BLUECAT

Infrastructure Assurance | Solution brief

Infrastructure Assurance for Check Point Quantum

Network observability and health

Challenge

Undetected firewall issues can expose your network to security breaches or lead to an outage. Existing monitoring tools are reactive, only notifying users of an issue after it occurs, and do not provide actionable next steps.

Solution

BlueCat Infrastructure Assurance proactively alerts Check Point Quantum firewall and security gateway users to issues and provides remediation steps that IT operations teams can use to resolve problems before they cause significant damage.

Benefits

- Proactively identify issues to avoid outages
- Optimize the performance of security infrastructure
- Reduce mean time to resolution
- Work more effectively

Request a demo

Automating best practices and operational device issue detection in your security infrastructure

Without automation, IT operations teams would spend countless hours gathering diagnostics and device data to keep firewalls running. IT teams that manage firewalls often have limited resources, resulting in an even greater need for automated diagnostics and issue detection. The typical security engineer spends much of their time identifying and remediating known errors.

IT operations teams can avoid costly outages if they receive advanced notice about common issues that can lead to bigger problems. These issues might include hidden configuration drift, forgotten ongoing maintenance tasks, or a lack of adherence to vendor, industry, and/or high availability best practices.

This solution brief presents how BlueCat Infrastructure Assurance automates detection of operational device issues, which are often hidden, in your security infrastructure. This brief provides specific examples from a variety of use cases for Check Point Quantum firewall and security gateway customers to simplify Day 2 operations, adhere to best practices, and ensure maximum reliability. It also covers key differentiators from other solutions and key solution benefits.

Solution overview

Infrastructure Assurance avoids network disruption with automation. Think of it as a virtual expert that can expand team skills and is on duty 24/7.

Infrastructure Assurance provides deep visibility into your security infrastructure to flag early warning signs of issues. With our domain expertise codified into Infrastructure Assurance, the platform knows what to look for, analyzing your firewalls to ensure they are healthy.

Should it find something, the platform proactively alerts IT operations teams that a service failure—or any level of degradation of service—might be coming. Our auto-triage capability will investigate a problem without any human intervention. It gathers additional contextual diagnostic information, analyzes, and performs everyday troubleshooting tasks and root cause analysis.

Then, Infrastructure Assurance provides a list of recommended remediation steps that IT operations teams can use as a guide to help address the problem. IT operations teams gain firewall-specific knowledge from issue descriptions and recommended remediations built from the real-world experience of certified security experts.

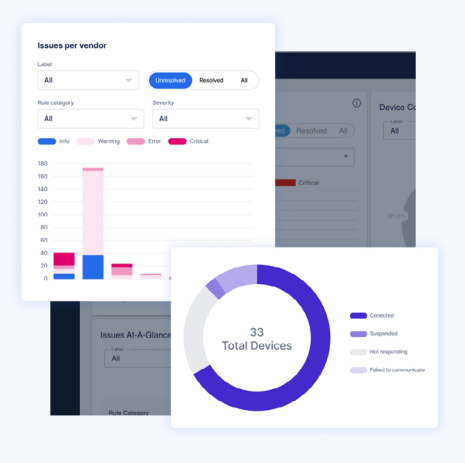
Effectively, we've automated best practices to help you improve the efficiency of your security operations, reduce mean time to resolution, and prevent costly disruptions.

Use cases

For Check Point Quantum firewall and security gateway customers, moving beyond the reactive mindset when things go awry is within reach. In this section, we outline eight scenarios that you might encounter, with specific real-world examples of detected issues. Each explores how Infrastructure Assurance can help ensure that your security infrastructure is working as intended.

Once issues are detected, Infrastructure Assurance provides actionable information to help IT operations teams address them. This includes a description of the problem, remediation steps, and links to articles on Check Point's support portal.

Use case 1: Stateful health checking



Infrastructure Assurance continuously assesses the health of Check Point Quantum firewalls and security gateways by comparing expected device configurations against the current status. The goal is to find and address lurking issues before they impact services.

Sample common issues detected, based on real experience, include:

- Debug mode enabled, causing performance issues
- SecureXL templates (Drop, Accept, NAT, NMR, NMT) disabled
- SecureXL Fast Accelerator (rules exist)
- Ensure DOS blade deny list, rate limit, and log drops are enabled and penalty box counter monitoring
- Aggressive aging enabled
- Intrusion Prevention System (IPS) is bypassed
- Dynamic Balancing status is off

Use case 2: External critical services

Firewalls have near real-time dependency on many external services. It is important to monitor the connection to these critical services. Infrastructure Assurance's automation features ensure, through regular testing, that communication with these external services is always available.

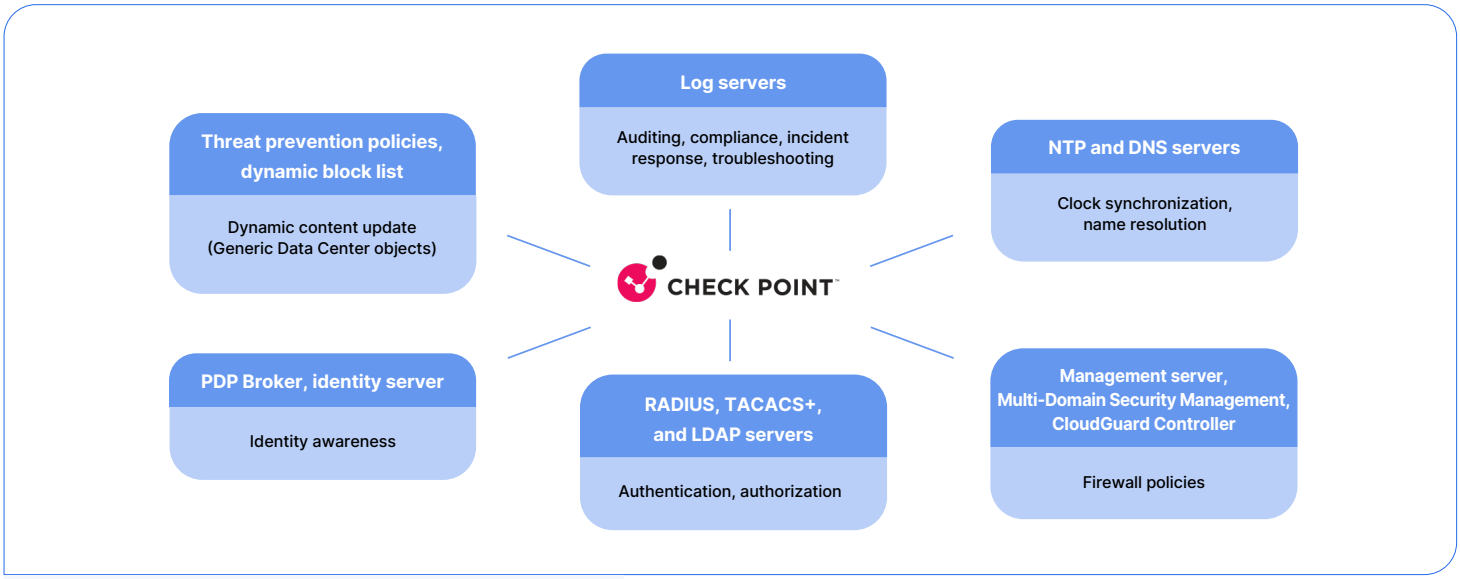


Figure 1. External services required by Check Point Security gateways

Critical services that a firewall requires include clock synchronization with an NTP server, access to DNS for name resolution, and forwarding syslog to an external server for auditing, compliance, troubleshooting, or incident response.

Firewalls also need up-to-date policies from their management and authentication servers. Identity awareness is another key use case. Infrastructure Assurance will ensure connectivity to Identity Collector and that collection events are not zero and check for PDP Broker status.

Your firewalls are importing objects (such as IP addresses, URLs, and domains) from an external web server to protect against malicious hosts. Infrastructure Assurance will ensure dynamic content update is working by checking Generic Data Center objects status.

Use case 3: High availability readiness

To prevent a single point of failure on your network, you made the investment to deploy redundant infrastructure to ensure always-on services. Unfortunately, despite the investment, failovers do not always go smoothly. Infrastructure Assurance constantly detects high availability unreadiness from cross-device inconsistencies. This includes ensuring the configuration state and adherence to best practices.

Examples of high availability readiness issues that Infrastructure Assurance might detect and provide alerts for include:

- Static routing tables mismatch
- Policy Based Routing (PBR) rules mismatch
- CoreXL or SecureXL configuration mismatch
- Hotfixes and jumbo hotfixes mismatch
- Cluster has preemption enabled
- Bond operating without sufficient subordinate interfaces
- Virtual Router Redundancy Protocol (VRRP) cluster members in master/master state
- Use a bond interface defined as sync for redundancy
- Cluster configuration not synchronized

Use case 4: CloudGuard Network Security

Enterprises deploy Check Point CloudGuard Network Security to the public cloud as workloads are shifted to the cloud.

Infrastructure Assurance is typically deployed on premises. In this example, Check Point CloudGuard Network Security is deployed in AWS and Check Point secure gateways are deployed on premises. Infrastructure Assurance interacts with CloudGuard Network Security in public clouds and with Check Point management servers, CloudGuard controllers, and secure gateways in traditional private data centers.

Infrastructure Assurance provides the same level of support as on-premises Check Point secure gateways. In addition, specific auto-detect elements detect connectivity failure, policy installation failure, and update failure between

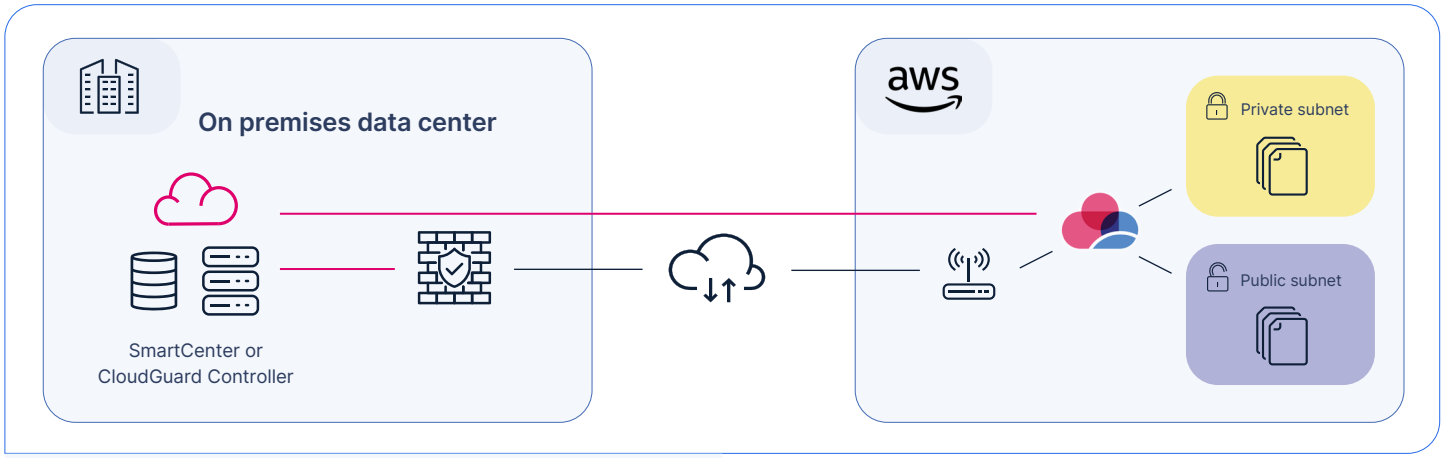


Figure 2. Check Point network security infrastructure in a hybrid cloud environment

CloudGuard Controller and CloudGuard instances.

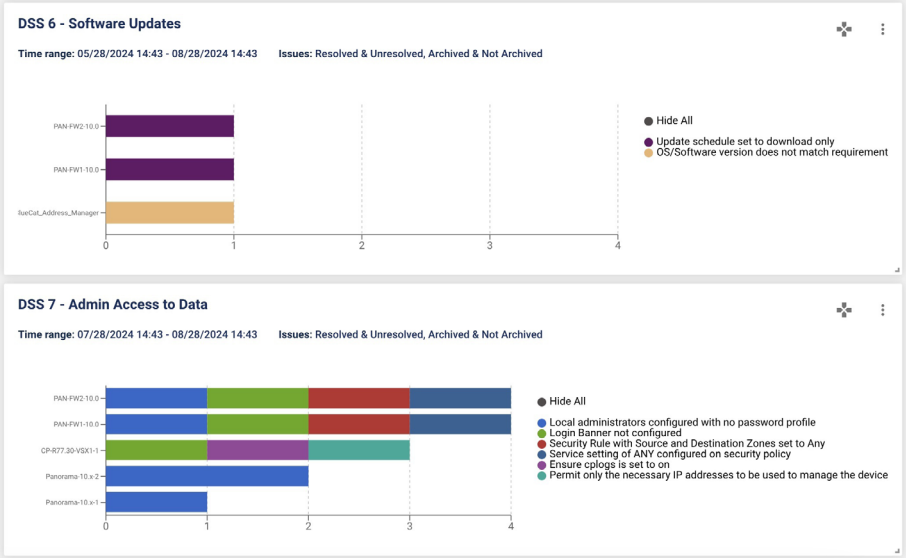
Examples of actions that Infrastructure Assurance might take for CloudGuard Network Security include:

- Ensure CloudGuard Controller is running as a process on the management server
- Check connectivity between CloudGuard Controller and AWS
- Check errors on data center scanners
- Check the connection between CloudGuard Controller and CloudGuard instances
- Check if Identity Awareness web API is running
- Check if CloudGuard Controller is updating CloudGuard instances
- Check for imported objects from the data center

Use case 5: Auto-detect security risks and ensure compliance

Enterprises are hypervigilant about how they secure their security infrastructure. Device hardening is necessary to reduce the attack surface. Infrastructure Assurance has hundreds of automation elements to identify security risks and compliance violations. Regardless of your regulatory compliance requirements, we likely have the security control validations in place to help you prepare for your audit.

For example, here are snapshots from a Payment Card Industry Data Security Standard (PCI DSS) compliance report:



Use case 6: Misconfigurations

Device misconfiguration is another major cause of unplanned downtime. Configuration errors can create security gaps in your network, making it vulnerable to cyberattacks. Infrastructure Assurance continuously detects misconfigurations by verifying against a gold standard for your network. Misconfiguration issues that Infrastructure Assurance might alert you to include:

- Configuration mismatch
- DNS, NTP, logging servers, management servers configured, RADIUS, or time zone configured do not match the requirement
- A critical file has been modified

Use case 7: Automate easily forgotten maintenance tasks

Maintaining availability requires ongoing maintenance. Tasks like device configuration backup are essential to ensure your security infrastructure is safe from failure and disruption. Infrastructure Assurance automates device configuration backup and proactively notifies you if the backup is unsuccessful.

One of the most easily forgotten maintenance tasks is certificate renewal. Your firewalls use certificates for a variety of purposes. Valid certificates are needed for site-to-site VPN, SSL VPN, and the web portal. Not having a valid certificate will likely impact services. Infrastructure Assurance provides warnings in advance if certificates are about to expire, giving you ample time to act.

Infrastructure Assurance also checks for valid licenses to ensure software license compliance, whether for vendor support, hardware, software, or access to threat intelligence. Automating these maintenance activities can truly help maintain the health and performance of your firewalls.

Use case 8: Automated troubleshooting

When an issue is detected, Infrastructure Assurance will automatically apply device-specific domain knowledge to the problem. It will analyze the problem to accelerate root cause analysis.

Let’s look at an example: A Border Gateway Protocol (BGP) peer down issue is detected. Infrastructure Assurance runs its own investigative steps to gather additional contextual diagnostic information and perform in-depth analysis. It follows a troubleshooting workflow with branches curated by industry experts. Applying domain knowledge is critical to determining what relevant information to collect while the problem is happening to make an accurate diagnosis.

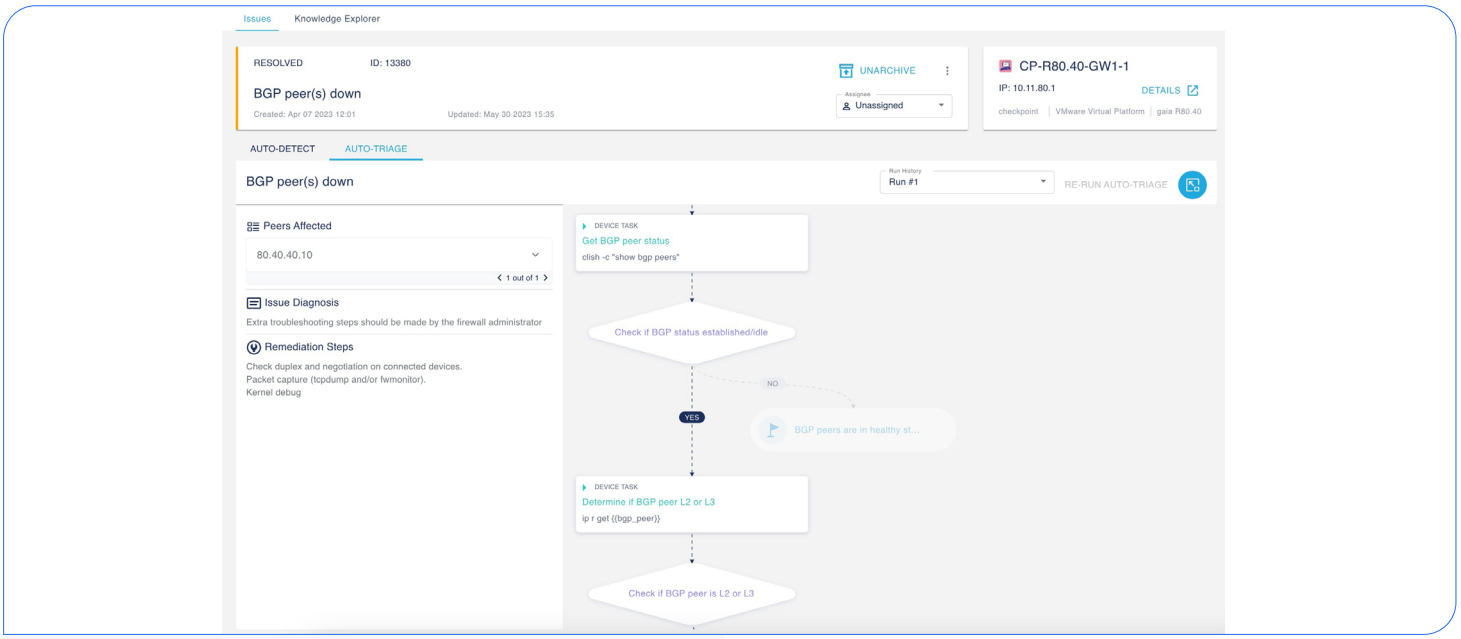


Figure 3. Auto-triage for a BGP peer down issue—is it Layer 2 or Layer 3 peering?

Layer 2 BGP peer troubleshooting

For Layer 2 connectivity, Infrastructure Assurance performs various tests, including testing for unicast packets and BGP port accessibility, checking for carrier counters, and examining ARP table entries. Possible root causes that can be identified are:

- Interface errors due to drops or collisions
- Link flapping
- BGP port 179 is down

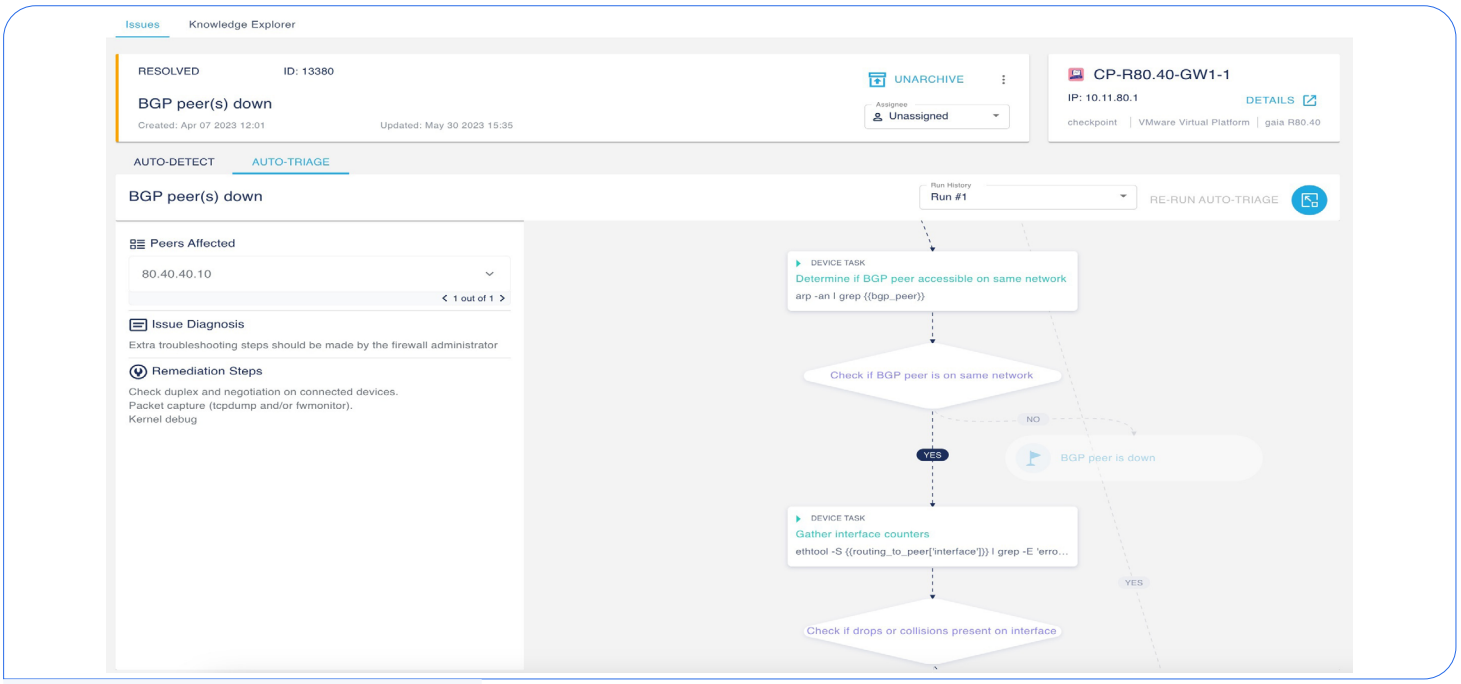


Figure 4. Auto-triage of a BGP Layer 2 peering issue

Layer 3 BGP peer troubleshooting

For Layer 3 connectivity, Infrastructure Assurance performs ping tests, unicast packet reachability tests, and BGP port reachability tests. Possible root causes are:

- Routing issues such as missing static routes
- BGP port 179 is down
- Firewall blocking access

Depending on the configuration and situation, Infrastructure Assurance walks down a different branch of the troubleshooting workflow. Sometimes, we can identify the root cause and present prescriptive remediations for speedy resolution. Even if determining the root cause is not possible, you have captured useful diagnostic information about the problem for escalation. With auto-triage, we have effectively automated remediation steps without human intervention, further reducing time to resolution and increasing efficiency.

Key differentiators

There are four major differences between Infrastructure Assurance and other network monitoring and management solutions.

1. Our automation elements are developed by our community of experts. By bringing expertise from our community, security vendors, and Fortune 1,000 customers, we can gather the most relevant and important device knowledge. Crowd sourcing brings together ideas and expertise that would not otherwise be available.

2. When deploying Infrastructure Assurance in a security environment, customers immediately receive notifications about misconfigurations, errors, security risks, vulnerabilities, and lack of adherence to best practices. Because Infrastructure Assurance knows what to look for, the platform can continually and preemptively identify issues to avoid bigger problems. Other network monitoring solutions lack specific, codified domain expertise.

3. When it detects the symptoms of various potential problems, Infrastructure Assurance automates the troubleshooting process to determine root causes. Other network monitoring and management solutions provide alerts but stop there. It's left to IT operations teams to conduct troubleshooting and root cause analysis themselves. Automated detection and analysis of issues can prevent them from recurring and reduce downtime.

4. Once root causes have been determined, Infrastructure Assurance goes further than other monitoring solutions by providing a list of actionable remediation steps that IT operations teams can take. IT operations teams gain specific knowledge from the issue descriptions and recommended remediations compiled from the real-world experience of experts. These specific, actionable insights also reduce troubleshooting time.

Solution benefits

IT operations teams enjoy several benefits when using Infrastructure Assurance as a solution for hidden issue detection and recommended remediation. They include:

- **Avoid downtime.** Proactively identify misconfigurations, high availability inconsistencies, forgotten maintenance tasks, and other best practices to avoid outages.
- **Optimize the performance of your security infrastructure.** Automation streamlines IT operations, allowing IT teams to deliver optimal security services to your organization.
- **Reduce mean time to resolution.** Accelerate troubleshooting by conducting automated root cause analysis, without human intervention.
- **Work more efficiently.** Infrastructure Assurance surfaces valuable and actionable information that will immediately facilitate your IT operations team's work.

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

bluecat.com

Version SB-IA-CP-09-09-2024

Next steps

Discover how Infrastructure Assurance can proactively alert you to issues to help avoid network outages.

Request a demo