Enterprise Strategy Group™ by TechTarget

9 Pitfalls of Not Using Enterprise-grade DDI

How the Wrong Approach Impacts Cloud Deployments, Security Risk, and Operational Agility

Jim Frey | Principal Analyst, Networking
Adam DeMattia | Senior Research Director

ENTERPRISE STRATEGY GROUP

FEBRUARY 2025

infoblox®

This Enterprise Strategy Group eBook was commissioned by Infoblox
and is distributed under license from TechTarget, Inc.

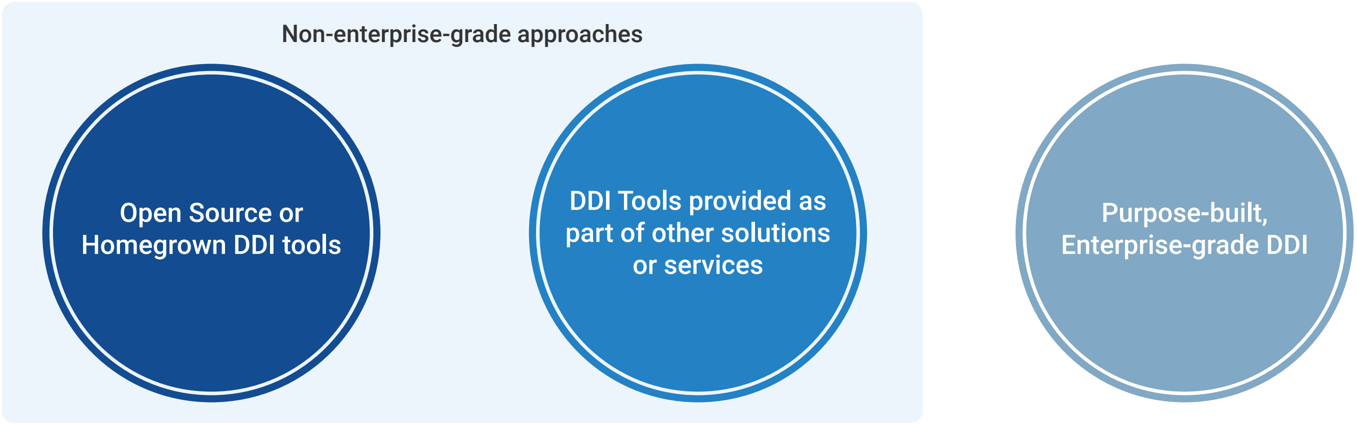
Contents

Introduction

As IT environments grow in size and complexity, a number of IT decision points will be reached that are critical for continued success. Best practices dictate that enterprises pay close attention not only to scaling applications and resilient IT infrastructure, but also to the essential services that enable them to work together seamlessly. Such is the case with functions that are commonly referred to as DDI, which is shorthand for DNS (domain name system), DHCP (dynamic host control protocol), and IPAM (IP address management). These functions make it possible for endpoints, including servers, end-user compute systems, handsets, smart devices, internet-based resources, and more, to find and connect to each other, as well as communicate as part of application execution and service usage. In short, DDI is nothing short of essential.

There are three primary approaches to fulfilling essential DDI requirements. Many teams start out using tools that are provided as part of a broader solution or services, essentially making do with what is picked up along the way when building out the infrastructure. Other organizations will consolidate and build out a DDI solution, leveraging some combination of open source and homegrown projects. And finally, there are fully integrated, purpose-built, enterprise-grade DDI solutions that can meet the need, such as those offered by Infoblox.

Approaches to DDI



Non-enterprise-grade approaches

Open Source or Homegrown DDI tools

DDI Tools provided as part of other solutions or services

Purpose-built, Enterprise-grade DDI

Recently completed primary research executed by Informa TechTarget's Enterprise Strategy Group and commissioned by Infoblox has found that the DDI approach taken has wide-reaching ripple effects. Taking the DIY or "as provided" routes, rather than selecting an enterprise-grade approach, results in a range of downsides and disadvantages impacting security, operations, application development, and cloud deployments. In short, anything less than a purpose-built, enterprise-grade DDI strategy raises risks and threatens IT success.

Back to Contents

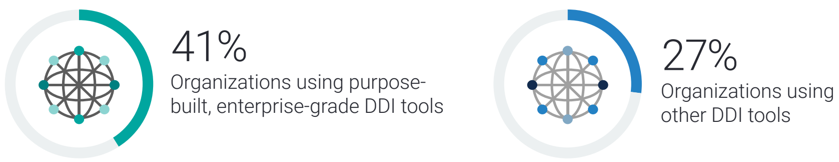
Nine Pitfalls

Besides representing an essential set of critical network services, the DDI approach that an organization chooses can significantly impact a wide range of processes, practices, and outcomes. Following are nine areas, spanning hybrid cloud, operations, and security, where analysis has revealed differences that are the most striking between those organizations that choose a purpose-built, enterprise-grade DDI path and those that do not.

1. Less Confidence in Cloud Adoption

One of the first places that DDI selection shows an impact is with cloud services. When it comes to IT and security teams' ability to deliver on cloud adoption requirements, those using non-enterprise-grade DDI reported 34% lower rates of "complete confidence" than those using enterprise-grade tools. This indicates that non-enterprise-grade DDI tooling is leaving gaps, raising risks for this imperative strategy.

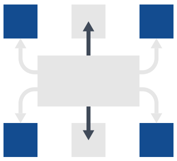
Complete Confidence in Meeting Cloud Adoption Requirements.



2. Lower Cloud Automation Success

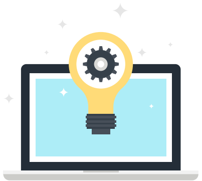
Cloud automation is the key to agility and resilience. Yet, organizations using non-enterprise-grade DDI struggle with automation, lagging by up to 28% in critical areas like patch management.

Full Automation Achievement for Cloud Functions Among Non-enterprise-grade DDI Users.



25% LOWER
Load balancing

19% LOWER
Audit reporting

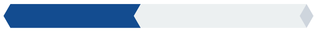


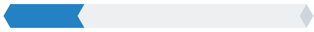
28% LOWER
Patch management

3. Cloud Outage Woes

A poor DDI strategy doesn't just slow cloud adoption; it threatens cloud resilience. Organizations using subpar DDI tools report quarterly cloud outages 44% more frequently and, as a result, were not enjoying longer time periods between outages to the same degree. When outages do happen, 38% more teams not choosing enterprise-grade DDI reported that it took hours to recognize, extending costly downtime.

Cloud Outage Frequencies for Non-enterprise-grade DDI Deployments vs. Enterprise-grade DDI Deployments.

44% HIGHER

Quarterly

25% LOWER

Annually

27% LOWER

Never in the last 12 months

Average Time Required for Non-enterprise-grade DDI Teams to Recognize Outages vs. Those Using Enterprise-grade DDI.

38% HIGHER

Hours

28% LOWER

Minutes

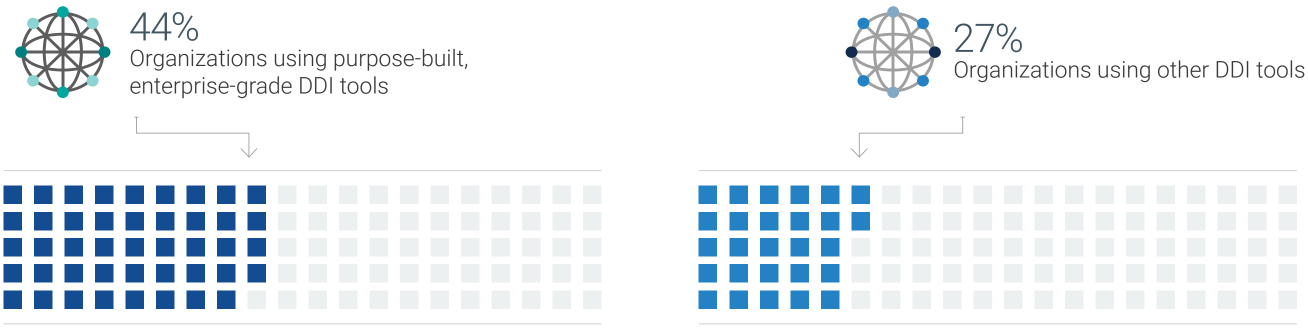
36% LOWER

Seconds (near-real time)

4. Less Hybrid Visibility Confidence

Visibility across complex environments is a challenge for anyone using cloud and hybrid infrastructures. Having the confidence to identify and report on cloud infrastructure consumption, assets in use, and network traffic with completeness and accuracy is essential for optimizing operational success. And yet, those using non-enterprise-grade DDI reported 30% less confidence in this regard than those using enterprise-grade DDI.

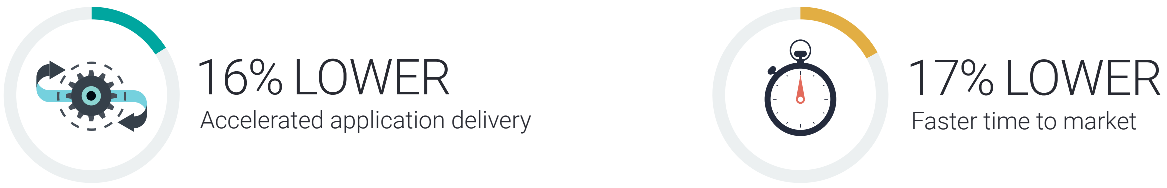
Complete Confidence in Visibility Across Cloud Environments.



5. Lower Achievement of Key Hybrid, Multi-cloud Objectives

Every organization has a range of objectives for the outcomes of hybrid and multi-cloud deployments, spanning efficiency, visibility, cost, and security. Unfortunately, those that use non-enterprise-grade DDI tools are falling behind in key areas, reporting that their approach to network and security technology has had less significant material impact on achieving objectives than those using an enterprise-grade DDI approach.

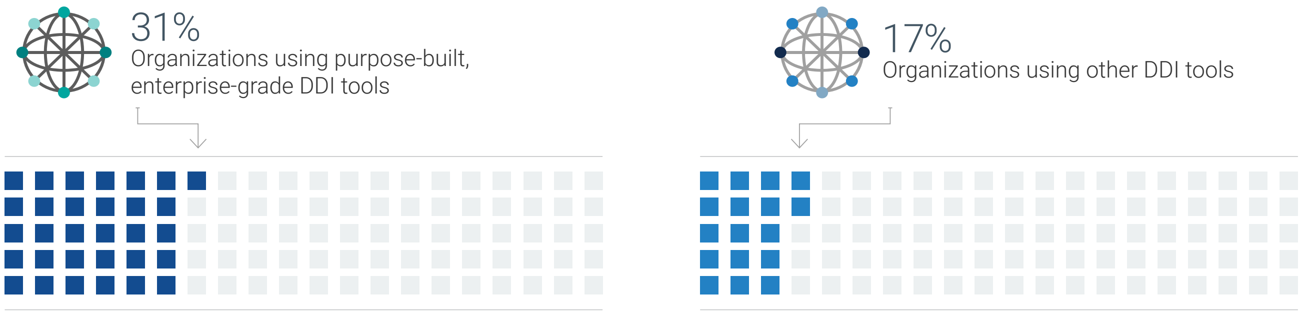
Significant Impact on Hybrid and Multi-cloud Objectives: Those Using Non-enterprise-grade DDI Tools vs. Those Using Enterprise-grade DDI Tools.



6. Less Strategic View of IT

One measure of success for IT and security teams is the way in which they are perceived by other groups, such as the application developers. In other words, how well are IT and security teams serving their internal customers? The most advanced level of regard is when application developers view IT and security teams as a competitive differentiator. For those not using enterprise-grade DDI, IT and security teams are viewed as a competitive differentiator at barely more than half the rate of those deploying enterprise-grade DDI. This remarkable difference reflects that the highest levels of professionalism and service become difficult to achieve without embracing enterprise-grade DDI.

Application Developers That View IT and Security Teams as a Competitive Differentiator.

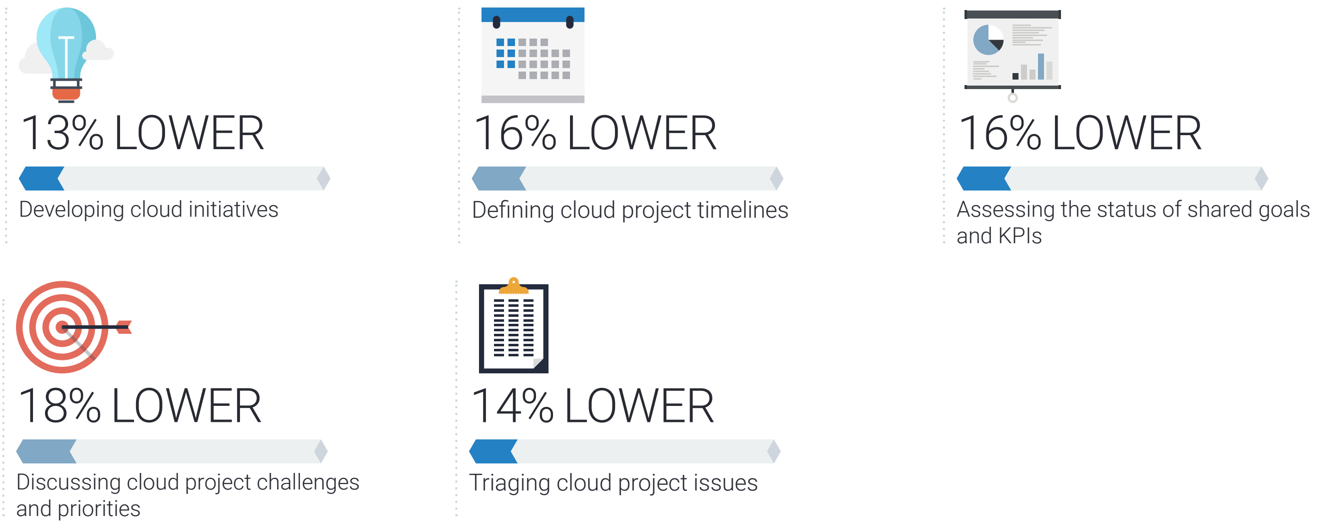


Back to Contents

7. Less Effective Collaboration

One of the most important organizational dynamics that contributes to overall success is the degree to which teams work together collaboratively and in pursuit of higher-level objectives. When it comes to the network and security staff, those using non-enterprise-grade DDI tools reported lower levels of collaboration than peers using enterprise-grade DDI across several scenarios. This could be readily explained by non-enterprise-grade DDI tools providing less universally accessible and consistent insights into the operating environment.

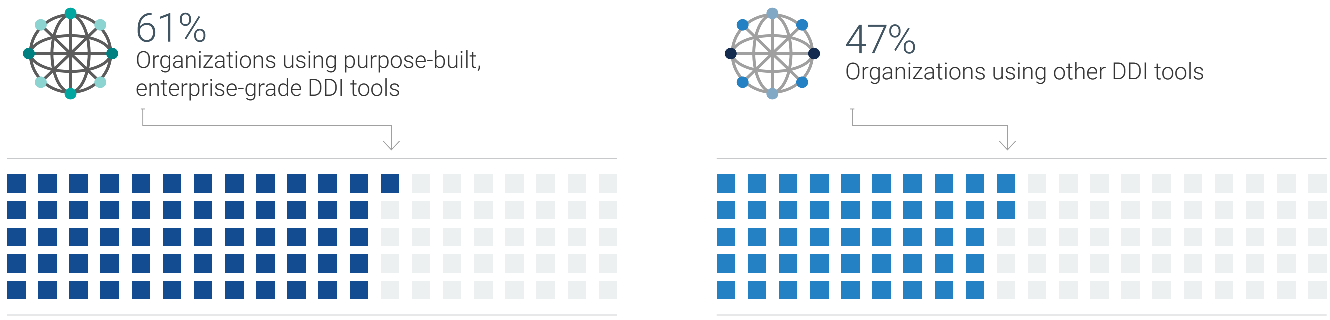
Occurrence of High Degrees of Network and Security Staff Collaboration for Non-enterprise-grade DDI Users vs. Those Using enterprise-grade DDI.



8. Less Leveraging of DNS for Protection

There are several specific security use cases where the use of DNS can make a substantial difference in protecting users. But not everyone has seen the same level of success across all such use cases, and, in some cases, there are substantial differences. For instance, when it comes to detecting and blocking malware and ransomware, those using non-enterprise-grade DDI reported leveraging DNS at a rate that is 23% lower than those using enterprise-grade DDI. This is a missed opportunity to reduce risk and improve protection.

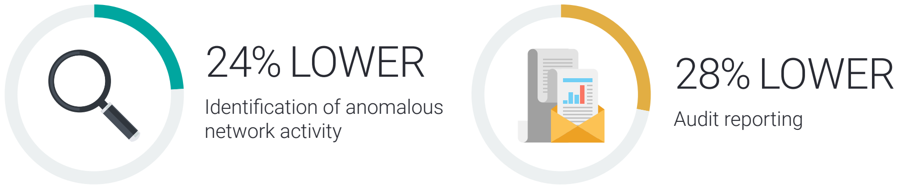
Leveraging DNS Extensively for Detection and Blocking of Malware and Ransomware.



9. Lower Levels of Cloud Security Automation

As with automation of workload operations, most organizations are also actively seeking to automate security management tasks in their cloud environments. But those using non-enterprise-grade DDI are finding it to be more difficult in certain scenarios than their peers using enterprise-grade DDI. Users of non-enterprise-grade DDI tools often lack the data completeness and richness of interfaces for successfully addressing automation objectives.

Full Automation of Cloud Security Management Tasks for Non-enterprise-grade DDI Tools vs. Those Using Enterprise-grade DDI Tools.



Back to Contents

Conclusion

Organizations have options when it comes to deploying DDI, from DIY, to mixes of provided tools, to embracing a purpose-built, enterprise-grade DDI solution. Enterprise network and security teams are at various points of their journeys in this regard, and it's clear that those that have yet to embrace purpose-built, enterprise-grade DDI are falling behind their peers in several ways across cloud, security, and operations objectives. They are seeing lower levels of success in cloud deployments and cloud automation and much slower rates of cloud outage awareness. Additionally, they are lagging behind their peers in fully supporting application teams. And they are falling short on effective IT-security collaboration, leveraging DNS for protection, and automating cloud security.

These findings paint a clear picture, and the risks and downsides are too great to ignore. Enterprise IT and security teams should look closely at moving to purpose-built, enterprise-grade DDI solutions to capture the advantages they can bring for a wide range of business and technical must-haves.

How Infoblox Can Help

Infoblox unites networking, security, and cloud to build a foundation for operations that is as resilient as it is agile. Infoblox seamlessly integrates, secures, and automates global network operations so that organizations can move fast without compromise.

infoblox®

Back to Contents

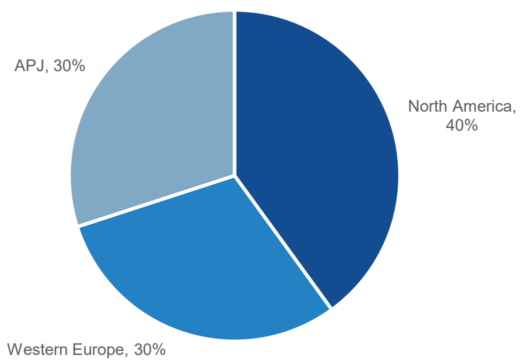
Research Methodology and Respondent Demographics

Data in this report references a comprehensive online research survey of 1,000 networking and security decision-makers and influencers knowledgeable about their organization's public cloud environment.

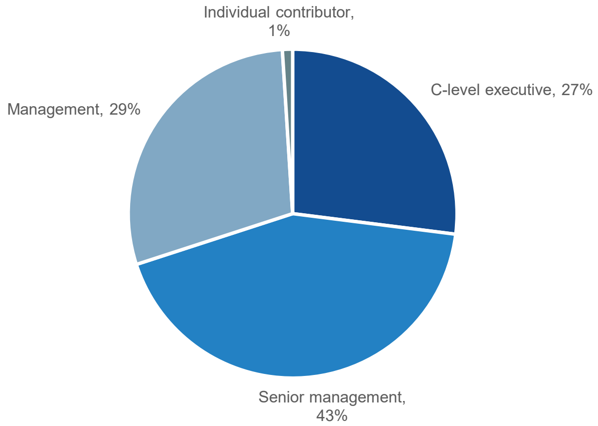
Organizations represented span private- and public-sector organizations across the globe, including respondents based in North America (U.S. and Canada), Western Europe (France, Germany, Spain, and the U.K.), and the Asia-Pacific region (Australia, India, Japan, New Zealand, and Singapore). The survey was fielded between December 15, 2023 and January 17, 2024. The margin of error at the 95% confidence level for this sample size is + or - 3 percentage points. The demographics of the survey respondents are displayed here.

Note: Due to rounding, the totals in figures and tables throughout this report may not add up to 100%.

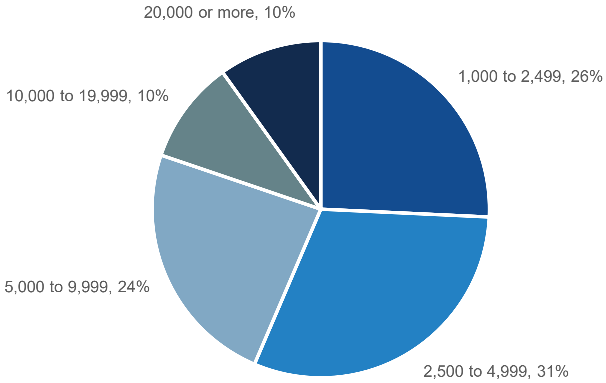
Respondents by region. (Percent of respondents, N=1,000)



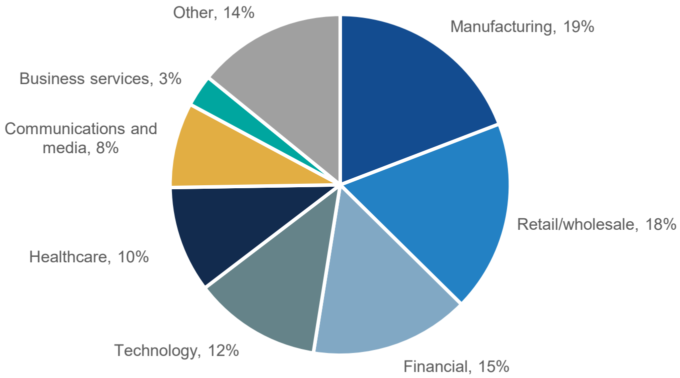
Respondents by current job title/level. (Percent of respondents, N=1,000)



Respondents by company size. (Percent of respondents, N=1,000)



Respondents by industry. (Percent of respondents, N=1,000)



Enterprise Strategy Group™ by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.