Security Across the Hybrid Network

No-Code Network Security Automation

NetBrain

A report published by the Identity Theft Research Center found that there was a new record for data breaches reported worldwide with over 1800 data breaches - surpassing the previous year total by 68%.

Further, as reported on their annual cost of the data breach report, IBM discovered that for those teams without security automation, it took them an average of 239 days to even discover that their cloud networks were breached. Then it took them an additional 85 days to contain the breach.

239 days +85

That's 324 total days under a breach, and even longer for a return to normal operations. What does this mean in terms of impact? Well, one way to classify loss is financial cost.

In 2022, IBM reported in that same report that the global average cost of a single data breach was $4.35 million, and that picture looks even worse in the U.S., where that figure more than doubles to $9.44 million.

239

days to identify average cloud breach [1]

324

days to contain [1]

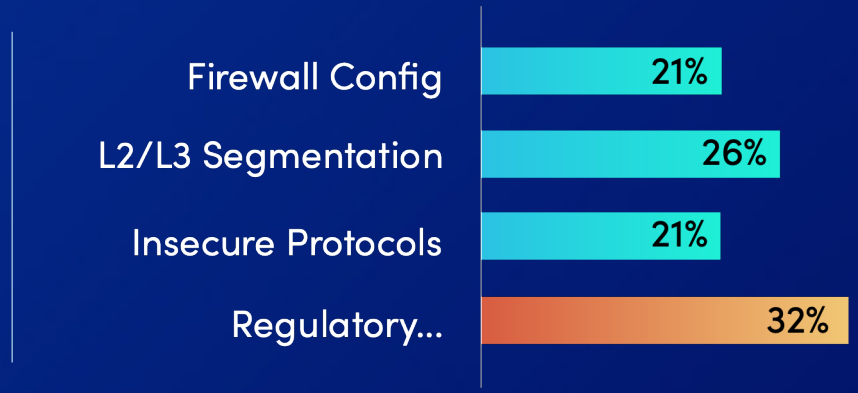
[1] According to IBM

Challenges Security Teams are Facing

Deployment of advanced security technologies can create the illusion of comprehensive protection, but all too often, subsequent changes to the infrastructure can increase risk.

In a LinkedIn study by NetBrain this year, respondents indicated their biggest network security problem is regulatory compliance.

But, all facets of network security received significant votes, suggesting security is a problem across the board.



Current Strategies to Confront These Challenges Come Up Short

There has been a lot of focus on device health monitoring, maintenance, and operations. This is because IT deploys very expensive machines to implement security designs, and they must protect the health of their investments. But, if the configuration and performance of those devices drift from their designed security intents, the effectiveness is lost even if device health appears optimal. This configuration drift, or sub-optimal settings, leads to the network being out of compliance and users experiencing degraded application performance. Often these huge vulnerabilities go undetected until the threat has already penetrated the network. We must not think of device health as the same as network health.

Complex networks are harder to secure because of:

- Lack of control and visibility
- More devices and traffic on the network
- More tools to manage the network
- The same number of operations personnel

"In order to close the gap between device health and network security, it is crucial for NetOps and SecOps organizations to shift their focus towards proactive measures, as opposed to relying predominantly on reactive approaches, which have traditionally been the preferred method. When end users detect issues that are not captured by device monitoring tools, they report them as incidents to the support team via ITSM tickets. This requires engineers to promptly respond, investigate, and resolve these unique problems.

However, in the realm of security, by the time end users start encountering issues, it is already too late. The network has been compromised, and the business is likely experiencing financial losses. And worse, most issues that are assumed or treated as one-offs, typically have occurred before, sometimes many times, but the troubleshooting knowledge wasn't captured for reuse. This results in repetitive work by valuable engineering resources costing time and leading to delayed incident responses, which in turn can lead to ticket backlogs.

Add in the additional time delay when escalating more complex issues and the threat spreads further, you're MTTR averages start to suffer, and your organization becomes more at risk. It becomes a vicious cycle that's hard to escape.

All of these represent reactionary procedures and protocols do not scale with networks and businesses as they expand. Traditionally, these teams could keep adding staff and resources, but now we're at a point where experts are no longer an infinite resource. We have to evolve the current security operations strategy to help IT keep up with the business.

Confronting the Challenges of Network Security

But what does that evolution entail? What can we do to confront these challenges?

1. Expand visibility
   You can't manage what you can't see, but for large hybrid-cloud networks, it's a problem of scale. We know adding every individual network component to our monitoring systems is cumbersome, time- and code-intensive. Automation offers a better way to discover your network and security policies and configurations.

2. Capture subject matter experts' knowledge
   Nothing could ever match the creativity of human problem solving, not even AI. But why wait months or years nurturing AI to learn your network when unmatched expertise already resides in house? But, where humans come up short is efficiency, speed, and knowledge sharing across all levels of IT. The few experts an organization has are not available 24x7 and are stretched thin with other projects. A better way would be to capture troubleshooting experience so everyone can benefit from the steps and actions that expert took to resolve that issue, or a similar one.

3. Sharing knowledge across the organization
   When knowledge is harnessed, it can be leveraged by anyone to democratize operations at scale, reducing repetitive work and expediting troubleshooting. The ability to capture incidents and share and collaborate in real time reduces the need for escalations and hand-offs.

NetBrain Next-Gen No-Code Network Automation Enforces Network Security

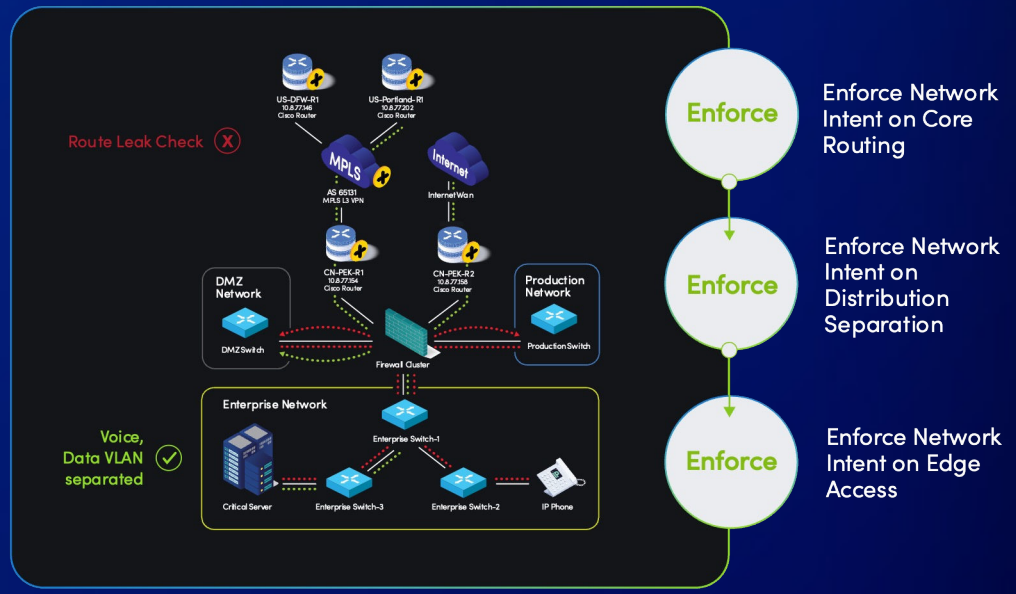
A better way is to digitize expert knowledge and pair it with machine efficiency. The NetBrain Next-Gen platform does this without code by capturing all of your network's security policies, KPIs and configurations and turning them into automation called network intents. Network intents store all of the troubleshooting and design intelligence and make it available 24/7 to IT operations teams.

Digitizing your security designs for how your network should operate includes understanding and checking:

- Whether traffic should take path A or path B
- Whether remote users are allowed to access a database. How should the ACL enforce that?
- HA Firewall pair configurations
- Telnet settings
- Interface and port settings
- NAC 802.1x compliance check
- Device access requirements
- Ensure rogue devices are not connected to secure VLANs

Background

Applications, services, and users live on different networks and subnets, so network and security architects add segmentation to different networks with policies to allow or deny application traffic.



NetBrain Next-Gen can be programmed to enforce HA firewalls mirrored configurations to ensure the network is secure. It can proactively enforce ACLs to verify they always have a certain set of rules. When an HA failover or a security breach occurs, it's too late to discover that configuration drift has left your network vulnerable. Use NetBrain Next-Gen to run network intents regularly for device, edge, border, and zone level network security and alert you when security is out of compliance.

Complete Visibility

NetBrain Next-Gen automates the discovery of the entire hybrid network and builds a live digital twin of devices, topology, flow, and intents. Multi-vendor support and dynamic mapping technologies mean no corner of your hybrid-cloud network ever goes unobserved. SIEM integrations allow for quick identification of devices and network paths to quickly respond to any incidents.

Accelerate Malware Mitigation with One-IP Table

With NetBrain Next-Gen's One-IP Table, you can search any compromised endpoint or network device easily by IP address, MAC address, or DNS name to take immediate action. When your security or monitoring solution detects a device infected with malware, time is of the essence and finding that device on the network can be like finding a needle in a haystack. Every second lost gives the malicious code more time to spread throughout the organization.

One-IP Table

Help

IP Address	LAN Segment	MAC Address	Switch Port	VLAN ID	DNS Name	Gateway	Description	Data Source	VLAN Group
192.168.3.71	192.168.3.64/26	0250:7966:6838	CA-TOR-SW1.Ethernet1/1	500	APP2-TOR.Ethernet0/0	APP2-TOR.Ethernet0/0		Device Interface	APP2-TOR##Ethernet0/0
192.168.1.25	192.168.1.16/28	02bb.cc01.0000	US-BOS-SW3.Ethernet3/0	101	APP4-BOS.Ethernet0/0	US-BOS-SW2.Vlan101		Device Interface	APP4-BOS##Ethernet0/0
192.168.1.30	192.168.1.16/28	02bb.cc80.d000		101	US-BOS-SW3.Vlan101	US-BOS-SW1.Vlan101		Device Interface	APP4-BOS##Ethernet0/0
192.168.3.1	192.168.3.0/30	02bb.cc00.3000	CA-TOR-SW2.Ethernet1/0		CA-TOR-R1.Ethernet0/0	CA-TOR-R1.Ethernet0/0	contact NetBrain-IT	Device Interface	CA-TOR-R1##Ethernet0/0
192.168.3.2	192.168.3.0/30	02bb.cc00.1001	CA-TOR-R1.Ethernet0/0		CA-TOR-SW2.Ethernet1/0	CA-TOR-R1.Ethernet0/0	contact NetBrain-IT	Device Interface	CA-TOR-R1##Ethernet0/0
192.168.3.5	192.168.3.4/30	02bb.cc00.3010	CA-TOR-SW1.Ethernet1/0		CA-TOR-R1.Ethernet0/1	CA-TOR-SW1.Ethernet1/0	contact NetBrain-IT	Device Interface	CA-TOR-R1##Ethernet0/1
192.168.3.6	192.168.3.4/30	02bb.cc00.2001	CA-TOR-R1.Ethernet0/1		CA-TOR-SW1.Ethernet1/0	CA-TOR-SW1.Ethernet1/0	contact NetBrain-IT	Device Interface	CA-TOR-R1##Ethernet0/1
192.168.3.132	192.168.3.128/26	02bb.cc80.1000		300	CA-TOR-SW2.Vlan300	CA-TOR-SW2.Vlan300		Device Interface	CA-TOR-SW1##Vlan300
192.168.3.141	192.168.3.128/26	02bb.cc02.f030	CA-TOR-SW1.Ethernet2/0	300		CA-TOR-SW2.Vlan300		ARP Table	CA-TOR-SW1##Vlan300
192.168.3.155	192.168.3.128/26	02bb.cc00.f000	CA-TOR-SW2.Ethernet2/3	300		CA-TOR-SW2.Vlan300		ARP Table	CA-TOR-SW1##Vlan300

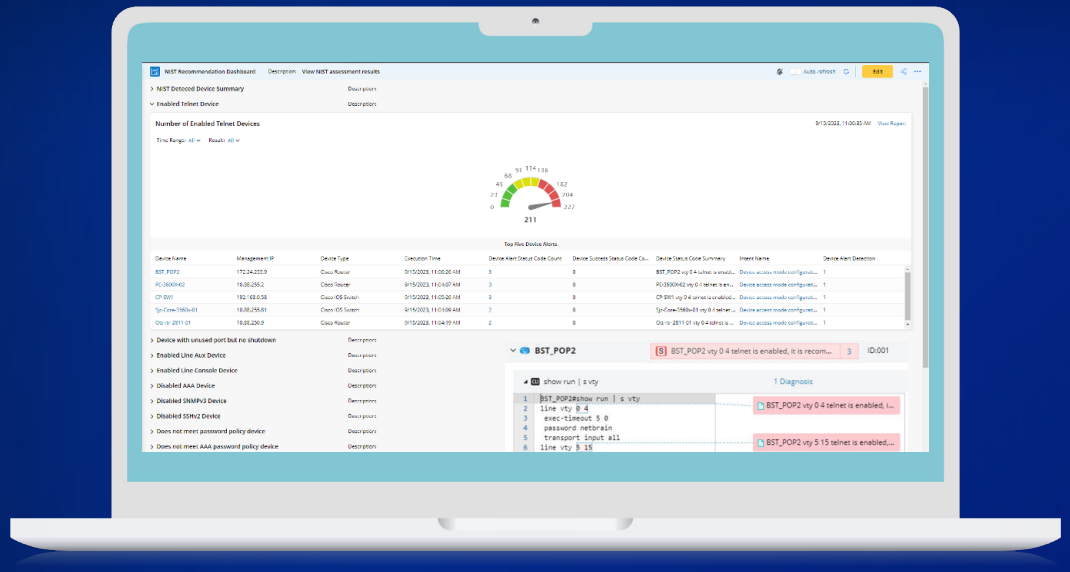
Continuous Network Assessments to Enforce Zero-Trust Security Strategies

NetBrain Next-Gen's proprietary no-code Intent technology makes it easy to capture intelligent assessments of your network's security implementation and store them as executable automation without any scripting. Compare live network configurations to your organization's security best practices, standards, and templates. Capture this logic once on a single network device and then replicate to every like device on the network or apply this logic to a completely new situation or scenario within the network. NetBrain Intents then proactively monitor security configurations and alert support teams to any compliance deviations.

Zero Trust security is founded on the principle of "never trust, always verify." It assumes that no user or device, whether inside or outside the network perimeter, should be granted unrestricted access by default.

In a zero-trust environment, continuous network assessment serves as the bedrock for security efficacy. It involves the real-time monitoring, analysis, and verification of various network components, such as users, devices, and application paths.

Consequently, this allows NetOps teams to sustain the agility needed of their infrastructure while keeping security policies relevant and effective as the network evolves. But not all automation solutions are equal. With NetBrain's unparalleled visibility, network Intents intelligently verify that every node in your network—from user access points to local data centers to cloud services—are continuously vetting entry into the network.



Dashboards, Reports, and Alerts

NetBrain Next-Gen helps staying informed about the state of your network security efforts and its compliance with your organization's design standards with customizable dashboards and on-the-fly reports with the configurations included. Intent results and maps are available as exportable documentation in CSV, Microsoft Word and Visio.

Additionally, configurable notifications alert your support staff of any anomalies in your network's security compliance.

Reduce Risk with Protective Change Management

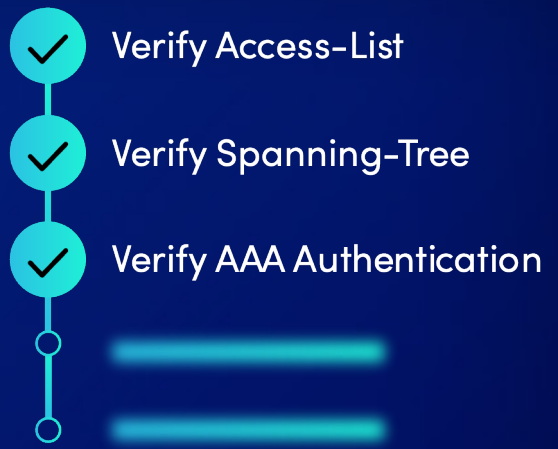
Network change and configuration drift undermine implemented security measures over time resulting in more frequent and time-consuming security audits. Visualize infrastructure changes across the hybrid network and identify all impacted devices, services, and application dependencies – in seconds.

Even successful device changes can result in unintended consequences. Now, ensure design intentions for network device changes and the resulting connectivity changes are preserved. Push security control changes at scale with verification and logging. Leverage rollbacks to quickly restore any previous configuration. Identify and push firmware updates to vulnerable or end of life devices.

By pairing human decision-making knowledge with machine speed automation, you can eliminate repetitive workflows and significantly reduced meantime to repair. You can take any action that would take a human minutes or hours and have the machine do it for you in seconds, proactively. Your entire support infrastructure can leverage intents as automation when troubleshooting.

Respond to Threats Immediately with Automated Diagnosis

Our research indicates 50% of all incidents are repetitive in nature, meaning that the same or similar issues have been reported in the past. Your IT knows how to solve these issues when they arise and can capture those solutions as executable intents. Sometimes it takes hours for a human to respond to a ticket. Why not respond with machine speed? Execute diagnostic steps as soon as an issue is reported. By the time a support engineer acknowledges the ticket, NetBrain Next-Gen is ready with the root cause and recommended resolution steps all available directly from the ticket with our APIs and deep integration with the leading ITSM providers.



Get Started

Half of all respondents according to InformaTech's 2022 State of Network Management report indicated security is their top network management priority, making it the top priority by a wide margin. What's held NetOps and SecOps back is getting the right technology into the right hands and NetBrain's no-code automation is that platform.

NetBrain Next-Gen transforms your network operations plan from an inefficient and reactive one, to a proactive, streamlined approach that leverages the knowledge and expertise you already have. It supports what you already have, and what you'll have in the future, including all multi-vendor on-premises and public cloud components. It captures the expertise of your subject matter experts without any code to allow their knowledge to be replicated across the network and shared with their peers. NetBrain automation scales NetOps more efficiently, at a level previously only associated with additional headcount, higher costs and increased business risk.

See 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

NB-EB-SATHN-052523