence, allocate IP addresses and ports and spin-up and spin-down workloads in a multi-cloud environment.

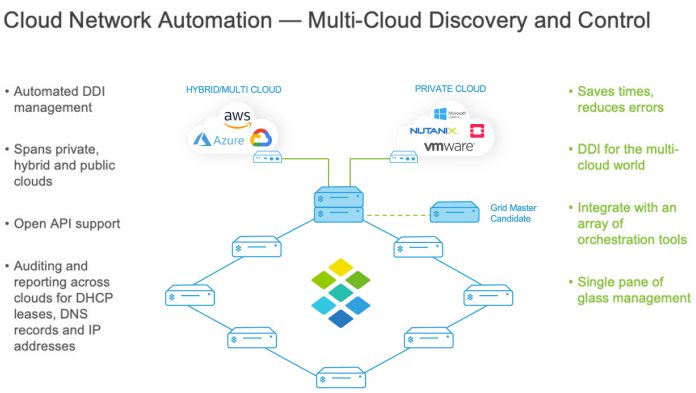

Figure 9: Cloud Network Automation Discovery and Control

- **Better manage IT resources**
  Use built-in controls and automatic auditing to delegate and free up highly paid employees for more strategic work.
- **Reduce service interruption risk**
  Easily validate network designs and identify misconfigured networks, switches and misplaced servers.
- **Gain management flexibility through cross-functional harmony**
  When security, server and network teams share trusted data, they can make quick, reliable decisions, delegate tasks and eliminate departmental dependencies.

Learn How Authoritative IPAM Delivers Network Insights

Integrated DDI Management

Traditional systems such as BIND/DHCP, Microsoft DNS/DHCP and spreadsheets do not adequately address the needs of a modern network. Integrating IPAM with DNS is crucial to keeping both systems accurate and synchronized. When a new device is deployed on a network, the assignment of an IP address comes first, usually followed immediately by a request to add the host to DNS. By integrating DNS and IPAM, this process becomes a single step—the DNS record is created at the same time as the IP assignment.

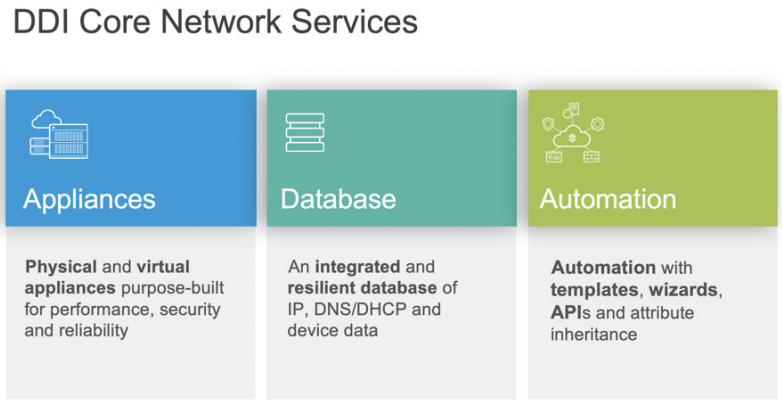

Figure 10: Integrated Core Network Services

With the help of integrated DDI services, network teams can:

- Consolidate DNS, DHCP, IP address management and other core network services into a single platform, managed from a common console
- Centrally orchestrate DDI functions across diverse infrastructure with integrated capabilities for hybrid and public cloud and virtual and private cloud environments

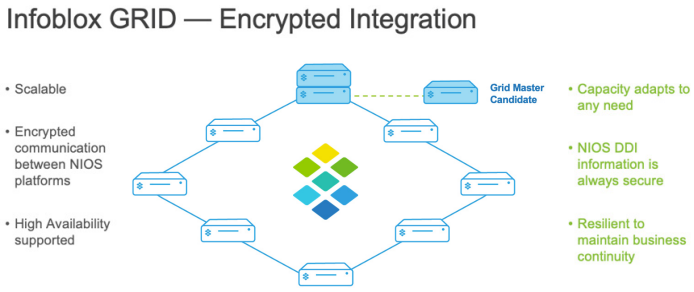

Figure 11: Infoblox Grid Platform

- Access rich, integrated reporting and analytics capabilities for capacity planning, asset management, compliance control and auditing
- Improve efficiency and automate routine operations by seamlessly integrating with other IT systems

Integrated DDI extends beyond protocol services such as single-point data entry, accurate address assignment, inter-system data federation, inventory tracking, change control delegation and name resolution. As organizational networks evolve, integrated DDI services become the essential networking technology to link branch offices, remote workers, mobile devices, the cloud and more.

Support for Virtual SDN

While the transition to software-defined networking (SDN) comes with some noted benefits such as mobility and flexibility, if it is not supported by equally competent DDI, it can be challenging for a business to function after the transition. The biggest of these challenges involve uninterrupted networking and robust security.

- In traditional architecture, it was relatively simple to map the communication within the limited number of on-premises appliances that work in controlled environments. As we add IoT devices, BYOD and SD-WAN to the network, communication mapping becomes more complicated.
- With several endpoints or access points out of the control environment, network infrastructure needs DDI services providing better monitoring for secure operations.

IDC estimates that the worldwide data center SDN market will be worth more than $12 billion in 2022, recording a compound annual growth rate (CAGR) of 18.5 percent during the 2017–2022 period. The market generated $5.15 billion in 2017, up more than 32.2 percent from 2016.

Support for IPv6 Adoption

The IPv6 migration has been underway for several years now, yet many organizations have yet to make the full transition from IPv4 onto the new standard. IPv6 provides a vast abundance of IP addresses needed for the billions of smartphones, wearables and IoT devices coming online. However, many organizations are still lagging behind when it comes to having a DDI infrastructure in place to support IPv6. As a consequence, they risk losing communication, revenue and customers if they don't plan for IPv6 adoption now.

To take full advantage of IPv6, organizations need to have in place a dedicated IPv6 practice and specialized tool sets, which most IT organizations today still lack. Further, as Gartner says, organizations undertaking a large-scale IPv6 deployment are likely to need a dedicated DDI platform. Federal CIO Suzette Kent cited increased adoption in the private sector over the last five years:

"Mobile networks, data centers and leading-edge enterprise networks, for example, have been evolving to IPv6-only networks. It is essential for the federal government to expand and enhance its strategic commitment to the transition to IPv6 in order to keep pace with and capitalize on industry trends."

***- Suzette Kent,** Federal Chief Information Officer*

By analyzing all the DNS mapping of network infrastructure, organizations can understand whether they can immediately shift to IPv6 or have some critical network dependencies that need IPv4 support. In case they find themselves in the second category, they can opt for dual-stack implementation. Migrating from IPv4 to IPv6 buys time and increases flexibility, which is crucial for organizations. But it does add a layer of complexity in the network infrastructure. When organizations select a DDI network partner, they should check whether it provides dual support for IPv4 and IPv6.

DNS Security

DNS is the foundation of every network conversation and also the first target for the majority of network cyberattacks. DNS is a leading vector for cyberattacks precisely because it's essential for network connectivity, DNS traffic is necessarily unencrypted and traditional security solutions are not designed to protect DNS traffic. As a result, unencrypted DNS communications remain a prime target for cyberattackers.

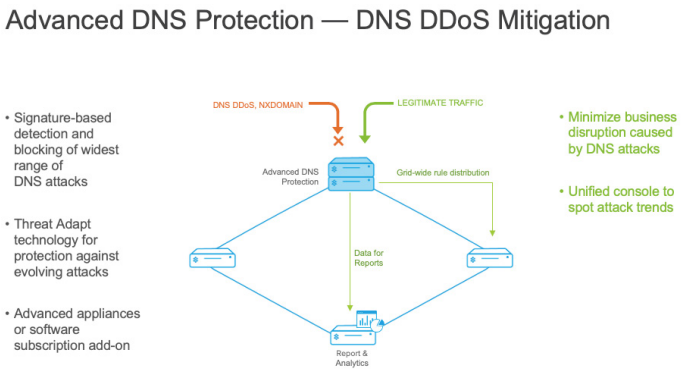

Figure 12: DNS Security

While choosing a DDI solution, it makes sense to account for the DNS security that the solution supplies to ensure the overall protection of network infrastructure. DNS infiltration and related attacks include DNS DDoS, NXDOMAIN, DNS data exfiltration (through known tunnels), malware, ransomware and other DNS hijacking exploits. To mitigate DNS-related attacks, organizations should consider smart DNS solutions such as those that use DNS as an enforcement point close to endpoints and the network edge and that can detect malicious activity sooner than traditional perimeter defense tools can.

DDI has traditionally been regarded as a means to simplify and automate network management while provisioning and integrating other cloud orchestration systems. But as DNS security has come to the forefront for organizations, it's now become a top priority that DDI solutions also provide smart DNS security.

Reporting and Analytics

The components of modern DDI services furnish invaluable data for networking teams. This data helps in keeping an eye on network operations, endpoint usage and vulnerabilities that can have negative impacts—thus alerting networking professionals of upcoming attacks or failures that could lead to network outage.

The benefits of advanced reporting and analytics are wide ranging:

- **Audit/compliance**
  Get visibility into historical core DNS data
- **Application availability and performance**
  View and measure DDI data to assess resource utilization
- **Security**
  Ensure prompt threat detection by keeping an eye on core DNS data
- **Capacity planning**
  Remove the guesswork from IP use

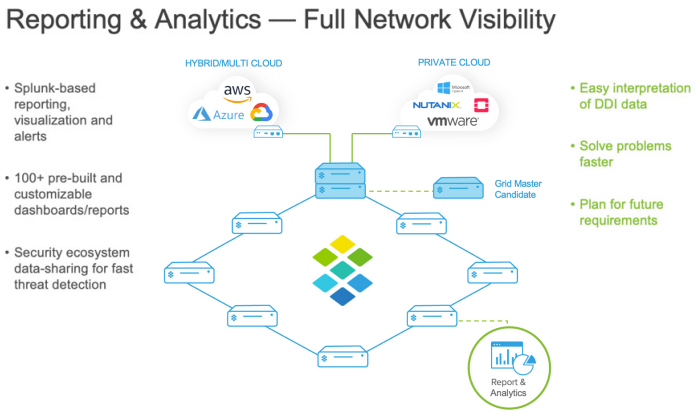

Figure 13: The data furnished by advanced DDI is highly valuable for security operations, troubleshooting and planning.

Modern DDI platforms provide pre-built and customizable reporting tools that help networking teams in multiple crucial ways. Gauging application running status, security threats and resource utilization in a timely and orderly manner are just a few of the benefits these tools supply.

Understanding DDI Deployment Options: On-Premises, Cloud and Unified

The DDI market is growing fast. It is expected to expand at a CAGR of 16.3 percent over the period 2017–2022. This growth is accelerating through the proliferation of DDI deployment options. Here's a brief look at DDI services in on-premises, cloud and unified/hybrid environments.

On Premises: Still the Gold Standard

On-premises DDI has been around the longest and has evolved the most compared to emerging cloud offerings. With on-premises DDI implementations, because the licensed software and servers both reside in the organization's data center, these solutions afford a high level of control and security. In addition, the most mature and advanced on-premises DDI solutions provide reporting and analytics, integrated architecture and "single pane of glass" visibility.

on-premises DDI services can deliver:

- Five nines or 99.999 percent availability that translates to less than five minutes of downtime in a year
- Highly secure networking solutions that ensure the highest levels of data security
- Networking operations that are closest to the servers to ensure high network output and control
- A feature-rich networking infrastructure that ensures that the organization is well-equipped
- Connection options that enable networking teams to manage DDI centrally and automatically from the cloud

On-premises DDI services are the best bet for organizations in which maintaining tight control over server access is a prime concern or where supporting traffic-intensive DDI operations within primary facilities is mission critical. Examples include banking and financial services, telecommunications, defense facilities, research labs, healthcare and high-risk IT organizations.

The On-Premises Journey toward the Cloud

As with so many aspects of digital technology, DDI has been transformed in recent years by virtualization and the cloud. One of the biggest outcomes of this evolution is that, unlike in the early days of the commercial Internet, organizations today are now focused on DDI as an integrated solution rather than deploying separate DNS, DHCP and IPAM instances as individual services. This evolution started with the virtualization revolution that made it possible to deploy DDI solutions on the customer's choice of hardware. Today, with the advent of technologies such as Docker, Containerd and Kubernetes, DDI solutions can now be delivered as modular containers that run as lightweight instances managed from the cloud. The latest step in this revolution? Container-based architecture, also known as cloud-native architecture. Of course, deploying DDI as containerized microservices can be done within an on-premises data center. Yet cloud-native means just that: technology that is not only optimized to run in public or private cloud environments but that also is built for the cloud from the ground up.

Cloud-Managed DDI Is the Future

The beauty and core value of the cloud are that it frees the organization—and the IT team—from the day-to-day chores required to maintain the machines, devices and appliances that support data processing, storage and networking.

A key attribute of cloud-native applications is that functions must be isolated from the system they run on. The deployment method matters, but the location is mostly irrelevant. With cloud-managed DDI, the need for hardware appliances in branch and remote locations is eliminated because they are replaced with virtual software-defined counterparts that can be managed centrally and remotely from the cloud. The flexibility that virtual machines provide opens the door to integration with many vendors.

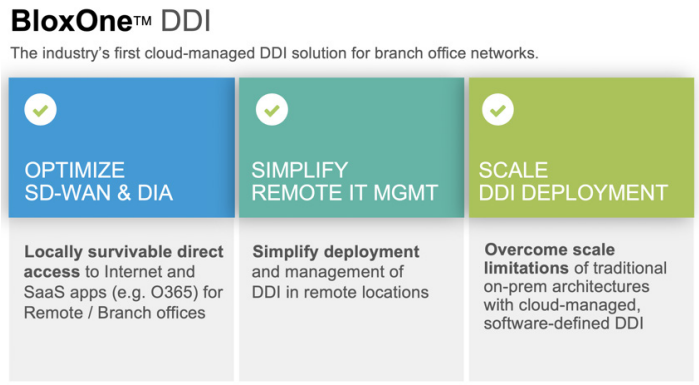

Figure 14: Benefits of BloxOne™ Cloud-Managed DDI

Cloud-managed DDI makes life easier for the network administrator and business operators by solving many of the biggest challenges of modern networking. At the core of the cloud-managed DDI evolution lies the need for a reliable and straightforward computing experience anywhere and at any scale. Here are a few of the main drivers for cloud-managed DDI adoption:

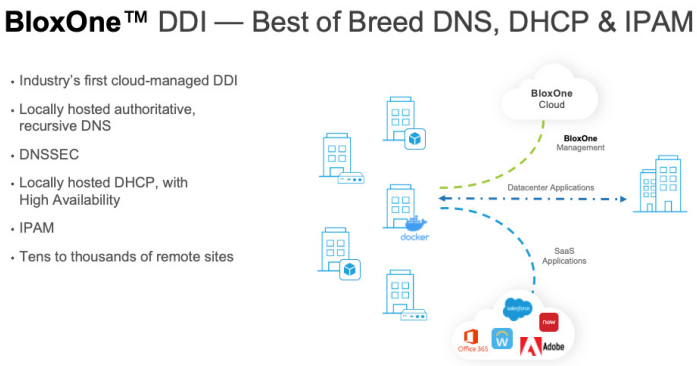

Figure 15: Cloud-Managed DDI

- **Automation at scale:** Provisioning, management and policy control can be automated from a central point in the cloud for all remote locations, such as retail stores.
- **Local survivability:** This is crucial for industries like retail, manufacturing and oil and gas. If a point-of-sale system or a drilling machine with hundreds of connected sensors cannot get IP addresses due to lack of access to headquarters, all related business operations would halt.
- **Enterprise edge without hardware investments:** Lightweight and agile cloud DDI solutions allow organizations to execute DDI functions at the enterprise edge without deploying dedicated hardware at each connection.

- **Increased SD-WAN adoption:**
  As enterprises deploy SD-WAN, they're fundamentally looking for a more straightforward experience for their branch office networks. While SD-WAN is an essential aspect of enabling this simplicity and agility, a cloud-managed DDI solution with lightweight virtual appliances at the branch enables local survivability and helps organizations fully realize the benefits of SD-WAN.

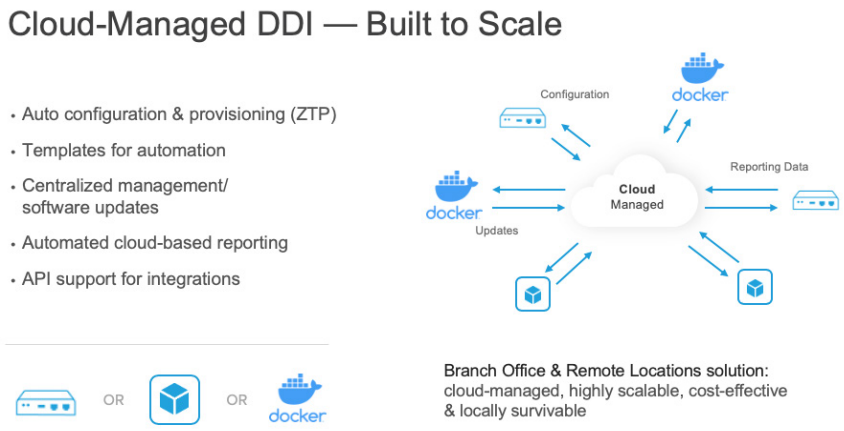

Figure 16: Scalability of Cloud-Managed DDI

A DDI solution that is cloud native and uses software-defined architecture for core network services such as DNS, DHCP and IP address management is the best fit for organizations interested in complete cloud migration in the near future. It helps deliver a uniform customer experience, paving the way for SD-WAN and IoT adoption, both of which are on a steep upward trend.

For a deeper dive into the drivers behind cloud DDI, here's an IDC Technology Spotlight, Unlocking the Power of the Cloud: Why SD-WANs Need Cloud-Enabled DDI

Unified DDI

Although many organizations firmly believe that the cloud is the future, they are not always ready to migrate their entire data center to the cloud at once for various reasons. Head office data security, network output and the IT team's preference for bare metal over virtual infrastructure are few of these reasons. In such scenarios, on-premises DDI solutions already integrated with virtualization platforms such as VMware or Microsoft Azure provide the needed feasibility with a unified DDI approach.

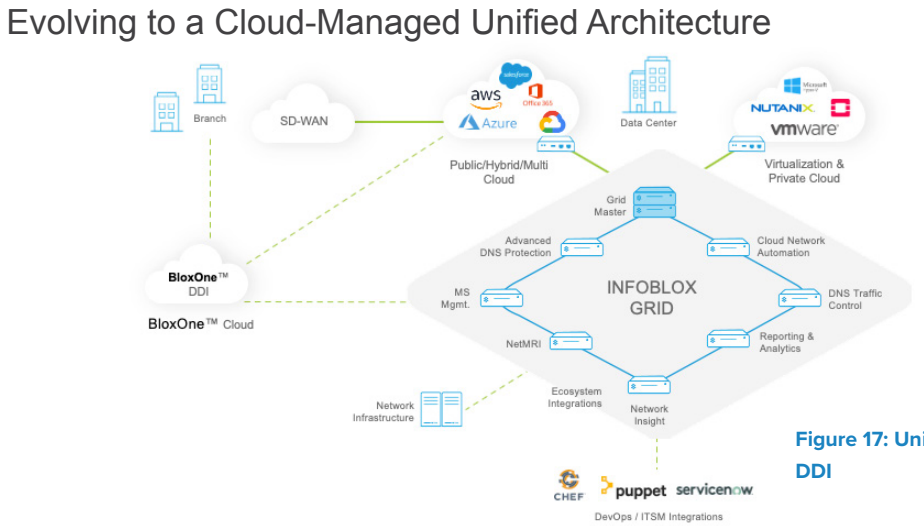

Figure 17: Unified DDI

To strike the fine balance between cloud-managed DDI and local survivability, unified DDI can be configured using lightweight commodity appliances sited on location. This helps ISVs and enterprises to build upon the existing on-premises DDI components and leverage cloud computing features. A strong selling point of unified DDI is that customers can continue using their current on-premises DDI solution as they migrate to cloud-managed DDI. In this way, organizations can:

- Streamline and automate complex DDI provisioning across on-premises and private, hybrid and public cloud deployments
- Centrally and automatically discover, track and monitor devices and assets across diverse physical, virtual and cloud infrastructure
- Automate the provisioning of DNS records and IP addresses for virtual machines
- Protect devices and data from the widest range of DNS-based threats
- Take advantage of pre-built customized integrations with other network automation and orchestration platforms
- Maximize SOC efficiency with faster threat investigation and research

Unified DDI deployments offer an architecturally efficient, centralized point of visibility and control for on-premises data centers with visibility for remote locations and cloud SaaS environments; this single point of view is crucial for many unique business models evolving in the modern networking age.

Learn how NIOS enables cutting-edge computing with virtualization

Conclusion: Getting Ahead with Future-Ready DDI Services

Conventionally, organizations used DDI as a facilitator for business processes and workflows. While this holds true even today, the future is much more challenging. Several factors, such as increased attacks on DNS servers, the emergence of IoT platforms, the proliferation of BYOD at the workplace, cloud transformation, SDN adoption and the surge in remote working, are the major market trends that reinvent the DDI paradigm.

It would be too much to say that no one could have predicted the COVID-19 pandemic. Indeed, public health and infectious disease experts have been warning for years that global society was vulnerable to exactly the kind of global catastrophe that struck in early 2020. Perhaps less understood were the second-order effects, especially all of the IT priorities that had to be reshuffled to accommodate a global workforce relegated to hundreds of millions of home offices.

How many IT decision makers said in late 2019: "We need to optimize our DDI infrastructure because our workforce is now 100 percent remote—and fast!"? Safe to say not many. The good news is that the DDI technology sector has advanced quickly in recent years, and those hard-pressed IT decision makers have a wide range of powerful, proven DDI solutions to choose from today—whether conventional on-premises systems, full cloud offerings or unified DDI approaches.

> *By 2023, there could be more than 20 times as many smart devices at the edge of the network as in conventional IT roles.*

Such key verticals as telecom and IT, banking, financial services, insurance, government and defense, healthcare and life sciences, education, retail and manufacturing have shown tremendous commitment to modernizing their DDI infrastructure. This modernization is possible with advanced DDI capabilities achieved by edge computing, distributed cloud data centers, virtualization and cloud applications. On-premises DDI is likely to continue to be the first choice among enterprises where security and control are the highest priorities. Yet as cloud and unified DDI approaches continue to close the gap in performance, security and manageability, these options will become increasingly attractive to IT decision makers.