BACKBOX
SOLUTION BRIEF

FORTINET

Fortinet and BackBox Integrated Network Cyber Resilience Solution

Trusted Network and Security Device Automation

Solution Highlights

- Automate OS updates and vulnerability patches for all devices from Fortinet and other vendors across your network in a timely manner, to prevent known vulnerabilities from causing breaches.
- Automate backup of Fortinet FortiGate NGFWs and other security devices. Each backup is verified to ensure its integrity and can be restored with one click.
- Store backups off-site and encrypted for secure updates. Keeping a rich history of backups also helps with troubleshooting or in the event of an undetected vulnerability.
- Reduce the time and effort it takes to update systems to the latest OS releases.
- Support multi-step updates for older versions of FortiOS, Fortinet's OS security operating system.
- Fully support CIS Benchmark compliance out-of-the-box, including ongoing automated configuration audit, drift prevention, reporting, and optional automated remediation. Ensure your CMDB is always up-to-date and that security vulnerabilities don't go undetected with Dynamic Inventory capabilities.

The Challenge

Modern, multi-cloud, enterprise-class networks are incredibly complex and require constant changes to maximize uptime and minimize vulnerabilities. This complexity is exacerbated by the pace of change within networks to support new applications and services for businesses and their customers. Manually automating the configuration of all network and security devices to ensure business continuity can often be difficult, time-consuming, and prone to human error.

Network and security devices require constant OS updates, patches, and configuration changes to protect from vulnerabilities and be cyber resilient. Failure to perform these updates in a timely manner exposes the network to security threats and the potential for costly downtime. In the absence of regular backups, which often happens when backups are complex to perform or require manual steps, networks experience slower recovery from downtime following outages.

The Solution

To tackle these challenges, organizations need a trusted automation platform to make repetitive network tasks efficient and reliable, work within existing network architecture and operations, and scale for both enterprise and deployments. BackBox delivers such a platform with out-of-the-box capabilities for backup, OS updates, compliance auditing and auto-remediation, Dynamic Inventory Reporting, and closed-loop management of vulnerability patching.

BackBox and Fortinet Solution

The Fortinet and BackBox solution provides automated backup and single-click recovery of FortiGate NGFWs, eliminating the need for time-consuming and ineffective manual processes or creating and managing in-house scripts.

BackBox Dynamic Inventory collects asset information from FortiGate NGFWs and then reports on inventory information, including license information, device model, serial number, and more. Inventory information can also be passed to other systems, like an ITSM or CMDB, via the BackBox API.

BackBox can change operating system-level parameters on multiple devices with a single click. This allows admins to delegate administrative tasks to individuals who do not require full policy access, minimizing potential human errors that might lead to configuration errors.

BackBox also provides seamless integration to verify that Fortinet devices are configured in alignment with internal and industry security policies and regulations, such as the CIS Benchmarks, and can automatically remediate.

BENEFITS OF THE COMBINED SOLUTION:

- Automated, verified FortiOS updates of Fortinet devices to protect from vulnerabilities.
- Automated, reliable backups for Fortinet devices.
- Single-click disaster recovery and step-by-step disaster recovery procedures.
- Validation and automatic remediation of configurations against policies and regulations.
- Performance and status monitoring of Fortinet devices.
- Automated discovery of newly connected Fortinet devices for easy asset management.

BackBox Network Cyber Resilience Platform

BackBox is designed for complex, hybrid, multi-cloud, and multi-vendor networks. With BackBox, network teams, and service providers can save time and deliver better, more secure IT services.

BackBox offers a simple way to intelligently automate the backup, restoration, and compliance of all devices on a network by providing centralized configuration automation of devices such as firewalls, routers, switches, and load balancers. Each of these devices plays a critical role in the availability and security of an organization's network. BackBox ensures they all continue to function effectively and effortlessly, streamlining operations for optimal performance.

Employing centralized management for all device backups also allows BackBox to relay other vital information, such as the status of devices and the network status, to end users. This lets BackBox assist with predicting when and where outages are more likely to occur, helping organizations prevent such events.

Fortinet FortiGate NGFWs

FortiGate NGFWs simplify security complexity and provide visibility into applications, users, and networks. Innovative security processor units (SPUs) technology delivers high-performance application layer security services (NGFW, SSL inspection, and threat protection), coupled with the industry's fastest SSL inspection engine, to help protect against malware hiding in SSL/TLS encrypted traffic. The platform also leverages global threat intelligence to protect individual customers by using Fortinet's FortiGuard Security Subscription Services to enable visibility and control for next-generation protection against advanced threats, including zero-day attacks.

Use Case 1

CENTRALIZE AND AUTOMATE OS UPDATES AND VULNERABILITY PATCHES

The Challenge:
OS updates and patch management are a critical aspect of maintaining network security. The versions of OS that run on the network infrastructure must be closely managed to ensure continuity of service and remediation of known security vulnerabilities. However, manually keeping track of the frequent OS updates and patches of firewalls and other network and security devices is getting more challenging, especially with limited resources.

The Solution:
BackBox offers automated FortiOS updates and patches for Fortinet FortiGate NGFWs, and will do the same for network and security devices from 180 other vendors, all from a centralized location, and typically with a single automation. This eliminates the need to hop from one tool to another to update different devices, saving time and resources. With a single click, users can use BackBox to update FortiOS alongside hundreds of devices seamlessly.

Use Case 2

ENFORCE COMPLIANCE WITH CIS BENCHMARKS

The Challenge:
With configuration updates getting more frequent due to the acceleration of new threats and malicious actors, ensuring all security and network devices are up-to-date and compliant with CIS Benchmarks, internal policies, and industry regulations is challenging.

The Solution:
By eliminating the need to check device configuration for compliance manually, BackBox provides contextually-aware automation templates that remove the drudgery and reduce risk by validating that a specific configuration for Fortinet FortiGate NGFWs and devices from other vendors meets best practices and can automatically remediate those that do not. Rechecks can be scheduled to run daily or at whatever frequency desired. Administrators receive notifications of configuration drift and can auto-remediate to bring the organization back into compliance.

Use Case 3

AUTOMATE BACKUPS

The Challenge:
Manual backups for network and security devices like firewalls are time-consuming and prone to human errors. In addition to security infrastructure, network engineers must perform regular backups on routers, switches, and other network devices from multiple vendors, via numerous user interfaces, further increasing risk.

The Solution:
Seamless integration between BackBox and Fortinet FortiGate NGFWs enables automated, centralized, and secure backups for all configuration information from Fortinet devices and devices from other vendors. This ensures rapid recovery and minimal downtime.

Use Case 4

MONITOR PERFORMANCE AND STATUS

The Challenge:
To verify proper network operations and prevent issues from affecting the network, performance information and status of network and security devices should be checked regularly. However, writing automation scripts to perform these tasks can be very time-consuming, while manually performing these tasks is prone to human errors.

The Solution:
Through centralized management for all network device backups, BackBox collects and relays vital information, such as the status of Fortinet FortiGate NGFWs and devices from other vendors, to end users. This lets BackBox assist with predicting when and where outages are more likely to occur, which helps organizations take proactive actions to prevent such events.

BACKBOX

About BackBox

More than 500 enterprises worldwide trust BackBox as their preferred network cyber resilience platform. BackBox supports network devices from over 180 vendors, offering thousands of pre-built automations and a no-code way to create new ones. BackBox empowers teams with the confidence to automate critical network processes, maintain business continuity during disruptions, and recover swiftly. From backups and OS updates to configuration compliance and vulnerability management, BackBox ensures that automations deliver consistent, reliable outcomes.

To learn more, visit **backbox.com**

About Fortinet

Fortinet (NASDAQ: FTNT) makes possible a digital world that we can always trust through its mission to protect people, devices, and data everywhere. This is why the world's largest enterprises, service providers, and government organizations choose Fortinet to securely accelerate their digital journey. The Fortinet Security Fabric platform delivers broad, integrated, and automated protections across the entire digital attack surface, securing critical devices, data, applications, and connections from the data center to the cloud to the home office. Ranking #1 in the most security appliances shipped worldwide, more than 595,000 customers trust Fortinet to protect their businesses.

Learn more at **www.fortinet.com**