BLUECAT

LiveAssurance for Palo Alto Networks NGFW

Network observability and health

Challenge

Undetected issues with firewalls 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 LiveAssurance proactively alerts Palo Alto Networks Next-Generation Firewall 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 live 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 up and 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 a notable portion 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 combination of a lack of adherence to vendor, industry, and/or high availability best practices.

This solution brief presents how BlueCat LiveAssurance 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 Palo Alto Networks Next-Generation Firewalls 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

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

LiveAssurance provides deep visibility into your security infrastructure to flag early warning signs of issues. With our domain expertise codified into LiveAssurance, 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 there might be a service failure—or any level of degradation of service—coming. Our auto-triage capability will investigate a problem without any human intervention. It gathers additional contextual diagnostic information, analyzes, and performs common troubleshooting tasks and root cause analysis.

Then, LiveAssurance 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 Palo Alto Networks Next-Generation Firewalls 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. Each explores how LiveAssurance can help ensure that your security infrastructure is working as intended.

Once issues are detected, LiveAssurance provides actionable information to help IT operations teams address it. This includes a description of the issue, remediation steps, and links to articles on Palo Alto Networks' support portal.

Use cases 1: Stateful health checking

LiveAssurance continuously assesses the health of Palo Alto Networks NGFW by comparing expected device configurations against the current status. The goal is to find lurking issues and address them before they impact services.

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

- Debug mode enabled
- Next hop inaccessible
- Policy-Based Forwarding rule is down
- SSL decryption—sessions near capacity, SSL decryption memory usage is high, tracking of SSL global counters and notification if the device has opted to drop packets or leave traffic encrypted
- Maximum number of routes nearing limit
- Packet drop counters increasing significantly—TCP flow non-sync packets, flow policy-deny, NAT'ed packets
- Capacity of dynamic address groups approaching device limit

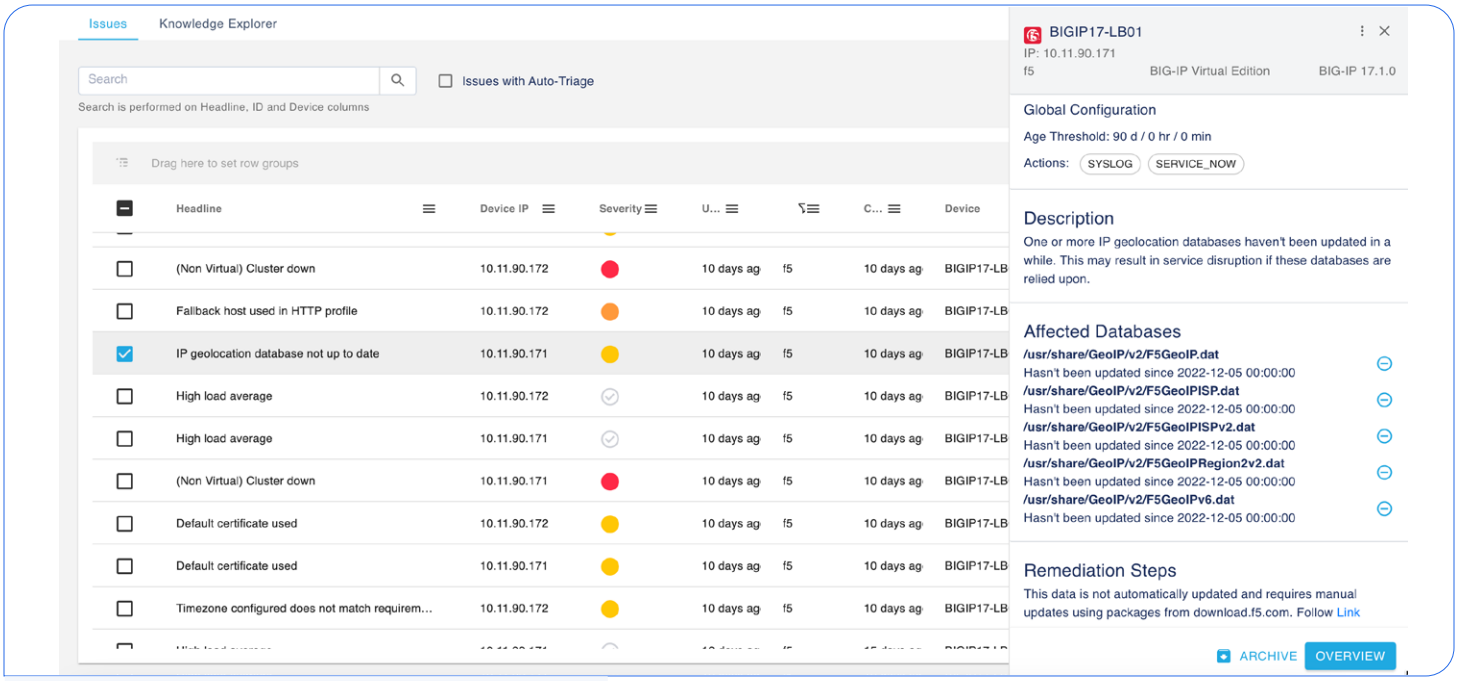

Figure 1. LiveAssurance displays Stateful Health Issues and Remediation Steps

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. Through regular testing, LiveAssurance's automation features ensure that communication with these external services is available at all times.

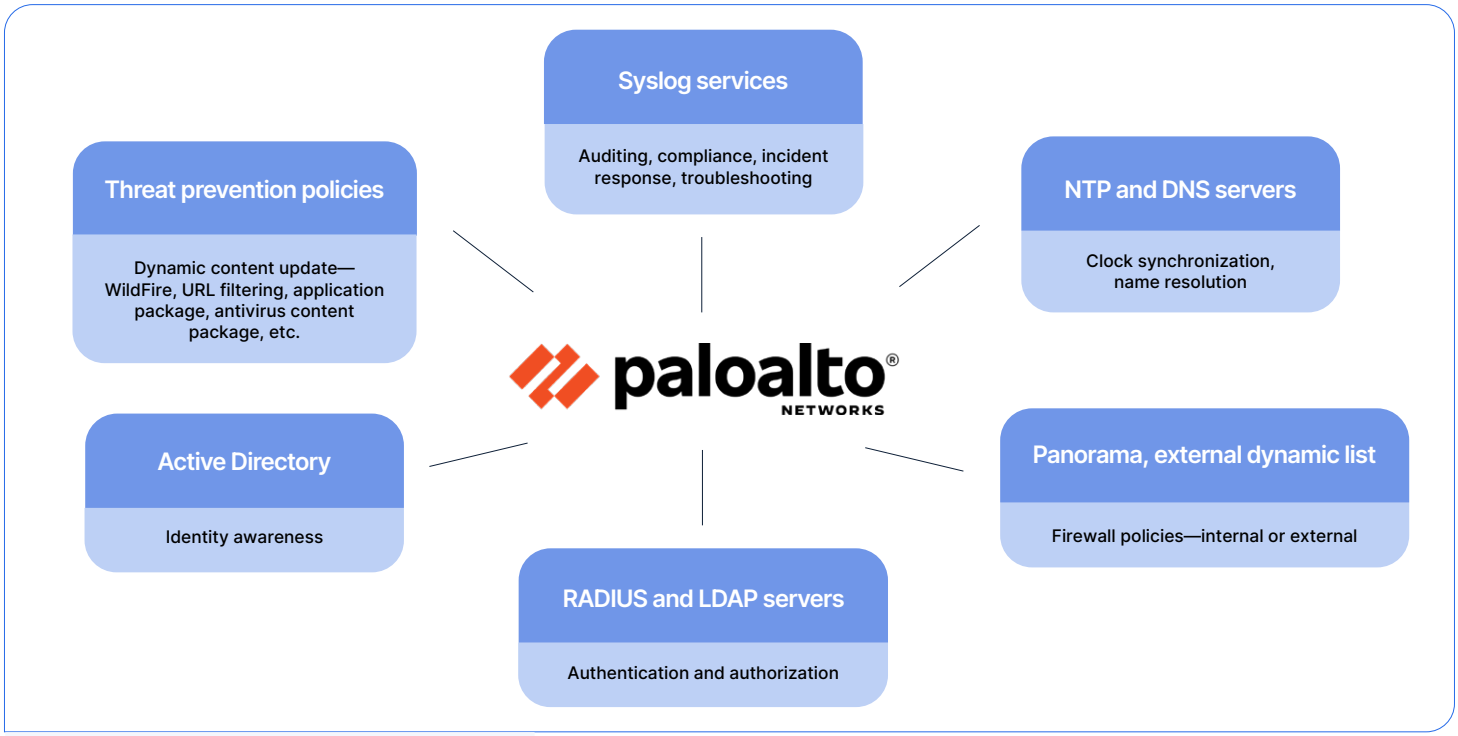

Figure 2. LiveAssurance communicates with External Critical Services

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 may need continuous access to Active Directory for identity awareness to make forwarding decisions. They also need access to RADIUS or LDAP servers for user authentication and authorization.

To equip firewalls with the latest preventative intelligence, firewalls frequently get updates from WildFire, the URL filtering cloud, and other tools. Timely updates are key to protecting your networks before threats become widespread. LiveAssurance continuously checks that packages are kept up to date by always maintaining an active connection. It also ensures best practices are followed. This includes, for example, always making sure that the action is set to "download-and-install" and that the frequency for WildFire is set to one minute.

Firewalls also need up-to-date policies from Panorama. Your firewalls are likely importing objects (such as IP addresses, URLs, and domains) from an external web server to protect against malicious hosts. The list of objects is known as an external dynamic list (EDL). LiveAssurance goes beyond just checking for reachability to the web server hosting the EDL. It also ensures that the EDL is not empty and that it has not reached its capacity.

Use case 3: Misconfigurations

Device misconfiguration is another major cause of unplanned downtime. Configuration errors can create security gaps in your network, making it vulnerable to cyberattacks. LiveAssurance continuously detects misconfigurations by verifying against a gold standard for your network. It even notifies you if a scheduled commit from Panorama failed.

Misconfiguration issues that LiveAssurance might alert you to include:

- Default route in static route table not available
- Static routing table has changed
- DNS, Panorama, NTP, or RADIUS configuration does not match requirement
- SNMP community string or SNMP trap community string configuration does not match requirement
- Time zone configuration does not match requirement
- Panorama—commit not scheduled or scheduled commit failed
- Authentication profile(s) misconfigured
- EDL(s) configured is/are not used in policy

Use case 4: 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.

LiveAssurance constantly detects high availability unreadiness from cross-device inconsistencies. This includes configuration state and ensuring adherence to best practices. Examples of high availability readiness issues that LiveAssurance might detect and provide alerts for include:

- High availability interface not receiving traffic
- High availability pair member in suspended state for too long
- Cluster has preemption enabled
- Cluster configuration not synchronized
- High availability configurations not meeting best practices

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. BlueCat LiveAssurance 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:

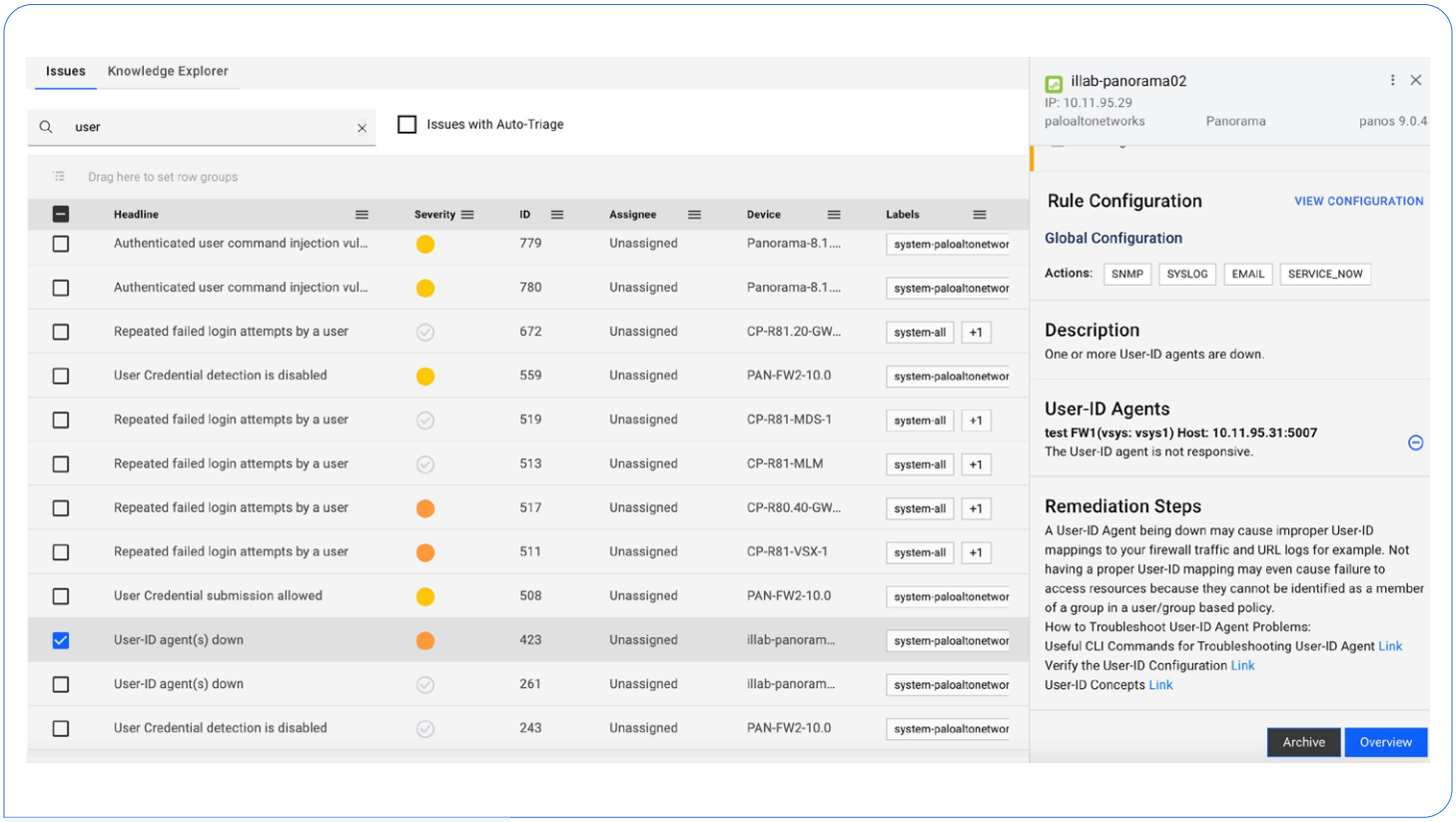

Figure 3. Snapshot of LiveAssurance's PCI DSS compliance report

Use case 6: Automate easily forgotten maintenance tasks

Maintaining availability requires ongoing maintenance. Tasks like device configuration backup are important to ensure your security infrastructure is safe from failure and disruption. LiveAssurance 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 inbound SSL inspection, user authentication, device authentication for GlobalProtect VPN, IPSec site-to-site VPN, EDL validation, User-ID agent and TS agent access. Not having a valid certificate will likely impact services. LiveAssurance provides warnings in advance if certificates are about to expire, giving you ample time to take action. LiveAssurance also checks for valid licenses to ensure software license compliance whether it is 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 7: Automated troubleshooting

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

Let's look at a simple example: A firewall is unable to reach its EDL server. Before doing the actual troubleshooting, LiveAssurance gathers the information it needs to perform effective troubleshooting, just like a human would. In this example, effective troubleshooting means understanding if a proxy is in the picture, what the service route gateway is, etc.

To reach the EDL server, the first step is to make sure that the firewall can reach its EDL service route gateway. To do that, we issue a ping command from the firewall. You can see the output of the ping command being executed. In this case, the firewall can reach its service route gateway.

Knowing that the firewall can reach the outside world, the next step is to get the external IP address of the EDL server. To do that, we need to resolve the IP address of the EDL server. We factor if a proxy is applicable in the environment. In this example, it is not. We simply fetch the URL of the EDL server and resolve the IP address.

To ensure that we can resolve the IP address, we make sure that we can reach the DNS server by issuing a ping command. If we can reach the DNS server, we can safely conclude that the root cause of the problem is due to DNS resolution.

In this example, we are able to reach the DNS server but cannot resolve the IP address. Therefore, we can conclude that the root cause of the problem is due to DNS resolution.

It is not always possible for LiveAssurance to determine the root cause of a problem. The goal is to capture the problem the moment it occurs. Doing so provides a better chance of collecting information about events and conditions that led to the problem so you don't need to re-create the failure. This is particularly useful for intermittent problems. Re-creating a problem can be difficult; worse, it is often not feasible.

Use case 8: Digital transformation change requests

Change requests (CRs) are an unavoidable part of digital transformation initiatives for critical infrastructure in both staged and live production environments. While CRs are necessary, they also bring significant challenges and risks if not executed correctly. Recognizing the warning signs that patches or upgrades have not been successfully applied is a manual process, which can prolong the time needed to remediate errors.

Manifest, in BlueCat LiveAssurance, simplifies change management across diverse IT environments to ensure critical infrastructure is back to the normal state after applying updates. Network teams can schedule automated snapshots of device state and configuration before and after requested updates to confirm services are back up and running.

Key differentiators

There are four major differences between BlueCat LiveAssurance and other network monitoring and management solutions.

1. The automation elements in this solution 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. Crowdsourcing provides a mechanism to bring together ideas and expertise that would not otherwise be available.
2. When deploying LiveAssurance in a security environment, customers immediately receive notifications about misconfigurations, errors, security risks, vulnerabilities, and lack of adherence to best practices. Because LiveAssurance 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, LiveAssurance 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, LiveAssurance 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 BlueCat LiveAssurance as a solution for hidden issue detection and recommended remediation. They include:

- **Achieve zero 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.** LiveAssurance surfaces useful and actionable information that will immediately facilitate your IT operations team's work

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 demo

SB-LiveAssurance_01-12-2026