KILTER by BACKBOX

DATA SHEET

# Securing Kilter

ENSURING THE SECURITY OF MODERN NETWORK DEVICES

## Introduction

This document outlines the methods used to maintain a safe and secure operating environment. The information provided is intentionally high-level. If BackBox customers need more details, they can be shared upon request, provided a non-disclosure agreement (NDA) is in place.

### Key Considerations

- Kilter is primarily a virtual appliance that manages the entire platform, including the underlying operating system.
- Kilter is SOC 2 Type 2 certified. This certification ensures that security is a fundamental part of its development and delivery processes. Kilter has been verified by third parties to maintain ongoing, effective security controls. SOC 2 Type 2 reports are available upon request, subject to a signed NDA.

### Development Process and Internal Measures

The BackBox development environment is very secure.

- BackBox adheres to industry best practices and surpasses expectations in most areas. A formal Software Development Life Cycle (SDLC) is established and enforced.
- BackBox has independent third parties regularly conduct penetration testing.
- Static and dynamic code analysis testing is performed on every build of the platform to ensure security and code cleanliness.

© 2026 BackBox. All right reserved.

KILTER by BACKBOX

# The Kilter Platform

This section covers the on-premises management engine, cloud-hosted management engine, and on-premises offload engines (agents).

**Hardened Operation System**

- System libraries and binaries are minimized to only essential components.
- Kilter maintains Operating System updates; no manual updates of Operating System packages are required.

**Host-based Firewall Implemented to Restrict IP Access**

**Vulnerability Scanning, Penetration Testing, and Risk Assessments are Conducted Regularly**

**Secure Multi-tenancy and Role-based Access Control (RBAC)**

- Tenants are logically isolated.

**Secure Automations**

- All automations are run in an individual, ephemeral, and secure state, meaning they cannot overlap or interact with one another.

**Secure Communication**

- All communications are encrypted using TLS or a service-specific configuration.
  - Communication between the management engine and offload engines (agents) is supported in both directions.
  - Management ------> Agent
  - Agent ------> Management
    - This direction supports the Zero Trust Network Architecture model.

# Cloud-hosted Kilter Instance

We have numerous measures in place to safeguard our cloud-hosted service. These include:

- Cloud service providers' native tools are used to ensure access is restricted to customers and employees.
- Access to hosted instances is restricted to customers and the BackBox DevOps team.
- Optional AI Enrichment & Automation Creation Features.
- BackBox now offers AI licenses to accelerate teams whose Kilter platform is internet-enabled, enabling users to resolve issues faster.

© 2026 BackBox. All right reserved.

BACKBOX

# About BackBox

More than 500 enterprises worldwide trust Kilter by BackBox as their preferred network cyber resilience platform. Kilter supports network devices from over 180 vendors, offering thousands of pre-built automations and a no-code way to create new ones. Kilter 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, Kilter ensures that automations deliver consistent, reliable outcomes.

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