360°
Powered by Tempus

Audit of Xcitium Transparency Page

Q1 2025

MRG Effitas

MRG Effitas Ltd.

MRG Effitas is a world-leading, independent IT security efficacy testing & assurance company. We are trusted by antimalware vendors across the world.

Management team:
Chris Pickard
Chief Executive Officer

Zsombor Kovacs
Chief Technical Officer

Website:
www.mrg-effitas.com

Email:
contact@mrg-effitas.com

Twitter:
@mrgeffitas

Contents

Introduction

MRG Effitas is recognised globally as a world leader in independent IT research.

We specialize in providing comprehensive and reliable evaluations of antivirus efficacy, enabling businesses and consumers to make informed decisions about the best antivirus solutions available in the market. Our core focus is to assess the effectiveness of various antivirus solutions.

In this audit report, we present the results of our evaluation of a Transparency Page maintained by Xcitium. The Transparency Page contains telemetry data collected from endpoints weekly and includes information about unknown files that are classified as Clean, Potentially Unwanted Applications (PUA) or Malware by Valkyrie Verdict engine and threat intelligence system.

The telemetry data collected by the antivirus solution provider is an important source of information that provides valuable insights into the performance of the antivirus software. The data provides an overview of the security threats faced by users, including the types of threats encountered and the frequency of these threats.

The Transparency page is available here:
https://www.xcitium.com/labs-statistics/

Executive Summary

This Certification Programme is designed to serve as a reflection of product efficacy based on the audit of the telemetry results.

MRG Effitas was engaged to audit and validate the results presented on the Transparency Page. The objective of this audit was to evaluate the accuracy and reliability of the telemetry data presented on the Transparency Page and assess the ability of the antivirus software to detect and mitigate security threats.

To ensure the validity and reliability of our audit results, we selected representative sample sets of files from the Clean, PUA, and Malware categories. We used a statistical calculation to determine the appropriate sample size for each category, with a 95% confidence level and a 5% error rate.

The sample size calculation involved analysing the total number of files in each category and determining the minimum number of files required to achieve a statistically significant result. We used a formula that considered the sample size, the level of confidence desired, and the margin of error.

Based on our calculations, we randomly selected samples from each category. This ensured that our audit results represented the entire set of Clean, PUA, and Malware files and provided a reliable assessment of the antivirus software's effectiveness in detecting and mitigating security threats.

Our auditors thoroughly analysed the randomly selected sample of files, using a range of testing techniques to validate the accuracy of the telemetry data presented on the Transparency Page. This included analysing the file characteristics, behaviour, and other attributes to ensure that the files were correctly classified by the antivirus software.

Overall, our audit report provides a comprehensive assessment of the effectiveness of the antivirus software based on a statistically significant sample of files from the Clean, PUA, and Malware categories. Our findings demonstrate the reliability and accuracy of the telemetry data presented on the Transparency Page and provide valuable insights into the performance of the antivirus software in detecting and mitigating security threats.

During our Q1 2025 Audit, the Xcitium Transparency Page powered by the Valkyrie Verdict engine and threat intelligence system managed to attain our certifications.

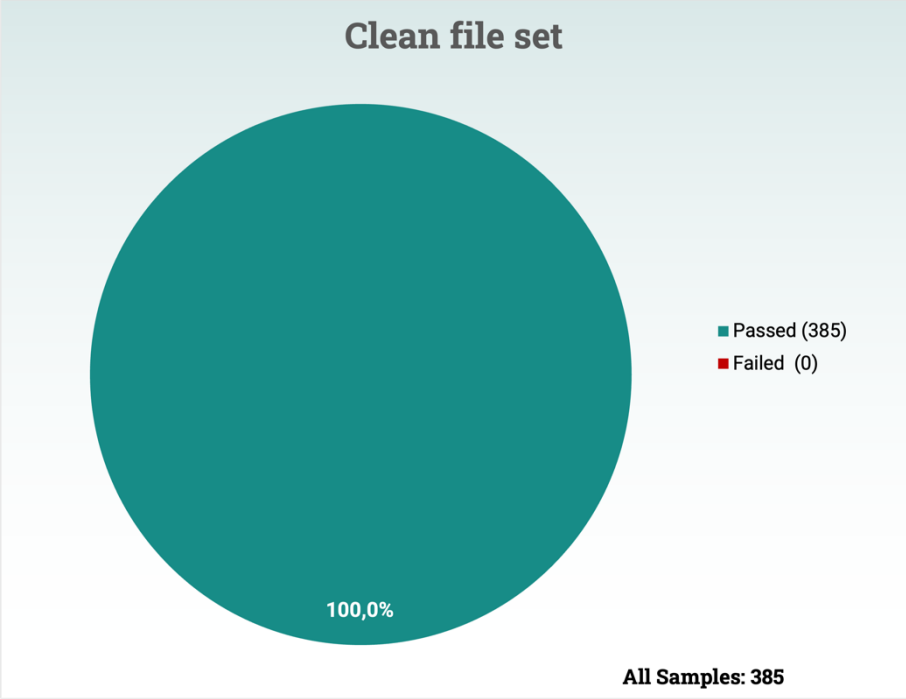
Tests Employed

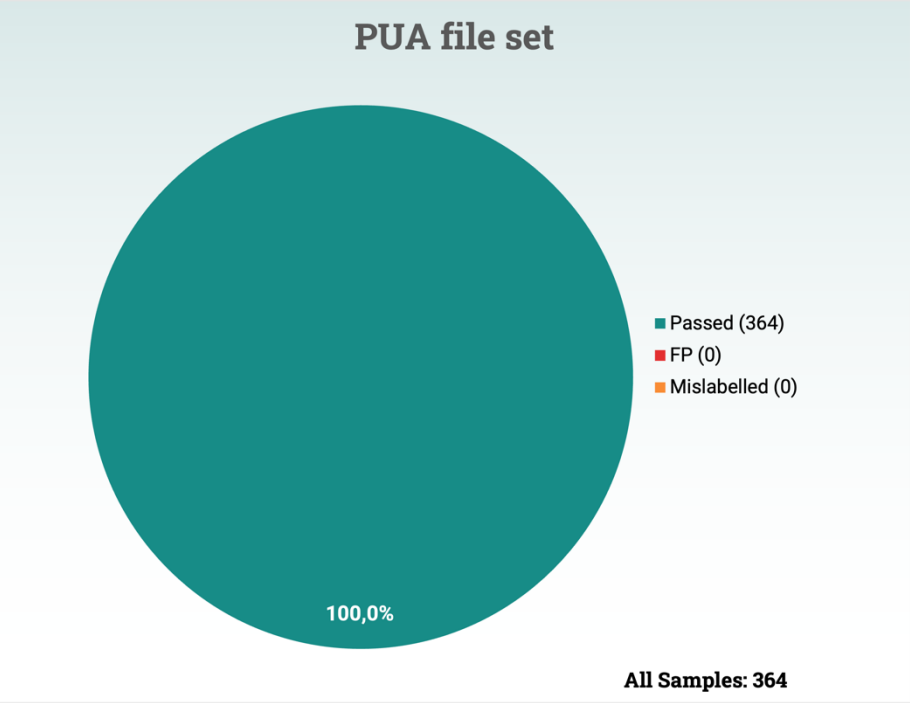
In this audit (Q1 2025), we ran the following tests:

Audit of the Clean file set

Clean files are computer programs that have been verified as safe and free of any malicious content. These files are essential for the proper functioning of computer systems and are usually distributed by legitimate sources. Clean files can include system files, software programs, and other applications that the software developer has tested and verified. It is essential to ensure that only clean files are installed on a system to prevent the introduction of malware or other security threats. Antivirus software can scan and verify files as clean, providing an added layer of protection against potential security risks.

The total file size of the "% of the unknown that turn out to be Clean" column was **948 567**. Based on the sample size calculation we randomly selected **385** samples for the audit.





Audit of the PUA / Adware file set

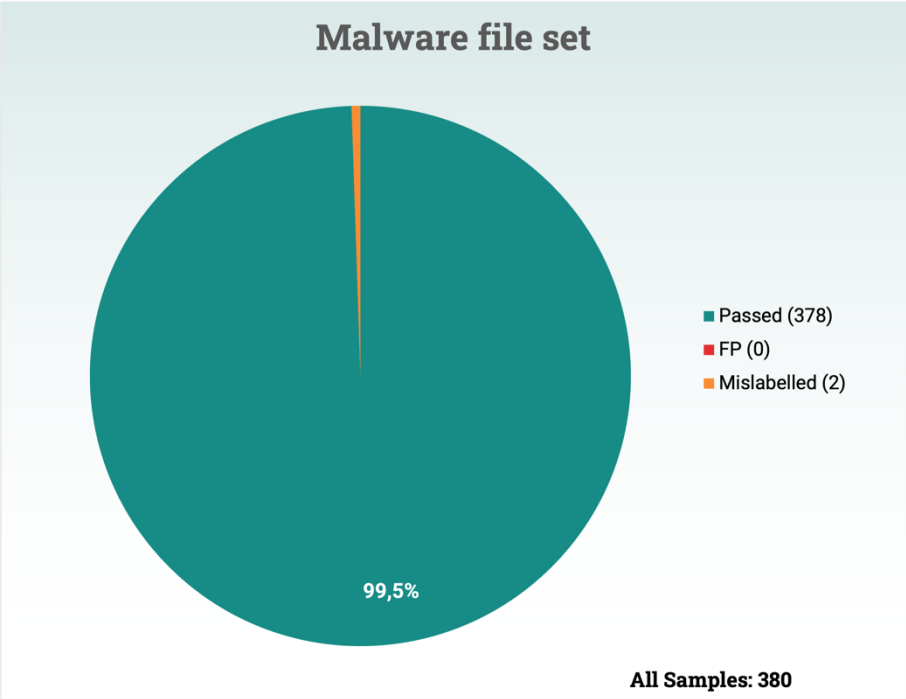
The PUA samples are deceptive, or potentially unwanted applications (PUA), that are not malicious but are generally considered unsuitable for most home or business networks. They usually contain adware, install toolbars, or have other vague objectives. They may also contribute to consuming computing resources or network bandwidth. PUAs can be deceptive, harmful, hoax, show aggressive popups and mislead or scare the user. They may provide some unconventional ways of uninstalling the application, maybe retain some of their components on the device without the user's consent.

The total file size of the "% of the unknown that turn out to be PUA" column was **6 645**. Based on the sample size calculation we randomly selected **364** samples for the audit.

Audit of the Malware file set

Malware files are one of the biggest threats facing computer systems today. Malware is specifically designed to infiltrate and harm computer systems, steal sensitive information, and compromise security. Malware constantly evolves, with new and more sophisticated strains. This makes it challenging for security professionals to keep up with the latest threats and develop effective strategies to combat them. Malware can have devastating consequences for businesses and individuals, so investing in robust antivirus software and implementing cybersecurity best practices are crucial.

The total file size of the "% of the unknown that turn out to be Malware" column was **33 731**. Based on the sample size calculation we randomly selected **380** samples for the audit.



Certification

The quarterly MRG Effitas certification is given if we cannot find failed cases during the audit of the "% of the unknown that turn out to be Clean" set, and the value of the “% of Infection/Breach” is zero percent.

The "% of the unknown that turn out to be PUA” and “% of the unknown that turn out to be Malware" columns audits are not part of the certification.

Certified

The Xcitium Transparency Page is awarded by the MRG Effitas Certification for Q1 2025

Appendix

Methodology of the audit process

1. At the end of each quarter, we add up the sample numbers in each file view columns and calculate how many samples need to be randomly selected from the set for inspection.
2. The sample size calculation is based on this process: 95% confidence level with a 5% margin of error.
3. Three sample sets are created. The first set contains randomly selected samples from the "% of the unknown that turn out to be Clean" column, the second set contains randomly selected samples from the "% of the unknown that turn out to be PUA" and the third set contains randomly selected samples from the "% of the unknown that turn out to be Malware" column.
4. The selected sample set then goes through our data analysis process.
5. During the analysis, we use third-party services and, if necessary, we manually analyse the files as well.

Results of the "% of the unknown that turn out to be Clean" column audit.

- **The result is marked as “Passed”** If it is proven that all selected samples are clean.
- **The result is marked as “Failed”** If it turns out that at least one of the selected samples is PUA or malware.

Results of the "% of the unknown that turn out to be PUA" column audit.

- **The result is marked as “Passed”** If it is proven that all selected samples are PUA.
- **The result is marked as “FP”** If it turns out that at least one of the selected samples is clean.
- **The result is marked as “mislabelled”** If it turns out that at least one of the selected samples is malware.

Results of the "% of the unknown that turn out to be Malware" column audit.

- **The result is marked as “Passed”** If it is proven that all selected samples are malicious.
- **The result is marked as “FP”** If it turns out that at least one of the selected samples is clean.
- **The result is marked as “mislabelled”** If it turns out that at least one of the selected samples is PUA.

MRG Effitas