# Cloud REVIEWER V5.02

# Security Monitoring OVERVIEW

This document describes the Security Controls applied to Cloud Reviewer V5.02 as of August 2023.

**THE CONTENT IN THIS DOCUMENT IS INTENDED FOR USE AS PART OF A PROPOSAL DOCUMENT AND IS THEREFORE ALWAYS SUBJECT TO THE APPROPRIATE REVIEW AND APPROVAL PROCESSES TO ENSURE ACCURACY AND COMPLIANCE WITH CURRENT RESPONSE GUIDELINES. SCREENSHOOTS INCLUDED AS EXAMPLES CAN CHANGE IN GRAPHIC FORMAT BUT NOT IN CONTENTS. TASK AUTOMATION CAN CHANGE DUE TO TECHNOLOGY EVOLUTIONS.**

# Copyright and Restricted Rights Legend

Via della Pace, 154
Grosseto, 58015
Italy

https://www.securityreviewer.net
https://securityreviewer.atlassian.net

# Notices

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Security Reviewer Suite (Cloud Reviewer included) intellectual rights are registered at Italian's SIAE OLAF Office as well as at Washington Copyright Office. Other names may be trademarks of their respective owners.

# Overview

**Cloud Reviewer SaaS** is an all-one Cloud-native application security suite platform, multi-tenant, fully managed and provisioned as a service. Analyses like 3rd parties' libraries and open source (SCA), Static (SAST) and Dynamic (DAST) analyses at your hand with complete management of vulnerabilities found, False positives, results, reports, data export. **Mobile binary analysis** and **Firmware Analysis** are also available in the Enterprise version.

Cloud Reviewer is part of Security Reviewer Suite.

## SAST

Scans uncompiled code and doesn't require complete builds. Sets the new standard for instilling security into modern development.
An application can be made of different Programming Languages.
Cloud Reviewer recognizes all programming languages that are composing the analyzed app, as well as the Dominant Language (i.e. the Language with higher LOC).

## DAST

With **Dynamic Reviewer DAST** Safe-PenTest module, you can inspect your web application as blackbox during running, no need to backup your data, as well as in whitebox safe mode (discovered exploits won't be executed). It detects vulnerabilities, show the Exploits, but doesn't apply them. It also detects Client-side vulnerabilities.

## SCA

**SCA** (Software Composition Analysis) identifies project dependencies on 3rd-party components. **SCA** will automatically determine if those components have known, publicly disclosed, vulnerabilities as well as licenses-related issues.

## Mobile binary Analysis

**Mobile Reviewer** is a worldwide brand of Security Reviewer offered as on demand service for MAST (Mobile binary Analysis). A robust, cloud infrastructure is behind this offer. It provides: Mobile binary inspection (Android, iOS, Windows Mobile) and Hybrid Analysis (Source Code and binary correlated).

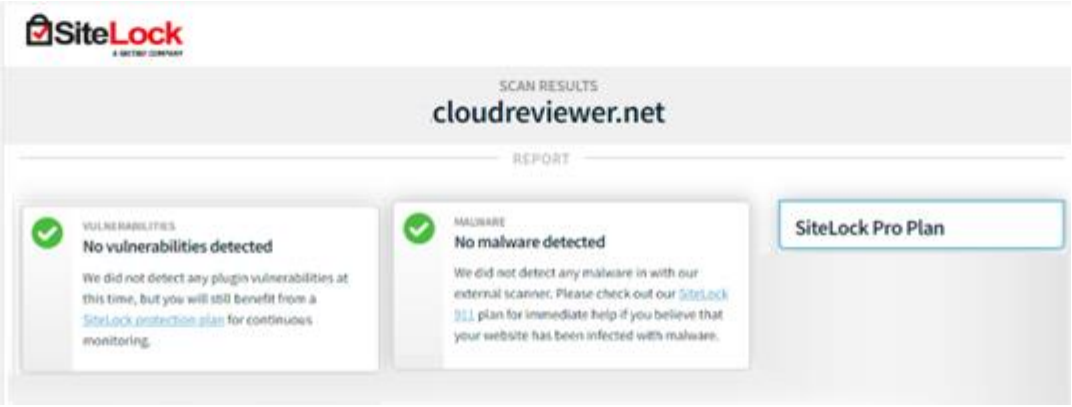
## Firmware Analysis

Firmware Reviewer on demand service provides in-depth firmware analysis (binaries, file systems, containers, virtual machines, IoT, UEFI, Appliances, Network Devices, Smart Meters, Surveillance devices, Drones, etc.), allowing to explore vulnerabilities at the same time to keeping the software securely in your own hands, for your eyes only. It can be used for a bunch of binary file formats, with No need of related physical device.

# Web Site Security Monitoring

Our primary defense is **Web Site Security Monitoring** that includes daily **Web Site scans** to find threats, real-time notifications, automated malware removal, vulnerability and patching to fix threats, a **Web Application Firewall** to block and prevent harmful traffic before it ever reaches our site, a **Content Delivery Network** (CDN) to accelerate our site speed and a **Firewall PCI** Report to help our site comply with Banking Institutions. We are using **SiteLock*Business** Website Security software, which guards Sensitive Information and Customer Data, protects our Cloud services from malware, DDoS attacks, phishing scams, bad bots and other types of malicious code and cyber threats. This includes the protection of the site code and Web applications.

Customers under NDA can ask for a copy of latest Security Reports.



SiteLock

SCAN RESULTS

cloudreviewer.net

REPORT

VULNERABILITIES

No vulnerabilities detected

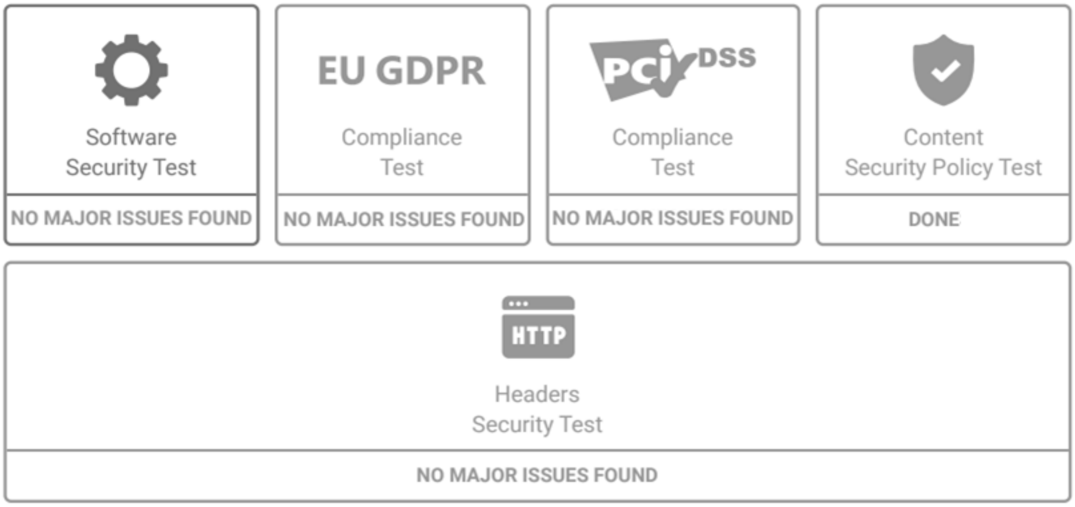
We did not detect any plugin vulnerabilities at this time, but you will still benefit from a SiteLock protection plan for continuous monitoring.

MALWARE

No malware detected

We did not detect any malware in with our external scanner. Please check out our SiteLock 911 plan for immediate help if you believe that your website has been infected with malware.

SiteLock Pro Plan



Software Security Test

NO MAJOR ISSUES FOUND

EU GDPR Compliance Test

NO MAJOR ISSUES FOUND

PCI DSS Compliance Test

NO MAJOR ISSUES FOUND

Content Security Policy Test

DONE

HTTP Headers Security Test

NO MAJOR ISSUES FOUND

# Trust Seal

Trust plays an important role in the success of any SaaS Service. Online users tend to abandon a SaaS platform, and others will not feel comfortable sharing information if they see a site as weak. So, for begin users to trust and remove their doubts, one way of doing this is by displaying a SiteLock*Business **Trust Seal** on our site. Once our customers see this, they will know that they are viewing a secure and malware-free site. The Trust Seal is a badge that we integrated on your website to ensure customers feel safe visiting and providing information to our site.

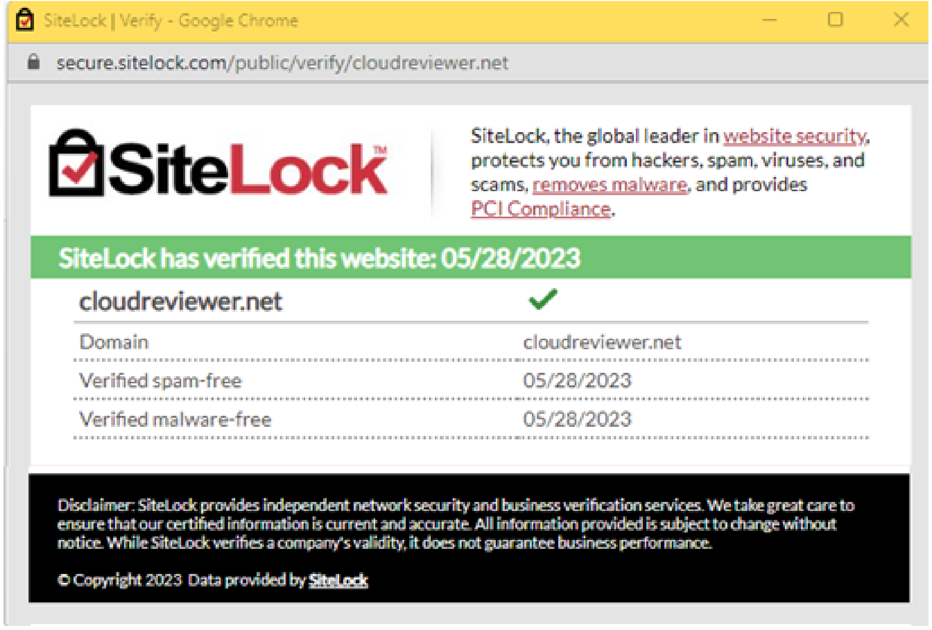
SiteLock*Business Trust Seal is active in our website, it works by pulling data from SiteLock secure scanners running on our website, and not through the Firewall. The Trust Seal is visible on every page footer:

CLOUDREVIEWER.NET
SiteLock
SECURE
Passed
28-May-2023

If SiteLock secure scanners determine our website is clean, it will display "Passed" in green along with the date it determined it was clean. Please note that the date displayed will be the last scan that was run and came back clean.

If SiteLock secure scanners determine our site got infected with malware or has a vulnerability and was not resolved after 72 hours, the Trust Seal will automatically be removed. After resolved these issues, the Trust Seal will automatically be displayed again on our website.

If you click on the Trust Seal, it will bring up a new window as shown below.



secure.sitelock.com/public/verify/cloudreviewer.net

SiteLock, the global leader in website security, protects you from hackers, spam, viruses, and scams, removes malware, and provides PCI Compliance.

SiteLock has verified this website: 05/28/2023

cloudreviewer.net ✓

| | |
|---|---|
| Domain | cloudreviewer.net |
| Verified spam-free | 05/28/2023 |
| Verified malware-free | 05/28/2023 |

Disclaimer: SiteLock provides independent network security and business verification services. We take great care to ensure that our certified information is current and accurate. All information provided is subject to change without notice. While SiteLock verifies a company's validity, it does not guarantee business performance.

© Copyright 2023 Data provided by SiteLock

# Third-Party PenTest

Further than Web Site Security Monitoring, we provide a daily-based **Third-party PenTest**, using **intruders.io** Pro and **ImmuniWeb** services. We obtain **weekly SOC2 and GDPR compliance reports**, that we share with existing Customers under NDA. Modern hackers don't wait to act and usually execute their attacks within days of new vulnerabilities being discovered. Intruder.io ensures that we are secured against even the very latest threats and have time to act before it's too late. We obtain:

- **Attack surface monitoring**. Reduce our attack surface by continuously monitoring for changes and exposures
- **Reporting & Compliance**. Regularly pass security compliance certifications and standards, such as ISO 27001/27002, SOC 2 and Cyber Essentials, by evidencing that vulnerability scanning, and penetration testing processes are in place
- **Intelligent results.** Quickly understand our real attack surface and prioritize fixing the security issues that leave us most exposed
- **Vanguard vulnerability management**. Find what scanners can't with Intruder Vanguard - a continuous penetration testing service supported by some of the world's leading security professionals
- **External vulnerability scanning**. Hackers are constantly looking for security flaws they can use to compromise sensitive information or steal personal data for financial gain, or to cause havoc and disruption for businesses all over the globe. To do this, they make use of a wide range of tools and vulnerability scanners to automate their efforts and find new targets. So, external vulnerability scanning is an essential process of protecting our business, by finding our security weaknesses before the hackers do
- **Internal vulnerability scanning**. While our external network is the easiest to access for hackers, and available for attack 24/7, our internal systems can also be reached with a little extra effort. For example, by an email containing a malicious attachment, or link to a web page that exploits known unpatched software on an employee's device. Similarly, unpatched software or the lack of hardening of internal systems can help an attacker move around internal systems once they've gained an initial foothold. Internal vulnerability scanner allows us to eliminate threats to our business, by discovering security holes in our systems automatically, as soon as new vulnerabilities are released
- **Penetration testing**. We apply a portfolio of penetration testing services, delivered to the industry's highest standard of excellence by properly qualified security professionals. Whether we need a penetration test to comply with security regulations such as ISO 27001 and PCI DSS, or we wish to review the security of your internet-facing applications for our own peace of mind, external experienced penetration testers will deliver a service that fits our needs
- **Web application vulnerability scanning**. The complexity of software development means web application vulnerabilities are one of the most popular attack vectors. Our Web application vulnerability scanning helps developers build secure products by integrating into their existing environment, and continuously catching vulnerabilities as they're being introduced.

# Compliance

We regularly submit Cloud Reviewer to third-party scanning, for verifying emerging regulatory and compliance requirements:

Protected by intruder

ImmuniWeb® AI for Application Security

AICPA SOC

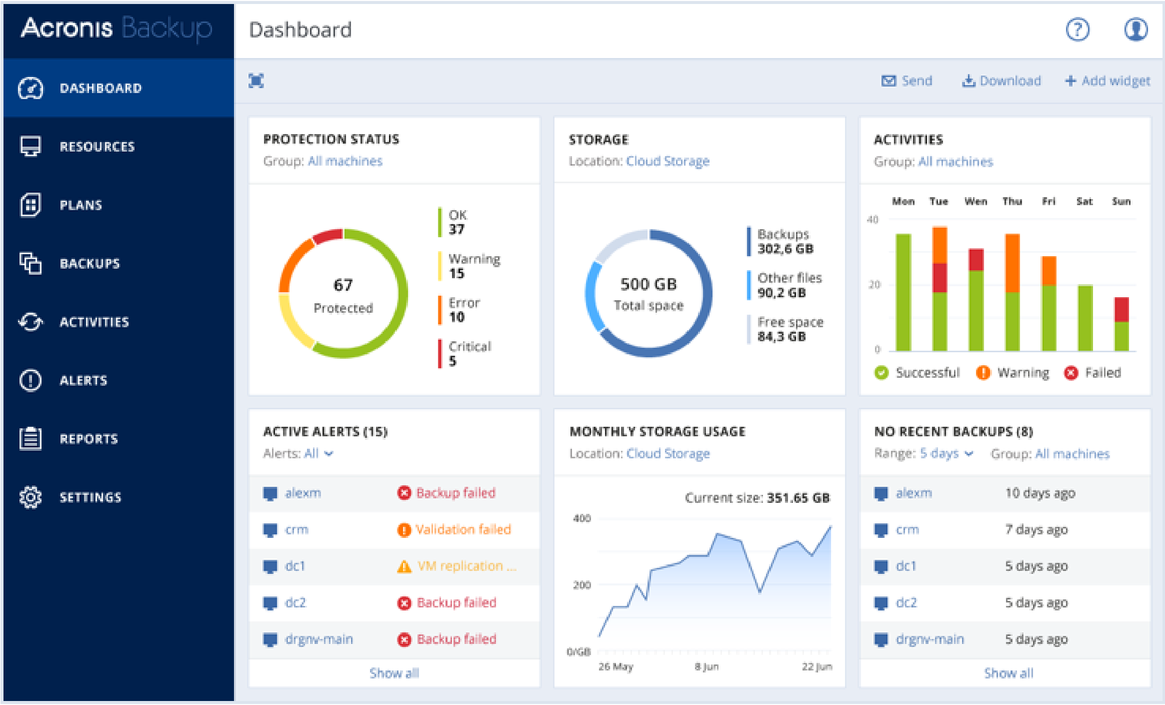
CYBER ESSENTIALS

- EU & UK GDPR
- Singapore PDPA
- Hong Kong PDPO
- South Africa POPIA
- India IT Act
- Brazil LGPD
- HIPAA / HITECH
- FTCA, GLBA, FCRA / FACTA
- NIST SP 800, FISMA, CMMC
- New York SHIELD, NYDFS
- California CCPA, CPRA
- ISO 27001 / ISO 27002
- Singapore MAS
- PCI DSS

# Two different Backups

We regularly execute Secure backups of our Web Sites to protect against ransomware, hardware corruption and human errors with two different reliable backup solutions:

- **Acronis Backup**. One of the world's leading data backup technologies: a solution that combines "extremely safe" with "extremely easy". We protect our business with automated full image-based backups of our entire system, files, and data every 4 hours. 15 seconds - that's all - Acronis Backup needs to recover our data. The Acronis dashboard shows all back-restore events.



ACTIVE ALERTS (15)
Alerts: All

| | |
|---|---|
| alexm | Backup failed |
| crm | Validation failed |
| dc1 | VM replication ... |
| dc2 | Backup failed |
| drgnv-main | Backup failed |

Show all

NO RECENT BACKUPS (8)
Range: 5 days Group: All machines

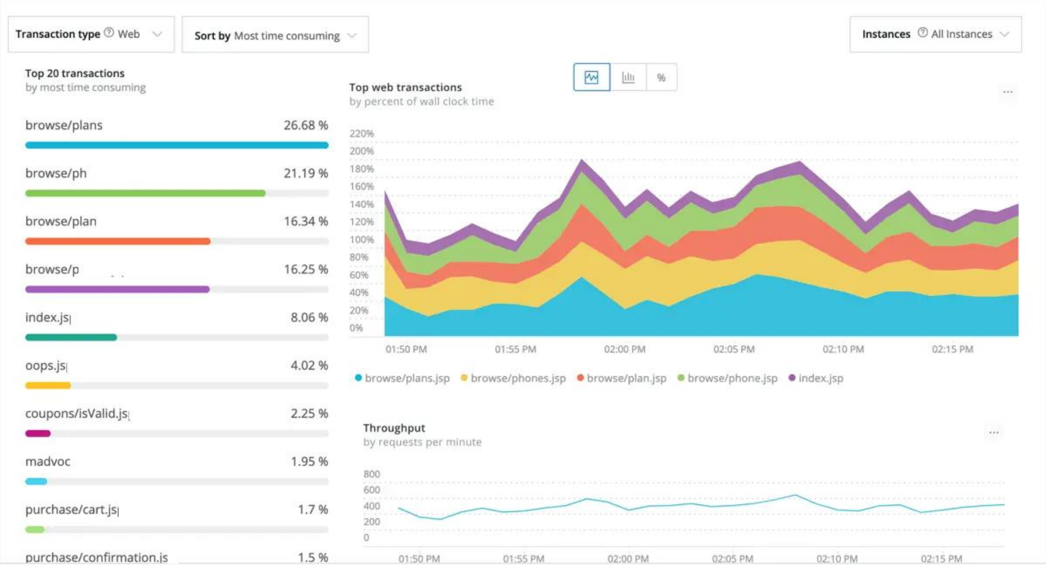
| | |
|---|---|
| alexm | 10 days ago |
| crm | 7 days ago |
| dc1 | 5 days ago |
| dc2 | 5 days ago |
| drgnv-main | 5 days ago |

Show all

- **Online Backup**. We scheduled automatic online daily backups of all site files, folders, and databases via secure connection to SiteLock. With SiteLock Website Backup, we can choose the version to restore or download our backed-up files in one click. All online backup data is encrypted in transit and stored in a secure SOC2 & HIPAA compliant data environment so customers can be sure their data and their business are safe. In the SiteLock Dashboard, we can see all the relevant information and notifications – including backup history, status, and storage space used. Online third-party backup services bring an elite level of security to the backup process, as these bypasses the vulnerabilities often attached to backup plugins. These vulnerabilities could potentially allow threat actors to access data or even perform functions that should be limited to administrative-level users

# Infrastructure Observability

Another level of defense we provide, is our **Infrastructure Observability** solution, based both on commercial and open source **APM** solutions. This provides a 360-wide platform observability and monitors our entire application stack, getting a live and in-depth view of our Network, Infrastructure, Applications, End-user experience, Machine Learning models and altering in case on Service-down, Performances bottlenecks, Recurrent errors. It also monitors the Response time, as an average of the total time spent across all Web Transactions occurring within a selected time frame on the server-side.



Transaction type Web

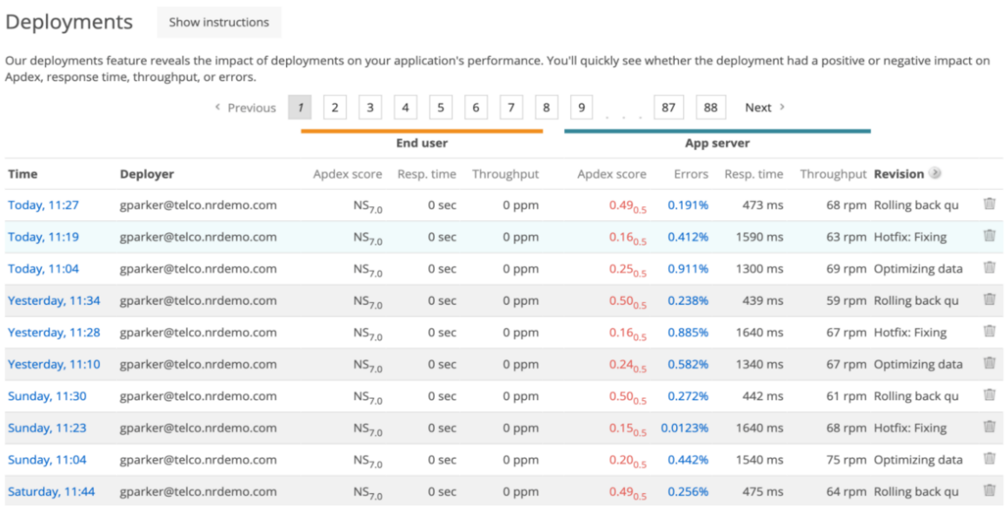
Sort by Most time consuming

Instances All Instances

**Top 20 transactions**
by most time consuming

| | |
|---|---|
| browse/plans | 26.68 % |
| browse/ph | 21.19 % |
| browse/plan | 16.34 % |
| browse/p | 16.25 % |
| index.js | 8.06 % |
| oops.js | 4.02 % |
| coupons/isValid.js | 2.25 % |
| madvoc | 1.95 % |
| purchase/cart.js | 1.7 % |
| purchase/confirmation.js | 1.5 % |

Also, it monitors Throughput as requests per minute through the application. Further, it measures Error rates as the percentage of errors over a set time period for our application, the Most Time-Consuming Transactions, Transaction Metrics and Traces, Service Map as how our distributed apps and services are performing, Performance of External Services, and Deployment Analysis, History, and Comparison.



## Deployments

Show instructions

Our deployments feature reveals the impact of deployments on your application's performance. You'll quickly see whether the deployment had a positive or negative impact on Apdex, response time, throughput, or errors.

‹ Previous 1 2 3 4 5 6 7 8 9 . . . 87 88 Next ›

| | | End user | | | App server | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Time** | **Deployer** | Apdex score | Resp. time | Throughput | Apdex score | Errors | Resp. time | Throughput | **Revision** |
| Today, 11:27 | gparker@telco.nrdemo.com | NS$_{7.0}$ | 0 sec | 0 ppm | 0.49$_{0.5}$ | 0.191% | 473 ms | 68 rpm | Rolling back qu |
| Today, 11:19 | gparker@telco.nrdemo.com | NS$_{7.0}$ | 0 sec | 0 ppm | 0.16$_{0.5}$ | 0.412% | 1590 ms | 63 rpm | Hotfix: Fixing |
| Today, 11:04 | gparker@telco.nrdemo.com | NS$_{7.0}$ | 0 sec | 0 ppm | 0.25$_{0.5}$ | 0.911% | 1300 ms | 69 rpm | Optimizing data |
| Yesterday, 11:34 | gparker@telco.nrdemo.com | NS$_{7.0}$ | 0 sec | 0 ppm | 0.50$_{0.5}$ | 0.238% | 439 ms | 59 rpm | Rolling back qu |
| Yesterday, 11:28 | gparker@telco.nrdemo.com | NS$_{7.0}$ | 0 sec | 0 ppm | 0.16$_{0.5}$ | 0.885% | 1640 ms | 67 rpm | Hotfix: Fixing |
| Yesterday, 11:10 | gparker@telco.nrdemo.com | NS$_{7.0}$ | 0 sec | 0 ppm | 0.24$_{0.5}$ | 0.582% | 1340 ms | 67 rpm | Optimizing data |
| Sunday, 11:30 | gparker@telco.nrdemo.com | NS$_{7.0}$ | 0 sec | 0 ppm | 0.50$_{0.5}$ | 0.272% | 442 ms | 61 rpm | Rolling back qu |
| Sunday, 11:23 | gparker@telco.nrdemo.com | NS$_{7.0}$ | 0 sec | 0 ppm | 0.15$_{0.5}$ | 0.0123% | 1640 ms | 68 rpm | Hotfix: Fixing |
| Sunday, 11:04 | gparker@telco.nrdemo.com | NS$_{7.0}$ | 0 sec | 0 ppm | 0.20$_{0.5}$ | 0.442% | 1540 ms | 75 rpm | Optimizing data |
| Saturday, 11:44 | gparker@telco.nrdemo.com | NS$_{7.0}$ | 0 sec | 0 ppm | 0.49$_{0.5}$ | 0.256% | 475 ms | 64 rpm | Rolling back qu |