BLUECAT™
Infrastructure Assurance

About BlueCat Infrastructure Assurance

BlueCat Infrastructure Assurance provides network and security automation that offers a deep level of visibility. BlueCat Infrastructure Assurance provides production-ready automation elements, continuously curated from vetted, community-sourced experience, to auto-triage issues in your network and security infrastructure. It automates repetitive tasks such as ongoing maintenance and high availability validation steps. Out of the box, it knows how to collect the most relevant data from your security or network infrastructure components and analyzes it according to known best practices.

How does BlueCat Infrastructure Assurance work?

BlueCat Infrastructure Assurance uses SSH, HTTPS, and SNMP protocols to connect and run collection scripts on network and network security devices using API calls, CLI commands, SNMP MIB, logs, or configuration files. These scripts run continually and undergo continuous analysis. BlueCat Infrastructure Assurance notifies users of potential issues, identifies the potential cause of the problem without human intervention, and provides diagnostic results along with actionable remediation steps.

Key capabilities

Auto-detection

BlueCat Infrastructure Assurance continuously analyzes device metrics to track device health posture, proactively notify users before problems occur (e.g., connection counts approaching the device limit), and avoid outages. Use cases include:

- **High availability verifications:** Ensure consistent configuration across clusters, and that redundant links and paths are both operational and correctly configured.
- **External services:** Monitor critical services for log service, identity awareness, authentication and authorization service, dynamic policies, or dynamic content updates with the latest threat intelligence.
- **Best practices:** Get recommendations for vendor-specific best practices and gold configuration conformance to avoid outages.
- **Security risks:** Enforce compliance with a defined set of internal or external policies and identify device vulnerabilities that matter.

Auto-triage

Upon BlueCat Infrastructure Assurance's detection of an issue, you can autonomously or manually run CLI commands and API queries according to best practices. BlueCat Infrastructure Assurance analyzes data to determine the cause of the problem, without any human intervention. Analysis results are presented visually in workflow diagrams, along with recommended resolution steps.

Automated configuration backup

With BlueCat Infrastructure Assurance, you can schedule daily, weekly, or monthly device backup to prepare for cases of device failure. This capability is supported for selected Check Point, Palo Alto Networks, Juniper Networks, Broadcom Symantec (formerly Blue Coat), F5, and Fortinet firewalls (check with your sales representative for details).

Operations management

BlueCat Infrastructure Assurance offers a variety of tools to accelerate troubleshooting, including:

- Visual tracking of critical metrics over time, allowing for correlating issues and timeframes for effective troubleshooting
- Custom report building and scheduling for devices that are not conforming to best practices, non-compliant, or harbor security risks
- Role-based access control to restrict access and read-only access privileges to certain users
- Granular device permissions to allow segregation of information between users, restricting their view to their respective purview
- Audit log to look back at changes and user activities

Integration

With BlueCat Infrastructure Assurance, you can improve the efficiency of IT teams through integration of email, syslog, APIs, and SNMP traps. Furthermore, users can:

- Carry out commands using APIs to retrieve information from or to post information to BlueCat Infrastructure Assurance
- Centralize authentication with Active Directory via Lightweight Directory Access Protocol (LDAP), RADIUS, or Security Assertion Markup Language (SAML) 2.0
- Integrate with ticketing systems such as ServiceNow
- Integrate with monitoring solutions such as Solarwinds Network Performance Monitor or BigPanda
- Integrate with data visualization tools such as Grafana or Tableau

Benchmark infrastructure

BlueCat Infrastructure Assurance's cloud-based analytics service contains production data collected from its users to provide proactive customer support. The data includes issues identified in user environments, scripts executed, and metrics collected.

System requirements

The sizing of BlueCat Infrastructure Assurance is critical to its overall stability and performance. Various sizes are available for different deployment scenarios. The requirements listed below are for up to 1,000 devices and are minimal recommendations. Please reach out to your BlueCat representative with questions.

Device count	Server	Browser
1-30	▪ 8 vCPU Xeon or i7 ▪ 8 GB RAM ▪ 180 GB HD (3000 IOPS)	▪ Chrome ▪ Edge
31-100	▪ 16 vCPU Xeon or i7 ▪ 16 GB RAM ▪ 180 GB HD (3000 IOPS)	
101-300	▪ 32 vCPU Xeon or i7 ▪ 64 GB RAM ▪ 400 GB HD (6000 IOPS)	

301-1,000	▪ 64 vCPU Xeon or i7 ▪ 96 GB RAM ▪ 400 GB HD (8000 IOPS)	

Supported devices

BlueCat	**BlueCat Address Manager (BAM):** ▪ BAM 1000/3000/5000/6000/7000 ▪ Virtual appliances running VMware Hyper-V or KVM ▪ Virtual cloud instances running in AWS, Azure, or Google Cloud ▪ Running 9.4 or later **BlueCat DNS/DHCP Server (BDDS):** ▪ BDDS 20/25/45/50/60/75/120 ▪ XMB ▪ Virtual appliances running VMware Hyper-V or KVM ▪ Virtual cloud instances running in AWS, Azure, or Google Cloud ▪ Running 9.4 or later
Broadcom Symantec (formerly Blue Coat)	**Hardware: ProxySG** ▪ Physical: SG S200, SG S400, SG S500 (physical ProxySG appliance) ▪ Virtual: SG-VA Alteon VA, Alteon VADC ▪ **Software:** ProxySG SGOS 6.5 and later ▪ **Content Analysis series:** CAS S200-A1, CAS S400-A1, CAS S400-A2, CAS S400-A3, CAS S400-A4, CAS S500-A1 ▪ Running CAS 2.3.5.1
Check Point	**Hardware (support includes open server deployments):** ▪ **Quantum Security Gateway appliances:** 700, 900, 1200R, 1550, 1590, 2200, 3100, 3200, 3600, 4200, 4400, 4600, 4800, 5100, 5200, 5400, 5600, 5800, 5900, 6200, 6500, 6600, 6800, 6900, 12200, 12400, 12600, 13500, 13800, 15400, 15600, 16000, 21400, 21600, 21700, 21800, 23500, 23800, 23900, 26000, 41000, 44000, 61000, 64000 ▪ **Quantum Lightspeed appliances:** QLS250, QLS450, QLS650, QLS800 ▪ **IPSO (Nokia) appliances:** IP150, IP290, IP390, IP560, IP690, IP1280, IP1220, IP2255 ▪ **Quantum Smart-1 security management appliances:** 405, 410, 625, 5050, 5150 **Software:** ▪ **Gaia** R80 -> R81.20 ▪ **Scalable Platform:** R76.40SP -> R81.10SP ▪ **IPSO:** R70 and later ▪ **Embedded Gaia:** R75.20 and later ▪ **CloudGuard Network Security:** R80 -> R81.20 ▪ **Maestro** R80.20SP -> R81.10SP ▪ **Multi-Domain Security Management (Provider-1)** R80 -> R81.20
Cisco	▪ **ASA 5500 Series:** 5505, 5510, 5512, 5515, 5520, 5525, 5540, 5545, 5550, 5555 ▪ **ASA 5500-X Series:** 5506-X, 5506W-X, 5506H-X, 5508-X, 5516-X, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X ▪ **ASAv:** Running ASA 9.x

F5	▪ **BIG-IP:** 5200v, 5250v, i5800, 7200v, 7250v/7255v, i7800, 10200v-F/10350v-N/10350v, i10800, i2250v
	▪ **VIPRION:** 2200/D114, 2400/F100, 4400/J100, 4480/J102, 4800/S100
	▪ **BIG-IP Virtual Edition (VE):**
	  ▪ Running TMOS 11.6 or later;
	  ▪ Software modules supported: Load Traffic Manager (LTM)

FireEye	▪ **NX series:** NX-VM, NX-900, NX-1400, NX-1500, NX-2400, NX-2500, NX-2550, NX-3500, NX-4420, NX-4500, NX-5500, NX-6500, NX-7400, NX-7420, NX-7550, NX-9450, NX-10450, NX-10000 ▪ Running wMPS 8.2.0
Fortinet	▪ **FortiGate:** 100E, 200E, 300D, 300E, 500D, 500E, 600D, 800D, 1000D, 1200D, 1500D, 2000E, 2500E, 3000D, 3100D, 3200D, 3700D, 3960E, 3980E ▪ **FortiGate-VM and FortiOS** (minimum 4GB RAM) ▪ Running 6.4.x and 7.0.x
Gigamon	▪ **GigaVUE visibility appliances (TA Series and HC series):** GigaVUE-TA10, GigaVUE-TA40, GigaVUE-TA100, GigaVUE-TA200, GigaVUE-HC1, GigaVUE-HC2, GigaVUE-HC3 ▪ Running GigaVUE-OS 4.7.01
Juniper Networks	▪ **SRX Series:** SRX100, SRX110, SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, SRX345, SRX650, SRX1400, SRX1500, SRX3400, SRX3600, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX ▪ **Software:** Junos 12.1X46 and later
Palo Alto Networks	**Hardware (support includes open server deployments):** ▪ **Next-Generation Firewalls:** PA-200, PA-220, PA-500, PA-800, PA-820, PA-2000, PA-3000, PA-3200, PA-4000, PA-5000, PA-5200, PA-7000 ▪ **VM-Series Virtual Next-Generation Firewalls:** VM-50, VM-100, VM-200, VM-300, VM-500, VM-700, VM-1000HV ▪ **Panorama:** M100 and M-500 ▪ **Software:** PAN-OS <= 11.0
Radware	**Hardware: Radware Alteon** ▪ Physical: Alteon 5K, 6K, 8K series (both in Standalone and VX Mode) ▪ Virtual: Alteon VA, Alteon VADC ▪ **Software:** Alteon OS 29.0 and later
Zscaler	**Zscaler App Connector** ▪ Running on RedHat 7.x or 8.x

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

bluecat.com

Next steps

Reach out to a BlueCat representative to schedule a demo.

Request a live demo