

Branch Modernization

Reduce Costs and Simplify Management with Infrastructure-Free Delivery of Critical Network Services

IMPACT SUMMARY



Reduces Branch Costs

Eliminates expensive on-site appliances and the high costs of equipment and ongoing maintenance that come with them.



Increases Operational Efficiency

Enables businesses to provision critical network services close to users to preserve performance, while managing and monitoring all sites from a single, centralized control point.



Accelerates Branch Deployments

Empowers IT to bring up new locations in minutes instead of weeks with standardized, repeatable, automated branch configurations.



Strengthens Edge Security

Extends consistent, preemptive threat protection to every branch, stopping attacks before they can spread.

85%

improvement in speed and efficiency in deploying and managing remote sites¹

5-10 minutes

to activate a new site²

Up to 40%

lower operational costs³

50%

reduction in equipment and associated costs to support critical network services⁴

INTRODUCTION

In the digital realm, large enterprises are going local. By adopting distributed network architectures like software-defined wide area network (SD-WAN) and secure access service edge (SASE), organizations in retail, financial services, healthcare and other sectors are pushing state-of-the-art digital experiences and productivity tools out closer to users and customers, where most business takes place. These efforts make it easier to support changing work patterns, local compliance requirements and new edge workloads like agentic AI. Yet they also create vast distributed infrastructures that can be difficult and expensive to support. Organizations must somehow ensure the performance, security and non-stop resiliency of mission-critical branch services, while minimizing the need for expensive equipment or advanced IT expertise at every site.

CHALLENGE

Enterprises operating large, distributed networks against a backdrop of budgetary constraints struggle constantly to bring branch users the digital capabilities and performance they require. Their challenges are only exacerbated when it comes to foundational network services like DNS, DHCP and IP address management (IPAM), which connect every branch device and application.

These mission-critical services must be delivered close to users or application performance quickly deteriorates. Traditional solutions involve dedicated hardware at each location, which must be deployed, configured and maintained by skilled on-site staff. Because of their dispersed nature, these solutions do not scale, at least not cost-effectively. Worse, as sprawling distributed architectures evolve, centralized IT organizations end up with inconsistent management practices across sites, fragmented visibility and configuration drift. Together, these complications increase the risk of service disruptions and security incidents, while impeding business agility.

Hardware-Heavy Branches Inflate Costs and Complexity

When it comes to delivering critical network services by traditional means, many organizations still depend on dedicated hardware stacks at each branch, along with localized maintenance and support. Every new site adds more appliances to procure, deploy and manage, driving up both capital and operating expenses (CapEx and OpEx). Frequent truck rolls for installation, upgrades and troubleshooting make it expensive and time-consuming to open locations, consolidate them or adapt the footprint as business conditions change. At the same time, businesses relying on traditional delivery models have few viable alternatives, at least for foundational network services. Many enterprises attempt to cut costs by backhauling DNS and DHCP through centralized data centers, often located vast distances from the branch locations they serve. The resulting latency frustrates users and, in some cases, renders performance-sensitive applications unusable. Additionally, the more sites an organization tries to serve from a centralized hub, the larger the fallout in the event of an outage.

Fragmented Visibility Hampers Operations

Most modern branches are hybrid, combining both on-premises and cloud-based infrastructure. As these complex architectures evolve and configurations drift, IT ends up having to treat each site as a unique environment. This makes it enormously difficult to centralize and consolidate management—a top priority as more enterprises seek to scale branch footprints without adding IT headcount. Teams must assemble data from disjointed tools and logs just to understand what is happening at individual sites. This fragmented view makes it more challenging to diagnose issues, optimize performance or plan capacity, resulting in longer outages, lower productivity and dissatisfied users.

Manual Workflows Slow Expansion and Change

Critical network services at each branch location are often configured and maintained manually. As the number of locations increases, these workflows become increasingly fragile, resulting in delays, configuration drift and higher likelihood of human error. New branches can take weeks to bring online. Changes roll out inconsistently and IT teams struggle to keep policies aligned with business and regulatory requirements across the digital estate.

Inconsistent Protection at the Edge Increases Risk

As more of the enterprise application stack migrates to the cloud, branches are increasingly using direct internet access and local breakouts at each site to enable better performance. Yet inconsistent security controls across locations expose the organization to additional risk (Figure 1). Gaps in policy enforcement, uneven inspection and misconfigurations at the edge can allow threats to bypass defenses or disrupt access to critical services. Consequently, the organization is left more vulnerable to malware, data loss and compliance violations, while security teams struggle to maintain a strong, consistent posture everywhere.

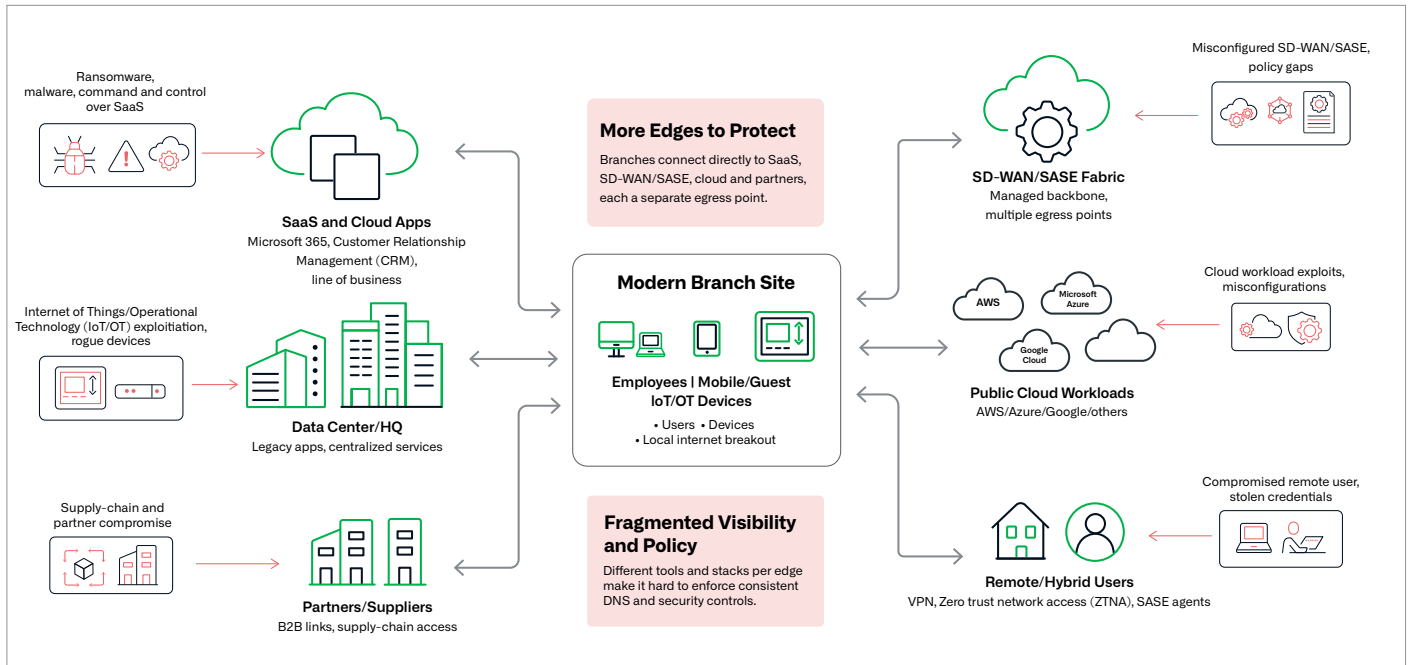


Figure 1. Expanding attack surface at the modern branch

SOLUTION

There is a clear playbook for overcoming these challenges and creating more secure, manageable and standardized branch networks. It entails three basic objectives:

1. **Deliver network services locally** to optimize performance and resiliency.
2. **Centralize control** so that teams can monitor, manage and secure the entire footprint from one place, using the same consistent workflows.
3. **Automate across the lifecycle** so IT can turn up new sites faster and enable simpler, more consistent ongoing management.

Infoblox helps organizations achieve all these objectives with the industry's only fully cloud-managed, infrastructure-free solution for delivering critical network services to distributed branches (Figure 2).

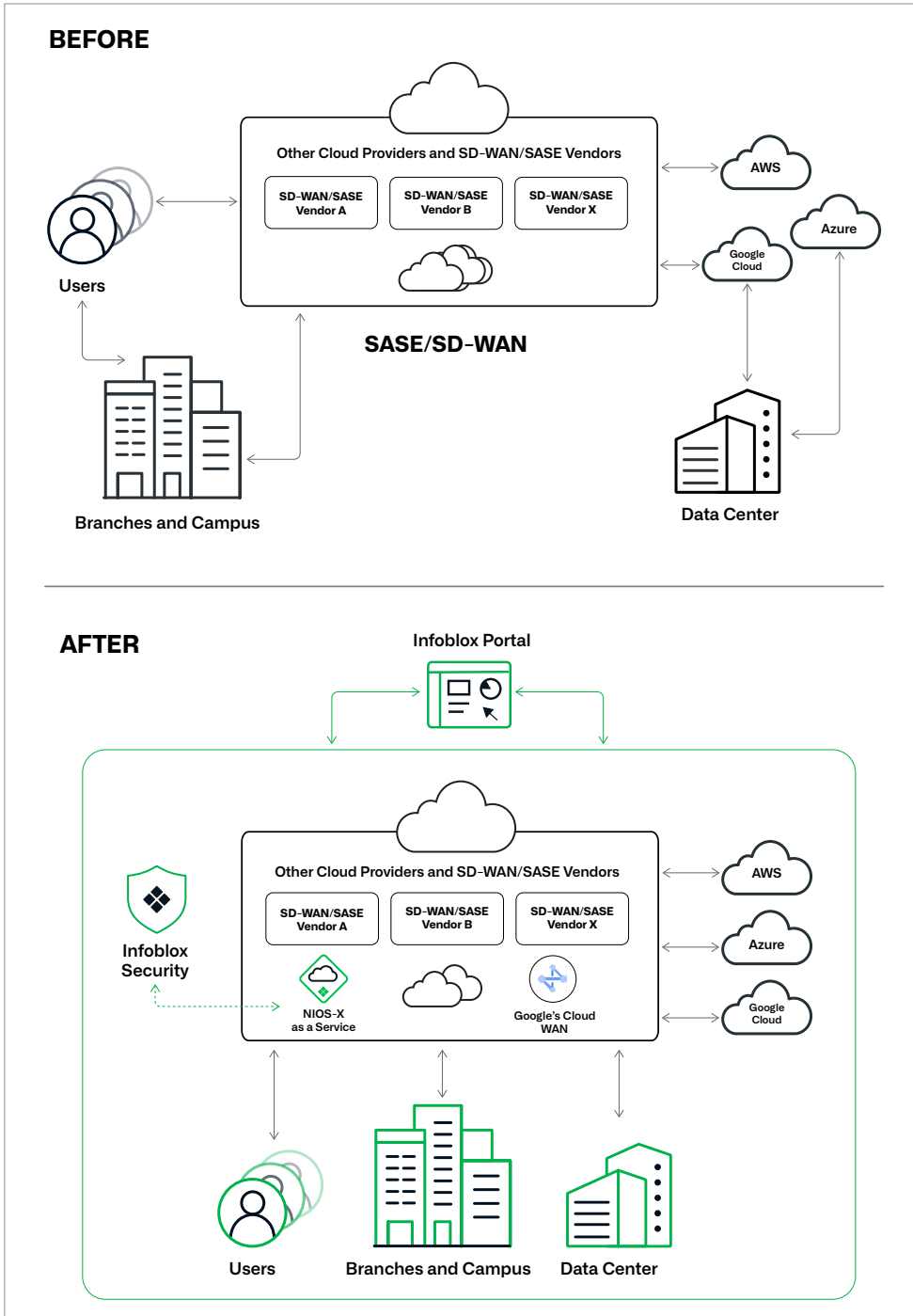


Figure 2. Distributed services, centralized control

Organizations can maximize performance and resiliency by delivering DNS and DHCP from the closest cloud point of presence (PoP) to every branch, without dedicated on-site hardware. They can see and manage the entire distributed architecture from a single, cloud-based control plane to drive down errors and outages and apply DNS-layer security to preemptively block threats. They can use scalable automation to accelerate deployments and ensure consistent, policy-driven configurations that boost security and resiliency at every site. The results: faster site deployments, lower CapEx and OpEx, and simpler, more resilient operations that keep branches ready for continuous digital growth.

Localized Service Delivery without Hardware

Infoblox provides the industry's only fully cloud-based, as-a-service solution for delivering DNS, DHCP and IPAM services to distributed branches. Organizations gain all the benefits of infrastructure-free delivery: lower CapEx and OpEx, reduced complexity and centralized manageability—without sacrificing performance or resiliency. Service scaling and high availability are built-in elements of the service, requiring zero effort from on-site branch personnel. Organizations can even add small virtual appliances for sites that require local survivability or data governance, without adding complexity.

Unified Monitoring and Management

Infoblox empowers IT teams to centrally manage critical network services for all hybrid, multi-cloud environments across all branch locations, from a single cloud-based control plane. These management capabilities extend to on-premises networks, public and private clouds, even external DNS services hosted by third-party providers. Network administrators can easily see and remediate overlapping IP ranges, dangling DNS records and other hidden risks across the distributed architecture, before they cause outages or breaches. Just as important, they can execute the full range of network operations at every branch location using the same consistent tools and workflows.

Additionally, IT can now maintain a single, authoritative source of IP information for the entire distributed enterprise. In the event of a network issue or security incident at any branch, teams no longer waste valuable cycles sifting through spreadsheets or taking other manual steps to understand an unfolding event. Instead, they can instantly surface the essential information, such as device type, network location and other details needed to respond, reducing mean time to resolution (MTTR).

Pervasive Automation

More than simply centralizing management, Infoblox gives organizations a single control point for automation. With traditional deployments, automating critical network services demands that IT maintain disparate scripts for each cloud environment and heterogeneous branch network design. Additionally, these scripts grow more fragile as the network environment expands and evolves. Through Infoblox, teams can automate all hybrid, multi-cloud DDI operations using a single API. They can also define policy once and automatically apply it everywhere, ensuring consistent security and control for all sites. They can accelerate new branch turn-ups from weeks to minutes by using repeatable site templates and maintaining consistent configurations everywhere, thereby simplifying remote management and troubleshooting.

Preemptive Security

Securing distributed branch locations has always been a challenge. Increasingly influenced by AI, the challenge is growing exponentially steeper. Today's threat actors use AI tools to design new custom exploits faster than traditional security can keep up. Infoblox provides advanced Protective DNS capabilities that block threats the moment they try to communicate with the outside world. The solution monitors every DNS query across every site and immediately detects attempts to connect with suspicious or malicious domains. It also anticipates threats by making use of threat intelligence that identifies attack building blocks lurking in the infrastructure attackers use. The solution traces these sources and blocks them before they reach the network, thereby extending protection to every branch, even against novel attacks never encountered before.

MODERNIZE BRANCH MANAGEMENT, DRIVE DOWN COSTS

As organizations scale to hundreds or thousands of branches, traditional infrastructure models cannot keep pace with the demands of digital interactions. Infoblox can deliver the unified visibility, preemptive security and pervasive automation needed to support modern distributed branches with the industry's only truly cloud-based, infrastructure-free solution for foundational network services. The outcomes: simpler operations, faster deployments and a distributed networking model agile enough to adapt to whatever the future brings.

SUCCESS ACROSS REAL CUSTOMER IMPLEMENTATIONS

- European RV provider onboarded 10 new entities across seven countries—without adding headcount or local partners
- Leading retailer now brings up new stores remotely and in just minutes
- U.S. health insurer now builds and deploys remote servers in seconds with Infoblox automation, a task that used to take 20 hours per week

KEY CAPABILITIES

Centralized Management: Control foundational network services across all branch sites from a single cloud portal.

Infrastructure-Free Service Delivery: Provide mission-critical DNS, DHCP and IPAM services to every site, without local hardware or sacrificing performance or resiliency.

Preemptive Threat Protection: Detect and block malicious activity at the source before it impacts endpoints or users.

Automated Configuration and Policy: Simplify operations and speed deployments by automatically applying the same consistent configurations and policy across all sites.

1. *Infoblox Authoritative IPAM for DNS and DHCP*, Tolly Test Report, June 2022.
<https://insights.infoblox.com/resources-analyst-reports/infoblox-analyst-report-tolly-report-infoblox-authoritative-ipam-for-dns-and-dhcp>
2. *HARTMANN Trusts Infoblox to Stabilize and Secure Networks across Continents*, Infoblox, 2023.
<https://www.infoblox.com/resources/case-studies/hartmann/>
3. *The Total Economic Impact™ Of Infoblox DDI*, Forrester, October 2023.
<https://info.infoblox.com/resources-analyst-reports-2023-the-total-economic-impact-of-infoblox-ddi>
4. Internal data from Infoblox customers.



Infoblox unites networking, security and cloud with a protective DDI platform that delivers enterprise resilience and agility. We integrate across hybrid and multi-cloud environments, automate critical network services and preemptively secure the business—providing the visibility and context needed to move fast without compromise.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com