BLUECAT™

Integrity Add-On | Data sheet

Network Discovery

Get full infrastructure visibility across segmented, hybrid environments

Close network infrastructure visibility

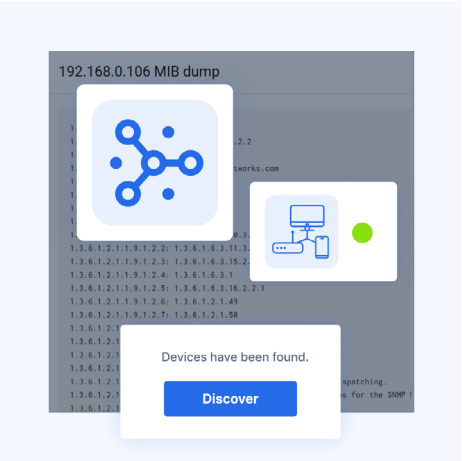
Modern networks have become increasingly fragmented, distributed, and virtualized—spanning data centers, clouds, remote offices, and tightly segmented environments. This complexity makes it harder than ever for teams to maintain an accurate understanding of what devices, services, and configurations truly exist across their infrastructure.

Traditional discovery tools often rely on centralized scanning or shallow protocol coverage, leaving major gaps behind firewalls, inside hypervisors, or across evolving network fabrics. These blind spots affect the accuracy of IT service management, the reliability of automation, and the network's security posture. Meanwhile, outdated or incomplete asset data increases operational risk.

Organizations need a modern, secure, and scalable way to establish trustworthy visibility across every network boundary and ensure downstream processes are powered by current, authoritative information.

The solution: Network Discovery

Network Discovery, an add-on to Integrity, BlueCat's DNS, DHCP, and IP address management (together known as DDI) solution for enterprises, delivers a modern approach to network infrastructure visibility. Using localized probes in BlueCat DNS/DHCP Servers (BDDSes) that operate within each network segment, it eliminates the need for risky firewall exceptions or centralized scanning architectures.



Network Discovery gathers device and configuration data via SNMP, ICMP scanning, SSH access, and vendor APIs, providing a richer and more accurate representation of the environment than legacy discovery tools. VMware support enables visibility into virtualized estates, while a reconciliation process ensures that only validated and authorized data is written into BlueCat Address Manager, Integrity's IP address management (IPAM) tool.

With controlled reconciliation and multi-method discovery, Network Discovery enables teams to maintain a current, authoritative view of their network, supporting improved security, automation, and IT service management practices.

Benefits

- **Segment-safe visibility**
  Localized probes provide complete asset insight without weakening firewall controls.
- **Richer asset intelligence**
  Multi-method discovery delivers deeper context on device state and configuration.
- **Trusted reconciliation**
  Operator validation ensures only accurate findings become authoritative IPAM data.
- **Operational confidence**
  Accurate, validated discovery data strengthens security posture and supports reliable automation.

Features

Per-network BDDS probe
Each BDDS acts as a localized discovery probe, operating within its own network segment to collect device and configuration details without requiring broad firewall access. This approach preserves segmentation, reduces exposure, and enables accurate discovery in distributed or restricted environments. Probes publish findings securely to Integrity for centralized review, ensuring teams maintain visibility without compromising security architecture.

VMware Hypervisor discovery
Support for VMware environments delivers visibility into virtualized network components, including hosts, virtual switches, and associated metadata. By integrating API-based discovery with traditional methods, Network Discovery helps teams understand relationships between physical and virtual infrastructure. This capability improves accuracy in environments where virtualization abstracts devices that traditional scanning often overlooks.

Controlled reconciliation
A reconciliation engine allows teams to validate, accept, or ignore discovered items before they become authoritative records. This controlled process prevents duplication, stale entries, and ungoverned updates to IPAM. With operator oversight, organizations maintain a clean and trustworthy source of truth that supports automation, IT service management processes, and security operations.

Multi-method discovery
Network Discovery gathers information via SNMP, ICMP scanning, SSH access, and vendor-specific APIs, allowing it to capture both high-level device presence and deeper configuration attributes. This multi-layered approach overcomes limitations of single-protocol tools and provides more complete insight into device roles, versions, and operational states. The result is a richer and more actionable asset inventory across hybrid environments.

BlueCat's Intelligent Network Operations (NetOps) solutions provide the analytics and intelligence needed to enable, optimize, and secure the network to achieve business goals. With an Intelligent NetOps suite, organizations can more easily change and modernize the network as business requirements demand.

Headquarters
4100 Yonge St. 3rd Floor, Toronto, ON, M2P 2B5
Phone: 1-416-646-8400 I 1-866-895-6931

bluecat.com

Next steps

Discover how you can boost your network infrastructure visibility across segmented, hybrid environments.

Learn more