# Backup Security & Compliance

This report details the configurations of all backup servers. It checks alignment with security best practices for the operating system and Veeam backup components. Use this report for a direct overview of your backup infrastructure's security compliance.

## Report Parameters

| | |
|---|---|
| Infrastructure objects: | Veeam Backup & Replication |
| Best practices types: | All items |
| Check result: | All items |

## Summary

### Backup Server Security & Compliance Status

| | |
|---|---|
| Total backup servers: | 7 |
| Passed: | 0 |
| Not implemented: | 7 |
| Unable to detect: | 0 |
| Other: | 0 |

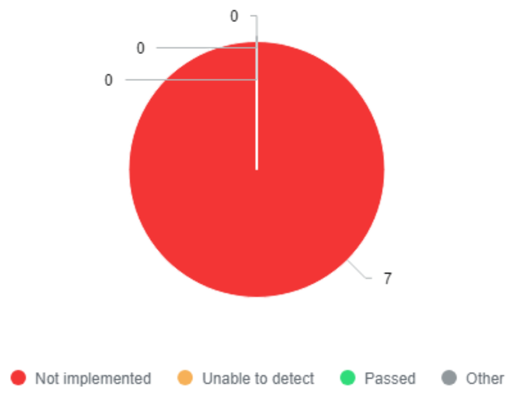
### Missed Security & Compliance Checks

| | |
|---|---|
| Unable to detect: | 8 |
| Not implemented: | 115 |
| Suppressed: | 0 |
| Not checked: | 6 |

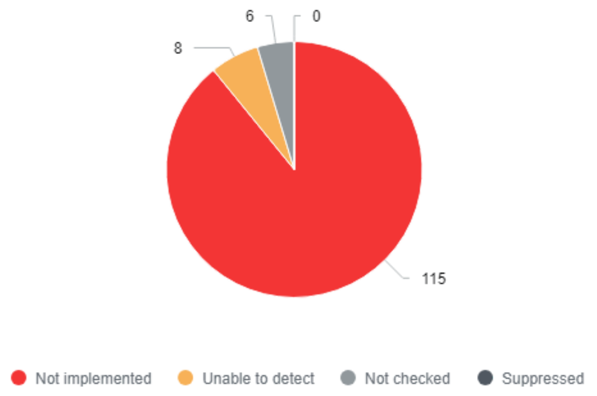
### Security & Compliance Last Check

| | |
|---|---|
| Less than a week: | 6 |
| From week to a month: | 0 |
| More than a month: | 1 |

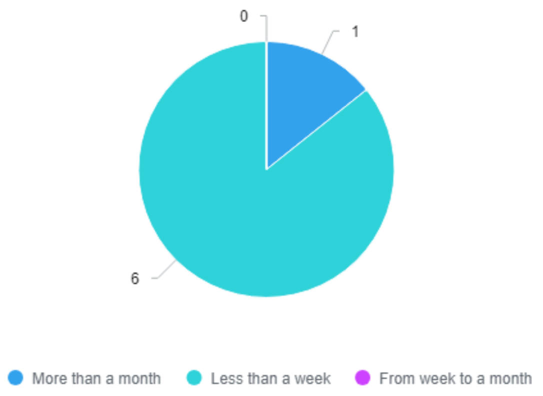
## Backup Server Security & Compliance Status



## Missed Security & Compliance Checks



## Security & Compliance Last Check



## Overview

### Not implemented

| Backup Server | Security & Compliance Last Check | Backup Infrastructure Security Best Practices | Product Configuration Best Practices | Best Practices Suppressed | Backup Server Security & Compliance Status |
|---|---|---|---|---|---|
| 172.24.30.100 | 9/16/2025 12:00 AM | 12 of 14 | 12 of 23 | 0 | Not implemented |
| backupserver001.tech.local | 9/16/2025 12:00 AM | 2 of 14 | 11 of 22 | 0 | Not implemented |
| backupserver002.tech.local | 9/16/2025 12:00 AM | 12 of 14 | 13 of 23 | 0 | Not implemented |
| onebackup.tech.local | 9/16/2025 12:00 AM | 13 of 14 | 12 of 23 | 0 | Not implemented |
| srv17.tech.local | 12/30/1899 2:00 AM | 2 of 14 | 10 of 22 | 0 | Not implemented |
| srv18.tech.local | 9/16/2025 12:00 AM | 3 of 14 | 11 of 22 | 0 | Not implemented |
| srv98.tech.local | 9/16/2025 12:00 AM | 3 of 14 | 10 of 22 | 0 | Not implemented |

## Details

### 172.24.30.100

| Backup Server | Best Practice Name | Best Practice Check Result | Recommendation |
|---|---|---|---|
| 172.24.30.100 | Address space layout randomization (ASLR) should be used | Passed | To reduce the risk of compromise, program data should be stored in random memory locations. |
| 172.24.30.100 | All backups should have at least one copy (the 3-2-1 backup rule) | Not implemented | To be compliant with the 3-2-1 rule, at least one backup copy job should be created or a scale-out backup repository with the copy mode or archive tier should be added. |
| 172.24.30.100 | Audit binaries should be owned by root | Passed | Access to the audit binaries should be restricted to prevent unauthorized changes that may affect system performance or result in incomplete event logging. |
| 172.24.30.100 | Auditd should be enabled and configured to forward audit logs | Passed | To ensure that the system is properly monitored, the Linux audit system should be enabled and configured with log forwarding. |
| 172.24.30.100 | Backup encryption passwords should follow length and complexity recommendations | Passed | To minimize the possibility of unauthorized access, passwords should meet Veeam requirements for password complexity. The password is at least 12 characters long. The password contains at least one uppercase character, one lowercase character, one special character and one numeric character. |
| 172.24.30.100 | Backup jobs to cloud repositories should use encryption | Passed | To reduce the cloud attack surface, job-level encryption should be enabled. |
| 172.24.30.100 | Backup server should not be a part of the production domain | Passed | Adding the backup server and other backup infrastructure components to a management domain in a separate Active Directory forest is the best practice for building the most secure infrastructure. For medium-sized and small environments, backup infrastructure components can be placed to a separate workgroup. |
| 172.24.30.100 | Backup services should be running under the LocalSystem account | Not implemented | The account used to run Veeam services must be a LocalSystem account. |
| 172.24.30.100 | Compliance mode should be used for repositories with backup immutability enabled | Passed | The Compliance retention mode should be used for object storage repositories with immutability enabled. This is a more secure option compared to the Governance retention mode. |
| 172.24.30.100 | Configuration backup should be enabled and use encryption | Not implemented | Configuration backup should be enabled to reduce the risk of data loss and manage the Veeam Backup & Replication configuration database easier. Data encryption for configuration backup should be enabled to secure sensitive data stored in the configuration database. |
| 172.24.30.100 | Credentials and encryption passwords should be rotated at least annually | Passed | For all user accounts added to the Credentials Manager, Cloud Credentials Manager, and Password Manager, passwords should be changed at least once a year. |
| 172.24.30.100 | Email notifications should be enabled | Not implemented | Email notifications should be enabled to monitor job statuses. |
| 172.24.30.100 | Firewall should be enabled | Passed | For Windows: Microsoft Defender Firewall with Advanced Security should be turned on. Also, rules for inbound and outbound connections should be set up according to your infrastructure and Microsoft best practices. For Linux: The firewall should be turned on. Also, rules for inbound and outbound connections should be configured according to your infrastructure and security best practices. |
| 172.24.30.100 | Hardened repositories should have the SSH Server disabled | Passed | SSH connection is necessary only for the deployment and upgrade of Veeam Data Mover. For security purposes, after adding the hardened repository to the backup infrastructure, the SSH connection |