Avoid network disruption

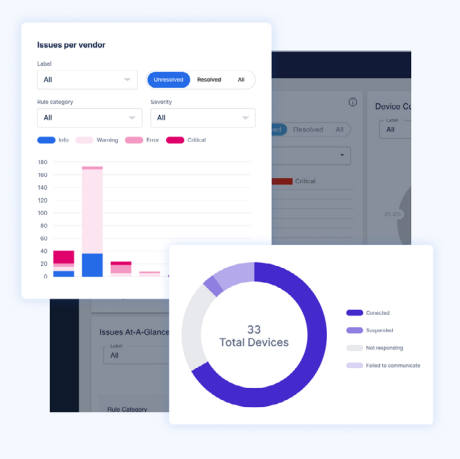
Use automation to identify, troubleshoot, and remediate issues

Proactive observability, troubleshooting, and remediation

BlueCat LiveAssurance provides deep visibility and automation to prevent network disruption. It is a proactive observability, troubleshooting, and remediation solution for your network and security infrastructure. LiveAssurance continuously measures security, performance, and configuration metrics, cross-referenced with benchmark data. When it finds an issue, it conducts auto-triage and root-level diagnosis without human intervention. And it serves up recommended remediation steps for IT operations teams to use based on known best practices and a knowledge base curated by a global community of experts.

The solution: BlueCat LiveAssurance

LiveAssurance 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. LiveAssurance notifies IT operations teams of potential issues, identifies the potential cause of the problem without human intervention, and provides diagnostic results along with actionable remediation steps. IT operations teams can then fix issues before they cause disruption.



Key capabilities

Auto-detection
LiveAssurance 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 standard 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 LiveAssurance's detection of an issue, you can autonomously or manually run CLI commands and API queries according to best practices. LiveAssurance 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.

Validate change requests

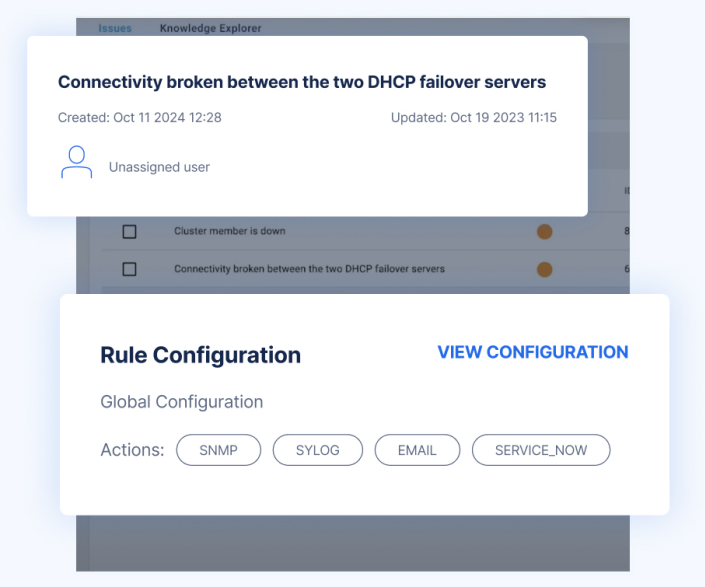
Validating changes and identifying signs of an unsuccessful change can be a time-consuming and manual process. With Manifest, LiveAssurance automates the process of validating that services have resumed following change requests. Using automation, Manifest conducts comprehensive snapshot comparisons and generates a record of changes made during an upgrade, patch, or configuration change. It gives IT operations teams peace of mind that critical infrastructure is back to its normal state after applying updates.

Automated configuration backup

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

Anomaly detection

LiveAssurance uses machine learning models to identify outliers and unusual behaviors. Awareness of anomalies helps identify early symptoms of emerging issues, allowing you to address them before they become bigger problems.



Operations management

LiveAssurance offers a variety of tools to bolster network operations management and 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
- System-defined reports for payment card industry (PCI) compliance and CVEs
- Role-based access control to restrict access and assign read-only access privileges for 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 LiveAssurance, you can improve the efficiency of IT operations teams through the integration of email, syslog, APIs, and SNMP traps. Furthermore, users can:

- Carry out commands using APIs to retrieve information from or post information to LiveAssurance
- Centralize authentication with Active Directory via LDAP, RADIUS, or SAML 2.0
- Integrate with ticketing systems such as ServiceNow
- Integrate with monitoring solutions such as Solarwinds or BigPanda
- Integrate with data visualization tools such as Grafana or Tableau

Benchmark infrastructure

LiveAssurance'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 LiveAssurance 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 sales representative with questions.

Device count	Server	Browser
1-30	• 8 vCPU Xeon or i7 • 8 GB RAM • 180 GB HD (3000 IOPS)	• Chrome, Edge, Firefox
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)** • 9.4 or later
	BlueCat DNS/DHCP Server (BDDS) • 9.4 or later
	BlueCat Edge Service Point • Service Point Version 4.7.0 or later
Broadcom Symantec (formerly Blue Coat)	**ProxySG and Content Analysis System (CAS)** • ProxySG SGOS 7.4 or later • Running CAS 3.1 or later
Check Point	**Check Point firewalls** • Quantum security gateway • Quantum Lightspeed • Maestro Hyperscale Orchestrator • Quantum Smart-1 • CloudGuard Network Security • Gaia R80.40 to R81.20 • Embedded Gaia: R77.20 to R80.20

Cisco	**Cisco ASA** • ASA 9.x or later
F5	**F5 Load Traffic Manager (LTM)** • F5 TMOS 11.6 or later
FireEye	**FireEye NX** • wMPS 8.2.0
Fortinet	**FortiGate NGFW** • FortiOS 6.x.y or later
Gigamon	**GigaVUE** • GigaVUE-OS 4.7.01 or later
Juniper Networks	**SRX Series Firewalls** • JunOS 12.1X or later
Palo Alto Networks	**Palo Alto Networks Next-Generation Firewalls** • Panorama mode and Log Collector mode • PAN-OS 10.1, 11.1, or later
Radware	**Radware Alteon** • Alteon OS 29.0 or later
Zscaler	**Zscaler App Connector** • Running on RedHat 7.x or 8.x

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 LiveAssurance can proactively alert you to issues to help avoid network outages.

Request a live demo