LiveAction
A BlueCat Company | SOLUTION BRIEF

LiveNX Assurance – Network Security for Palo Alto Networks Next-Generation Firewalls

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 LiveNX Assurance - Network Security 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

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

LiveNX Assurance - Network Security provides deep visibility into your security infrastructure to flag early warning signs of issues. With our domain expertise codified into LiveNX Assurance - Network Security, 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, BlueCat Information 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.

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

LiveNX Assurance - Network Security 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 your security infrastructure
- Reduce mean time to resolution
- Work more effectively

Seven Types of Use Cases

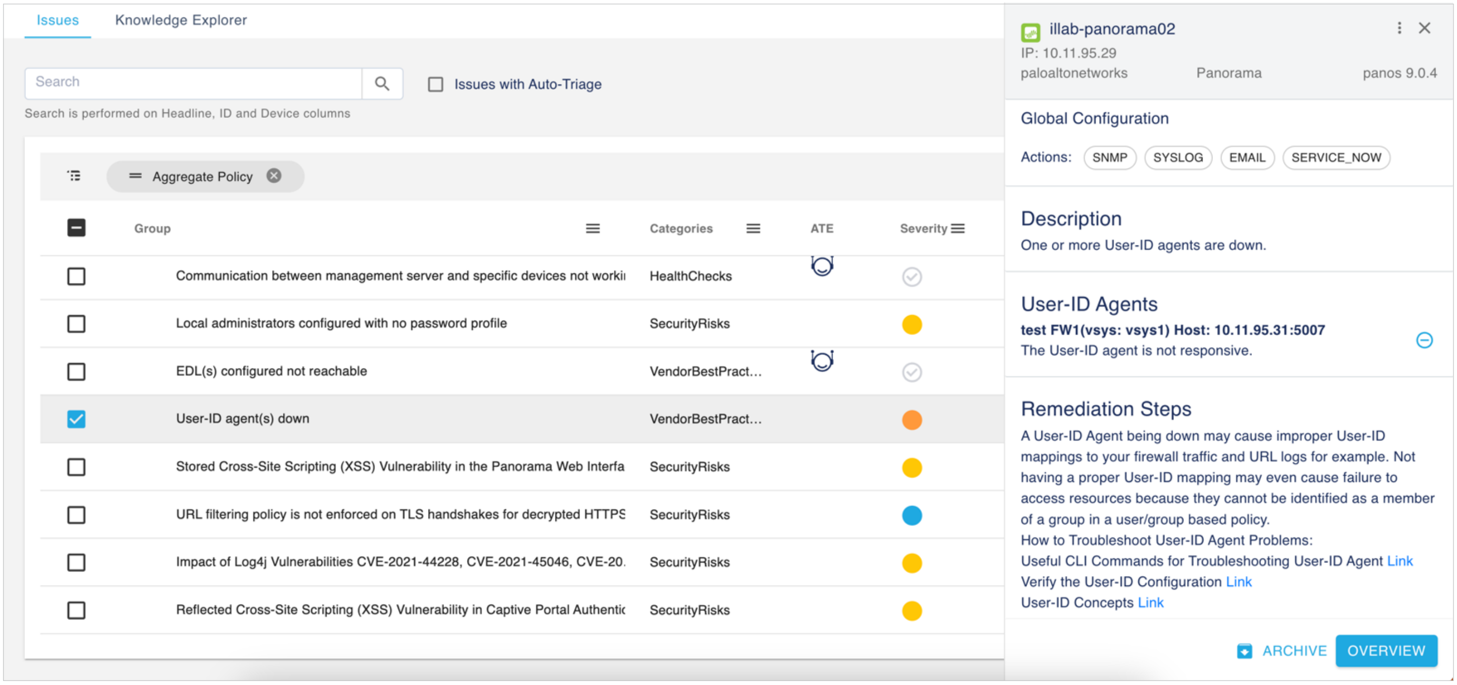
For Palo Alto Networks Next-Generation Firewalls customers, moving beyond the reactive mindset when things go awry is within reach. In this section, we outline seven scenarios that you might encounter, with specific real-world examples. Each explores how LiveNX Assurance - Network Security can help ensure that your security infrastructure is working as intended.

USE CASE 1 Stateful Health Checking

LiveNX Assurance - Network Security 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



Search is performed on Headline, ID and Device columns

☐	Group	Categories	ATE	Severity
☐	Communication between management server and specific devices not workii	HealthChecks	☺	✓
☐	Local administrators configured with no password profile	SecurityRisks		●
☐	EDL(s) configured not reachable	VendorBestPract...	☺	✓
☑	User-ID agent(s) down	VendorBestPract...		●
☐	Stored Cross-Site Scripting (XSS) Vulnerability in the Panorama Web Interfa	SecurityRisks		●
☐	URL filtering policy is not enforced on TLS handshakes for decrypted HTTPS	SecurityRisks		●
☐	Impact of Log4j Vulnerabilities CVE-2021-44228, CVE-2021-45046, CVE-20.	SecurityRisks		●
☐	Reflected Cross-Site Scripting (XSS) Vulnerability in Captive Portal Authentic	SecurityRisks		●

illab-panorama02
IP: 10.11.95.29
paloaltonetworks Panorama panos 9.0.4

Global Configuration

Description

One or more User-ID agents are down.

User-ID Agents

test FW1(vsys: vsys1) Host: 10.11.95.31:5007
The User-ID agent is not responsive.

Remediation Steps

A User-ID Agent being down may cause improper User-ID mappings to your firewall traffic and URL logs for example. Not having a proper User-ID mapping may even cause failure to access resources because they cannot be identified as a member of a group in a user/group based policy.
How to Troubleshoot User-ID Agent Problems:
Useful CLI Commands for Troubleshooting User-ID Agent Link
Verify the User-ID Configuration Link
User-ID Concepts Link

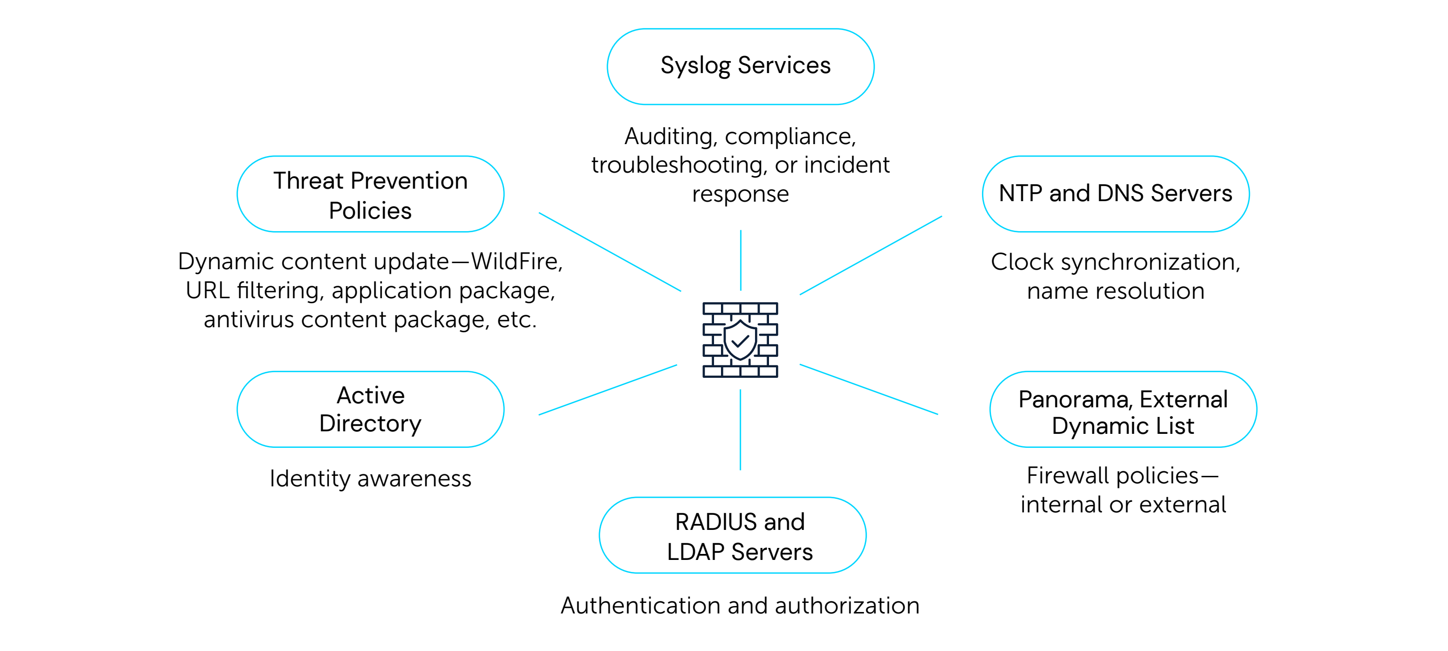
Once issues are detected, LiveNX Assurance - Network Security provides actionable information to help IT operations teams address it. This includes a description of the issue, remediation steps, and links to articles on Palo Alto Networks' support portal.

USE 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. LiveNX Assurance - Network Security's automation features ensure, through regular testing, that communication with these external services is always available.

Critical services that a firewall requires include:

- Clock synchronization with an NTP server
- Access to DNS for name resolution
- Forwarding syslog to an external server for auditing, compliance, troubleshooting, or incident response


Syslog Services
Auditing, compliance, troubleshooting, or incident response
Threat Prevention Policies
Dynamic content update—WildFire, URL filtering, application package, antivirus content package, etc.
NTP and DNS Servers
Clock synchronization, name resolution
Active Directory
Identity awareness
Panorama, External Dynamic List
Firewall policies—internal or external
RADIUS and LDAP Servers
Authentication and authorization

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 threat intelligence, firewalls frequently get updates from WildFire, URL filtering, and other tools. Timely updates are key to protecting your networks before threats become widespread. LiveNX Assurance - Network Security 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). LiveNX Assurance - Network Security 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 a major cause of unplanned downtime. Configuration errors can create security gaps in your network, making it vulnerable to cyberattacks. LiveNX Assurance - Network Security continuously detects misconfigurations by verifying against a gold standard for your network. It even notifies you if a scheduled commit from Panorama failed.

Misconfigurations and best practices that LiveNX Assurance - Network Security 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 Ensure High Availability

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. LiveNX Assurance - Network Security constantly detects high availability unreadiness from cross-device inconsistencies. This includes configuration state and ensuring adherence to best practices.

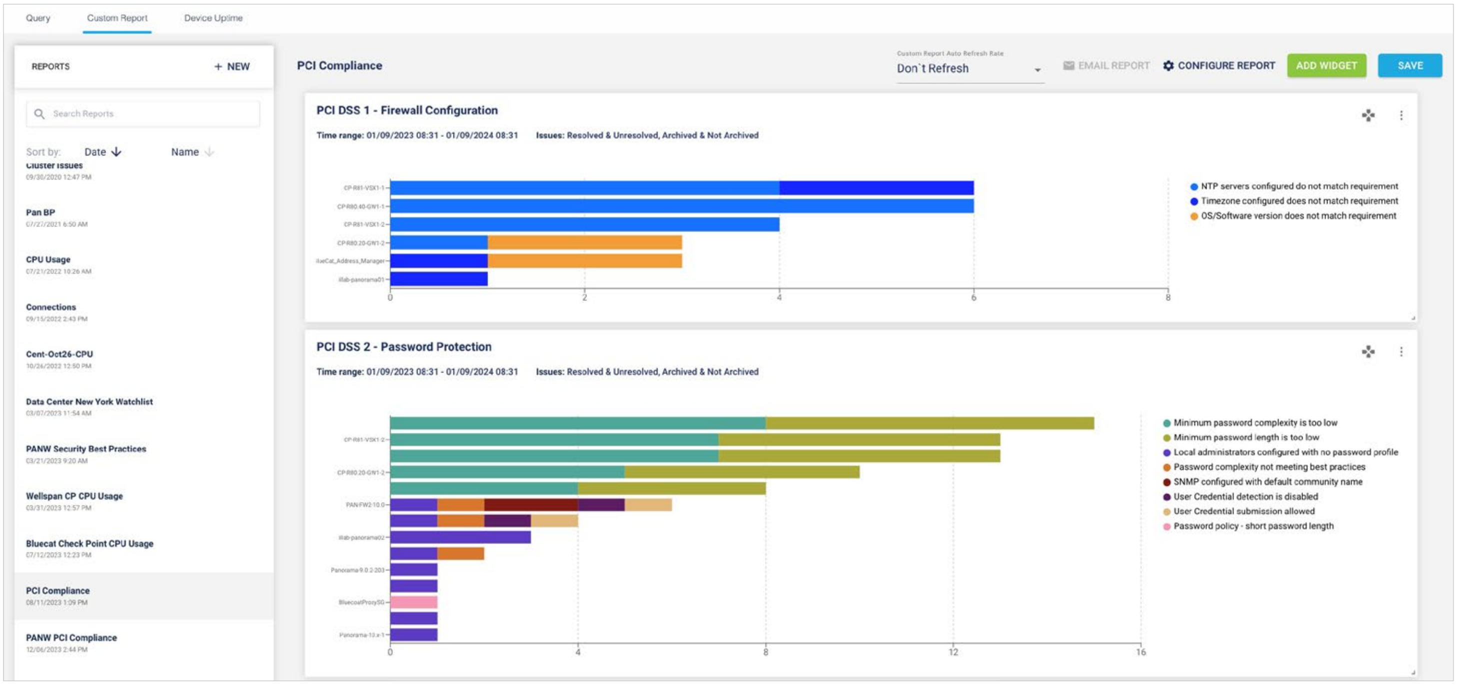
Examples of high availability readiness issues that LiveNX Assurance - Network Security might detect and provide alerts for include:

- 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 availabilty configurations not meeting best practices

USE CASE 5 Auto-Detect Security Risks and Ensure Compliance

Enterprises are hypervigilant about how they secure their infrastructure. Device hardening is necessary to reduce the attack surface. LiveNX Assurance - Network Security 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:


Query
Custom Report
Device Uptime
REPORTS
+ NEW
Search Reports
Sort by: Date ↓ Name ↓
Custom Report Auto Refresh Rate
Don`t Refresh
EMAIL REPORT
CONFIGURE REPORT
ADD WIDGET
SAVE
CP-R81-VSX1-1
CP-R80.40-GW1-1
CP-R81-VSX1-2
CP-R80.20-GW1-2
lueCat_Address_Manager
illab-panorama01
0
2
4
6
8
NTP servers configured do not match requirement
Timezone configured does not match requirement
OS/Software version does not match requirement
CP-R81-VSX1-2
CP-R80.20-GW1-2
PAN-FW2-10.0
illab-panorama02
Panorama-9.0.2-203
BluecoatProxySG
Panorama-10.x-1
0
4
8
12
16
Minimum password complexity is too low
Minimum password length is too low
Local administrators configured with no password profile
Password complexity not meeting best practices
SNMP configured with default community name
User Credential detection is disabled
User Credential submission allowed
Password policy - short password length

Cluster Issues
09/30/2020 12:47 PM

Pan BP
07/27/2021 6:50 AM

CPU Usage
07/21/2022 10:26 AM

Connections
09/15/2022 2:43 PM

Cent-Oct26-CPU
10/26/2022 12:50 PM

Data Center New York Watchlist
03/07/2023 11:54 AM

PANW Security Best Practices
03/21/2023 9:20 AM

Wellspan CP CPU Usage
03/31/2023 12:57 PM

Bluecat Check Point CPU Usage
07/12/2023 12:23 PM

PCI Compliance
08/11/2023 1:09 PM

PANW PCI Compliance
12/06/2023 2:44 PM

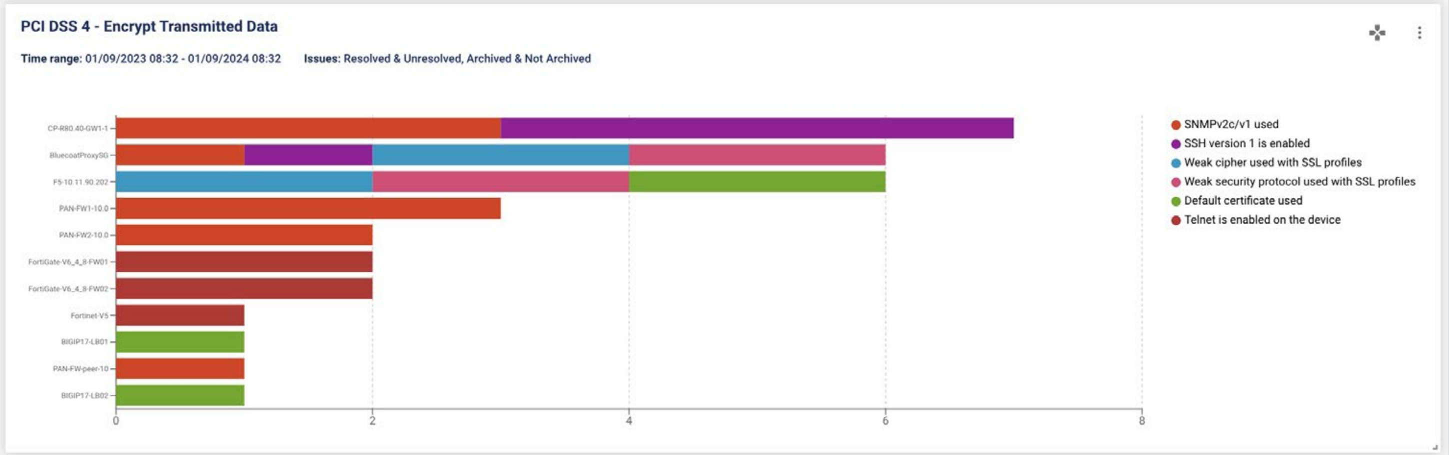
PCI Compliance

PCI DSS 1 - Firewall Configuration

Time range: 01/09/2023 08:31 - 01/09/2024 08:31 Issues: Resolved & Unresolved, Archived & Not Archived

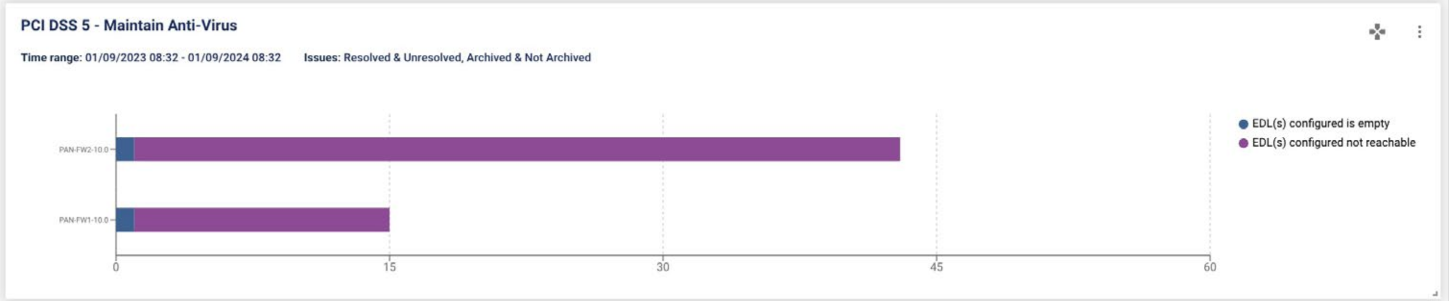
PCI DSS 2 - Password Protection

Time range: 01/09/2023 08:31 - 01/09/2024 08:31 Issues: Resolved & Unresolved, Archived & Not Archived



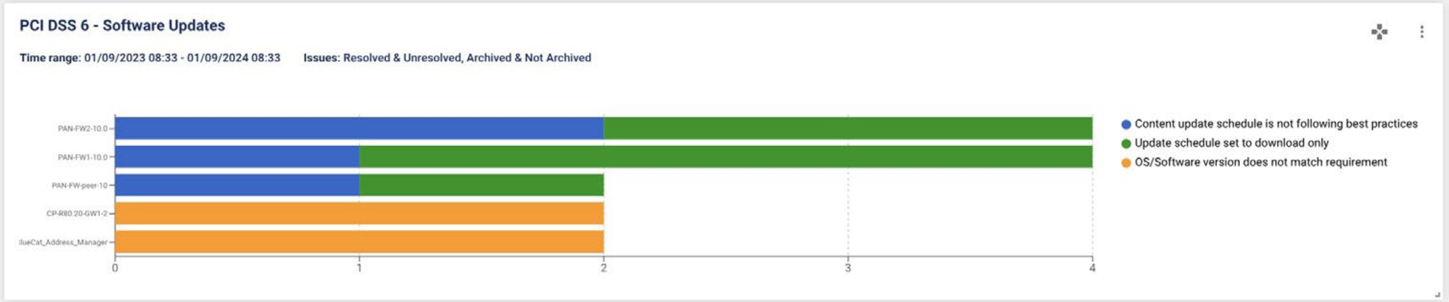
PCI DSS 4 - Encrypt Transmitted Data

Time range: 01/09/2023 08:32 - 01/09/2024 08:32 **Issues:** Resolved & Unresolved, Archived & Not Archived



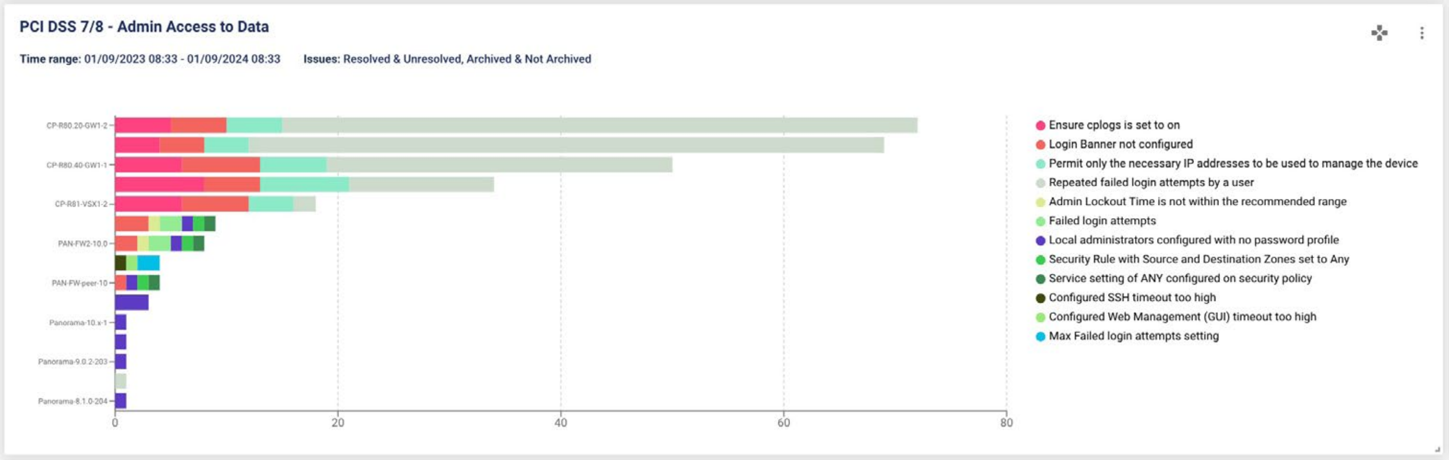
PCI DSS 5 - Maintain Anti-Virus

Time range: 01/09/2023 08:32 - 01/09/2024 08:32 **Issues:** Resolved & Unresolved, Archived & Not Archived



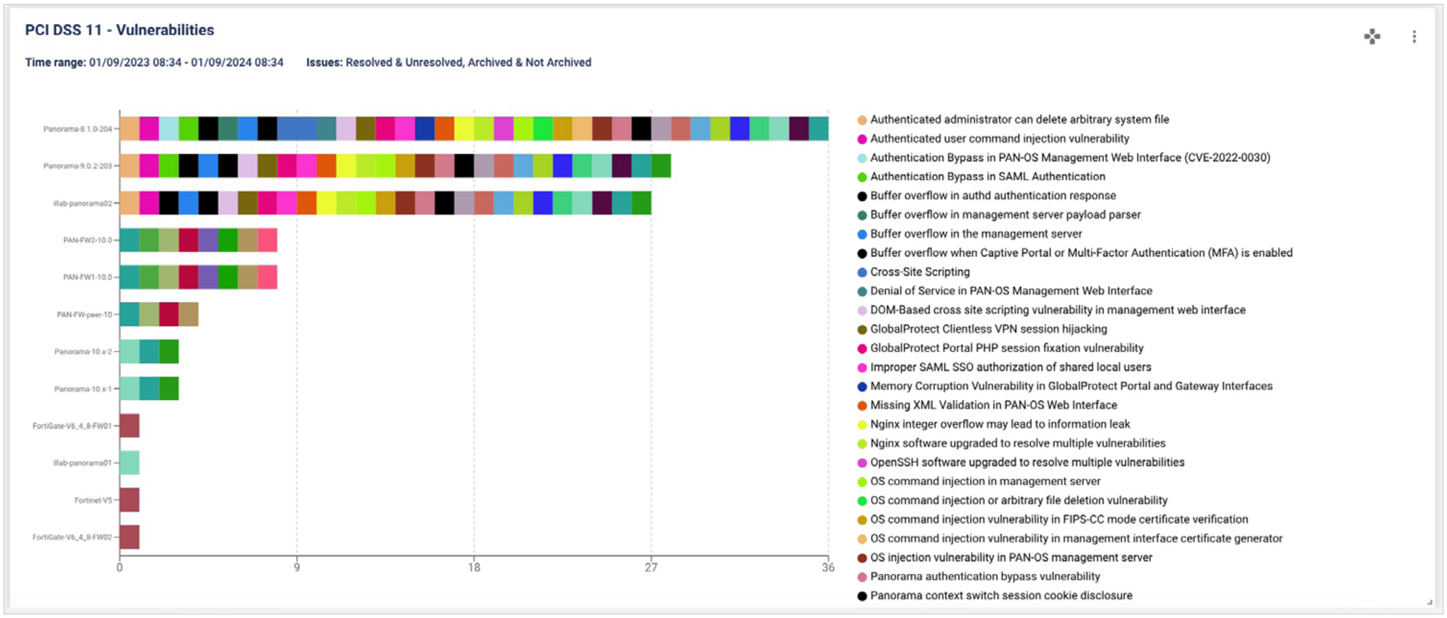
PCI DSS 6 - Software Updates

Time range: 01/09/2023 08:33 - 01/09/2024 08:33 **Issues:** Resolved & Unresolved, Archived & Not Archived



PCI DSS 7/8 - Admin Access to Data

Time range: 01/09/2023 08:33 - 01/09/2024 08:33 **Issues:** Resolved & Unresolved, Archived & Not Archived



PCI DSS 11 - Vulnerabilities

Time range: 01/09/2023 08:34 - 01/09/2024 08:34 **Issues:** Resolved & Unresolved, Archived & Not Archived

Panorama-8.1.0-204
Panorama-9.0.2-203
illab-panorama02
PAN-FW2-10.0
PAN-FW1-10.0
PAN-FW-peer-10
Panorama-10.x-2
Panorama-10.x-1
FortiGate-V6_4_8-FW01
illab-panorama01
Fortinet-V5
FortiGate-V6_4_8-FW02
0
9
18
27
36
Authenticated administrator can delete arbitrary system file
Authenticated user command injection vulnerability
Authentication Bypass in PAN-OS Management Web Interface (CVE-2022-0030)
Authentication Bypass in SAML Authentication
Buffer overflow in authd authentication response
Buffer overflow in management server payload parser
Buffer overflow in the management server
Buffer overflow when Captive Portal or Multi-Factor Authentication (MFA) is enabled
Cross-Site Scripting
Denial of Service in PAN-OS Management Web Interface
DOM-Based cross site scripting vulnerability in management web interface
GlobalProtect Clientless VPN session hijacking
GlobalProtect Portal PHP session fixation vulnerability
Improper SAML SSO authorization of shared local users
Memory Corruption Vulnerability in GlobalProtect Portal and Gateway Interfaces
Missing XML Validation in PAN-OS Web Interface
Nginx integer overflow may lead to information leak
Nginx software upgraded to resolve multiple vulnerabilities
OpenSSH software upgraded to resolve multiple vulnerabilities
OS command injection in management server
OS command injection or arbitrary file deletion vulnerability
OS command injection vulnerability in FIPS-CC mode certificate verification
OS command injection vulnerability in management interface certificate generator
OS injection vulnerability in PAN-OS management server
Panorama authentication bypass vulnerability
Panorama context switch session cookie disclosure

USE CASE 6 Proactive Maintenance Notifications

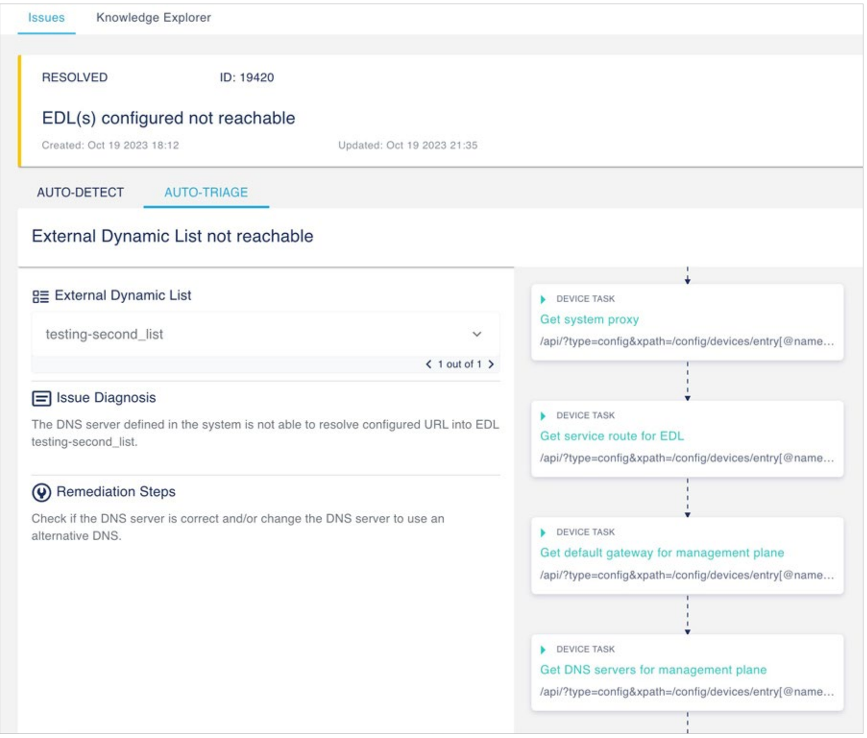
Maintaining availability requires ongoing maintenance. Tasks like device configuration backup are important to ensure your security infrastructure is safe from failure and disruption. LiveNX Assurance - Network Security automates device configuration backup and proactively notifies you if the backup 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, and User-ID agent and Terminal Services agent access. Not having a valid certificate will likely impact services. LiveNX Assurance - Network Security provides warnings in advance if certificates are about to expire, giving you ample time to act.

USE CASE 7 Automated Troubleshooting

When an issue is detected, LiveNX Assurance - Network Security 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, LiveNX Assurance - Network Security 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.



Issues | Knowledge Explorer

RESOLVED ID: 19420

EDL(s) configured not reachable

Created: Oct 19 2023 18:12 Updated: Oct 19 2023 21:35

AUTO-DETECT | AUTO-TRIAGE

External Dynamic List not reachable

External Dynamic List

testing-second_list

1 out of 1

Issue Diagnosis

The DNS server defined in the system is not able to resolve configured URL into EDL testing-second_list.

Remediation Steps

Check if the DNS server is correct and/or change the DNS server to use an alternative DNS.

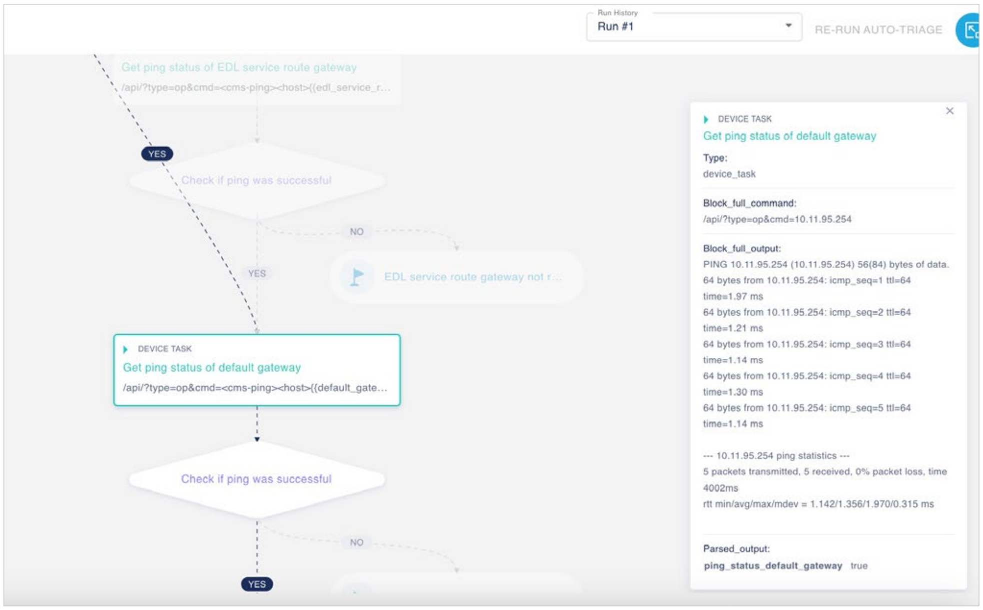
DEVICE TASK
Get system proxy
/api/?type=config&xpath=/config/devices/entry[@name…

DEVICE TASK
Get service route for EDL
/api/?type=config&xpath=/config/devices/entry[@name…

DEVICE TASK
Get default gateway for management plane
/api/?type=config&xpath=/config/devices/entry[@name…

DEVICE TASK
Get DNS servers for management plane
/api/?type=config&xpath=/config/devices/entry[@name…

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.



Get ping status of EDL service route gateway
/api/?type=op&cmd=<cms-ping><host>{{edl_service_r...

Check if ping was successful

EDL service route gateway not r...

DEVICE TASK
Get ping status of default gateway
/api/?type=op&cmd=<cms-ping><host>{{default_gate...

Check if ping was successful

DEVICE TASK
Get ping status of default gateway

Type:
device_task

Block_full_command:
/api/?type=op&cmd=10.11.95.254

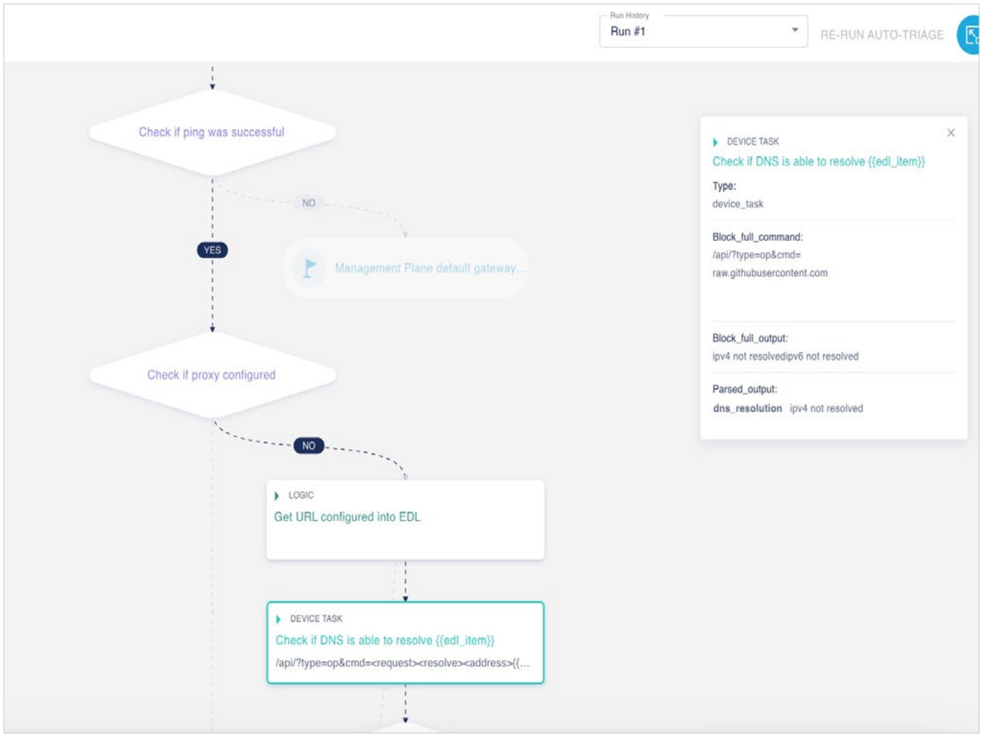
Block_full_output:

```
PING 10.11.95.254 (10.11.95.254) 56(84) bytes of data.
64 bytes from 10.11.95.254: icmp_seq=1 ttl=64
time=1.97 ms
64 bytes from 10.11.95.254: icmp_seq=2 ttl=64
time=1.21 ms
64 bytes from 10.11.95.254: icmp_seq=3 ttl=64
time=1.14 ms
64 bytes from 10.11.95.254: icmp_seq=4 ttl=64
time=1.30 ms
64 bytes from 10.11.95.254: icmp_seq=5 ttl=64
time=1.14 ms

--- 10.11.95.254 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time
4002ms
rtt min/avg/max/mdev = 1.142/1.356/1.970/0.315 ms
```

Parsed_output:
ping_status_default_gateway true

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.


Run History
Run #1
RE-RUN AUTO-TRIAGE
Check if ping was successful
NO
YES
Management Plane default gateway...
Check if proxy configured
NO
LOGIC
Get URL configured into EDL
DEVICE TASK
Check if DNS is able to resolve {{edl_item}}
/api/?type=op&cmd=<request><resolve><address>{{...

DEVICE TASK

Check if DNS is able to resolve {{edl_item}}

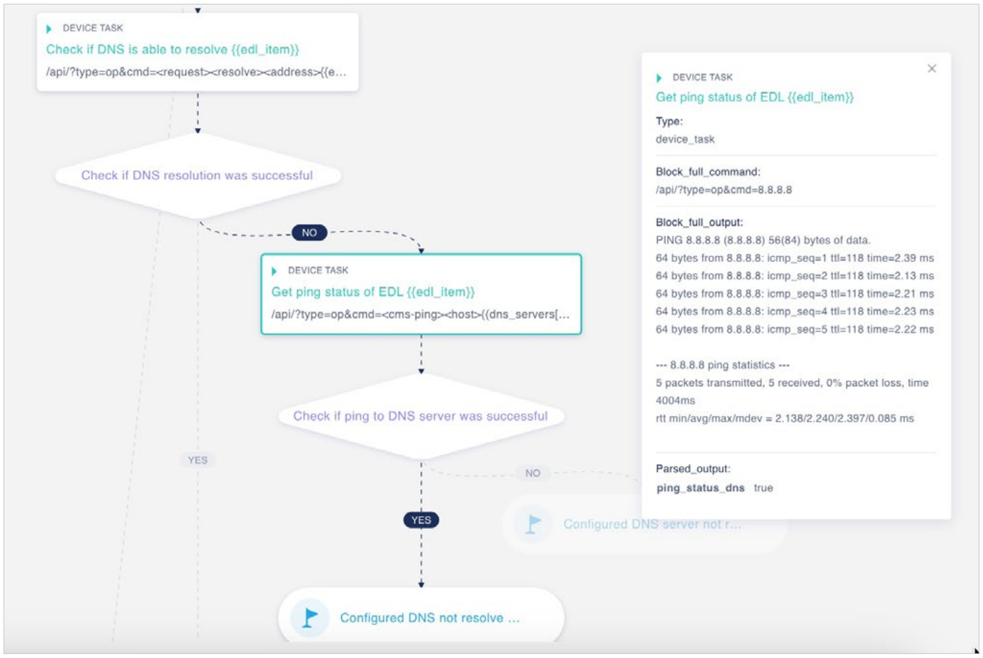
Type:
device_task

Block_full_command:
/api/?type=op&cmd=
raw.githubusercontent.com

Block_full_output:
ipv4 not resolvedipv6 not resolved

Parsed_output:
dns_resolution ipv4 not resolved

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.


DEVICE TASK
Check if DNS is able to resolve {{edl_item}}
/api/?type=op&cmd=<request><resolve><address>{{e...
Check if DNS resolution was successful
NO
DEVICE TASK
Get ping status of EDL {{edl_item}}
/api/?type=op&cmd=<cms-ping><host>{{dns_servers[...
Check if ping to DNS server was successful
YES
NO
YES
Configured DNS server not r...
Configured DNS not resolve ...

DEVICE TASK

Get ping status of EDL {{edl_item}}

Type:
device_task

Block_full_command:
/api/?type=op&cmd=8.8.8.8

Block_full_output:

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=2.39 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=2.13 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=2.21 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=2.23 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=118 time=2.22 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time
4004ms
rtt min/avg/max/mdev = 2.138/2.240/2.397/0.085 ms
```

Parsed_output:
ping_status_dns true

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 LiveNX Assurance - Network Security 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.

Key Differentiators

There are four major differences between LiveNX Assurance - Network Security 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. Crowdsourcing 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 LiveNX Assurance - Network Security 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.** LiveNX Assurance - Network Security surfaces useful and actionable information that will immediately facilitate your IT operations team's work.

LiveAction
A BlueCat Company

LiveAction, a BlueCat Networks company, provides end-to-end visibility of network and application performance from a single pane of glass. We provide enterprises with confidence that the network is meeting business objectives, full network visibility for better decisions, and reduced cost to operate the network.

www.liveaction.com | 901 Campisi Way, Suite 222 Campbell, CA 95008 | USA +1 (888) 881-1116