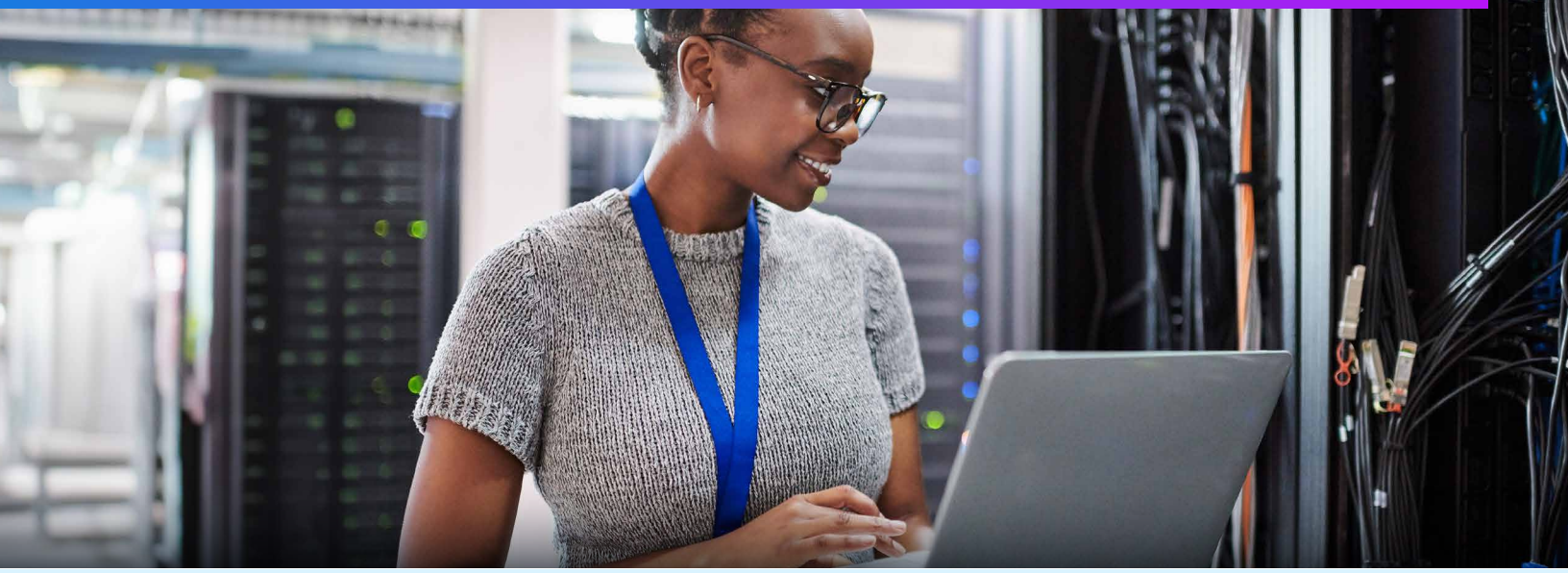
NetBrain
DEMOCRATIZING NETWORK AUTOMATION

Network-Wide Security Automation for Continuous Protection

Automate Security Expertise Across Hybrid Networks



In today's dynamic cybersecurity landscape, ensuring network security and compliance across sprawling, complex networks is more time-consuming and resource-intensive than ever. From maintaining consistent security configurations to proactively addressing vulnerabilities and responding swiftly to security incidents, organizations are faced with a myriad of complex tasks that demand efficient and effective solutions. Manually identifying and addressing vulnerabilities, ensuring compliance configurations, and continuously monitoring for threats is difficult, especially with limited staff and ever-evolving threats.

This brief explores how NetBrain's advanced no-code automation and visualization capabilities empower organizations to tackle network security challenges head-on, streamlining compliance efforts, automating vulnerability assessments, and enhancing threat response capabilities – all without labor-consuming overhead and setup.

Continuous Compliance and Monitoring

Assess Security Design and Policy Compliance

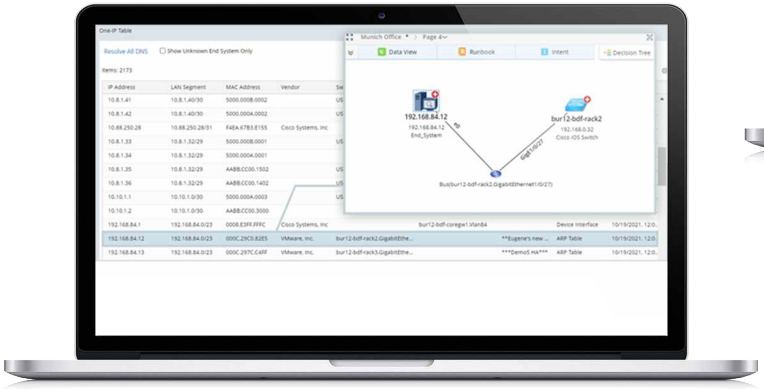
According to the NIST Special Publication 800-37 on risk management framework for information systems and organizations, "Organizations should maximize the use of ***automation***, wherever possible, to increase the speed, effectiveness, and efficiency of executing the steps in the Risk Management Framework (RMF)."

Leveraging no-code network automation redefines security design and policy compliance management across hybrid-cloud networks. It lets you quickly automate the implementation of security protocols and configurations network-wide, ensuring a consistent and robust security posture. Standardize security zones and firewall settings to bolster security measures and promptly identify and rectify configuration missteps that could potentially lead to vulnerabilities.

Automated network security assessments reinvent the way network security is addressed. Automation makes security validation assessments continuous enabling the guarantee of critical aspects of network security. By translating your security policies into automated assessment checks, you can ensure that:

- **Traffic follows across intended paths:** Validate if traffic flows through authorized routes.
- **Access is controlled:** Automate access control lists (ACLs) to restrict unauthorized user access to databases or sensitive resources.
- **High Availability (HA) is maintained:** Verify consistent configurations across HA firewall pairs.
- **Interfaces and ports are secure:** Automate checks for secure interface and port settings.
- **Network Access Control (NAC) is enforced:** Ensure proper 802.1x compliance for secure device access.
- **Rogue devices are identified:** Automate detection of unauthorized devices on secure VLANs.
- **Secure protocols are enforced:** Eliminate the use of unsecure protocols like Telnet, and FTP.
- **Secure communication protocols are utilized:** Automate verification of proper encryption protocols for secure communication.

Automation not only ensures continuous compliance but also helps in proactively preventing vulnerabilities and network design and policy compliance. Use automation to harden routers and switches, implement strict access policies (allow/deny), secure isolated networks, and validate firewall policies to lock down access and prevent unauthorized access attempts.



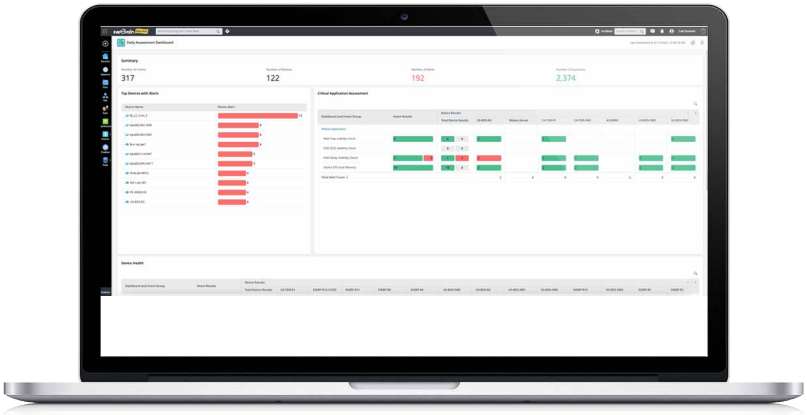
Assess Adherence with Regulatory and Industry Guidelines

Regulatory and industry standards undergo frequent updates, posing a significant challenge in ensuring compliance within intricate hybrid networks. A multitude of standards, including PCI DSS, HIPAA, ISO 27001/2, NIST, SOC 2, SOX, and GDPR, impose compliance requirements at both industry and governmental levels. Automation emerges as the essential solution for comprehending all network components, ensuring network segmentation and compliance with credit card processing systems, and verifying firewall access policies remain in place.

Ensure Ongoing Audit Readiness

The constant flux of network changes and configuration drift can erode your established security measures, leading to frequent and labor-intensive security audits. Typical audit preparation occurs only in advance of each audit to get all the data ready. A better way is to ensure the network is compliant all the time.

NetBrain's no-code network automation platform, Next-Gen, provides continuous network assessments, ensuring your business remains compliant at all times. Instead of manual data collection, use the no-code automation platform to capture and verify policies using continuous assessments, live interactive assessment summary dashboards, and change logs. Identify and automatically check your network against saved policies and identify any non-compliance with government standards and industry and regulatory mandates to streamline your compliance efforts and reduce risk.



Cybersecurity Defense and Response

A security event is an incident that can cause a breach by a bad actor in pursuit of data exfiltration. 24x7 monitoring by SOC teams and NSSPs requires visibility into the entire network to protect sensitive data.

NIST states, "The use of automation facilitates a greater frequency and volume of control assessments as part of the monitoring process. The ongoing monitoring of controls using automated tools and supporting databases facilitates near real-time risk management for information systems and supports ongoing authorization and efficient use of resources."

Network visibility into network configuration during real-time incidents is required to help defend the network borders. Anomaly detection and configuration validation protect the network from infiltration over time giving you valuable history of benchmark policies and configurations.

Automate the verification of secure communication protocols and the changing of vendor-supplied passwords. Leverage automation for protected change management processes to mitigate configuration drift risks.

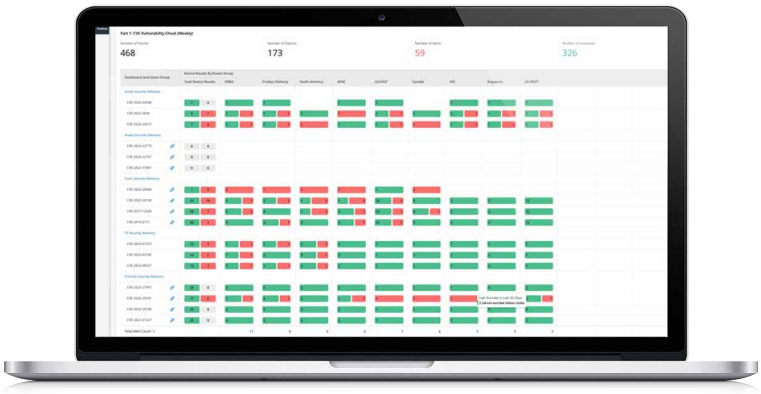
In the event of a security incident, automation enables swift troubleshooting and response. For example, if a rogue device is detected, NetBrain can identify the MAC address and communicate with incident management platforms, like ServiceNow, to help initiate lockdown procedures, protecting the network from further threats.

Vulnerability and Weakness Detection and Assessments

Streamline your security operations by automating vulnerability scans and assessments, reducing manual tasks, and improving overall efficiency.

Vulnerability Assessments

Stay on top of threats with automated CVE (Common Vulnerabilities and Exposures) scans so you can react faster. NetBrain enables you to quickly identify new vulnerabilities, create your own automations instead of waiting on vendors to provide updates, patches, and signature files so you can proactively address issues within minutes. Leverage pre-built security intents and dynamic dashboards for real-time visibility and proactive threat mitigation.



Weakness Assessments

Utilize CWE (Common Weakness Enumeration) to enumerate weaknesses and identify known threats or new, more secure design models. By modeling the rest of your network based on an initial network security deployment, automation can help replicate and expedite your network security rollout.

Version Updates

Ensure your network components are up-to-date by automating version checks for software, operating systems, and feature sets. NetBrain's automated approach to vulnerability and weakness detection empowers your team to address new threats swiftly, maintain compliance, and build a proactive security strategy based on real-time insights.

Safer Configuration Changes

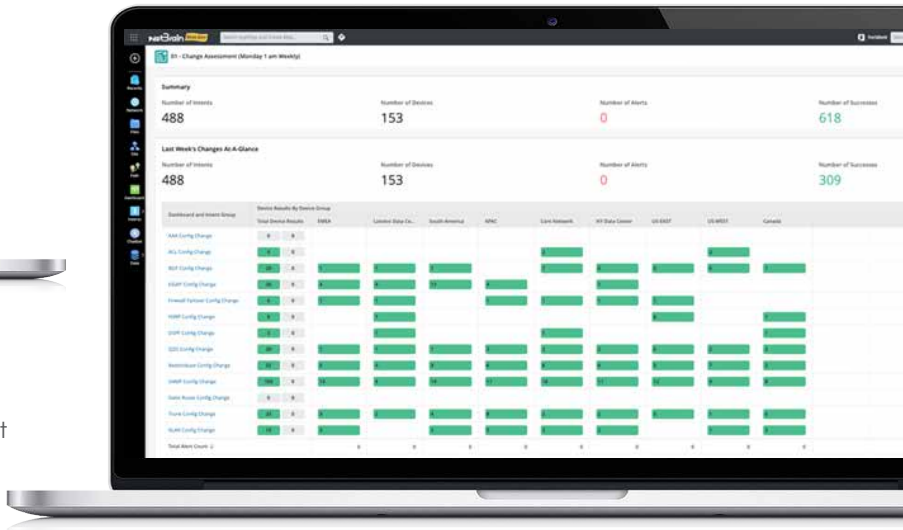
Maintaining consistent security configurations across complex network environments is crucial to prevent configuration drift and vulnerabilities. NetBrain's no-code automation ensures safer configuration changes and enhances network security.

Define and Verify Security Zones: Implement mirrored security zones and firewall settings, and verify connectivity across zones, including cloud infrastructure. Conduct path calculations to test accessibility and ensure high availability to mitigate attacks.

Automated Change Management: Visualize infrastructure changes and identify impacted devices, services, and application dependencies in seconds. Enforce security control changes at scale, with verification and logging, and leverage rollbacks for quick restoration of previous configurations.

Mitigate Misconfiguration Risks: Thoroughly validate the network before, during, and after changes to ensure network security and reliability. Automate repetitive tasks and reduce mean time to repair by leveraging machine-speed automation paired with human decision-making knowledge.

By adopting NetBrain's automation capabilities, your organization can proactively address configuration drift, enforce security policies, and mitigate risks associated with network changes, ultimately enhancing network security and efficiency.



Hybrid-Cloud Network Security Visibility

Not being able to see the entire hybrid cloud network means not being able to keep it secure. Give network security teams the visibility they need with end-to-end network visibility through dynamic mapping and hybrid-cloud pathing, not only devices, but topology, flow, and behaviors.

Multi-vendor support and dynamic mapping technologies mean no corner of your hybrid-cloud network ever goes unobserved.

With NetBrain's comprehensive automation capabilities, organizations can enhance their network security posture, reduce manual tasks, and achieve greater efficiency in managing hybrid-cloud network environments, ultimately ensuring ongoing visibility, compliance, and protection against emerging threats. Discover how NetBrain can help your organization achieve a more secure and resilient network infrastructure.

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.

NetBrain

NB-SB-NWSACP-050124

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