

Cloud Migration/Transformation

Build Secure and Resilient Critical Network Services to Accelerate Cloud Adoption

IMPACT SUMMARY



Simplifies Cloud Transformation

Streamlines migrations by combining holistic visibility, automated provisioning and direct integration with diverse cloud partners.



Improves Cloud Governance and Compliance

Maintains a comprehensive asset inventory to simplify audits, surface hidden risks and reduce resource waste.



Reduces Operational Complexity

Speeds deployments and minimizes errors and outages by managing foundational network services across hybrid and multi-cloud networks through a single API and interface.



Strengthens Security Posture

Uses predictive intelligence to detect suspicious and malicious traffic across the hybrid, multi-cloud environment, stopping threats before they can spread.

63%

more confidence in cloud visibility¹

44%

fewer cloud outages with 38% faster recovery¹

82%

faster troubleshooting and problem resolution²

75%

less time spent managing network resources²

INTRODUCTION

In the drive to get faster, leaner and more competitive, organizations are moving more of their enterprise IT stack to the cloud. As businesses progress along their cloud journeys (whether via lift-and-shift migrations, application refactoring or adopting cloud-native applications), many encounter a major barrier to success: runaway operational complexity. Without a simple, systematic way to control mission-critical network services at the enterprise level—encompassing both cloud and on-prem environments—that complexity begins to impede IT visibility and governance, expand the attack surface and make new deployments slower, riskier and more costly.

CHALLENGE

Almost every cloud journey starts by integrating cloud environments and applications with traditional IT operations. This shift to hybrid IT environments introduces significant complexity and risk, often disrupting long-established workflows across multiple teams. That is especially true for foundational DNS, DHCP and IP address management (IPAM) services, which keep every location, device and application connected.

Each cloud provider uses its own dedicated naming conventions, toolsets and workflows for provisioning new environments and performing other basic network operations—none of which apply to on-prem workloads or competing cloud platforms. The result is a highly fragmented IT environment that increases configuration errors and outages, introduces dangerous blind spots and adds extra time, effort and risk to nearly every network task.

Complex, Siloed Operations

In the early stages of a cloud journey, many organizations opt to use each cloud provider's native tools to manage DNS, DHCP and IP addresses in the new environment, while maintaining traditional workflows for on-prem networks. While this approach allows the organization to advance cloud objectives, it adds extra layers of complexity that make it more difficult to centralize or automate operations.

Teams must constantly switch between separate cloud and on-prem tools to provision and monitor critical network services in each environment—a manual, duplicative effort that significantly increases the likelihood of configuration errors, the leading cause of outages. As the business adds more cloud providers to avoid single points of failure and capitalize on each provider's unique strengths, the complexity continues to escalate (Figure 1).

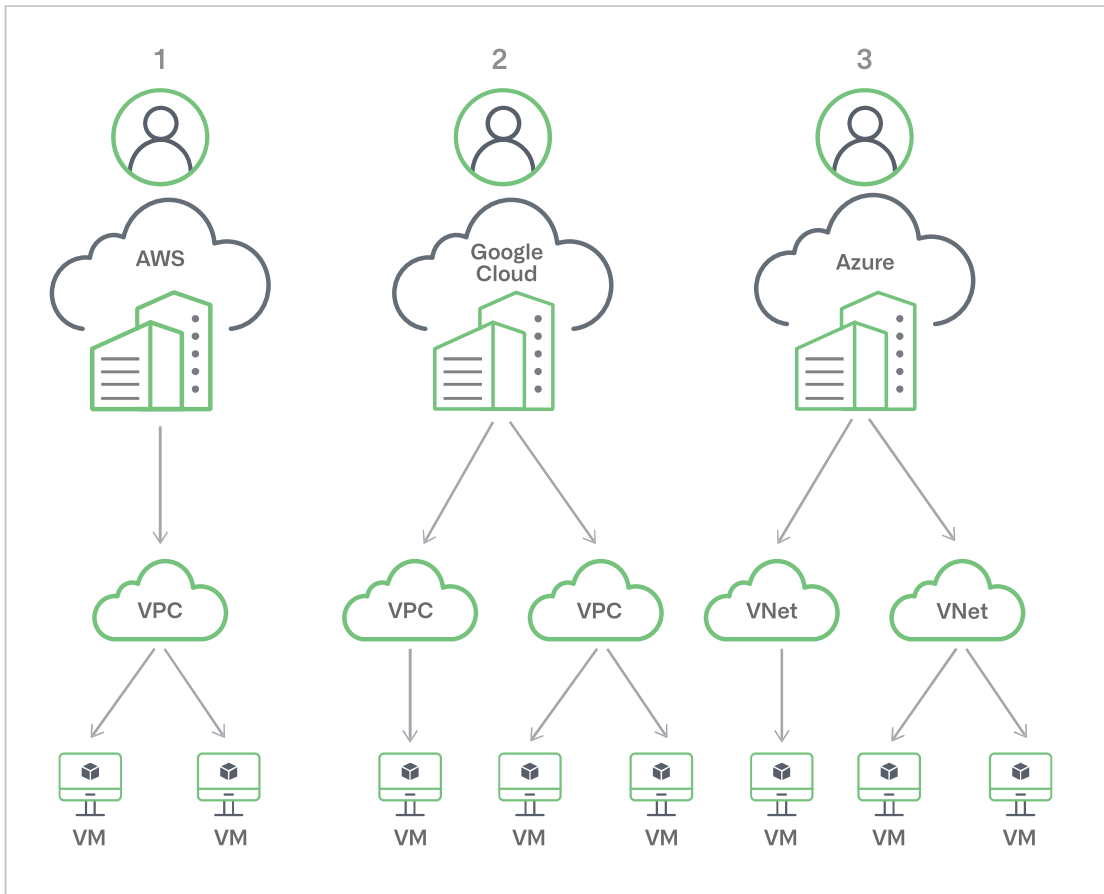


Figure 1. Hybrid, multi-cloud fragmentation forces teams to duplicate effort across providers for every virtual private cloud (VPC), virtual network (VNet), subnet and virtual machine (VM) they deploy

Fragmented Visibility

IT fragmentation forces teams to rely on multiple specialized toolsets to monitor the hybrid environment, each of which captures only a partial view. As a result, simply understanding what is connected to the network—let alone monitoring critical network services at the enterprise level—becomes exceptionally difficult. These blind spots complicate compliance audits and increase the risk of outage-causing IP range overlaps. They also undermine effective cloud governance, leading to orphaned assets, inconsistent policies and, in many cases, significant underutilization of costly public IP address ranges.

Slow, Manual Processes Undermine Cloud Objectives

With no centralized visibility and no authoritative IP information, IT teams struggle to move as quickly as a cloud-powered business demands. NetOps and CloudOps teams end up working in silos, communicating via helpdesk tickets and manual, out-of-band processes that slow deployments and erode cloud return on investment (ROI). If it still takes weeks to provision new cloud landing zones, the organization cannot pivot quickly to capture new opportunities or outpace competitors entering new markets—the very drivers for adopting cloud in the first place.

Elevated Risk

Innovative companies thrive in the cloud, as they can spin up new environments and applications in minutes. Yet over time, that agility introduces new challenges, as cloud resources are spun up and then forgotten, creating significant security and compliance risks. For example, it is common for teams to decommission cloud applications or websites that are no longer in use, but they often forget to delete the DNS records pointing to them—leaving an easy target for cyberattackers seeking to hijack the organization's domains and compromise the brand. IT fragmentation also slows the speed at which teams can respond to network problems and security incidents.

SOLUTION

Infoblox helps organizations reduce hybrid cloud complexity to simplify migrations, minimize risk and unlock the full value they expect from cloud transformation. With a single, centralized management plane for critical network services across hybrid and multi-cloud environments, businesses gain the end-to-end visibility, agility and control that form the foundation of a successful cloud-first enterprise.

Simplified Cloud Migrations

Infoblox unifies complex hybrid and multi-cloud IT operations, enabling teams to centrally provision and manage foundational network services across the entire digital estate from a single API and interface. Whether executing lift-and-shift migrations, refactoring applications or employing a combination of strategies, teams can use consistent naming conventions and workflows across both cloud and on-prem environments, dramatically simplifying migrations.

Additionally, native integrations with leading cloud providers (AWS, Microsoft Azure, Google Cloud), configuration management database systems (ServiceNow) and third-party network and security solutions (Meraki, CrowdStrike) speed time-to-value for cloud investments, while enabling enterprises to work seamlessly with the cloud partners they prefer.

Comprehensive Visibility

With a single, universal point of control for the entire hybrid environment, organizations can centrally monitor critical network services to eliminate blind spots and optimize cloud governance. IT teams gain near-real-time, single-pane-of-glass visibility into all assets in the hybrid cloud footprint, including workloads, IoT/OT devices and endpoints across all IP spaces, dramatically simplifying compliance audits.

Teams can monitor IP address and subnet usage to quickly identify forgotten and underutilized resources, improve capacity planning and detect overlapping IP ranges and other risks before they disrupt services. Additionally, by maintaining a comprehensive asset inventory and authoritative IP information for devices across the business, teams can respond to network issues and security incidents much faster. Instead of manually poring over spreadsheets to map network logs to specific endpoints, teams can instantly pinpoint affected devices, their location and associated context in seconds—and remediate issues before they escalate into crises.

Fast, Efficient Operations

When organizations start with broad, enterprise-wide visibility across hybrid environments and then add a common management layer on top, they gain the foundation to simplify and optimize cross-team collaboration. Automated, policy-driven IP address allocation means CloudOps teams can move faster, without waiting on NetOps to respond to ticket-based requests. Reducing manual handoffs also lowers the risk of errors and outages.

The ability to maintain consistent, enterprise-wide workflows and policies also makes automating hybrid network environments much easier. By building automation with a single API (instead of maintaining disparate scripts for each cloud and on-prem environment) organizations can accelerate deployments, using infrastructure-as-code (IaC) tools like Terraform and Ansible to standardize and automate resource provisioning (Figure 2).

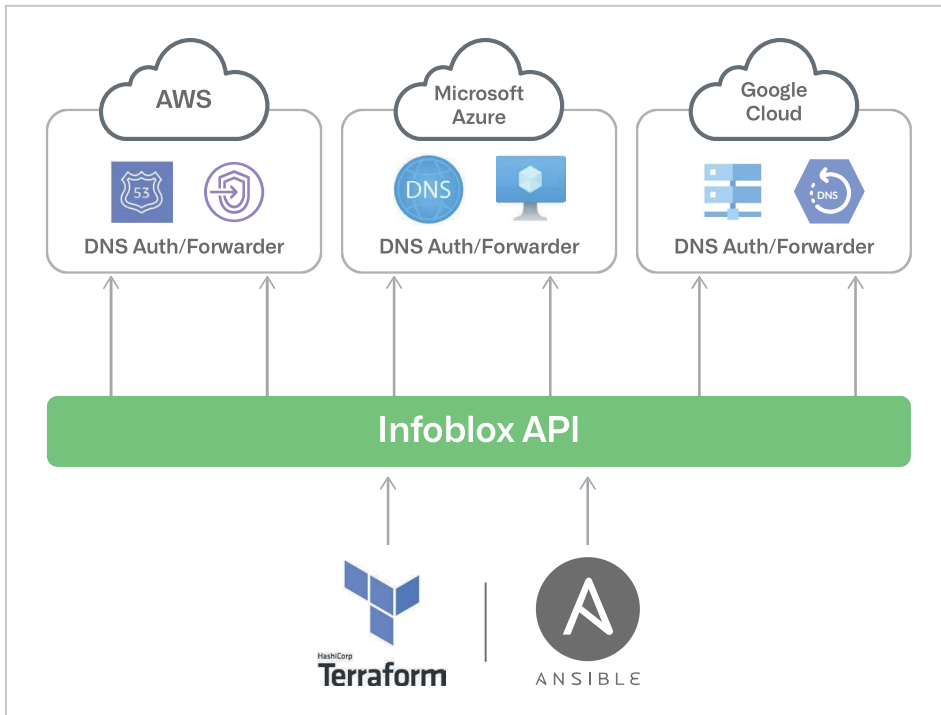


Figure 2. Infoblox's API for faster configuration and deployment across cloud providers

Enhanced Security Posture

Expanding into new cloud environments can unlock powerful new capabilities, but it also increases the attack surface, even as the added complexity makes the environment more difficult to monitor and protect. Infoblox provides advanced Protective DNS capabilities to preemptively block threats the moment they try to communicate with the outside world. By monitoring every DNS query across the entire hybrid environment, these defenses immediately detect attempts to connect with suspicious or malicious domains, trace the source and block the activity—providing built-in protection against attacks originating in any cloud or on-prem workload.

UNIFY HYBRID IT OPERATIONS TO ACCELERATE CLOUD TRANSFORMATION

In the modern digital marketplace, speed and agility increasingly define an enterprise's success. Staying competitive means being able to quickly move into new markets, pivot to new strategies and rapidly onboard new digital and AI innovations—all of which make cloud migration an urgent business priority. Yet if organizations fail to build an agile, automated foundation for the critical network services on which every cloud and on-prem workload depend, their cloud initiatives can quickly become bogged down in complexity.

Infoblox provides the unified management, visibility and agility to fuel successful cloud transformation. With automated, policy-driven network operations and comprehensive visibility across the hybrid environment, businesses can reduce errors and outages, speed deployments and ensure non-stop resiliency and security at every stage of the cloud journey.

Real Customer Examples:

- A financial services provider identified and eliminated 847 orphaned cloud resources, saving \$180,000 annually and reducing security risks through proactive asset discovery and governance.
- A healthcare organization cut response times by 75 percent using Infoblox's universal IP address mapping and asset visibility, ensuring faster recovery from outages and incidents.
- A U.S. retailer dramatically accelerated deployments, bringing new stores online remotely in minutes, enabling faster business expansion with minimal operational overhead.

KEY CAPABILITIES

Unified Control across Hybrid Networks: Reduce errors and outages by using consistent, standardized workflows for DNS, DHCP and IP operations across both cloud and on-prem environments.

Comprehensive Visibility: Centrally monitor all cloud and on-prem resources from a single interface to simplify audits, optimize governance and surface hidden risks.

Faster, Simpler Migrations: Accelerate provisioning of new cloud environments with policy-driven IaC automation that reduces deployment timelines from weeks to minutes.

Protective DNS Security: Expand the cloud footprint with confidence, preemptively blocking threats across the entire environment before they can spread.

1. 9 Pitfalls of Not Using Enterprise-Grade DDI, Enterprise Strategy Group (ESG), February 2025.
www.infoblox.com/resources/analyst-report/network-modernization-ddi-report/
2. Infoblox Authoritative IPAM for DNS and DHCP, June 2022.
www.infoblox.com/resources/analyst-report/tolly-report-infoblox-authoritative-ipam-for-dns-and-dhcp/



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