SOLUTION BRIEF

BloxOne™ DDI

Optimizing Office 365 Access, Simplifying Cloud Workload Management

The Office 365 Dilemma

The upside promise of Office 365 was exactly what you needed—a distributed software as a service (SaaS) cloud that delivered improved collaboration and productivity through a variety of micro-services and applications. So, you made the investment and deployed. But now you have a dilemma. Corporate Office 365 users are happy, but branch and remote users are complaining about reliability and performance.

In the design and planning process, how branch and remote users connect to Office 365 is sometimes overlooked. That's because enterprise networks were originally designed to centralize data at the headquarter data center, not provide direct Internet access from the branch. Where branch and remote traffic is routed through headquarters before reaching the Internet, most user queries have to travel a long network distance before accessing files and data. In addition, running Office 365 in branch locations puts a considerable strain on network resources, increases exposure to malicious Internet activity and impacts performance and reliability. Because Office 365 is a global distributed service, connectivity comes through front doors scaled-out across hundreds of Microsoft locations worldwide (see Figure 1). Optimum user experience is achieved by routing network requests to the closest Office 365 entry point in the Microsoft Global Network, not the geographic location of the Office 365 tenant.

Core Network Services

All network and cloud interactions depend on core network services, including DNS, DHCP and IPAM (DDI). DDI plays a foundational role in all IP-based communications. The Domain Name System (DNS) is the starting point for every network conversation. The Dynamic Host Configuration Protocol (DHCP) is the foundation of network identity and access. And IP address management (IPAM) is the authoritative source for all network connected assets. For branch and remote users, these network services are essential for fast, reliable and secure access to Office 365.

However, most traditional DDI solutions are deployed within the core data center and are not designed to accommodate a direct-to-cloud service like Office 365. Expensive branch hardware and legacy backhaul workflows that route DNS traffic back to the headquarters data center before reaching the Internet substantially diminish performance, lower productivity and generate unplanned service interruptions. So, if your network is still running on legacy DDI, Office 365's initial value and benefits are at risk and could, in fact, be costing you. How do you resolve this dilemma? Move your core network services to the cloud.

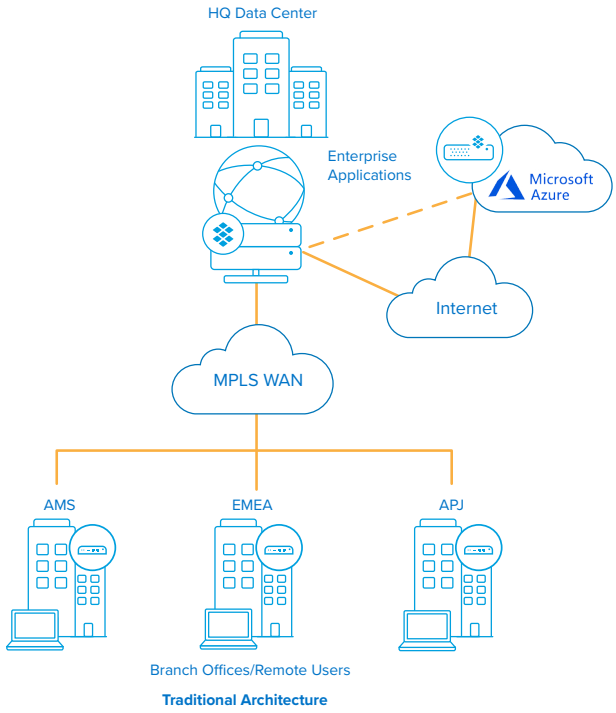

Figure 1: With traditional network architecture, traffic from remote locations had to route back through the HQ data center, and did not provide for direct connections to cloud apps from the branch.

DDI in the Cloud—Optimized Access, Simplified Workload Management

BloxOne™ DDI from Infoblox is the industry's first cloud-managed solution for core network services. BloxOne is the transformative, best-in-class platform from the core network services market leader and is designed specifically for the cloud. It's built on the basis that cloud applications require cloud DDI. Unlike traditional or old school network architectures, BloxOne DDI optimizes user experience and workflows by always connecting users to the nearest point of entry in the cloud. So, whether users are at headquarters, in branch offices or working remotely, they can connect reliably to Office 365 and all other SaaS applications. BloxOne's local DNS and DHCP architecture also enables branch and remote users to stay connected to cloud-based applications regardless of network service interruptions at the corporate headquarters. This design means reliability for thousands of remote offices, optimizing Office 365 access and improving user experience for performance and productivity.

BloxOne DDI is easy to scale and available through subscription for virtual machines or on-premises commodity devices, delivering significant savings through lower hardware costs. BloxOne DDI's cloud-first approach simplifies cloud workload management by centralizing and automating core network services. This approach allows network administrators to manage more users and environment workloads in less time.

The Challenge of Digital Transformation

In the familiar model of legacy architectures in traditional data centers, organizations established a strong perimeter defense against security threats, data infiltration, exfiltration and malware. But now, users no longer only have access to applications and data from inside the security perimeter, over dedicated WAN links from branch offices or remotely through VPN tunneling. Instead, users also have access to cloud applications directly from everywhere. Office 365 and SaaS have moved services and data outside conventional security infrastructures, shifting the secured perimeter exponentially as the cloud clearly has become the new network.

Further, networks are becoming increasingly complex, diverse and geographically distributed. By 2030, it's estimated that 80 percent of all new applications will be deployed in the cloud.[1] Organizations may have a private cloud, public cloud and hybrid cloud. Some parts of the network may have aging physical infrastructure running outdated software or firmware. These complexities combined with the increase in mobile connections raise the risk of rogue, unsecured and non-compliant devices that can easily be compromised and thereby impact service availability and performance.

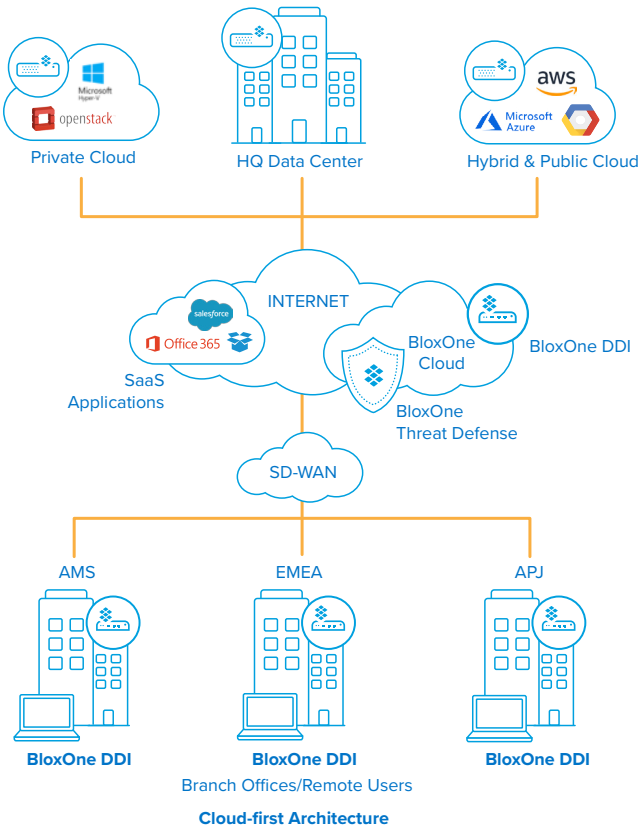

Figure 2: With BloxOne DDI, remote and branch office users can directly connect to the closest instance of Office 365 and other cloud-based SaaS apps.

Beyond this move to the cloud, the shift to SD-WAN is driving network transformation. Fully 95% of IT decision makers report that they've deployed or plan to deploy SD-WAN in the next two years.[2] While this use of SD-WAN enables branch offices to connect directly to the Internet, most branch offices do not have the security protection found in headquarters data centers, leaving them susceptible to attack.

Moreover, the rapid proliferation of connected IoT devices opens new inroads to security vulnerability. By 2030, experts estimate that there will be over 125 billion network-connected IoT devices.[3] However, these lightweight IoT devices typically are not robust enough to carry sufficient endpoint security to provide adequate protection.

Business disruptions from security events are costly from a financial, brand image and operational perspective. Recently, Norsk Hydro suffered a $40 million initial loss from a ransomware attack. Facebook lost $119 billion from its market cap after the Cambridge Analytica breach. These are just two of the escalating cases featured in daily media reports. DNS-based

1. LogicMonitor's Cloud Vision 2020: The Future of the Cloud Study. https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/#de066fc6261a.

2. IDC TECHNOLOGY SPOTLIGHT - Unlocking the Power of the Cloud:Why SD WANs Need Cloud Enabled DDI. August 2019.

3. The Internet of Things: a movement, not a market. IHS Markit. https://technology.ihs.com/596542/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030-ihs-markit-says.

attacks remain the number one attack vector, as statistics on cyberthreat frequency, complexity and impact continue to increase. Making matters worse, the Ponemon Institute reports that the average time taken to identify a breach is 196 days, notwithstanding the challenges and time required to recover after a catastrophic event.

How then, do we protect an infinitely growing perimeter against ever-increasing cyberthreats? As cloud applications require cloud-based DDI, so do they require an equally proficient cloud-based security solution.

Security in the Cloud—Precise Visibility, Scalable Protection Everywhere, Automated Response

Not stopping at cloud-based DDI services, Infoblox also delivers best-in-class cloud-based security. BloxOne Threat Defense protects headquarters, branch and remote users, data and infrastructure from cyberthreats, automatically from the cloud. It guards your brand by securing existing on-premises networks as well as those in the cloud. It drives security orchestration, automation and response (SOAR) solutions, slashes time to investigate and remediate cyberthreats, optimizes the performance of the entire security ecosystem and reduces the total cost of enterprise threat defense.

Using deep integrations with DDI as the foundational security architecture, BloxOne Threat Defense turns core network services into your most valuable security asset. Combining BloxOne DDI with BloxOne Threat Defense enables your entire security stack to work in unison and at Internet scale to detect and anticipate threats sooner and stop them faster.

With BloxOne Threat Defense, organizations can secure every connection regardless of device or location across physical, virtual or cloud infrastructure. By sharing real-time data, security teams can slash incident response times by two-thirds. Access to rich network context and aggregated threat intelligence data powers the performance of SOAR platforms. Further, it drives productivity, making threat analysts three times more efficient, providing single-pane-of-glass visibility, including forensic data for complete investigative review. It also blocks DNS-based data malware and exfiltration activity by closing communication channels used by malware, Domain Generation Algorithm (DGA) and dozens of other threats.

BloxOne DDI and BloxOne Threat Defense from Infoblox—next level simplicity, reliability, and security for today's cloud-based world. Because the network that works best is the network you never notice.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com