

Enterprise-Wide Visibility and Discovery

Comprehensive Visibility and Cross-Domain Intelligence for Network Assets

IMPACT SUMMARY



Eliminates Blind Spots

Provides pervasive visibility to detect overlapping IP ranges, forgotten records and other hidden risks before they cause outages or breaches.



Reduces Complexity

Speeds deployments and simplifies cross-team operations by providing a single, authoritative source of IP and asset data across the digital estate.



Improves Governance

Maintains continuously validated asset inventory to reduce stale, duplicate and incomplete records, simplify audits and improve CMDB accuracy.



Accelerates Troubleshooting

Reduces resolution times for network and security incidents by providing network identity and AI-powered context and location for network devices.

75%

less time spent managing network resources¹

82%

faster troubleshooting and problem resolution¹

63%

more confidence in cloud visibility²

100%

audit success rates¹

INTRODUCTION

What are the biggest problems undermining networking and security operations? The ones businesses cannot see. With a typical enterprise hosting thousands of connected devices across data centers, clouds, branches, Internet of Things (IoT)/operational technology (OT) systems and more, organizations face a crisis in infrastructure visibility. The same cloud and IT strategies that drive business growth are creating new layers of complexity—and dangerous blind spots. Additionally, while AI adoption is driving efficiency and insights, agentic AI and large language model (LLM)-based automation make wrong decisions faster when underlying infrastructure data is inaccurate or incomplete. Configuration management database (CMDB) initiatives struggle to provide the accuracy and confidence teams need to operate effectively.

CHALLENGE

While organizations have thousands of assets across their infrastructure generating valuable intelligence, most businesses are not actually seeing and using that data. Instead, it is scattered across dozens of disconnected cloud and on-premises tools, creating gaps that attackers can exploit and IT teams struggle to bridge. At the same time, many organizations rely on CMDBs that are incomplete, outdated and manually maintained, making them an unreliable source of truth for fast-moving hybrid environments. Without centralized, comprehensive visibility, organizations are left vulnerable to undetected threats, cloud IP addresses are wasted and compliance becomes more difficult. Worse, troubleshooting and security investigations take much longer—delays that can turn minor incidents into full-blown crises.

Fragmented Visibility

As IT networks expand to new locations and clouds, simply understanding what is connected to the network becomes increasingly difficult, leaving enterprises with dangerous blind spots. The biggest reason: NetOps, CloudOps and SecOps teams use their own dedicated toolsets, each providing only a partial view (Figure 1). It creates a persistent CMDB problem: when discovery data is fragmented across siloed systems, CMDB records drift from reality and teams are left reconciling conflicting information instead of acting on it. This fractured visibility increases the likelihood of shadow IT, orphaned assets and overlapping IP ranges that can cause outages and other undetected risks. It is common, for example, for enterprises to have hundreds, even thousands of forgotten DNS records and decommissioned resources across their hybrid, multi-cloud environments, any of which could become launchpads for domain takeovers or other attacks.

Fragmented visibility and inaccurate CMDB impact the adoption of agentic AI and LLM-based automation. These systems depend on complete, accurate and continuously updated data to make decisions. If the underlying data is incomplete or inaccessible, organizations face an AI reliability problem.

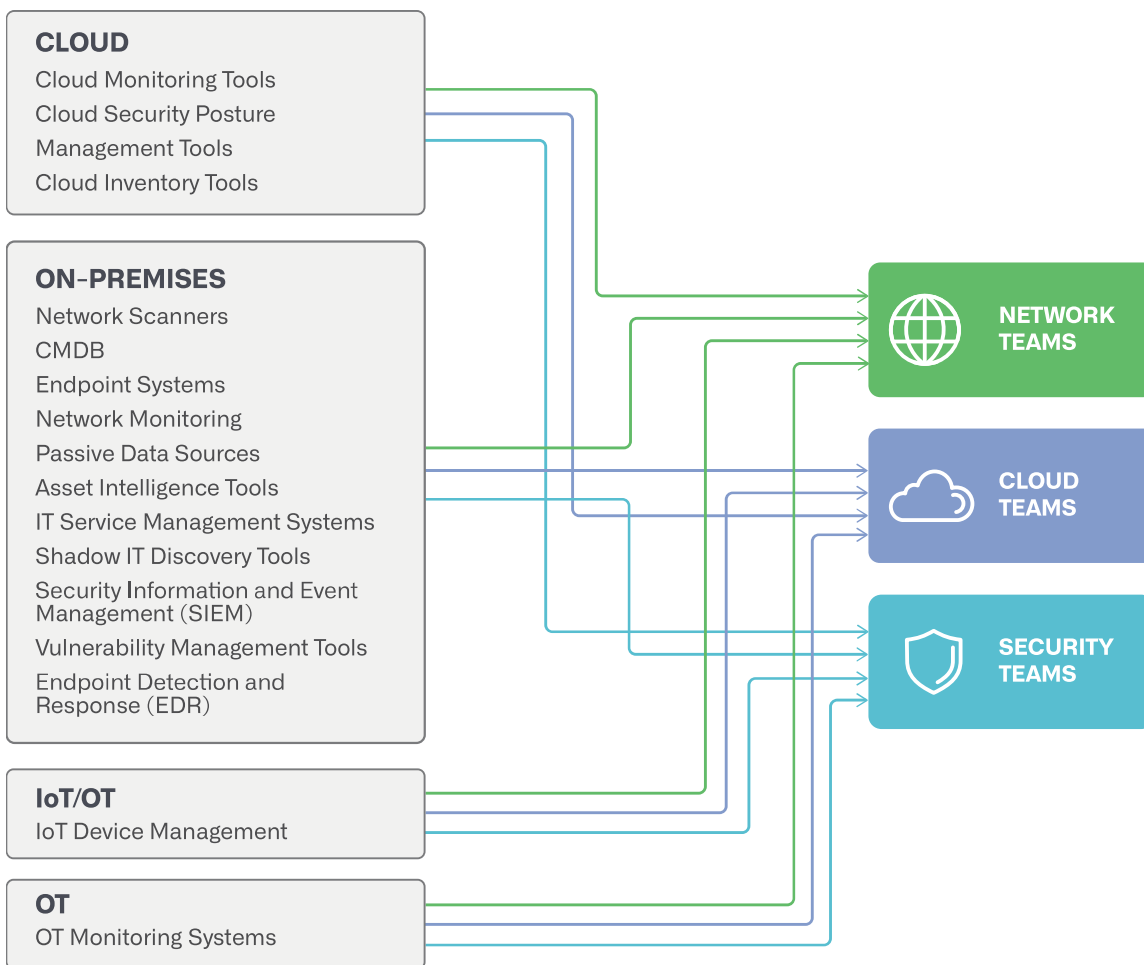


Figure 1. Fragmented visibility

Incomplete Asset Discovery

When asset inventories and configuration management databases (CMDBs) do not reflect reality, businesses leave themselves exposed to wasted resources, non-compliant systems, regulatory penalties and exploitable misconfigurations. Hybrid, multi-cloud environments amplify these challenges by scattering ownership data and policy control across multiple siloed tools for different environments, each of which ends up storing different, often conflicting asset information. This is also why CMDB initiatives so often fall short. If discovery is incomplete, the CMDB cannot stay accurate. Some organizations have reported spending more than \$2 million just to reconcile outdated CMDB data.

Siloed, Manual Operations

Having an accurate asset inventory is essential for effective network, cloud and security operations. Yet in most organizations, the dedicated toolsets that NetOps, CloudOps and SecOps rely on do not synchronize information (Figure 2). Worse, the enterprise typically pays for redundant asset intelligence feeds for each team—yet still cannot capture a complete, authoritative picture of what is connected to the network.

Compounding these problems, many organizations still rely on spreadsheet lookups and manual, out-of-band communications between teams to track asset data. These inefficiencies introduce delays and errors at the best of times but become major impediments when responding to network issues and security incidents. Teams must cross-reference multiple systems to identify affected assets, often starting with just an IP address, with no context about the type of device, who uses it or where it is located. Threats sometimes propagate for days while teams manually track down this information.

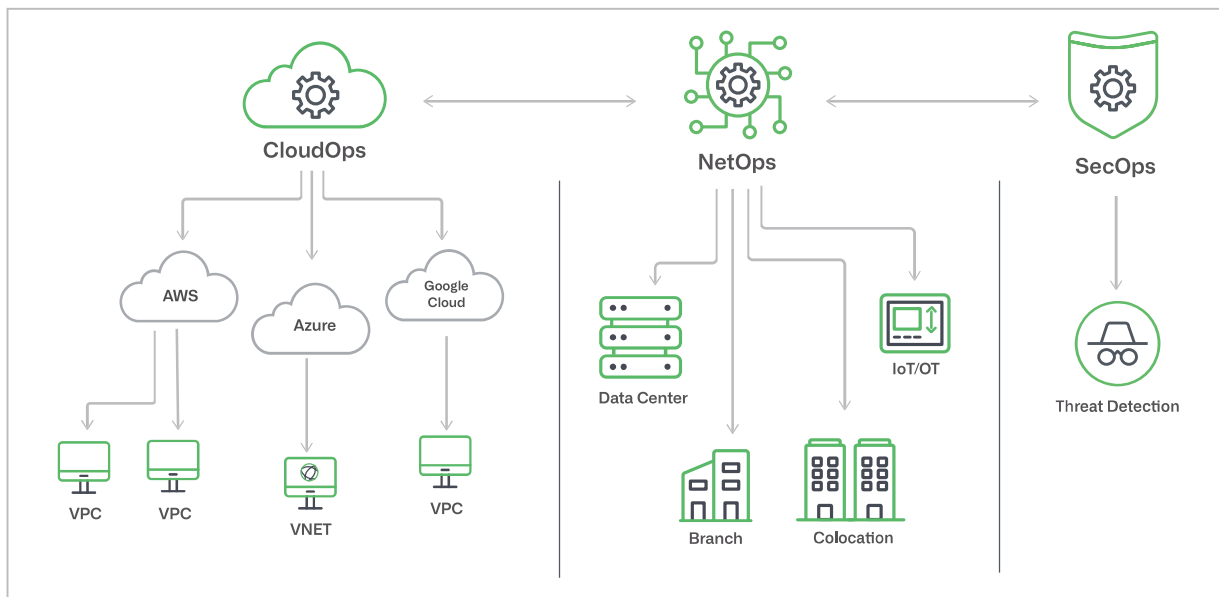


Figure 2. Siloed operations

SOLUTION

There is a secret weapon organizations can use to solve these challenges, and it is already deployed everywhere across their environments. It is DNS, DHCP and IP address management (IPAM), collectively known as DDI. Every device connecting to the network uses DNS and DHCP—no exceptions, no blind spots. Therefore, organizations already have a universal, authoritative source of truth for every connected asset across the business. They just have to take advantage of it. Infoblox delivers automated asset discovery and authoritative visibility by providing a single, centralized point of control for the critical network services that every asset uses to connect. By combining DNS/DHCP information with enhanced network discovery engines, third-party APIs and Infoblox's proprietary AI-powered analysis and correlation, teams can maintain an accurate, comprehensive asset inventory. As a result, they can eliminate blind spots, strengthen CMDB trust, improve cloud governance, accelerate troubleshooting and surface hidden risks.

Authoritative Asset Inventory

Infoblox automatically discovers assets across the enterprise—including on-premises networks, public and private clouds, Windows environments and devices registered in third-party CMDB, network and security solutions like ServiceNow, Meraki and CrowdStrike—to capture a complete, authoritative inventory (Figure 3). It then applies AI-powered analysis and correlation to understand exactly what each asset is, what it is doing and whether it presents a risk.

Now, IT teams can answer critical questions—What type of resource is this? Who uses it? Where does it live?—for every cloud and on-premises connection. This cross-domain intelligence dramatically simplifies compliance, enabling teams to complete audits in minutes instead of days. It also provides a platform for more effective governance, allowing organizations to eliminate shadow IT and orphaned assets, detect decommissioned applications and recover and reuse valuable cloud and IP address resources.

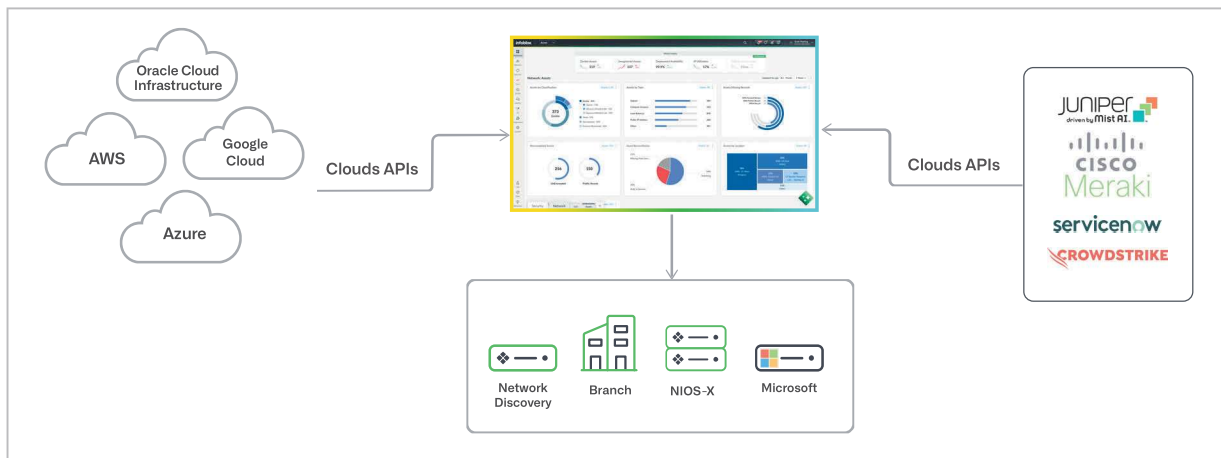


Figure 3. Visibility from multiple sources

Comprehensive Visibility

With Infoblox, IT teams gain a complete, real-time view of devices, workloads and resources across the digital estate. They can detect risks, such as overlapping IP ranges, anywhere in the hybrid, multi-cloud environment, and correct them before they become expensive outages. At the same time, they can surface hidden threats like unmanaged and unregistered assets, dangling DNS records and other vulnerabilities before they can be exploited for domain takeovers and cyberattacks. When security incidents or network issues do arise, teams can immediately find essential context for affected devices to accelerate investigations and reduce mean time to repair/remediation/resolution (MTTR).

Achieving comprehensive visibility also provides the foundation needed to ensure automation and AI operate reliably at scale. With complete and accurate CMDB data, systems powered by AI are enabled to make correct decisions, empowering each IT team. NetOps can enable intelligent IPAM, autonomous provisioning and self-healing networks. SecOps gains autonomous threat response, intelligent incident management and AI-powered security automation. CloudOps teams get intelligent cost optimization, autonomous resource allocation and self-provisioning infrastructure.

Faster, More Efficient Operations

Infoblox breaks down operational silos between NetOps, CloudOps and SecOps teams, so they can collaborate in real time, using the same source of asset and IP information (Figure 4). CloudOps teams no longer have to rely on manual, ticket-driven processes to request new IP ranges, enabling them to work more quickly and autonomously. Meanwhile, NetOps can see and automatically allocate IP resources everywhere—public clouds, IoT/OT environments, even external DNS services hosted by third-party software-as-a-service (SaaS) providers like Cloudflare and Akamai—so they can prevent IP conflicts and minimize waste. At the same time, security teams can detect unregistered devices and orphaned records, map the attack surface and proactively mitigate risks before they become incidents.

Simply working from an accurate, enterprise-wide system of record empowers teams to perform a wide range of network operations more quickly and efficiently. In fact, Infoblox customers have eliminated hundreds of staff hours annually that their teams previously devoted to manually reconciling inaccurate and incomplete asset data in CMDB—hours they can now redirect toward more strategic and valuable activities.

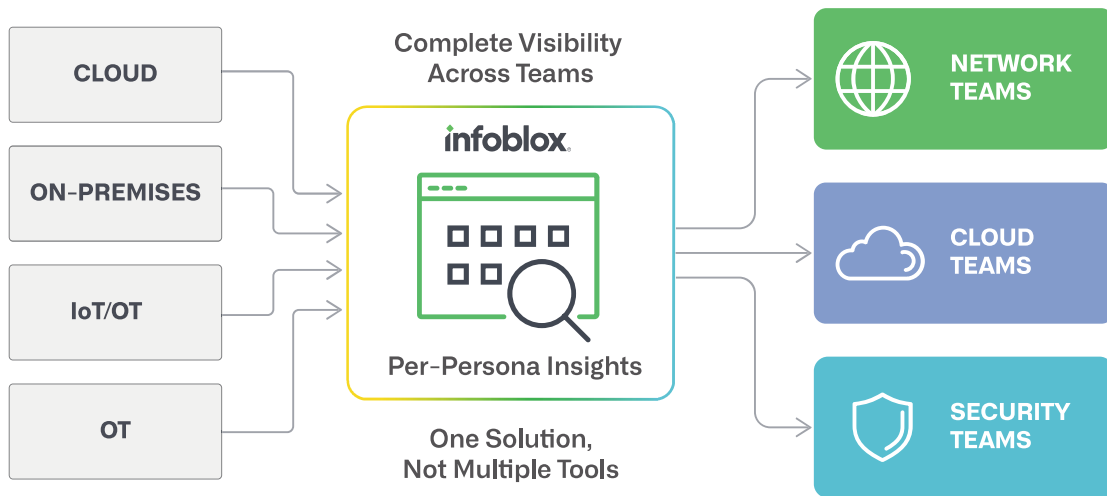


Figure 4. Single source of truth for all operations

WHAT YOU CANNOT SEE CAN HURT YOU

How many overlapping IPs currently exist in the environment that could cause outages in mission-critical applications? How many decommissioned resources are currently available to attackers seeking to hijack the business's domains? How accurate is the current CMDB? These questions are critical to the security, resiliency and efficiency of every enterprise, especially in the age of AI. Yet too many IT leaders cannot answer them with confidence.

Infoblox can provide the pervasive visibility that IT teams need to protect the security and resiliency of complex, hybrid and multi-cloud environments. With authoritative asset information and AI-powered insights, businesses can simplify and accelerate a broad range of IT operations, optimize resource utilization and surface hidden risks. These capabilities do more than solve inaccurate CMDB inventories. They transform how every team operates in an increasingly complicated, cloud-connected digital world.

Real Customer Examples

- One financial services organization discovered 847 orphaned cloud resources they did not know existed, saving \$180,000 annually.
- An enterprise identified and remediated more than 2,400 dangling DNS records that were exposing them to domain takeovers.
- A healthcare organization reduced MTTR by 75 percent thanks to comprehensive visibility and device attribution.

KEY CAPABILITIES

Automated Asset Discovery with Actionable Insights: Gain a comprehensive inventory of all assets across hybrid, multi-cloud environments to identify shadow IT, unmanaged devices, underutilized cloud environments and other opportunities to reduce risk and waste.

Proactive Detection of Network Risks: Detect and remediate overlapping IP ranges, unregistered devices and outdated DNS records before they cause downtime or compliance failures.

Enhanced Security Posture: Identify dangerous vulnerabilities such as unmanaged assets and dangling records before they can be exploited for cyberattacks.

Streamlined Cross-Team Collaboration: Reduce manual effort, and speed troubleshooting and security investigations by enabling network, cloud and security teams to share the same authoritative source of truth for all enterprise devices.

1. *Infoblox Authoritative IPAM for DNS and DHCP: 3-Year TCO Evaluation*, Tolly Report, June 2022.
www.infoblox.com/resources/analyst-report/tolly-report-infoblox-authoritative-ipam-for-dns-and-dhcp/
2. *9 Pitfalls of Not Using Enterprise Grade DDI*, Enterprise Strategy Group (ESG), February 2025.
www.infoblox.com/resources/analyst-report/network-modernization-ddi-report/



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