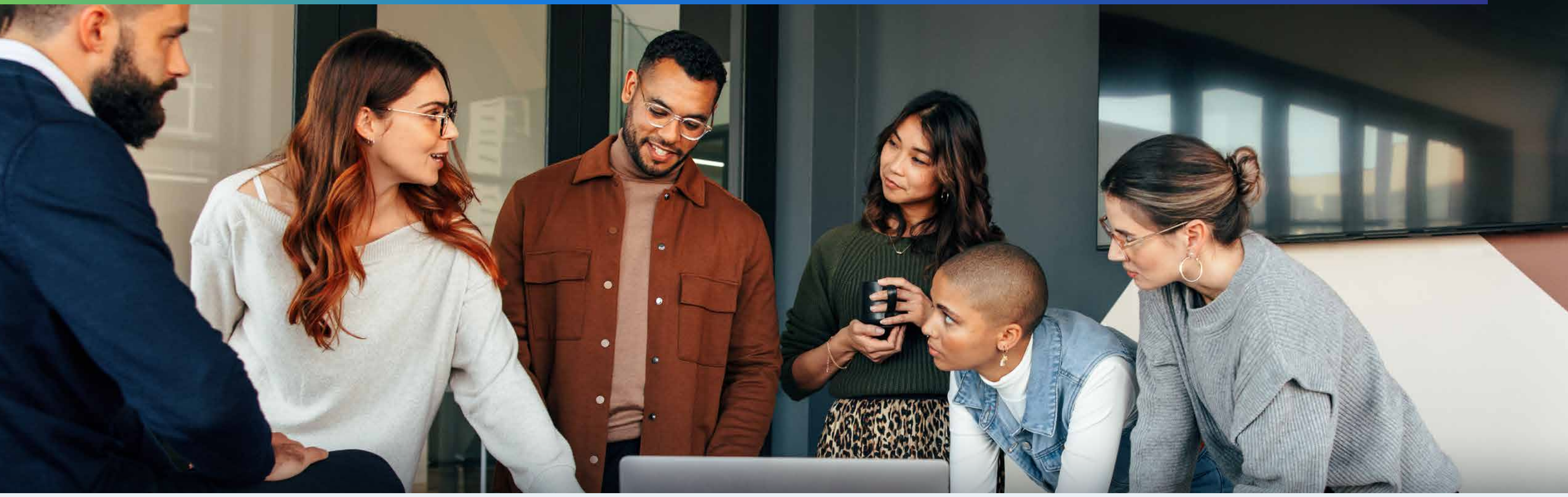
SOLUTION BRIEF

Top 10 Automated Network Assessments



While network automation has become a game-changer for those who have adopted it for ongoing network operations, a bigger challenge has been how to prevent outages in the first place. As it turns out, no-code network automation is the key to making that a reality.

By continuously assessing the network services and all of their underlying components you deliver, you can spot problems long before they manifest into production impacts. Using NetBrain's intent-based network automation and its continuous network assessment capability, you can verify every aspect of the network continuously to identify potential issues. These include identification of network changes and drift, the status or health check of each networking components, the operational status of all security boundaries and control policies, the performance of network service to support key applications, performance of cloud services and overall capacity, and even the verification that previously seen problems are not being seen elsewhere in the network.

Network Assessments: Automated for Complete and Continuous Assurance

NetBrain Next-Gen, the no-code network automation platform, now provides comprehensive ready-to-use network assessment templates which can be customized on demand. It uses the power of no-code automated Intents to summarize and make sense of the network's expected results and behaviors. These automated Intents unlock the ability for anyone to leverage network automation to not only diagnose and troubleshoot and make safe network changes, but also continuously assess the network against internal and external standards to prevent outages and service degradations due to unidentified network problems, risk, and bottlenecks.

Top 10 Continuous Network Assessments and Dashboards

Is it possible to gain deep insight into the operational health and service delivery capabilities of your hybrid cloud-connected network? Yes. With NetBrain NextGen and its Continuous Assessment technology, you can quickly craft any number of operational assessments along with rich drill-down dashboards for any operating condition you can imagine- without writing a single line of code. And to get you started, NetBrain includes its robust assessment library with hundreds of the most common assessments that network professionals need to maintain production. Continuous Network Assessments addresses critical infrastructure and service delivery challenges with confidence.

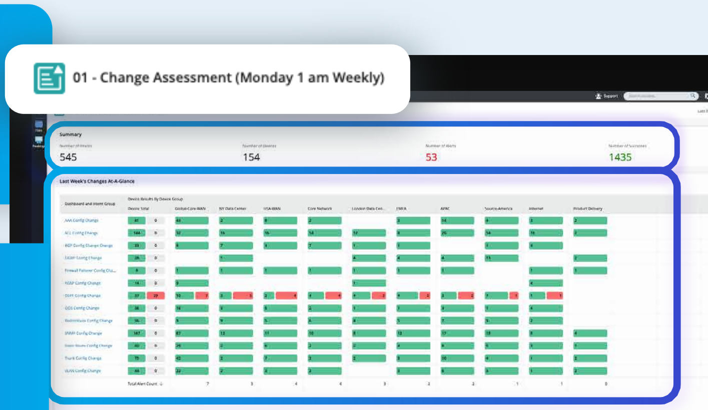
The Next-Gen platform provides the ability to create and modify assessment summary dashboards on the fly without code for any possible use case. Use the Summary Dashboard feature to easily monitor critical information across thousands of devices and discover the root cause for issues in one view.

1. Change Assessment

As Monday morning arrives, reports of a few network outages spark concern. The immediate question arises: What has changed over the weekend, and where have these changes occurred? This brings up the need to more quickly identify network changes that transpired over the weekend. The urgency stems from the need to determine if these reported outages share a common origin or if they are disparate incidents. This becomes pivotal in swiftly addressing and resolving the issues at hand, ensuring the network's stability, and minimizing disruptions.

After weekend network changes, Monday morning brings outages. Now, you're left pondering the changes' details, their locations, and their potential ties to network issues, amidst the complexity of thousands of devices and contributions from multiple teams.

How can you gain awareness and determine the starting point for investigation?



01 - Change Assessment (Monday 1 am Weekly)

Summary

Number of Intents	Number of Devices	Number of Alerts	Number of Successes
545	154	53	1435

Last Week's Changes At-A-Glance

Dashboard and Intent Group	Device Results By Device Group										
	Device Total		Global-Core-WAN	NY Data Center	USA-WAN	Core Network	London Data Cen...	EMEA	APAC	Source-America	Internet	Product Delivery
AAA Config Change	41	0	43	2	8	2		3	14	4	3	2
ACL Config Change	144	0	32	16	16	18	12	8	26	14	16	2
BGP Config Change Change	33	0	8	7	9	7	1	1		1	4	
EIGRP Config Change	26	0		1			4	4	4	13		2
Firewall Failover Config Cha...	8	0	1	1	1	1	1	1	1		1	1
HSRP Config Change	14	0	9				1				4	
OSPF Config Change	37	22	10 7	3 5	2 4	4 4	4 2	4 2	3 2	7 1	1 1	
QOS Config Change	38	0	16	3	5	2	1	1	3	1	4	
Redistribute Config Change	56	0	9	9	5	6	4	5	7	9	2	
SNMP Config Change	167	0	87	12	11	10	8	13	17	19	8	4
Static Route Config Change	40	0	29	2	6	2	2	4	8	6	3	1
Trunk Config Change	75	0	42	2	7	2	2	3	30	4	1	2
VLAN Config Change	44	0	22	2	3	2		3	5	3	1	2
	Total Alert Count ↓		7	3	4	4	3	2	2	1	1	0

Use No-Code Automation to continuously evaluate and summarize a Change dashboard for:

- **Device results by device group**
- **ACL configuration changes**
- **Routing configuration changes**
- **Switching configuration changes**
- **Failover configuration changes**

2. Anti-Drift Assessment

Human error, often stemming from manual network changes, has emerged as a leading cause of network outages. To address this challenge, network anti-drift assessment plays a crucial role in identifying and rectifying deviations from established configuration rules and best practices. By automating the enforcement of these rules, organizations can significantly reduce the prevalence of human error and safeguard network stability.

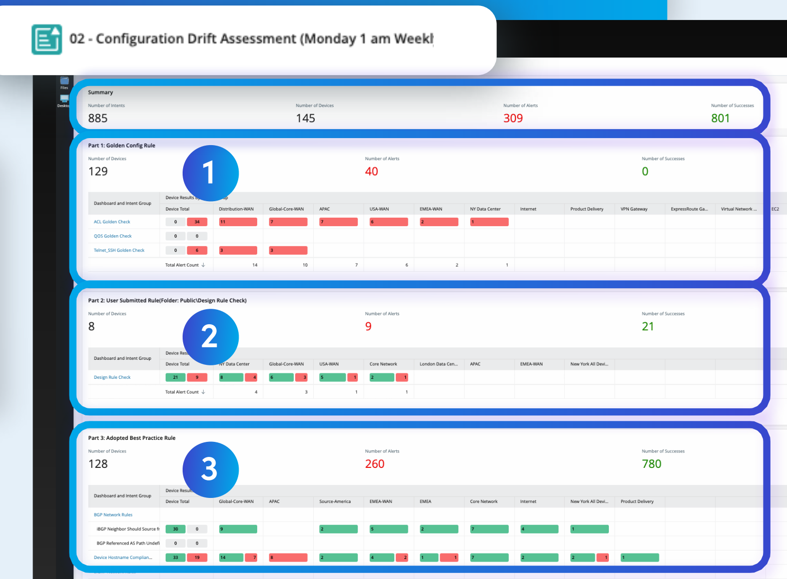
Anti-drift assessment encompasses three primary categories of rules:

1. **Design and Best Practice Rules:** These rules outline industry-wide best practices for network configurations, ensuring that the network aligns with recognized standards and guidelines.
2. **Golden Config Rules:** These rules represent the organization's specific configuration standards, mandating adherence to internal policies and procedures.
3. **User-Submitted Design Rules:** These rules capture network architects' and engineers' expertise, encapsulating design principles and guidelines tailored to the organization's unique network topology and requirements.

Too many outages were caused by human errors...

How can we identify all the places where the config has drifted in the entire network?

Use No-Code Automation to continuously enforce three types of rules via automation can cut down human errors drastically.



02 - Configuration Drift Assessment (Monday 1 am Weekl

Summary

Number of Intents	Number of Devices	Number of Alerts	Number of Successes
885	145	309	801

Part 1: Golden Config Rule

Number of Devices	Number of Alerts	Number of Successes
129	40	0

Dashboard and Intent Group	Device Results													
	Device Total		Distribution-WAN	Global-Core-WAN	APAC	USA-WAN	EMEA-WAN	NY Data Center	Internet	Product Delivery	VPN Gateway	ExpressRoute Ga...	Virtual Network ...	EC2
ACL Golden Check	0	34	11	7	7	6	2	1						
QOS Golden Check	0	0												
Telnet_SSH Golden Check	0	6	3	3										
	Total Alert Count ↓		14	10	7	6	2	1						

Part 2: User Submitted Rule(Folder: Public\Design Rule Check)

Number of Devices	Number of Alerts	Number of Successes
8	9	21

Dashboard and Intent Group	Device Res								
	Device Total		NY Data Center	Global-Core-WAN	USA-WAN	Core Network	London Data Cen...	APAC	EMEA-WAN	New York All Devi...
Design Rule Check	21	9	8 4	6 3	5 1	2 1				
	Total Alert Count ↓		4	3	1	1				

Part 3: Adopted Best Practice Rule

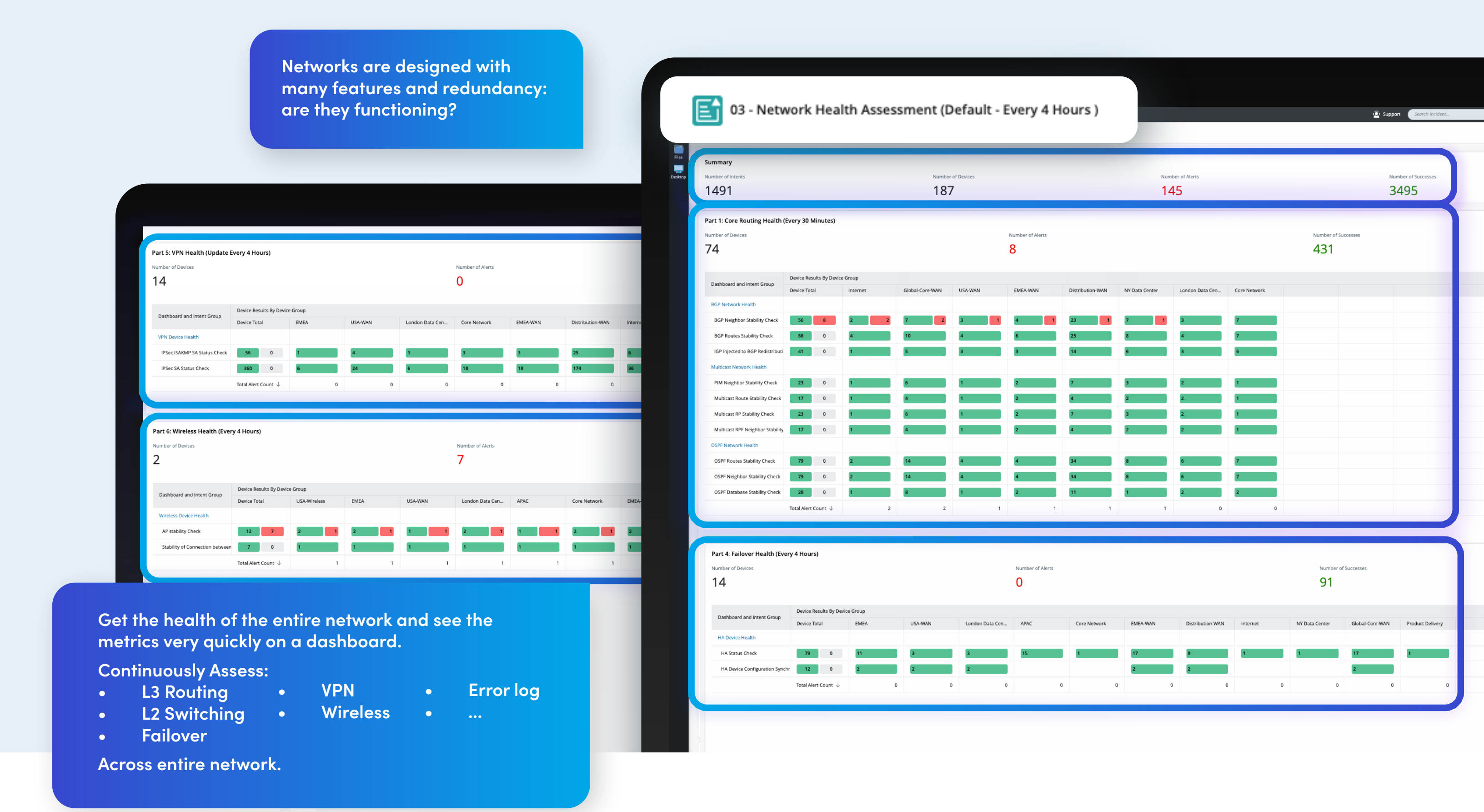
Number of Devices	Number of Alerts	Number of Successes
128	260	780

Dashboard and Intent Group	Device Resul										
	Device Total		Global-Core-WAN	APAC	Source-America	EMEA-WAN	EMEA	Core Network	Internet	New York All Devi...	Product Delivery
BGP Network Rules											
iBGP Neighbor Should Source fr	30	0	9		2	5	2	7	4	1	
BGP Referenced AS Path Undefi	0	0									
Device Hostname Complian...	33	19	14 7	8	2	4 2	1 1	7	2	2 1	1

By automating the enforcement of these rules, organizations can effectively prevent configuration drift and minimize the risk of human error. This proactive approach not only enhances network stability but also improves overall network performance and security.

3. Network Health Assessment

Sophisticated network redundancy provides reliable and high-performance connectivity. However, these features, if not properly monitored and maintained, can become sources of potential issues. Continuous network health assessment plays a critical role in identifying and addressing potential problems before they escalate into major outages.



Networks are designed with many features and redundancy: are they functioning?

03 - Network Health Assessment (Default - Every 4 Hours)

Summary

Number of Intents	Number of Devices	Number of Alerts	Number of Successes
1491	187	145	3495

Part 1: Core Routing Health (Every 30 Minutes)

Number of Devices	Number of Alerts	Number of Successes
74	8	431

Dashboard and Intent Group	Device Results By Device Group								
	Device Total	Internet	Global-Core-WAN	USA-WAN	EMEA-WAN	Distribution-WAN	NY Data Center	London Data Cen...	Core Network
BGP Network Health									
BGP Neighbor Stability Check	56 / 8	2 / 2	7 / 2	3 / 1	4 / 1	23 / 1	7 / 1	3	7
BGP Routes Stability Check	68 / 0	4	10	4	6	25	8	4	7
IGP Injected to BGP Redistributi	41 / 0	1	5	3	3	14	6	3	6
Multicast Network Health									
PIM Neighbor Stability Check	23 / 0	1	6	1	2	7	3	2	1
Multicast Route Stability Check	17 / 0	1	4	1	2	4	2	2	1
Multicast RP Stability Check	23 / 0	1	6	1	2	7	3	2	1
Multicast RPF Neighbor Stability	17 / 0	1	4	1	2	4	2	2	1
OSPF Network Health									
OSPF Routes Stability Check	79 / 0	2	14	4	4	34	8	6	7
OSPF Neighbor Stability Check	79 / 0	2	14	4	4	34	8	6	7
OSPF Database Stability Check	28 / 0	1	8	1	2	11	1	2	2
	Total Alert Count ↓	2	2	1	1	1	1	0	0

Part 4: Failover Health (Every 4 Hours)

Number of Devices	Number of Alerts	Number of Successes
14	0	91

Dashboard and Intent Group	Device Results By Device Group											
	Device Total	EMEA	USA-WAN	London Data Cen...	APAC	Core Network	EMEA-WAN	Distribution-WAN	Internet	NY Data Center	Global-Core-WAN	Product Delivery
HA Device Health												
HA Status Check	79 / 0	11	3	3	15	1	17	9	1	1	17	1
HA Device Configuration Synchr	12 / 0	2	2	2			2	2			2	
	Total Alert Count ↓	0	0	0	0	0	0	0	0	0	0	0

Part 5: VPN Health (Update Every 4 Hours)

Number of Devices	Number of Alerts
14	0

Dashboard and Intent Group	Device Results By Device Group							
	Device Total	EMEA	USA-WAN	London Data Cen...	Core Network	EMEA-WAN	Distribution-WAN	Interne
VPN Device Health								
IPSec ISAKMP SA Status Check	56 / 0	1	4	1	3	3	25	6
IPSec SA Status Check	360 / 0	6	24	6	18	18	174	36
	Total Alert Count ↓	0	0	0	0	0	0	

Part 6: Wireless Health (Every 4 Hours)

Number of Devices	Number of Alerts
2	7

Dashboard and Intent Group	Device Results By Device Group							
	Device Total	USA-Wireless	EMEA	USA-WAN	London Data Cen...	APAC	Core Network	EMEA-
Wireless Device Health								
AP stability Check	12 / 7	2 / 1	2 / 1	1 / 1	2 / 1	1 / 1	2 / 1	2
Stability of Connection between	7 / 0	1	1	1	1	1	1	1
	Total Alert Count ↓	1	1	1	1	1	1	

Get the health of the entire network and see the metrics very quickly on a dashboard.

Continuously Assess:

- L3 Routing
- L2 Switching
- Failover
- VPN
- Wireless
- Error log
- ...

Across entire network.

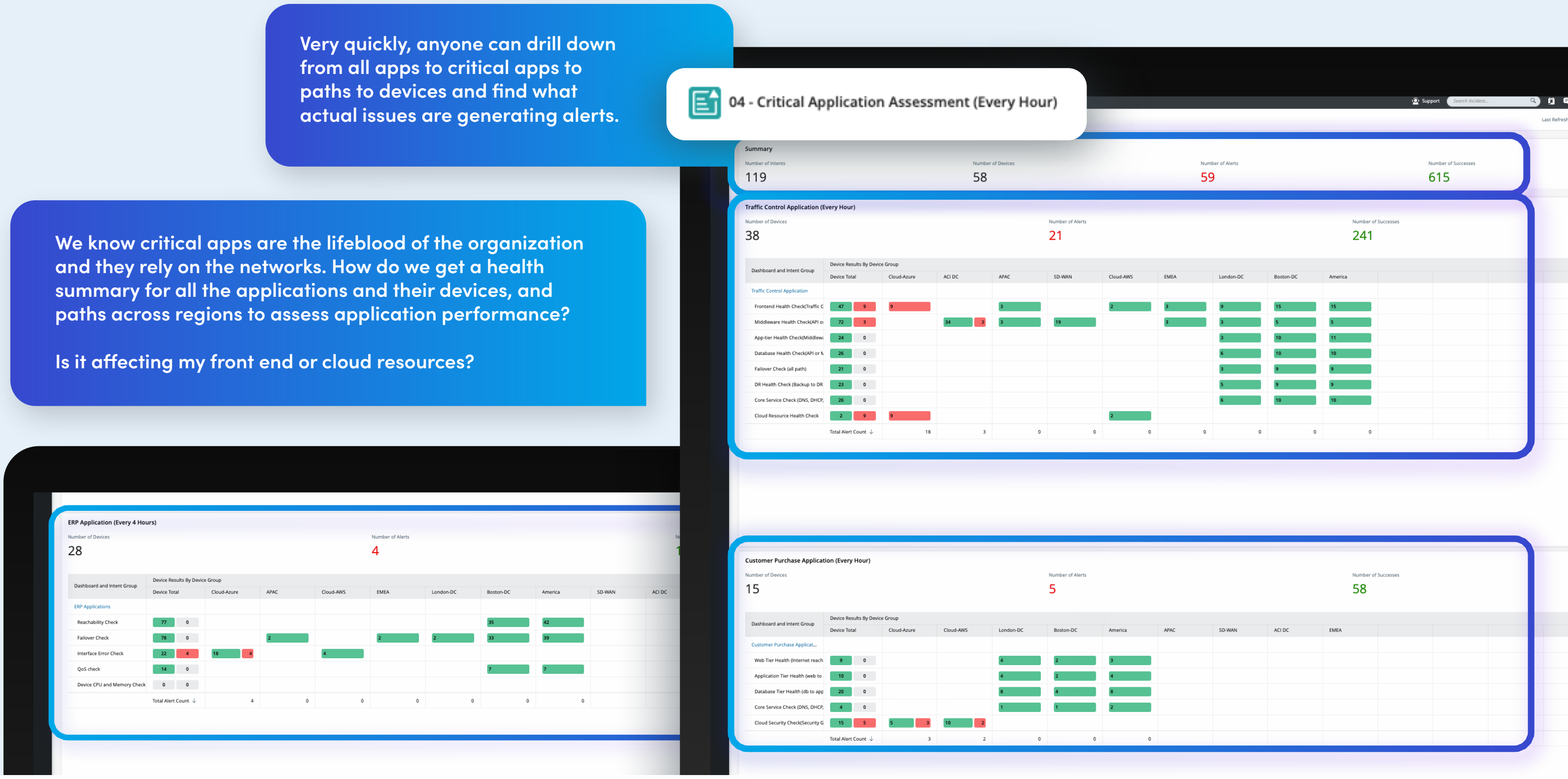
Network health assessment encompasses a comprehensive evaluation of:

- Core Routing Health: Analyze BGP, OSPF, and multicast stability.
- Edge Routing Health: Analyze EIGRP and OSPF stability.
- L3 Routing: Assess the health and performance of routing protocols, ensuring optimal path selection and traffic flow.
- L2 Switching: Monitor the health and performance of switching infrastructure, including switch utilization, error rates, and spanning tree operations.
- Failover: Verify the functionality and readiness of failover mechanisms, ensuring seamless network transitions in the event of primary device failures.
- VPN: Evaluate the security and performance of VPN connections, ensuring secure and reliable remote access.
- Wireless: Monitor the performance and security of wireless networks, including signal strength, coverage, and access control mechanisms.
- Error Log: Analyze network error logs to identify potential issues and proactively address them before they impact network operations.

By continuously assessing these critical network components, organizations can proactively identify and resolve potential problems, ensuring optimal network performance, availability, and security.

4. Critical Application Assessment

By continuously monitoring and evaluating the health of mission-critical applications, organizations can identify and address potential issues before they impact users or disrupt business processes. This proactive approach helps prevent costly outages, optimize application performance, and enhance overall system reliability.



Very quickly, anyone can drill down from all apps to critical apps to paths to devices and find what actual issues are generating alerts.

04 - Critical Application Assessment (Every Hour)

Summary

Number of Intents: 119
Number of Devices: 58
Number of Alerts: 59
Number of Successes: 615

Traffic Control Application (Every Hour)

Number of Devices: 38
Number of Alerts: 21
Number of Successes: 241

Dashboard and Intent Group	Device Results By Device Group									
	Device Total	Cloud-Azure	ACI DC	APAC	SD-WAN	Cloud-AWS	EMEA	London-DC	Boston-DC	America
Traffic Control Application										
Frontend Health Check(Traffic C	47 9	9		3		2	3	9	15	15
Middleware Health Check(API o	72 3		34 3	3	19		3	3	5	5
App-tier Health Check(Middlew	24 0							3	10	11
Database Health Check(API or N	26 0							6	10	10
Failover Check (all path)	21 0							3	9	9
DR Health Check (Backup to DR	23 0							5	9	9
Core Service Check (DNS, DHCP,	26 0							6	10	10
Cloud Resource Health Check	2 9	9				2				
	Total Alert Count ↓	18	3	0	0	0	0	0	0	0

We know critical apps are the lifeblood of the organization and they rely on the networks. How do we get a health summary for all the applications and their devices, and paths across regions to assess application performance?

Is it affecting my front end or cloud resources?

ERP Application (Every 4 Hours)

Number of Devices: 28
Number of Alerts: 4

Dashboard and Intent Group	Device Results By Device Group									
	Device Total	Cloud-Azure	APAC	Cloud-AWS	EMEA	London-DC	Boston-DC	America	SD-WAN	ACI DC
ERP Applications										
Reachability Check	77 0						35	42		
Failover Check	78 0		2		2	2	33	39		
Interface Error Check	22 4	18 4		4						
QoS check	14 0						7	7		
Device CPU and Memory Check	0 0									
	Total Alert Count ↓	4	0	0	0	0	0	0		

Customer Purchase Application (Every Hour)

Number of Devices: 15
Number of Alerts: 5
Number of Successes: 58

Dashboard and Intent Group	Device Results By Device Group									
	Device Total	Cloud-Azure	Cloud-AWS	London-DC	Boston-DC	America	APAC	SD-WAN	ACI DC	EMEA
Customer Purchase Applicat...										
Web Tier Health (Internet reach	9 0			4	2	3				
Application Tier Health (web to	10 0			4	2	4				
Database Tier Health (db to app	20 0			8	4	8				
Core Service Check (DNS, DHCP,	4 0			1	1	2				
Cloud Security Check(Security G	15 5	5 3	10 2							
	Total Alert Count ↓	3	2	0	0	0				

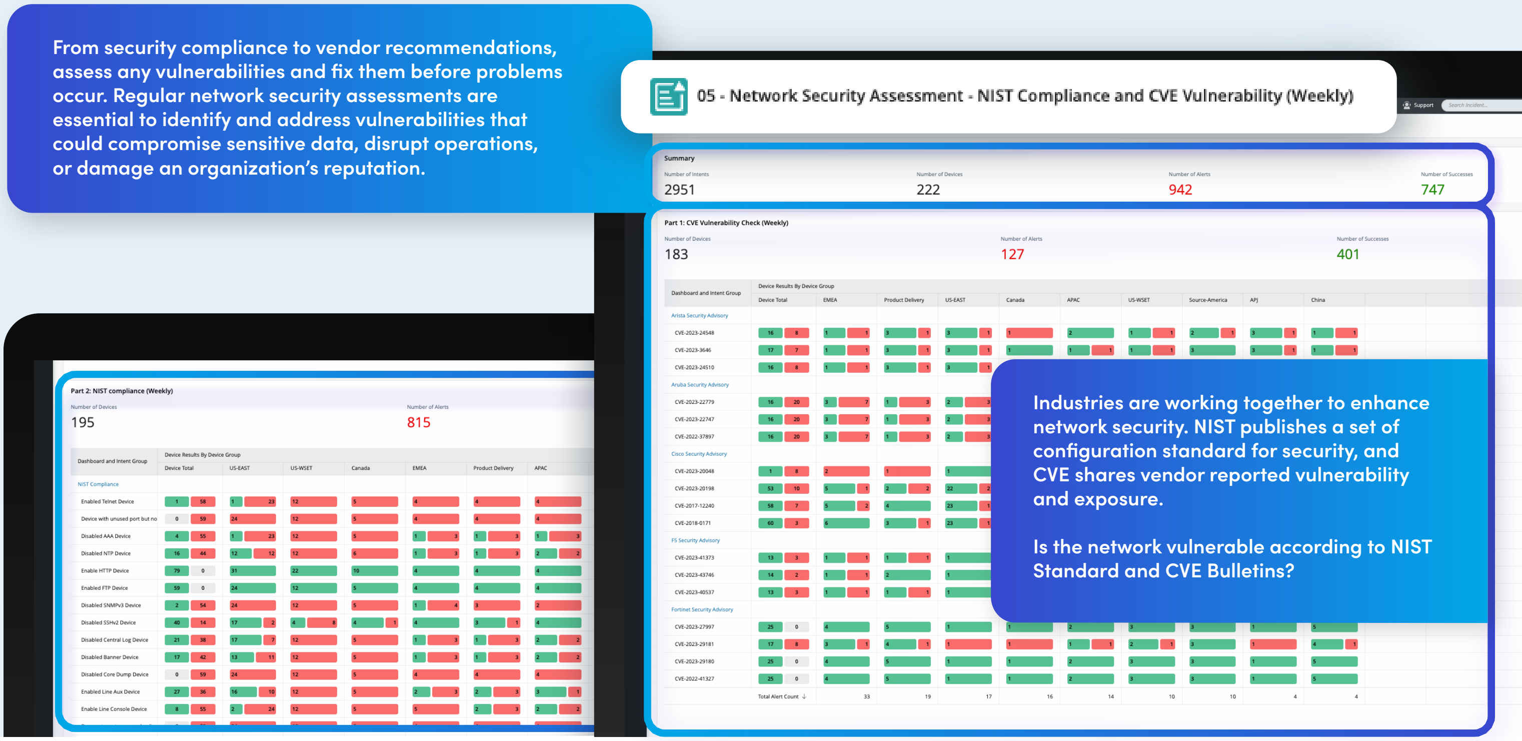
Application health assessment encompasses a comprehensive evaluation of various application metrics and components, including:

- CPU Capacity: Monitor CPU utilization to identify potential bottlenecks and ensure that applications have sufficient resources to handle their workloads.
- Memory Capacity: Track memory usage to detect potential memory leaks or insufficient allocation, ensuring that applications have adequate memory to operate efficiently.
- QoS Drops: Analyze Quality of Service (QoS) metrics to identify packet loss or latency issues that could affect application performance.
- Critical Interface Utilization: Monitor the utilization of critical network interfaces to ensure that data traffic is flowing smoothly and not causing performance bottlenecks.
- Tasks: Automate tasks such as log analysis, event monitoring, and resource threshold alerts to proactively identify and address potential application issues.

By continuously assessing these critical application metrics, organizations can gain valuable insights into application health, enabling them to optimize performance, prevent outages, and maintain a positive user experience.

5. Security Assessment

Is the network vulnerable according to NIST Standard and CVE Bulletins? From security compliance to vendor recommendations, assess any vulnerabilities and fix them before problems occur. Regular network security assessments are essential to identify and address vulnerabilities that could compromise sensitive data, disrupt operations, or damage an organization's reputation.



From security compliance to vendor recommendations, assess any vulnerabilities and fix them before problems occur. Regular network security assessments are essential to identify and address vulnerabilities that could compromise sensitive data, disrupt operations, or damage an organization's reputation.

05 - Network Security Assessment - NIST Compliance and CVE Vulnerability (Weekly)

Summary

Number of Intents	Number of Devices	Number of Alerts	Number of Successes
2951	222	942	747

Part 1: CVE Vulnerability Check (Weekly)

Number of Devices	Number of Alerts	Number of Successes
183	127	401

Dashboard and Intent Group	Device Results By Device Group									
	Device Total	EMEA	Product Delivery	US-EAST	Canada	APAC	US-WSET	Source-America	APJ	China
Arista Security Advisory										
CVE-2023-24548	🟩 16 🟥 8	🟩 1 🟥 1	🟩 3 🟥 1	🟩 3 🟥 1	🟥 1	🟩 2	🟩 1 🟥 1	🟩 2 🟥 1	🟩 3 🟥 1	🟩 1 🟥 1
CVE-2023-3646	🟩 17 🟥 7	🟩 1 🟥 1	🟩 3 🟥 1	🟩 3 🟥 1	🟩 1	🟩 1 🟥 1	🟩 1 🟥 1	🟩 3	🟩 3 🟥 1	🟩 1 🟥 1
CVE-2023-24510	🟩 16 🟥 8	🟩 1 🟥 1	🟩 3 🟥 1	🟩 3 🟥 1						
Aruba Security Advisory										
CVE-2023-22779	🟩 16 🟥 20	🟩 3 🟥 7	🟩 1 🟥 3	🟩 2 🟥 3						
CVE-2023-22747	🟩 16 🟥 20	🟩 3 🟥 7	🟩 1 🟥 3	🟩 2 🟥 3						
CVE-2022-37897	🟩 16 🟥 20	🟩 3 🟥 7	🟩 1 🟥 3	🟩 2 🟥 3						
Cisco Security Advisory										
CVE-2023-20048	🟩 1 🟥 8	🟥 2	🟥 1	🟩 1						
CVE-2023-20198	🟩 53 🟥 10	🟩 5 🟥 1	🟩 2 🟥 2	🟩 22 🟥 2						
CVE-2017-12240	🟩 58 🟥 7	🟩 5 🟥 2	🟩 4	🟩 23 🟥 1						
CVE-2018-0171	🟩 60 🟥 3	🟩 6	🟩 3 🟥 1	🟩 23 🟥 1						
F5 Security Advisory										
CVE-2023-41373	🟩 13 🟥 3	🟩 1 🟥 1	🟩 1 🟥 1	🟩 1						
CVE-2023-43746	🟩 14 🟥 2	🟩 1 🟥 1	🟩 2	🟩 1						
CVE-2023-40537	🟩 13 🟥 3	🟩 1 🟥 1	🟩 1 🟥 1	🟩 1						
Fortinet Security Advisory										
CVE-2023-27997	🟩 25 ⬜ 0	🟩 4	🟩 5	🟩 1	🟩 1	🟩 2	🟩 3	🟩 3	🟩 1	🟩 5
CVE-2023-29181	🟩 17 🟥 8	🟩 3 🟥 1	🟩 4 🟥 1	🟥 1	🟥 1	🟩 1 🟥 1	🟩 2 🟥 1	🟩 3	🟥 1	🟩 4 🟥 1
CVE-2023-29180	🟩 25 ⬜ 0	🟩 4	🟩 5	🟩 1	🟩 1	🟩 2	🟩 3	🟩 3	🟩 1	🟩 5
CVE-2022-41327	🟩 25 ⬜ 0	🟩 4	🟩 5	🟩 1	🟩 1	🟩 2	🟩 3	🟩 3	🟩 1	🟩 5
	Total Alert Count ↓	33	19	17	16	14	10	10	4	4

Industries are working together to enhance network security. NIST publishes a set of configuration standard for security, and CVE shares vendor reported vulnerability and exposure.

Is the network vulnerable according to NIST Standard and CVE Bulletins?

Part 2: NIST compliance (Weekly)

Number of Devices	Number of Alerts
195	815

Dashboard and Intent Group	Device Results By Device Group						
	Device Total	US-EAST	US-WSET	Canada	EMEA	Product Delivery	APAC
NIST Compliance							
Enabled Telnet Device	🟩 1 🟥 58	🟩 1 🟥 23	🟥 12	🟥 5	🟥 4	🟥 4	🟥 4
Device with unused port but no	⬜ 0 🟥 59	🟥 24	🟥 12	🟥 5	🟥 4	🟥 4	🟥 4
Disabled AAA Device	🟩 4 🟥 55	🟩 1 🟥 23	🟥 12	🟥 5	🟩 1 🟥 3	🟩 1 🟥 3	🟩 1 🟥 3
Disabled NTP Device	🟩 16 🟥 44	🟩 12 🟥 12	🟥 12	🟥 6	🟩 1 🟥 3	🟩 1 🟥 3	🟩 2 🟥 2
Enable HTTP Device	🟩 79 ⬜ 0	🟩 31	🟩 22	🟩 10	🟩 4	🟩 4	🟩 4
Enabled FTP Device	🟩 59 ⬜ 0	🟩 24	🟩 12	🟩 5	🟩 4	🟩 4	🟩 4
Disabled SNMPv3 Device	🟩 2 🟥 54	🟥 24	🟥 12	🟥 5	🟩 1 🟥 4	🟥 3	🟥 2
Disabled SSHv2 Device	🟩 40 🟥 14	🟩 17 🟥 2	🟩 4 🟥 8	🟩 4 🟥 1	🟩 4	🟩 3 🟥 1	🟩 4
Disabled Central Log Device	🟩 21 🟥 38	🟩 17 🟥 7	🟥 12	🟥 5	🟩 1 🟥 3	🟩 1 🟥 3	🟩 2 🟥 2
Disabled Banner Device	🟩 17 🟥 42	🟩 13 🟥 11	🟥 12	🟥 5	🟩 1 🟥 3	🟩 1 🟥 3	🟩 2 🟥 2
Disabled Core Dump Device	⬜ 0 🟥 59	🟥 24	🟥 12	🟥 5	🟥 4	🟥 4	🟥 4
Enabled Line Aux Device	🟩 27 🟥 36	🟩 16 🟥 10	🟥 12	🟥 5	🟩 2 🟥 3	🟩 2 🟥 3	🟩 3 🟥 1
Enable Line Console Device	🟩 8 🟥 55	🟩 2 🟥 24	🟥 12	🟥 5	🟥 5	🟩 2 🟥 3	🟩 2 🟥 2

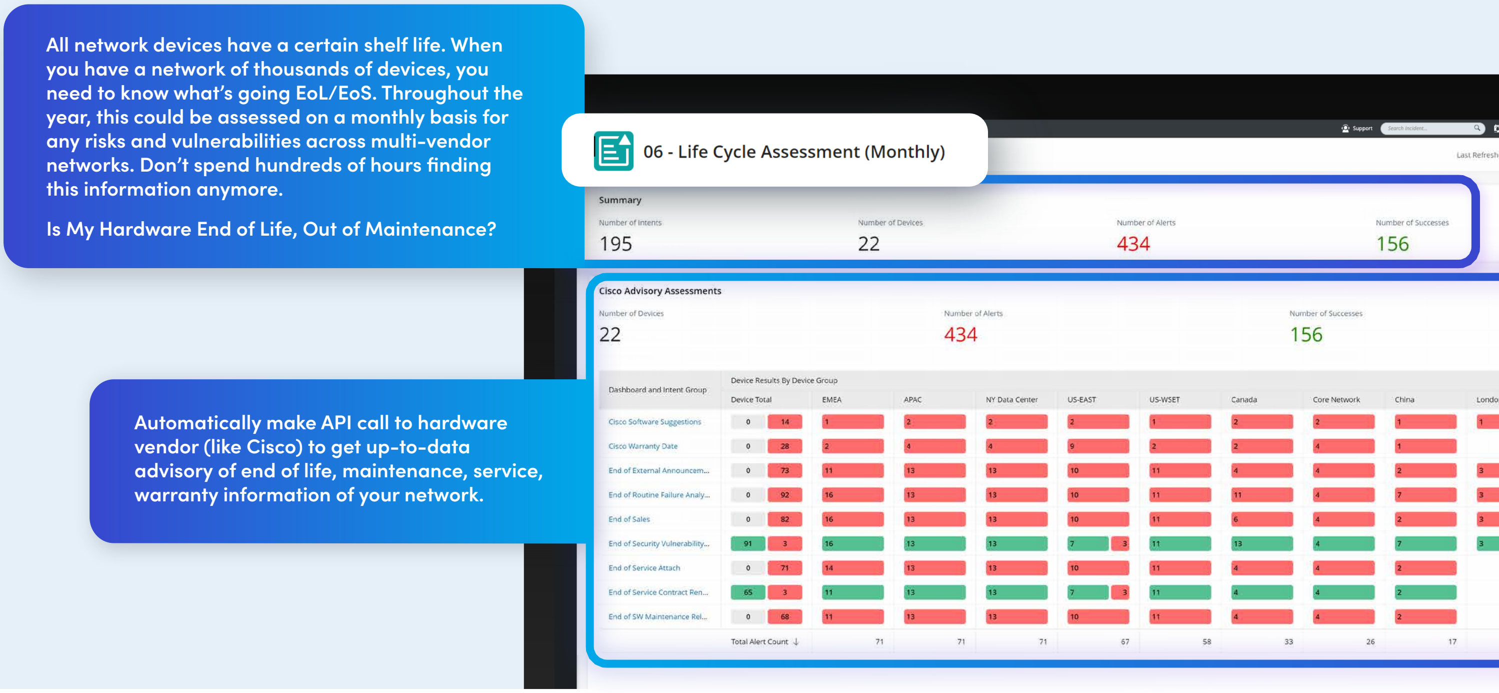
Network security assessments should encompass a comprehensive evaluation of various security aspects, including:

- Compliance with Standards: Evaluate adherence to industry-recognized security standards, such as those established by the National Institute of Standards and Technology (NIST).
- Vulnerability Detection: Identify and prioritize vulnerabilities found in network devices, operating systems, and applications, utilizing the Common Vulnerabilities and Exposures (CVE) catalog.
- Misconfigurations: Detect and rectify misconfigurations that could create security gaps, such as weak passwords, insecure protocols, and unauthorized access permissions.
- Intrusion Detection/Prevention (IDS/IPS): Analyze IDS/IPS logs to identify potential intrusion attempts and take appropriate corrective actions.
- Network traffic analysis: Monitor network traffic to detect anomalies that could indicate suspicious activity or network attacks.

By automating these security assessments, organizations can continuously monitor their network posture, proactively identify, and address vulnerabilities, and maintain a robust defense against evolving cyber threats.

6. Lifecycle Assessment

A comprehensive lifecycle assessment dashboard helps organizations stay informed about the lifecycle status of their network hardware, ensuring timely upgrades and replacement decisions.



All network devices have a certain shelf life. When you have a network of thousands of devices, you need to know what's going EoL/EoS. Throughout the year, this could be assessed on a monthly basis for any risks and vulnerabilities across multi-vendor networks. Don't spend hundreds of hours finding this information anymore.

Is My Hardware End of Life, Out of Maintenance?

Automatically make API call to hardware vendor (like Cisco) to get up-to-data advisory of end of life, maintenance, service, warranty information of your network.

06 - Life Cycle Assessment (Monthly)

Summary

Number of Intents	Number of Devices	Number of Alerts	Number of Successes
195	22	434	156

Cisco Advisory Assessments

Number of Devices	Number of Alerts	Number of Successes
22	434	156

Dashboard and Intent Group	Device Results By Device Group									
	Device Total	EMEA	APAC	NY Data Center	US-EAST	US-WSET	Canada	Core Network	China	Londo
Cisco Software Suggestions	0 14	1	2	2	2	1	2	2	1	1
Cisco Warranty Date	0 28	2	4	4	9	2	2	4	1	
End of External Announcem...	0 73	11	13	13	10	11	4	4	2	3
End of Routine Failure Analy...	0 92	16	13	13	10	11	11	4	7	3
End of Sales	0 82	16	13	13	10	11	6	4	2	3
End of Security Vulnerability...	91 3	16	13	13	7 3	11	13	4	7	3
End of Service Attach	0 71	14	13	13	10	11	4	4	2	
End of Service Contract Ren...	65 3	11	13	13	7 3	11	4	4	2	
End of SW Maintenance Rel...	0 68	11	13	13	10	11	4	4	2	
	Total Alert Count ↓	71	71	71	67	58	33	26	17	

By leveraging automated API calls to hardware vendors, such as Cisco, the lifecycle assessment dashboard provides real-time information on:

- End-of-Life (EOL) Status: Identify hardware that is approaching or has reached its EOL date, allowing for proactive planning and replacement strategies.
- Maintenance Status: Determine the maintenance status of hardware, ensuring that it is covered under vendor support for timely issue resolution and security patching.
- Service Contract Status: Monitor the validity of service contracts to avoid unexpected lapses in vendor support.
- Warranty Information: Track warranty coverage to ensure that hardware is eligible for repairs or replacements if necessary.

The dashboard empowers organizations to make informed decisions about hardware lifecycle management, optimizing their network for performance, security, and cost-effectiveness.

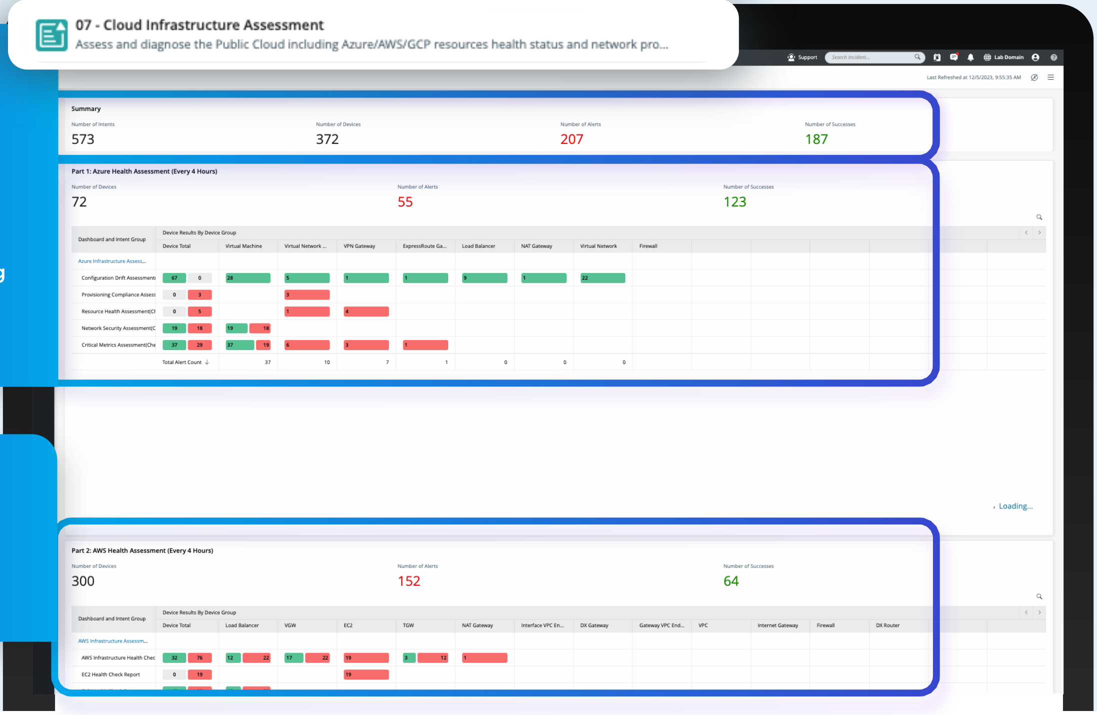
7. Hybrid-Cloud Network Assessment

By applying automation to hybrid-cloud network assessment, organizations can continuously monitor and assess their cloud networks across multiple cloud providers, including Microsoft Azure, Amazon AWS, and Google Cloud for insights into:

- Network Resource Utilization: Track metrics, such as CPU, memory, and network bandwidth, to identify potential bottlenecks and optimize resource allocation.
- Network Connectivity: Continuously monitor network connectivity between cloud environments and on-premises infrastructure, ensuring seamless data transfer and application performance.
- Virtual Appliance Health: Assess the health and performance of virtual appliances, such as firewalls and load balancers, that are critical for network security and traffic management.
- Cloud-Specific Metrics: Gain deeper insights into network performance and resource utilization in each cloud.

Cloud networks are virtual, but its problems are not. Organizations are moving to the cloud, and they need to have more visibility into the cloud. Not just a map or paths, but more metrics on interconnectivity so they're not blind to what is happening and potential issues.

Is my cloud healthy?



07 - Cloud Infrastructure Assessment

Assess and diagnose the Public Cloud including Azure/AWS/GCP resources health status and network pro...

Last Refreshed at 12/5/2023, 9:55:35 AM

Summary

Number of Intents	Number of Devices	Number of Alerts	Number of Successes
573	372	207	187

Part 1: Azure Health Assessment (Every 4 Hours)

Number of Devices	Number of Alerts	Number of Successes
72	55	123

Dashboard and Intent Group	Device Results By Device Group								
	Device Total	Virtual Machine	Virtual Network ...	VPN Gateway	ExpressRoute Ga...	Load Balancer	NAT Gateway	Virtual Network	Firewall
Azure Infrastructure Assess...									
Configuration Drift Assessment	67 0	28	5	1	1	9	1	22	
Provisioning Compliance Assess	0 3		3						
Resource Health Assessment(Cl	0 5		1	4					
Network Security Assessment(C	19 18	19 18							
Critical Metrics Assessment(Che	37 29	37 19	6	3	1				
	Total Alert Count ↓	37	10	7	1	0	0	0	

Part 2: AWS Health Assessment (Every 4 Hours)

Number of Devices	Number of Alerts	Number of Successes
300	152	64

Dashboard and Intent Group	Device Results By Device Group												
	Device Total	Load Balancer	VGW	EC2	TGW	NAT Gateway	Interface VPC En...	DX Gateway	Gateway VPC End...	VPC	Internet Gateway	Firewall	DX Router
AWS Infrastructure Assessm...													
AWS Infrastructure Health Chec	32 76	12 22	17 22	19	3 12	1							
EC2 Health Check Report	0 19			19									

Apply automation to continuously assess your cloud network:

- Microsoft Azure
- Amazon AWS
- Google Cloud

By continuously assessing the hybrid-cloud network, proactively identify and address potential issues, optimize performance, and maintain a secure and resilient cloud infrastructure.

8. Triggered Automation

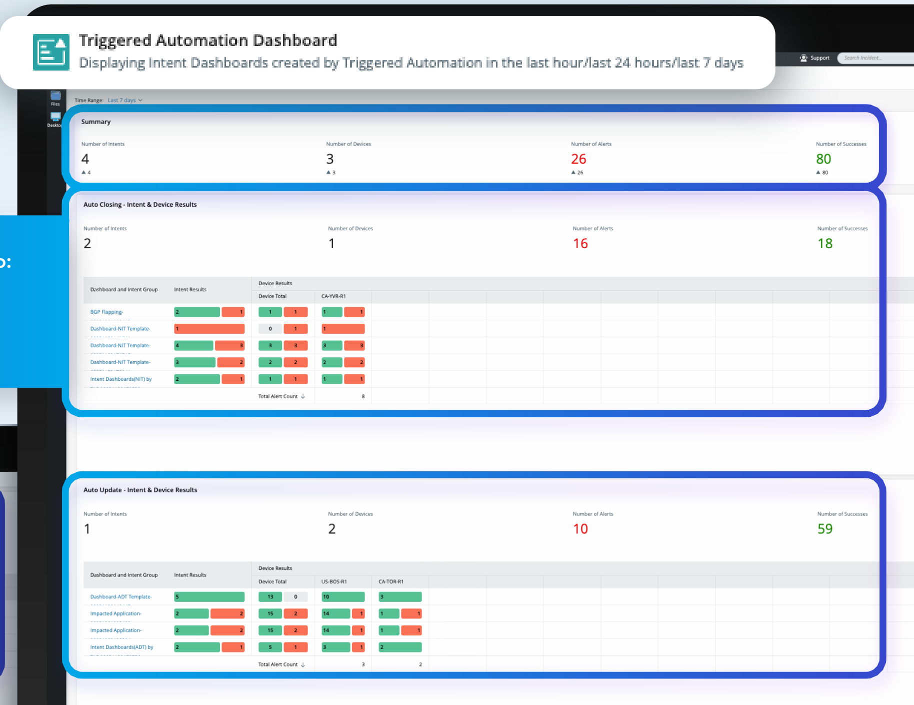
The triggered automation dashboard serves as a centralized hub for monitoring and responding to network incidents in real-time. By harnessing the power of automation, the dashboard streamlines incident management processes, enabling rapid diagnosis, prioritization, and resolution.

Customers get 1000s of incidents a month. What issues have occurred in the last hour and how many triggered and which have been auto-diagnosed?

What are the issues found at this hour?

Apply auto-diagnosis to incoming incident via API, leading to:

- Auto-closing ticket if problem is a noise
- Auto-opening if issues are found
- Auto-priority if impact is high



Triggered Automation Dashboard

Displaying Intent Dashboards created by Triggered Automation in the last hour/last 24 hours/last 7 days

Time Range: Last 7 days

Summary

Number of Intents	Number of Devices	Number of Alerts	Number of Successes
4 ▲ 4	3 ▲ 3	26 ▲ 26	80 ▲ 80

Auto Closing - Intent & Device Results

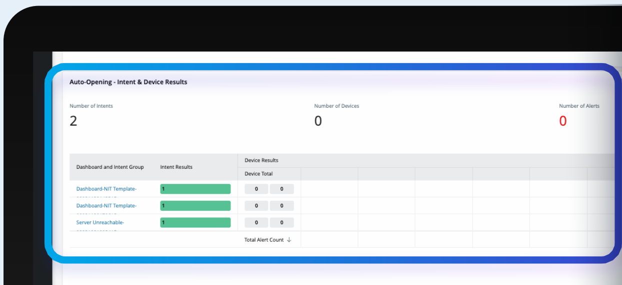
Number of Intents	Number of Devices	Number of Alerts	Number of Successes
2	1	16	18

Dashboard and Intent Group	Intent Results	Device Results	
		Device Total	CA-YVR-R1
BGP Flapping-	2 1	1 1	1 1
Dashboard-NIT Template-	1	0 1	1
Dashboard-NIT Template-	4 3	3 3	3 3
Dashboard-NIT Template-	3 2	2 2	2 2
Intent Dashboards(NIT) by	2 1	1 1	1 1
		Total Alert Count ↓	8

Auto Update - Intent & Device Results

Number of Intents	Number of Devices	Number of Alerts	Number of Successes
1	2	10	59

Dashboard and Intent Group	Intent Results	Device Results		
		Device Total	US-BOS-R1	CA-TOR-R1
Dashboard-ADT Template-	5	13 0	10	3
Impacted Application-	2 2	15 2	14 1	1 1
Impacted Application-	2 2	15 2	14 1	1 1
Intent Dashboards(ADT) by	2 1	5 1	3 1	2
		Total Alert Count ↓	3	2



Auto-Opening - Intent & Device Results

Number of Intents	Number of Devices	Number of Alerts
2	0	0

Dashboard and Intent Group	Intent Results	Device Results
		Device Total
Dashboard-NIT Template-	1	0 0
Dashboard-NIT Template-	1	0 0
Server Unreachable-	1	0 0
		Total Alert Count ↓

Upon receiving an incoming incident notification via API, the triggered automation dashboard applies intelligent auto-diagnosis capabilities:

- Auto-closing Ticket: If the incident is identified as noise, the ticket is automatically closed, reducing the workload for network engineers, and eliminating unnecessary escalations.
- Auto-opening Ticket: In cases where a network issue is found, automatically open a ticket, ensuring that the incident is promptly addressed and documented.
- Auto-prioritizing Ticket: If a high-impact issue is found, automatically assign the ticket to a high priority, alerting network engineers to the urgency of the situation and enabling rapid intervention.

By automating these critical incident management tasks, significantly reduce response times, minimize downtime, and enhance overall network resilience.

9. Past Outages Assessment

Are known problems happening again? After a network outage, assess any similar problems across a network. For every problem happened in your network before, could it happen again? In other part of network?

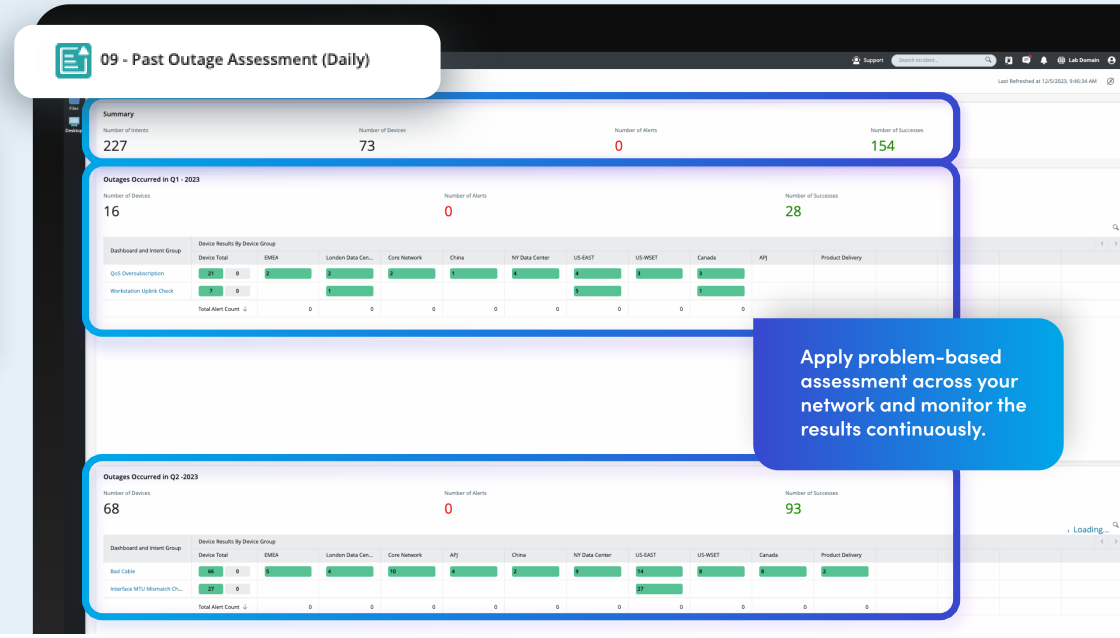
It could. Apply problem-based assessment across your network and monitor the results continuously. To effectively prevent future outages, organizations must conduct thorough post-outage assessments, analyzing the root causes of past incidents and identifying potential vulnerabilities that could lead to similar issues.

By analyzing past outages, organizations can:

- Identify Common Causes: Determine the recurring patterns and underlying factors that contribute to network outages, allowing for targeted mitigation strategies.
- Detect Unforeseen Vulnerabilities: Uncover hidden vulnerabilities or misconfigurations that may have been overlooked during initial assessments, preventing future outages.
- Enhance Network Resilience: Implement preventive measures and strengthen network infrastructure to reduce the likelihood of similar outages occurring again.

For every problem that happened in your network before, could it happen again? In other part of network?

Are known problems happening again? Where?



09 - Past Outage Assessment (Daily)

Summary

Number of Intents: 227
Number of Devices: 73
Number of Alerts: 0
Number of Successes: 154

Outages Occurred in Q1 - 2023

Number of Devices: 16
Number of Alerts: 0
Number of Successes: 28

Dashboard and Intent Group	Device Results By Device Group											
	Device Total		EMEA	London Data Cen...	Core Network	China	NY Data Center	US-EAST	US-WSET	Canada	APJ	Product Delivery
QoS Oversubscription	21	0	2	2	2	1	4	4	3	3		
Workstation Uplink Check	7	0		1				5		1		
	Total Alert Count ↓		0	0	0	0	0	0	0	0		

Outages Occurred in Q2 -2023

Number of Devices: 68
Number of Alerts: 0
Number of Successes: 93

Dashboard and Intent Group	Device Results By Device Group											
	Device Total		EMEA	London Data Cen...	Core Network	APJ	China	NY Data Center	US-EAST	US-WSET	Canada	Product Delivery
Bad Cable	66	0	5	4	10	4	2	9	14	8	8	2
Interface MTU Mismatch Ch...	27	0							27			
	Total Alert Count ↓		0	0	0	0	0	0	0	0	0	0

Apply problem-based assessment across your network and monitor the results continuously.

Continuous monitoring of past outage assessments is crucial to ensure that mitigation efforts are effective and that new vulnerabilities are not introduced. By proactively addressing past issues and learning from them, organizations can significantly enhance their network resilience and minimize the risk of future disruptions.

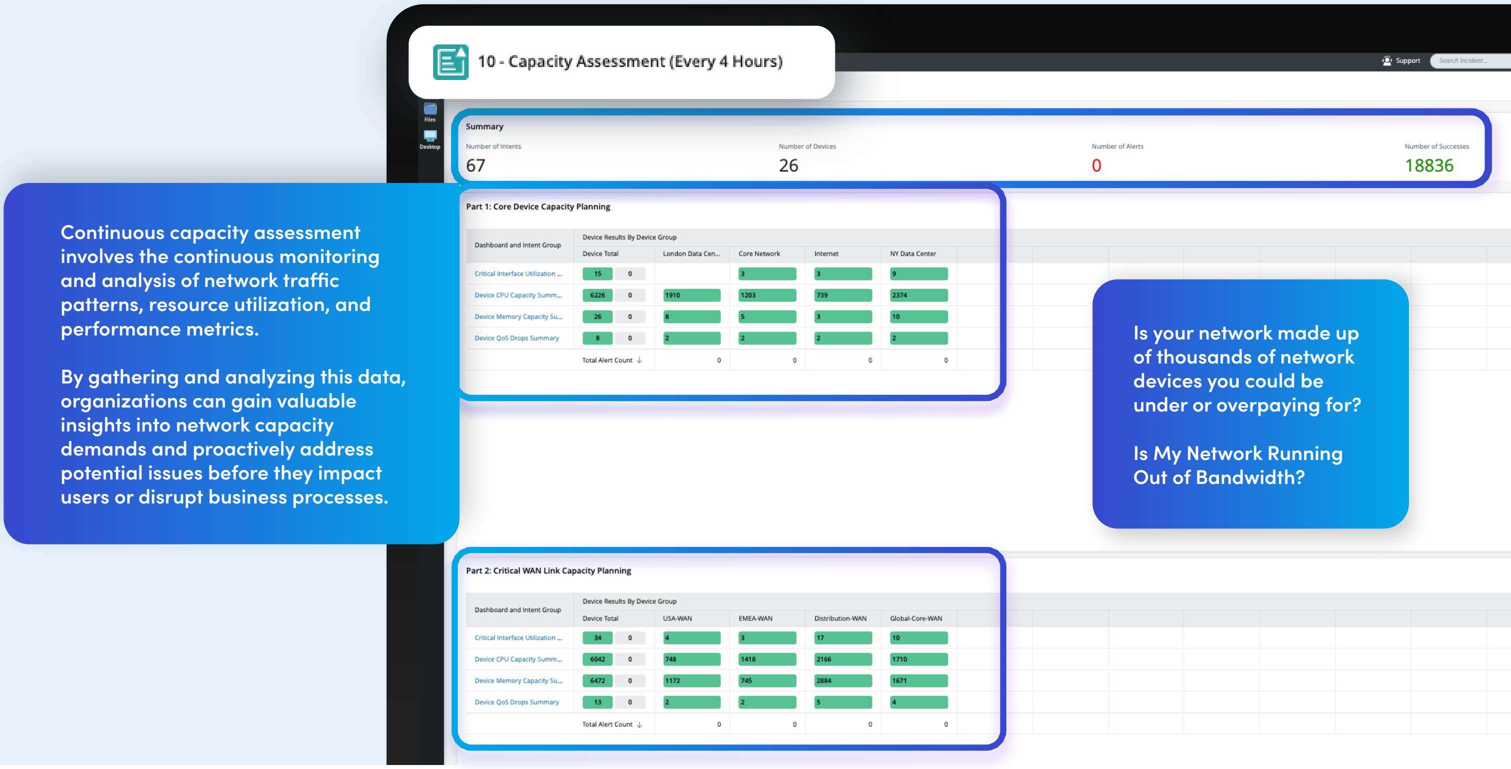
10. Capacity Assessment

Is the network running out of bandwidth? Continuous capacity assessment reduce the risk of over-utilization and under-utilization across network.

Capacity assessment involves the continuous monitoring and analysis of network traffic patterns, resource utilization, and performance metrics. By gathering and analyzing this data, organizations can gain valuable insights into network capacity demands and proactively address potential issues before they impact users or disrupt business processes.

Capacity assessment helps organizations avoid both over-utilization and under-utilization of network resources that could lead to congestion, latency, and packet loss, wasted resources and inefficient network operations.

Continuous capacity assessment enables proactive planning and scaling strategies by anticipating future capacity needs to avoid costly reactive measures and ensure that the network infrastructure can support evolving business requirements.



10 - Capacity Assessment (Every 4 Hours)

Summary

Number of Intents	Number of Devices	Number of Alerts	Number of Successes
67	26	0	18836

Part 1: Core Device Capacity Planning

Dashboard and Intent Group	Device Results By Device Group					
	Device Total		London Data Cen...	Core Network	Internet	NY Data Center
Critical Interface Utilization ...	15	0		3	3	9
Device CPU Capacity Summ...	6226	0	1910	1203	739	2374
Device Memory Capacity Su...	26	0	8	5	3	10
Device QoS Drops Summary	8	0	2	2	2	2
	Total Alert Count ↓		0	0	0	0

Part 2: Critical WAN Link Capacity Planning

Dashboard and Intent Group	Device Results By Device Group					
	Device Total		USA-WAN	EMEA-WAN	Distribution-WAN	Global-Core-WAN
Critical Interface Utilization ...	34	0	4	3	17	10
Device CPU Capacity Summ...	6042	0	748	1418	2166	1710
Device Memory Capacity Su...	6472	0	1172	745	2884	1671
Device QoS Drops Summary	13	0	2	2	5	4
	Total Alert Count ↓		0	0	0	0

Continuous capacity assessment involves the continuous monitoring and analysis of network traffic patterns, resource utilization, and performance metrics.

By gathering and analyzing this data, organizations can gain valuable insights into network capacity demands and proactively address potential issues before they impact users or disrupt business processes.

Is your network made up of thousands of network devices you could be under or overpaying for?

Is My Network Running Out of Bandwidth?

Several key metrics play a crucial role in capacity assessment:

- Bandwidth Utilization: Monitors the percentage of available bandwidth being consumed, indicating potential congestion points.
- Device Resource Utilization: Tracks the utilization of CPU, memory, and other resources on network devices, identifying potential bottlenecks.
- Application Performance Metrics: Evaluates the performance of critical applications under varying network conditions, highlighting potential capacity constraints.

By continuously monitoring these metrics and analyzing trends, organizations can gain 10 comprehensive understanding of their network capacity and make informed decisions to optimize performance and ensure scalability.

Get Started

It's time to stop settling for outdated snapshots and blind spots in your network security and performance. NetBrain Next-Gen's 10 pre-built, customizable assessments empower you to continuously monitor and optimize your entire hybrid network, from core infrastructure to critical applications. Take control of your network with no-code automation and unlock a world of agility, efficiency, and resilience. Download your free trial today and experience the future of network assurance.

Schedule a demo to see the assessments in action.

About NetBrain Technologies

Founded in 2004, NetBrain is the market leader for NetOps automation, providing network operators and engineers with dynamic visibility across their hybrid networks and low-code/no-code automation for key tasks across IT workflows. Today, more than 2,500 of the world's largest enterprises and managed service providers use NetBrain to automate network problem diagnosis, generate real-time documentation, accelerate troubleshooting, and enforce enterprise architectural rules.

+1 (800) 605-7964
info@netbraintech.com
www.netbraintech.com