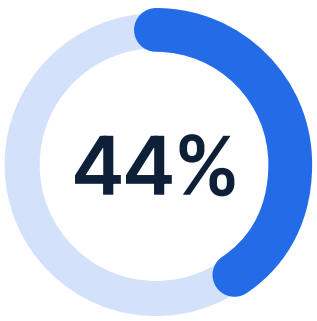
BLUECAT™

Integrity Micetro® | Explainer

Modernize mission-critical DDI

Secure, automate, and unify DNS, DHCP, and IPAM



of DDI managers identify network resilience as the top business benefit of investing in a commercial DDI solution.

Source:
From DIY DDI to BlueCat: Customers Earn ROI Within Three Months, Enterprise Management Associates

DDI complexity puts mission readiness at risk for U.S. defense and intelligence agencies

U.S. defense and intelligence agencies rely on the core network services of DNS, DHCP, and IP address management (together known as DDI) to keep mission systems reachable, resilient, and ready. But many federal environments still depend on fragmented tools, manual workflows, inconsistent data, and disconnected DNS and DHCP services across enterprise, cloud, remote, and operational networks.

This fragmentation results in real risk to mission readiness. Network teams lose time reconciling spreadsheets, chasing stale records, coordinating changes across silos, and responding to avoidable outages. As modernization accelerates, legacy DDI slows provisioning, limits visibility, and makes it harder to enforce consistent controls, underscoring the need for a unified approach.

Federal agencies need a way to manage DDI infrastructure across tactical environments, data centers, and the cloud from a single pane of glass to boost visibility and control.

DDI management your way: Appliance-based or an overlay on existing systems

BlueCat Integrity is a full appliance-based DDI solution that provides DNS and DHCP with centralized IP address management (IPAM), policy control, and automation. **BlueCat Micetro** is an overlay to help you manage existing DNS and DHCP services without forcing a major replacement project. With Micetro, network teams can centralize control while keeping current systems running.

With Integrity or Micetro, defense and intelligence network teams can:

- Manage DDI across tactical, base, and cloud environments
- See DNS, DHCP, and IP address data in one place
- Reduce manual work with APIs and automation
- Control who can make changes with role-based access
- Track changes with audit logs and event data
- Modernize at the pace that fits the mission

> **"Now, we not only see our entire IP address space in one view, but we can also manage both DNS and DHCP through the same interface."**

Senior security engineer, American multinational transportation company

A common DDI operating model built for federal modernization

A defense or intelligence network team may support users and systems across bases, remote locations, and cloud services. Without a common DDI view, each environment can become its own silo, leading to slower changes, more manual tracking, and riskier troubleshooting.

BlueCat's solutions give network teams a common DDI operating model. Whether you implement a full appliance-based deployment or an orchestration layer over what you already have, you can see and manage IP space, DNS records, DHCP services, and related changes from one place.

The result is modernized DDI for mission-critical networks that results in simpler daily operations, faster troubleshooting, and better control over the network services that agencies depend on.

Next steps

Learn how BlueCat can help defense and intelligence agencies modernize DDI for mission-critical networks.

Learn more