Infoblox
NEXT LEVEL NETWORKING

WHITE PAPER

Empowering Digital Transformation

Core Network, Value-Added and Security Services

TABLE OF CONTENTS

Executive Summary

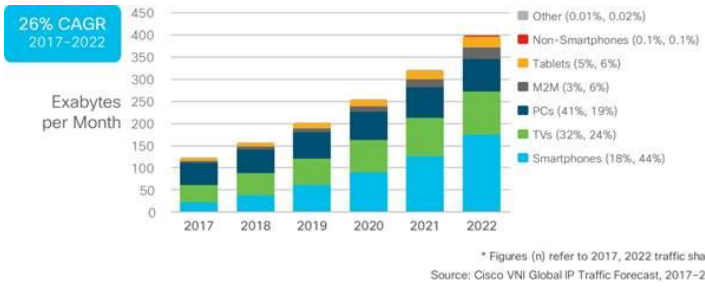
If your organization is struggling to keep pace with changing network technologies, we have good news—you can still positively impact customer satisfaction, raise customer loyalty and optimize your network for competitive advantage. Technology advancements are rapidly raising the bar on customer and employee experience and expectations. Applications must be available, fast, reliable and resilient for gathering and exchanging information, evaluating and buying products and services. Market leaders are deploying the latest technologies to make information more accessible and workflows faster, easier, cheaper and more reliable. Technologies like Office 365 and SaaS, multi-cloud, SD-WAN, IoT and hybrid security are defining and empowering a new connectivity paradigm to improve customer experience, speed to market, supply chain management and employee productivity. These intertwined business and technology trends have come to be understood as an integral movement: digital transformation. This whitepaper explores how emerging network technologies are driving digital transformation forward. We consider how disruptive network technology trends, modern network needs and gaps, a vision for future-ready services, and how organizations – even those lagging behind – can catch-up and take the lead in delivering an improved customer experience both now and in the future.

Digital Transformation

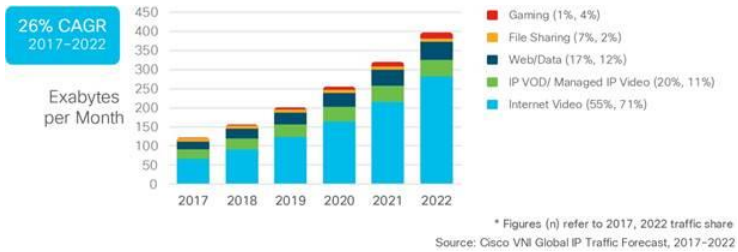
Digital transformation is changing virtually every aspect of our lives – how we connect, how we work, how we play and how we live. Organizations are applying the latest technologies to make life better. And the trend toward digital has already transformed a breadth of industries. Consider: Airbnb has re-configured and massively expanded lodging with privately-owned accommodations now easily available through an AI-powered web interface. Digital has re-delivered transportation services through non-corporate-owned Uber and Lyft vehicles. It's underwritten and funded loans in seconds without traditional credit scoring. It's driven and parked our cars without our engagement. And it's generated economic, social and personal value through a staggering exchange of global data among people, business, industries, networks and devices across every market vertical 24/7/365.

Expanding Global Connectivity

A major part of digital transformation is the sheer volumetric explosion of IP addresses and the related implications for core network services. According to the Cisco Visual Networking Index, global IP traffic is projected to grow at a compound annual growth rate of 26% through 2022. By then, it's expected that there will be 28.5 billion networked devices, up from 18 billion in 2017. Devices connected to IP networks are expected to exceed three times the global population. Wireless and mobile device traffic is expected to account for 71% of total IP traffic by 2022, while global IP video traffic will comprise 82% of all combined business and consumer IP traffic. To manage the increasing IP demands on private, public and hybrid cloud networks, organizations will need authoritative, scalable, resilient and secure platforms that can ensure visibility, automation and control. Delivering on the promise of always available and performing applications requires network modernization to match technology advancements and integrated end-to-end solutions to meet business demands and customer expectations.



* Figures (n) refer to 2017, 2022 traffic share
Source: Cisco VNI Global IP Traffic Forecast, 2017-2022



* Figures (n) refer to 2017, 2022 traffic share
Source: Cisco VNI Global IP Traffic Forecast, 2017-2022

Network Modernization with Core, Value-Add and Security Services

What are the foundational components required for the modern network? A combination of core, value-added, ecosystem and security solutions make up the minimum core components. And with tech advancements and lower-cost subscription models, functionality previously considered optional is now not only more affordable, it's become essential for visibility, automation and control in the modern network. Any list should begin with the following:

- **DNS, DHCP & IPAM (DDI):** All network and cloud interactions depend on core network services including DNS, DHCP and IPAM (DDI). All play a foundational role in IP-based communications. The Domain Name System (DNS) is the starting point for every network conversation. It translates common, memorable alphabetic domain names into numeric Internet Protocol (IP) addresses used by web browsers to find unique devices, interact and exchange resources. Dynamic Host Configuration Protocol (DHCP) is the foundation of network identity and access, and provides quick, automatic, central management and distribution of IP addresses to connect devices to networks. Finally, IP Address Management (IPAM) refers to the planning, tracking and management of DNS and DHCP services that assign and resolve IP addresses for machines on the network. With accurate network endpoint discovery, IPAM becomes the authoritative source for all network-connected assets.
- **Microsoft DNS/DHCP Sync Overlay:** Microsoft manages its own DNS and DHCP endpoints, but today's environment presents far more endpoints than Microsoft alone. For this reason, an agentless DDI overlay is non-optional for retaining Microsoft protocols, eliminating IP conflicts, DHCP and network outages, enabling and syncing full discovery of network endpoints, Active Directory (AD) Sites and Services and user/IP mapping. This is essential for visibility, automation, orchestration, cross-team collaboration, reporting and control.
- **On-Premise Network Discovery:** A detection tool is needed to enable full, accurate and automated discovery of layer-2 and layer-3 assets, visibility, IPAM sync, switch port management, rogue and compromised asset discovery, IP conflict resolution, reporting and analytics across geo-diverse on-premises, wireless and SDN environments for efficient, automated workflow management.
- **Multi-Cloud Discovery:** Like on-premise discovery and automation, a unified multi-cloud (e.g., VMware, OpenStack, Azure, AWS) integration solution is required for IPAM discovery and visibility, DNS/IP provisioning, virtual server DDI policy-based automation, DDI auditing and reporting.
- **Hybrid Security Ecosystem:** No one solution can possibly address all of the DNS-based global security risks that threaten daily network functions. That's why it's critical to leverage, integrate and automate with the leading network security solutions to activate a vast security network to protect your organization. Such a system automates quarantine and scans of newly discovered assets, real-time remediation and TrustSec policy via integrations with leading security vendors (e.g., McAfee, Cisco, Carbon Black, FireEye, etc.) and threat data sharing with endpoint, Network Access Control (NAC), Security Information and Event Management (SIEM) tools and many more.
- **Global Server Load Balancing (GSLB):** With the increasing volume of global network traffic and applications, a GSLB tool is an essential component to ensure reliable app uptime, performance and seamless failover. Organizations must have a method for distributing network traffic across geo-diverse, on-premise, public and hybrid cloud environments for ecommerce, customer-facing portals, web and internal business-critical applications. They must also have a way to control and restrict GDPR and privacy data within regions while ensuring business continuity and seamless disaster recovery (DR) in the event of a catastrophic event.
- **Reporting and Analytics:** Organizations possess a wealth of data in their networks, but the challenge is instant visibility, access and how to make that data actionable. That's why it's essential to have a reporting tool with pre-built and customizable dashboards and reports, search, predictive analytics, and data visualizations for endpoint, performance, deep security forensics, query logging, audit and control.
- **DNS Security:** DNS is the most common application attack vector for malware, data infiltration and

exfiltration. There have been over 780 million malware attacks in the past 10 years and that number is increasing daily. According to the Ponemon Institute, it takes over 196 days on average to identify a breach, and by then, business disruption and brand impact have already taken their toll. Without question, DNS protection is non-optional. It must intelligently monitor, detect and stop all types of DNS attacks, enable legitimate queries, maintains DNS integrity, adapt to evolving threats to improve rapid threat remediation.

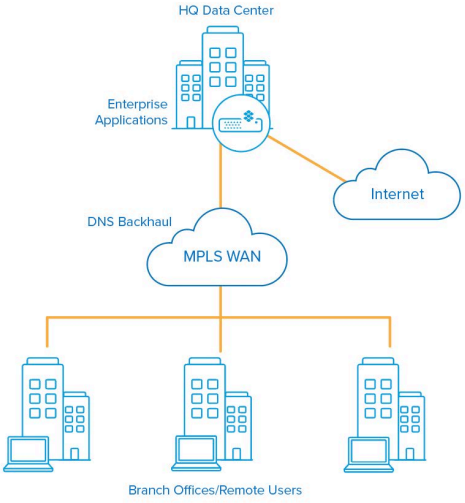
- **Cloud-Managed Security:** Today's security threats require a hybrid approach to secure every connection regardless of device or location across physical, virtual and cloud infrastructure. As organizations adopt hybrid-cloud architectures, they will need to integrate security orchestration, automation and response (SOAR) solutions, cut the time to investigate and remediate cyberthreats, optimize their security ecosystems and reduce threat detection costs – all in the pursuit of detecting and stopping threats faster.

These components should be integrated to share real-time data across teams and geographies through a single platform. They'd also be adaptable to a growing array of new technologies that are disrupting today's network landscape. We'll explore these components further, but let's take a brief look at the disrupting technologies they will have to support, including Office 365/SaaS, multi-cloud, SD-WAN, IOT and hybrid security.

Disrupting Network Technologies

Office 365/SaaS[1]

Organizations are moving from initial adoption to mainstream deployment of Office 365/SaaS applications – and for a variety of reasons. SaaS offers a lower cost-of-entry, using only what you need and paying as-you-go so that your costs are more predictable. SaaS provides rapid integration, prototyping and reduced time-to-benefit, thanks to quicker enterprise deployment. It also delivers upgrades, uptime, security and scalability. Plus, it allows access from anywhere there's an Internet connection. It's a combination of factors that add up to greater mobility, flexibility and productivity. To enable this technology, conventional network architecture is no longer adequate. A new architecture is required which in turn is driving network transformation.

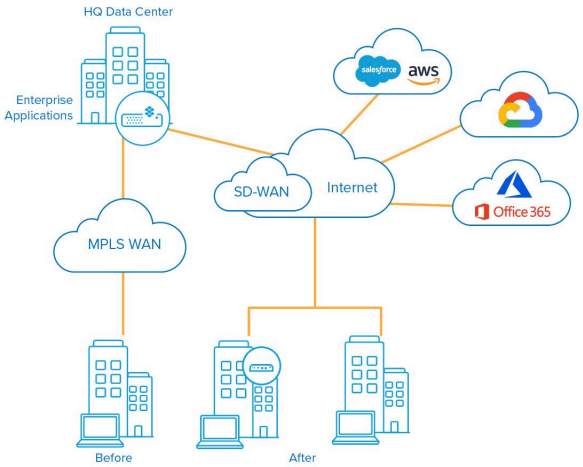


Traditional Architecture

Multi-Cloud[2]

It's estimated that 80% of new applications will be deployed in the cloud by 2030. Companies are choosing to distribute assets, redundancies, software and apps across several cloud-hosting environments to gain some distinct advantages. Multi-cloud strategies provide direct access to applications from everywhere and allows the choice of service based on geo-location for lowest latency. It also supports agnostic vendor choice and service selection to pick the best vendor offering to meet company needs. Further, multi-cloud promotes negotiating power and decreases dependency on a single vendor. It also lowers the risk of DDoS attacks and enables Disaster Recovery because application replicas can be kept in separate clouds and take the load during

delays or outages until service recovers. Multi-cloud also provides reliability, flexibility, agility across cloud and enterprise, scalability and cost-performance optimization.



Transforming Architecture: Multi-Cloud, SaaS & SD-WAN

SD-WAN[3]

Research estimates that 40% of enterprises expect to adopt SD-WAN by end of 2019. SD-WAN removes expensive routing hardware and provisions connectivity and services from the cloud. It enables organizations to eliminate a poor branch and remote user access experience, unreliable app performance and outages, and high opex and capex costs. It provides full visibility into the network, centralizes management across branch networks, increases bandwidth at lower cost, and ensures a consistent connection to branch geo-local apps and services. Overall, it delivers greater responsiveness, agility, control, security and local survivability.

IoT[4]

Gartner predicts that 5.8 billion IoT enterprise and automotive endpoints will be in use in 2020, growing to an estimated 125 billion by 2030. Utilities will deploy residential and commercial electrical smart metering IoT devices followed by physical security, intrusion detection and surveillance. Building automation through connected lighting devices, is expected to expand the most, while automotive, through specific embedded devices for service monitoring and fleet management, and healthcare, through chronic condition monitoring, are also expected to drive key growth areas. Networks must transform to manage the connectivity, capacity and security of these exponentially exploding volume of IoT endpoints.

Hybrid Security[5]

With the adoption of Office 365/SaaS, multi-cloud, SD-WAN, and IoT technologies, along with the unprecedented rise in cyber threats, data breaches, malware and DNS-based network attacks, the traditional security model can no longer sufficiently protect customer and corporate data and infrastructure. Perimeter security at the corporate datacenter simply can't keep up with the expanded threat surface of these disruptive technologies are propagating. The once finite headquarters security perimeter has given way to a boundless cloud perimeter as users access cloud applications directly from everywhere. Further, branch offices and remote users also connect directly to the Internet without the protection of the corporate security stack. It's simply too costly to deploy a full security solution in branch offices, and branch office firewalls are not adequate protection against malware attacks and data breaches that can compromise an entire organization. In addition, lightweight IoT devices do not have the capacity for full endpoint security. As if all these challenges weren't enough, additional issues such as siloed organizational structures, manual tools, lack of automation and limited security resources, all call for a new security approach and architecture to cover identity and access, critical services, physical security, data and infrastructure.

Transforming the Modern Network

Operational Service Gaps and Customer Experience

As disruptive technologies challenge existing standards, architectures, systems and processes, frequent and painful service gaps emerge across various use cases when operating in a traditional MPLS-WAN environment. These gaps impact customer experience and satisfaction and include access issues, delays, outages, manual, error-prone processes, lack of visibility, agility and automation, security vulnerabilities, high costs and more as noted in the table below:

Use Case	Attributes	Customer Experience Gap
Traditional HQ datacenter with branch offices	• Physical networking • Manual, static DNS/DHCP configurations • Spreadsheet managed DNS, DHCP & IPAM • Silos • Perimeter security	• Service delays & outages • Manual, time consuming, error-prone processes to sync cloud & enterprise deployments • Lack of automation • Security deficits
SaaS, migration from MPLS-WAN to SD-WAN	• As above plus… • DNS backhaul • Disparate array of DNS systems (Azure DNS, Cloud DNS, Route 53)	• As above plus • Poor user access • Poor app performance & reliability during WAN outages • High cost of core DNS, DHCP & IPAM & edge services • SaaS app best performance depends on user's closest cloud entry point • Lack of edge service visibility
MPLS-WAN to Multi-Cloud	• Disparate array of DNS systems (Azure DNS, Microsoft Server, Cloud DNS, Route 53, BIND) • Multi-Cloud management	• Service delays & outages • Manual, time consuming, error-prone processes to sync cloud & enterprise deployments • Lack of visibility & automation, complexity, policy management • Poor agility across cloud & enterprise • Cost management, fewer discounts • Skill challenges across various clouds • Security risk due to larger attach surface
SaaS & SD-WAN Security	• HQ security stack in the corporate datacenter • Limited security protection through stateful firewalls at the branch	• High cost to deploy the full HQ security stack at the branch • Increased exposure of SD-WAN branches to malware attack and data breach
SIEM/Soar Integration	• Manual tools & data collection • Silos	• Poor agility • Lack of visibility & automation • Long incident response times

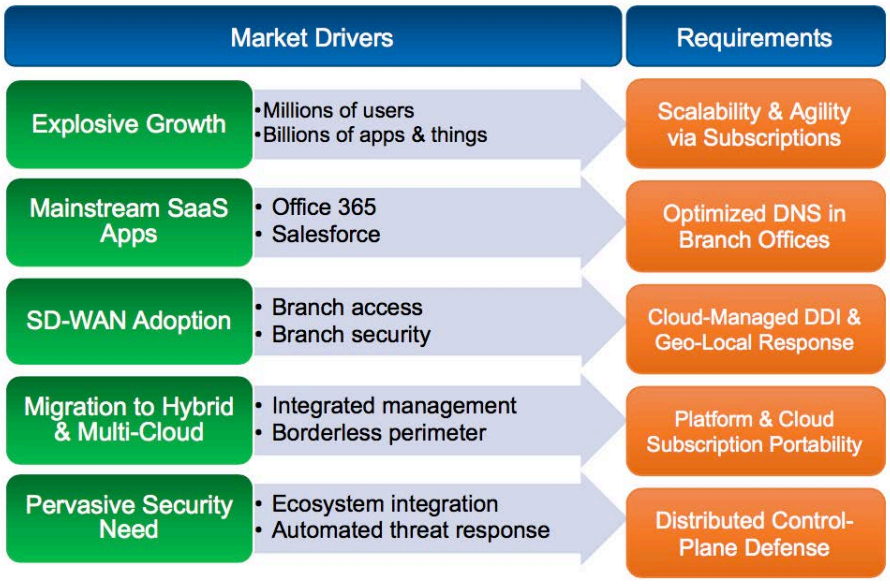
Modern Network Needs

In view of the transforming technologies and user expectations, these gaps highlight the needs of a modern commercial network:

- **Reliability**—Ensuring five-nines, 24/7/365 access and performance for optimal customer and user experience
- **Security**—Protecting data and infrastructure and minimizing impacts from threats, attacks malware, and breach
- **Extensibility**—Scaling locally and globally to meet business requirements
- **Manageability**—Reducing complexity, increasing agility and automating for efficiency
- **Cost Efficiency**—Managing operations to deliver quality at the lowest overall cost

Infoblox Delivers on Changing Network Requirements

Disruptive technologies, customer experience, service gaps and network needs all influence market drivers, which in turn fuel new requirements as noted in the table. With each successive wave of technology, from Private Cloud, to Hybrid/Multi-Cloud, to Software Defined, to Containerization and Cloud Native, the gap between commercial needs, capacity and budget to deliver on company objectives only widens. This is why Infoblox developed Next Level Networking—to optimize customer experience, enable future-ready network services, define a roadmap to execute on corporate objectives, and deliver market-leading solutions to support the journey.



Next Level Networking

DDI Core and Value-Added Services

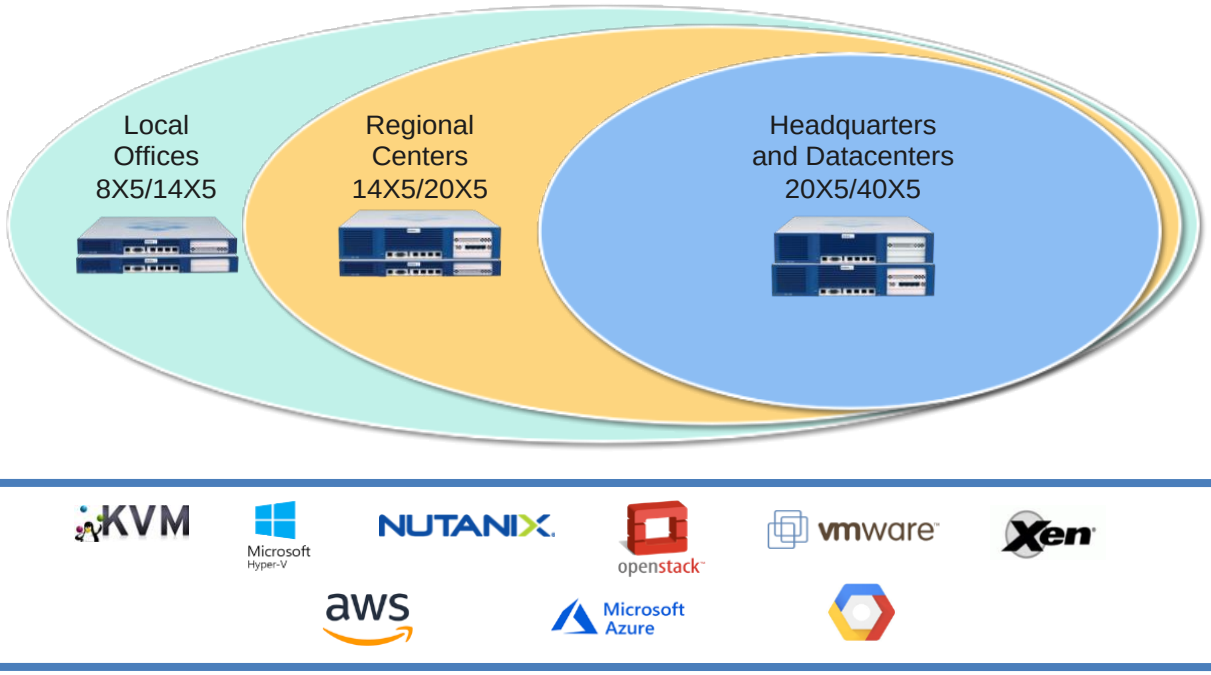
Next Level Networking is founded on physical and virtual appliances purpose-built for security and reliability, an integrated, authoritative and resilient database of DNS, DHCP, IP (DDI) and device data, and automation with templates, wizards, APIs and attribute inheritance. Let's take a closer look.

XXX5 Trinzic Appliances

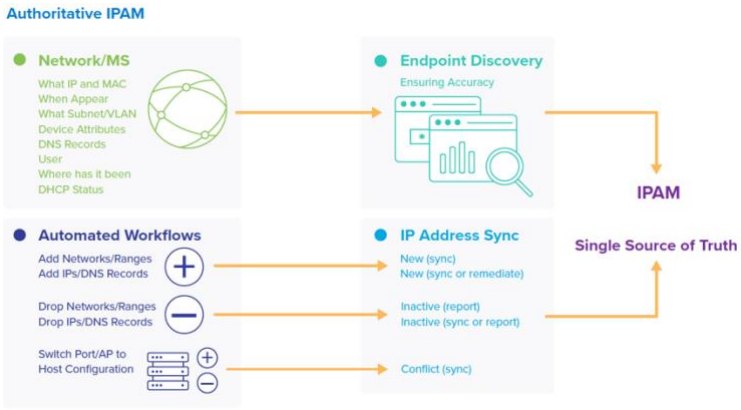
Infoblox XXX5 Trinzic Appliances

- Deliver better performance (on NIOS 8.4)
  - DNS: 2-3X performance improvement
  - DHCP: 38% faster
- Enable digital transformation to hybrid, multi- & public clouds
- Add new network drivers
- Deploy core network services without impacting DDI performance
- Empower value-added services
- Aligns with the NIOS roadmap

At the center of the Infoblox solution are the XXX5 Trinzic physical, virtual or cloud-based appliances. These are the latest generation of reliable, security-hardened, automated, distributed, high-availability and easy-to-manage machines that power Infoblox core network, security, cloud and the essential value-added service solutions. For Infoblox customers seeing age-related impacts of XXX0 generation Trinzic machines nearing the end of their nine-year tech support window (TE-8X0/14X0/22X0, 2/15/21; TE-40X0, 10/28/21), the XXX5 Trinzics enable an array of applications with the speed, capacity and functionality required to get the most from emerging digital technologies. They deliver a 2-3X performance improvement for DNS and 38% improvement for DHCP (based on tests running NIOS 8.4). Trinzic XXX5s provide the latest network drivers, deploy network services without impacting DDI performance, empower value-added services and are compatible with the NIOS development roadmap. They are designed to empower and optimize Infoblox value-added solutions, and improve the visibility, security, reliability and performance of branch office networking. They deliver the latest application features, offer portability between physical, virtual and cloud appliances and support predictable budget cycles.



Authoritative IP Address Management (IPAM)

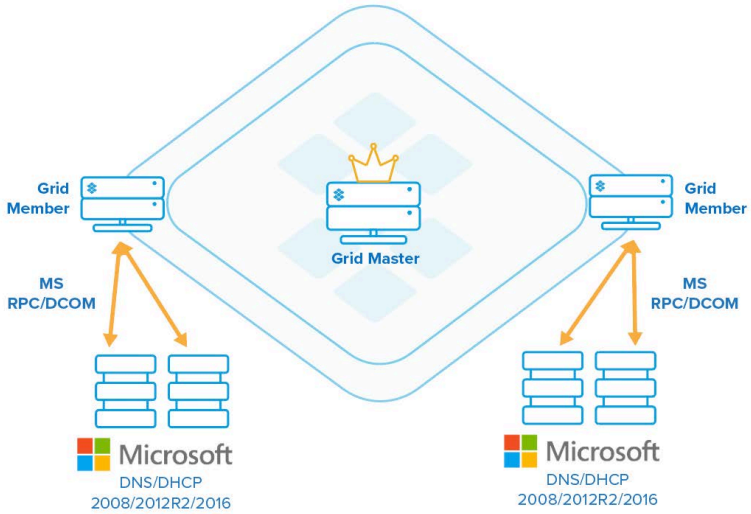


Authoritative IPAM provides a single-source of truth to accurately reflect the state of your network. It provides contextual visibility (i.e., the who, what, why, when, how, where and which) of your network assets (e.g., IP addresses, subnets or VLANs) and enables you to replace manual, error-prone tools and processes with efficient, automated workflows. It automatically delivers accurate visibility into network asset types, attributes, availability, user context, network activity, location, network type (on-premises, hybrid cloud, wired, wireless, SDN), topology, vendor infrastructure and more. It includes IPAM, Microsoft Management, and two discovery tools: Network Insight for on-premises discovery and Cloud Network Automation (CNA) for cloud discovery. These tools ensure full visibility, an accurate authoritative database, and a single source of truth to enable network automation for greater efficiency and cost savings.

IPAM – Network-Connected Assets

The Infoblox Grid simplifies and delivers IPAM as an on-premises and/or cloud, manual or automated core network service, for significant labor, time and workflow savings and resiliency. End points and applications that need IP addresses can be served in a consistent, automated and error-free manner through the Infoblox IPAM interface.

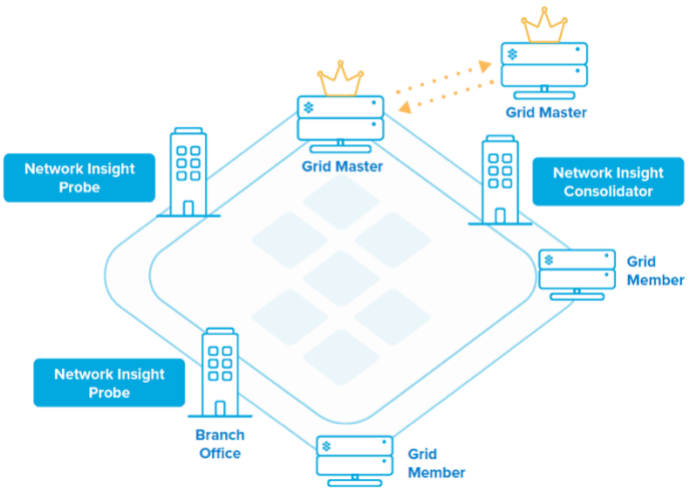
Microsoft Management – DNS/DHCP Overlay



With the skyrocketing demand for IP addresses fueled by ever-increasing applications, personal devices, IoT, IPv6, virtualization and more, many organizations struggle to manage IPs efficiently to deliver highly available network services. The struggle is greater for organizations preferring to retain existing Microsoft-based DNS/DHCP servers. These organizations are finding that in order to keep pace with IPAM scalability, redundancy and security needs, more servers, added technology and an automated IPAM system are essential. Infoblox Microsoft Management solves these challenges. By keeping the existing Microsoft DNS/DHCP protocols, Microsoft Management provides a non-intrusive agentless overlay to enhance the value of the existing Microsoft investment. It delivers central DNS/DHCP integration and management, automated DDI component syncing, cross-team collaboration, Active Directory Sites and Services integration and user/IP identity mapping. Infoblox Microsoft Management also provides resource planning for full visibility to solve IP conflicts, DHCP availability issues and network outages.

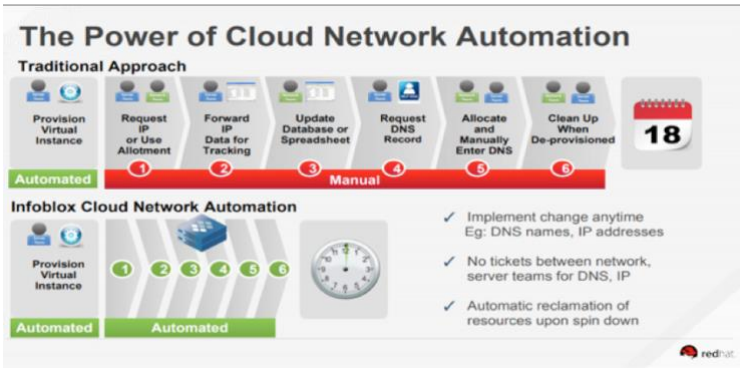
Network Insight – On-Premises Discovery and Control

If you manage geo-diverse, on-premises, wireless and SDN environments, end-to-end accurate and automated end-point discovery is essential. Network Insight delivers on-premises discovery, visibility, IPAM sync, switch port management and control. It unveils deep discovery of network devices, end-hosts, subnets, interfaces, components and topology. Finally, it detects and remediates IP conflicts and rogue and compromised assets, supplies continuous syncing of networks and IPs into IPAM, and automates router and switch port provisioning to keep you in control.



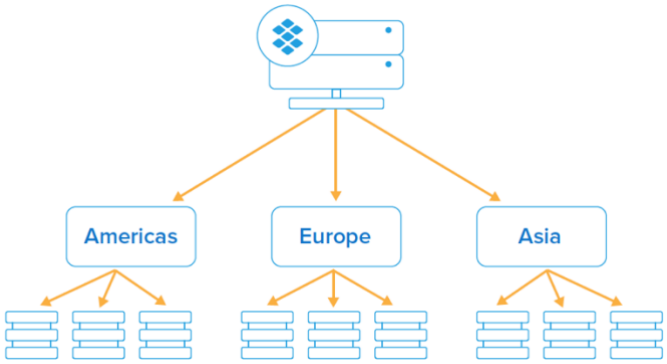
Network Insight Advisor is a critical value-added service that provides proactive monitoring of security advisories (end-of-life and end-of-service) to keep you current on network assets, so you don't inadvertently allow security vulnerabilities into your network.

Cloud Network Automation – Multi-Cloud Discovery and Control



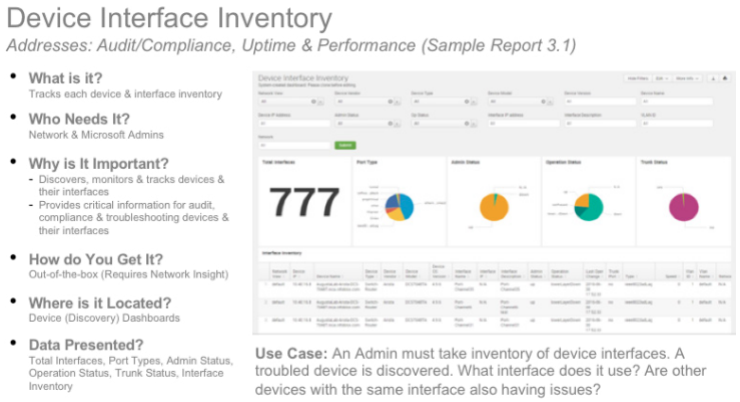
Like Network Insight for on-premises environments, Cloud Network Automation delivers IPAM discovery and visibility for assets located in the private, public or hybrid cloud. It's an indispensable tool that provides multi-cloud discovery, DDI sync and control for organizations with cloud initiatives. Not only does it supply visibility into AWS, Azure, Google Cloud, OpenStack and VMware platforms, it automates DNS/IP provisioning and deprovisioning, and coordinates allocation and release of IP addresses and DNS registrations with orchestration tools across servers, networks and storage. Authoritative IPAM ensures accurate DDI resource distribution across a hybrid environment—all from a single pane of glass. Automating manual processes can change workflows from days to seconds, increasing accuracy, reliability, coordination and efficiency. Plus, Infoblox has out-of-the box integrations with leading orchestration tools like Ansible, VMware vRA, CNI Kubernetes and more.

DTC — Global Network Traffic Control



DNS Traffic Control (DTC) is an affordable, integrated DNS Global Server Load Balancing (GSLB) solution that improves end-user experience, simplifies global traffic management and reduces capital and operating expenses. It delivers business continuity, reliable application uptime, high availability (HA), resiliency and disaster recovery (DR) by distributing network traffic across geo-diverse, on-premise, public and hybrid cloud environments for e-commerce, portals, web and internal business-critical applications. DTC Integrates authoritative IPAM with DNS and GSLB to intelligently direct user traffic to optimal servers. It provides a broad range of configurable balancing algorithms, along with flexible, automated, health checks to ensure server availability. It's scalable to meet changing data volumes and business needs. For optimal visibility, DTC uses a simple user interface and visualizer that displays Load Balanced Domain Names (LBDNs), pool and server relationships and attributes. Unlike other Application Delivery Controllers (ADCs), it allows real-time, pre-production testing of LBDNs, pools and servers to ensure readiness before go-live. DTC uses GeoIP and Extensible Attribute data to control traffic to region-specific zones for regulatory and privacy compliance (e.g., GDPR). A separate but integrated Splunk-based Reporting and Analytics tool offering pre-built and customizable DTC dashboards, reports, search, alerting and automated report distribution is available. Finally, DTC automates workflows by discovering, creating and controlling topologies using IP subnet, GeoIP and Extensible Attribute data. APIs can quickly add new server instances, provision new apps, integrate with other systems and automate routine tasks. Grid software deployments, configurations and updates are managed through a few clicks, saving time and money and resources, making DTC an essential tool for digital transformation.

Reporting and Analytics – Full Network Visibility



Use Case: An Admin must take inventory of device interfaces. A troubled device is discovered. What interface does it use? Are other devices with the same interface also having issues?

If you can't see it, you can't manage it. Infoblox Reporting and Analytics delivers summarized, granular and predictive analytics for full network visibility and quick problem resolution. Built on Infoblox DDI and the Splunk reporting and visualization engine, Infoblox Reporting and Analytics delivers fast plug-and play deployment, role-based access control, historical search, real-time alerting and predictive analytics to help you get the most from your data and network. It enables deep visibility into network data on-premises and in the private, public and hybrid cloud through a central management platform. Including over 100 pre-built, customizable dashboards and reports, Reporting & Analytics provides the flexibility to adjust filters, create new dashboards, reports, set distribution lists, alerting thresholds and frequencies and much more. Data is presented in summary view but thanks to the deep DNS-based integration, it's also accessible through granular query logging for security forensics and actionable, on-demand tracking to support audit, forecasting and control. Since query log data can place a considerable processing load on core network services, Infoblox provides a Data

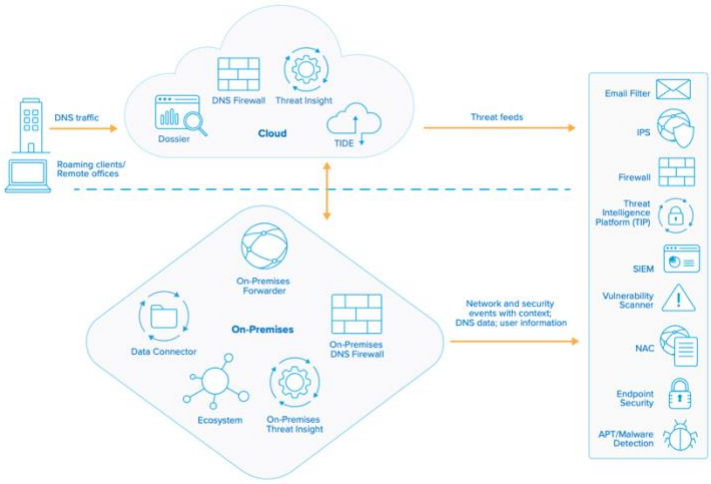
Connector that offloads much of the processing impact to keep services running at peak performance. Reporting & Analytics is the tool needed to see and manage everything on your network.

Security Solutions

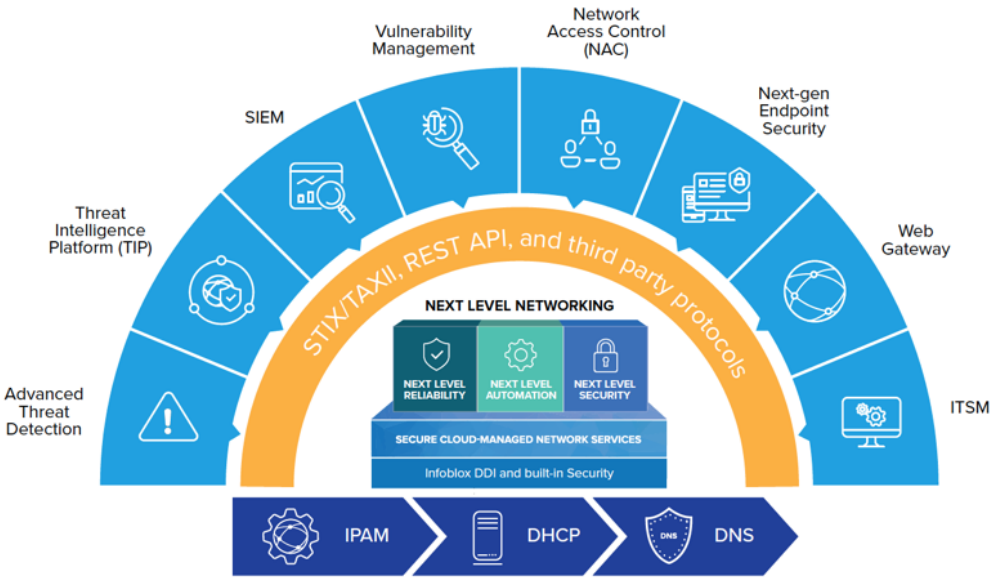
BloxOne Platform—Cloud-Managed Network Services

As noted earlier, technologies including Office 365/SaaS, multi-cloud, SD-WAN, IoT and hybrid security are driving critical business applications to the cloud. The Internet's edge is expanding to branch offices. Software defined solutions are simplifying workflows. Branch offices and remote users are increasingly in need of local access to applications to perform essential business functions. In the pursuit of digital transformation, organizations increasingly realize the need for agile, scalable and secure network services. In response, Infoblox developed the BloxOne Platform to make management of critical network services available from the cloud. BloxOne provides these services as containerized, scalable and highly customizable applications. This enables organizations to easily distribute functionality, including DDI and security, to the remotest parts of their operations, while improving customer experience and driving down cost. We'll now look at the first two BloxOne applications, BloxOne DDI and BloxOne Threat Defense.

BloxOne Threat Defense—Foundational Security at Scale

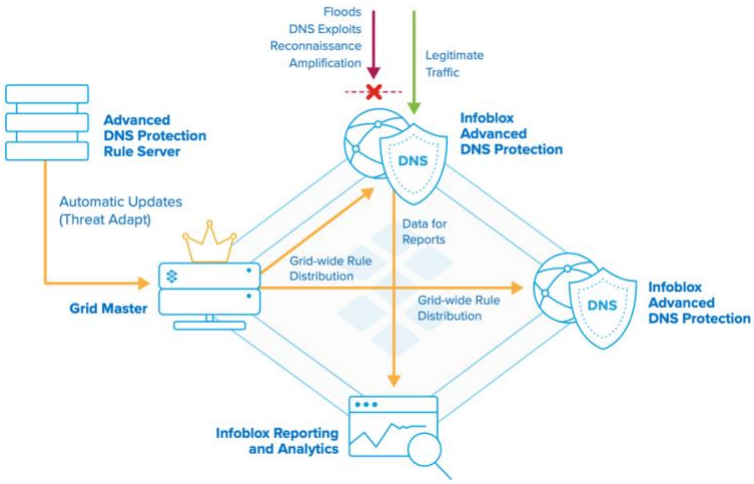


Infoblox BloxOne Threat Defense strengthens and optimizes your security posture from the foundation up. It maximizes brand protection by securing your existing networks as you pursue Office 365/SaaS, multi-cloud, SD-WAN, IoT and 5g initiatives. It uses a hybrid architecture for pervasive, inside-out protection, powers security orchestration, automation and response (SOAR) solutions by providing rich network and threat context, optimizes the performance of the entire security ecosystem and reduces your total cost of enterprise threat defense. It maximizes the efficiency of your security operations center by reducing incident response time though automatically blocking malicious activity, sharing contextual threat data with your ecosystem and reducing reviewable alerts. It also unifies your security policy with curated portable threat intel that can be shared through existing security systems to improve effectiveness and reduce cost. BloxOne Threat Defense also makes threat investigation and hunting faster through contextual data, insights and research that enable quick, accurate decisions and make your threat analyst team 3x more productive. BloxOne Threat Defense's hybrid security approach protects network assets wherever you're deployed through analytics in the cloud, threat intelligence scaling, remote resiliency and survivability and extensive integrations with your security ecosystem.



Security Ecosystem—Integrated Contextual Threat Data

Infoblox Security Ecosystem is a highly interconnected set of integrations that significantly improve the security, efficiency and ROI of third party and multi-vendor assets throughout the cybersecurity network. It enables security, increases agility and enhances situational awareness across networks of any scale or complexity. Integrations eliminate silos between network and security teams and provide consolidated visibility of on-premises, virtualized and cloud infrastructure. By automating workflows, the Ecosystem accelerates remediation of threat and network changes, enabling organizations to raise network security, performance, efficiency and cost control to the next level. Automation is driven by accurate network database records, APIs and extensive security vendor integrations. Automation enables contextual data sharing and customization with security, configuration management database (CMDB) and service management tools. Ecosystem automates quarantine and scans of newly discovered assets and provides real-time remediation and TrustSec policy by sharing threat data with endpoint, NAC, SIEM and other essential security solutions. It engages billions of indices via seamless 3rd party integrations with Cisco, Splunk, MacAfee, ServiceNow, Rapid7, Carbon Black, Qualys, FireEye, LogRhythm and many more. Because organizations generally do not have adequate detection and staffing resources to track, prioritize and investigate all potential and real security risks, vulnerabilities and attacks, Security Ecosystem is the essential contextual security tool required to manage the digitally expanding threat landscape.

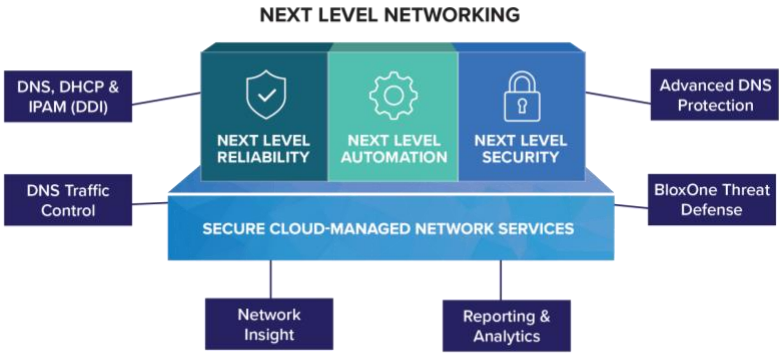


ADP – DNS Attack Defense

DNS provides mission-critical network connectivity to run your business. If your external DNS fails, your entire network is shut off from the Internet. DNS disruption impacts critical IT functions, including email, websites, VoIP and SaaS applications. Fortunately, Infoblox Advanced DNS Protection (ADP) delivers the widest range of DNS-based attack protection available. ADP continuously and intelligently monitors, detects and stops all types of DNS attacks including volumetric, low-volume stealth and exploits, while still enabling response to legitimate queries. It maintains DNS integrity and provides foundational security for five-nines network availability. Further, ADP adapts to evolving threats using Infoblox Threat Adapt™ technology to automatically update protection against evolving threats. Threat Adapt applies independent analysis and research to the latest attack techniques and changes configurations to automatically adapt for maximum DNS protection. ADP delivers full single pane-of-glass visibility into current and prior DNS attacks to improve rapid threat remediation. ADP leverages existing hardware and is deployed by license to keep costs low. It's the best protection available for on-premises and virtual DNS applications.

Infoblox's Vision—Core, Value-Added and Security Services

So, how does Infoblox empower digital transformation? It continues with a vision to take networking to the next level through reliability, automation, security and an integrated suite of secure cloud-managed, future-ready network services. Founded on security, our end-to-end solution is designed for physical, virtual and cloud architectures with a choice of capacities, leveraging extensive integrations and partnerships and delivering single pane-of-glass management to optimize customer experience.



In addition to DDI, setting Infoblox apart are the integrated value-added services no longer optional to the modern network. Not only are they critical for delivering customer experience, they provide the needed discovery, visibility, reliability, scalability, security, automation, and control that organizations need for actionable intelligence and decision-making:

- **Microsoft Management (DNS/DHCP Overlay):** Syncs Microsoft DNS/DHCP data into IP databases to capture visibility, eliminate conflicts and outages, and drive automation.
- **Network Insight (On-Premises Network Discovery):** Enables full on-premises endpoint discovery

into the authoritative IPAM database for visibility and automation.

- **Cloud Network Automation (Multi-Cloud Discovery):** Ensures private, public, hybrid and multi-cloud endpoint discovery into the authoritative IPAM database for visibility and automation.
- **Security Ecosystem (Hybrid Security Integration):** Integrates and leverages a breadth of existing and leading security vendors (e.g., McAfee, Cisco, Carbon Black, FireEye, etc.) to automate quarantines and scans of newly discovered assets, real-time remediation, TrustSec policy, threat data sharing and more with endpoint, Network Access Control (NAC), Security Information and Event Management (SIEM), and other hybrid security tools.
- **DNS Traffic Control (Global Server Load Balancing):** Delivers business continuity, reliable application uptime, high availability (HA), automated app provisioning, GDPR compliance, resiliency and disaster recovery (DR) by distributing network traffic across geo-diverse, on-premise, public and hybrid cloud environments.
- **Reporting & Analytics (Network Visibility):** Provides historical and present search, summary and deep forensic network data visibility and visualization via pre-built and customizable dashboards, reports, predictive analytics, and query logging for audit/compliance, performance monitoring, data modeling and control.

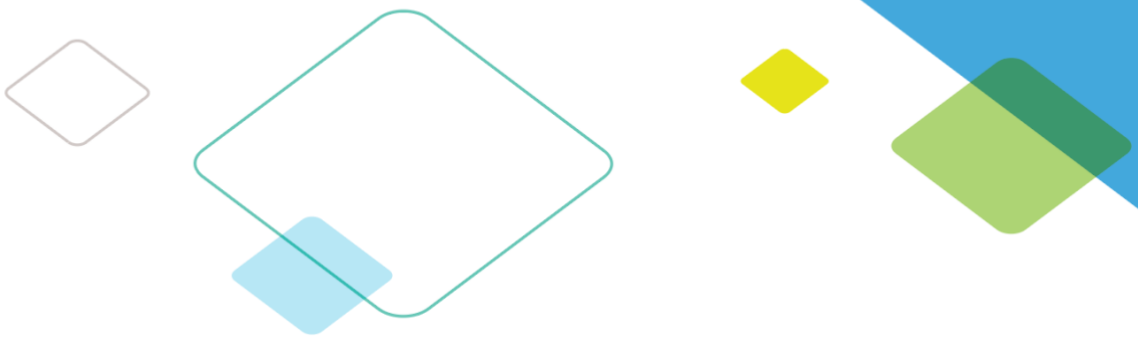
Conclusion

If you're focused on optimizing customer experience, facing new digital initiatives or are behind the network transformation curve, Infoblox can help. With over 20 years of industry experience, we are the clear leader in Secure Cloud-Managed Network Services. With over 8,500 customers, including 350 of the Fortune 500, and over 50 percent DDI market share, we deliver next-level integrated, cloud-managed, future-ready core network and security services for mission-critical on-premises, cloud and hybrid networks. Founded on security, our end-to-end solution is designed for physical, virtual and cloud architectures to provide you with the visibility, reliability, scalability, automation and control you need to optimize network customer experience. If any of this has piqued your interest, let's start a conversation.

Visit us at Infoblox.com, email us at info@infoblox.com or call us toll-free at 1.866.463.6256.

REFERENCES

1. https://www.handshake.com/blog/why-saas-cloud-benefits-vs-on-premise-software
2. https://www.networkworld.com/article/3237184/the-benefits-of-multi-cloud-computing.html
3. https://www.silver-peak.com/sd-wan/top-benefits-sd-wan
4. https://www.information-age.com/iot-accelerating-digital-transformation-initiatives-gartner-123484964/
5. https://www.silver-peak.com/sd-wan/top-benefits-sd-wan



Infoblox enables next-level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

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