BACKBOX
SOLUTION BRIEF

Zero Trust NetOps (ZTNO)

Six Actionable Pillars to Automate Zero Trust in a NetOps Environment

Overview

Network leaders are struggling to implement zero trust principles into their architectures, driven by their security and risk management initiatives. Network teams should try to get budget based on the fact that the company has set out to implement other zero trust initiatives, like zero trust network access (ZTNA). ZTNO provides a plan for network engineers to move forward with zero trust in their Network Operations (NetOps) environments.

The purpose of this solution brief is to share six actionable pillars that network teams can use to enable zero trust in their NetOps environment as part of their organization's zero trust strategy. It's important that these pillars define clear, tactical implementation steps to ensure that there's no ambiguity in translating zero trust goals into specific tactical steps that network engineers can implement.

These six pillars are collectively referred to as **Zero Trust NetOps (ZTNO).**

ZERO TRUST

Zero trust is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. Zero trust replaces implicit trust with continually assessed risk and trust levels, based on identity and context.

Most organizations have a zero trust strategy for information security. Increasingly, IT leaders, including network teams, are being asked to apply zero trust concepts to their network infrastructure and operations.

ZERO TRUST NETOPS

Zero Trust NetOps (ZTNO) supports and extends zero trust by enabling key controls around owned and controlled network devices and the network engineers that manage them, so that risk and trust are constantly assessed through onboarding and daily operations.

BackBox has defined six actionable pillars to employing a zero trust methodology in a NetOps environment. The first two pillars relate to the humans administering network devices, the latter four refer to the devices themselves. For all six pillars, ZTNO ensures that anything/anyone connecting to the network does so in a compliant way, and that devices are continuously checked for compliance on a regular basis.

ZTNO is implemented with a combination of automation, vulnerability management, and privileged access management.

The Six Pillars of Zero Trust NetOps

An effective zero trust strategy for the human side of NetOps means balancing the need for security with the need to manage network devices. The right level of protection is critical, as is ensuring that network engineers can do their jobs.

For the device side of NetOps, zero trust ensures that network devices can be onboarded quickly while remaining consistent with best practice standards for the organization. Over time, devices are continuously monitored to ensure that they remain 100% compliant with the desired configuration and that that no new vulnerabilities are allowed to remain in the network.

The six pillars of ZTNO are divided accordingly into two pillars relevant for human network engineers, and four pillars relevant for network devices.

1 Access Management

Secure access needs to be provided whether accessing network devices via API, WebURL, or CLI. BackBox accomplishes this by integrating role-based access controls with credential vaults and providing a secure, credentialed API. Additionally, automations can have permissions associated with them, so that administrators can perform their jobs and have exactly the right permissions (through association with the automation).

2 Audit and Control

Humans accessing network devices should do so only in an auditable manner. This is done with controls to log all changes to an immutable log, and even to record administrator sessions for replay. Roll-back of changes is also made possible through this centralized access point.

3 Device Configuration Onboarding

Device configurations should be made consistent with a 'golden configuration' during the onboarding process. This is done via policy enforcement that ensures the appropriate configurations. Done in an automated manner, this eliminates manual errors and improves the speed of onboarding new devices to the network.

4 Vulnerability Management Onboarding

During the onboarding process, devices are checked for known vulnerabilities which are then remediated prior to being added to the network. Vulnerabilities that aren't relevant can be ignored, while those that are relevant can be patched or updated based on vendor recommendations for mitigation.

5 Continuous Assessment

Once onboarded, devices are continuously assessed for both configuration compliance and new vulnerabilities. When configuration drift is discovered, configurations can be groomed into compliance automatically or notifications can be sent to alert administrators of non-compliance. Similarly with vulnerabilities, as new vulnerabilities are discovered, when deemed relevant they can be patched.

6 Reporting and Visibility

Rich reporting and visibility ensures that teams communicate and are aware of the steps taken to protect the network. Reports can be configured such that actionable data is highlighted for security and networking teams to keep the network as secure as possible.

BackBox Platform and Zero Trust

NETWORK AUTOMATION MANAGER

Network Automation Manager is the core component of BackBox responsible for automating the administration of network and security devices. As it pertains to zero trust, Network Automation Manager is responsible for ensuring 100% configuration compliance; both as devices are onboarded and over time as natural configuration drift occurs.

NETWORK VULNERABILITY MANAGEMENT

Network Vulnerability Management (NVM) ensures that new devices are added to the network only after remediating known vulnerabilities. Over time, NVM ensures that devices stay protected and that as vulnerabilities are discovered, they are quickly patched or fixed.

PRIVILEGED ACCESS MANAGER

All manual network engineering tasks require a solution like Privileged Access Manager (PAM) to manage administrator rights and compliance. This helps solve for two opposing desires – increasing the ability to inject change into the network while also decreasing the changes made by individuals. Ad hoc changes made by individuals add risk to the security and stability of the network and, as such, changes by individuals should be limited.

To do this, IT leaders and network administrators need a way to transition from network engineers having individual, direct accounts into their network and security devices to centralized accounts with a single access point to all devices.

This is the purpose of BackBox's PAM. It is the central point of control, as well as a single place to audit and record administrator sessions for compliance. PAM ties into credential vaults, provides immutable logs, recording and auditing of sessions, and serves as the foundation for zero trust NetOps for human network administration. Applying the granularity of PAM to achieve zero trust objectives ensures all access is appropriate, managed, and documented, regardless of how the perimeter has been redefined.

Benefits of Zero Trust NetOps

There are three key benefits of implementing ZTNO:

1. RESILIENCE. Networks have become the backbone of the business. When an application is down, a certain part of the business is affected. However, when the network is down, the entirety of the business is affected. Errors or attacks impact the entire business, which is one of the reasons networks are an important attack vector. Reducing the likelihood of configuration errors and malicious attacks reduces the impact to business over time and makes for a more resilient business.

2. FLEXIBILITY. Network engineers have more options when fixing problems because they can be given more granular access control through Privileged Access Manager. Automations themselves can also be given permissions, enabling lower-level administrators to have more power to fix issues, without risking damaging errors due to inexperience.

3. SPEED. Automating the onboarding of devices is critical to keeping network teams working smoothly and increasing the speed at which devices can be properly added to the network. Additionally, time consuming OS updates that are necessary for patching vulnerabilities are automated for efficiency, enabling them to happen as soon as vulnerabilities are discovered. Networks are patched faster, and protected sooner, from newly discovered vulnerabilities.

Conclusion

Zero trust is a security paradigm that explicitly identifies users or devices and grants them just the right amount of access so that the business can operate with minimal friction while risks are reduced. Most organizations are early in their zero trust journey and exploring Zero Trust Network Access (ZTNA). Alongside ZTNA initiatives, network teams can use ZTNO to help them create an implementation roadmap for zero trust in their NetOps environment.

The six actionable pillars to automate ZTNO should establish a clear set of zero trust requirements for NetOps engineers to help keep the network secure. These pillars are:

1. Access Management
2. Audit and Control
3. Device Configuration Onboarding
4. Vulnerability Management Onboarding
5. Continuous Assessment
6. Reporting and Visibility

The first two pillars apply to the humans managing the network, while the latter four apply to the devices that make-up the network. In combination, they provide a seamless roadmap for implementing Zero Trust NetOps and adding resiliency and flexibility to the network, while helping network engineers move more quickly to manage change.

About BackBox

Backbox is a Network and Security Device Automation Platform that supports over 180 vendors, with thousands of pre-built automations and a scripting-free way to build new ones. Enterprises and service providers worldwide trust BackBox to automate and audit anything an admin could do manually, with reliable automations that are flexible, scalable, and contextually aware. From backups and OS updates to configuration compliance, BackBox gives you confidence that your automations will deliver the expected outcome every time.

Find out more at www.backbox.com