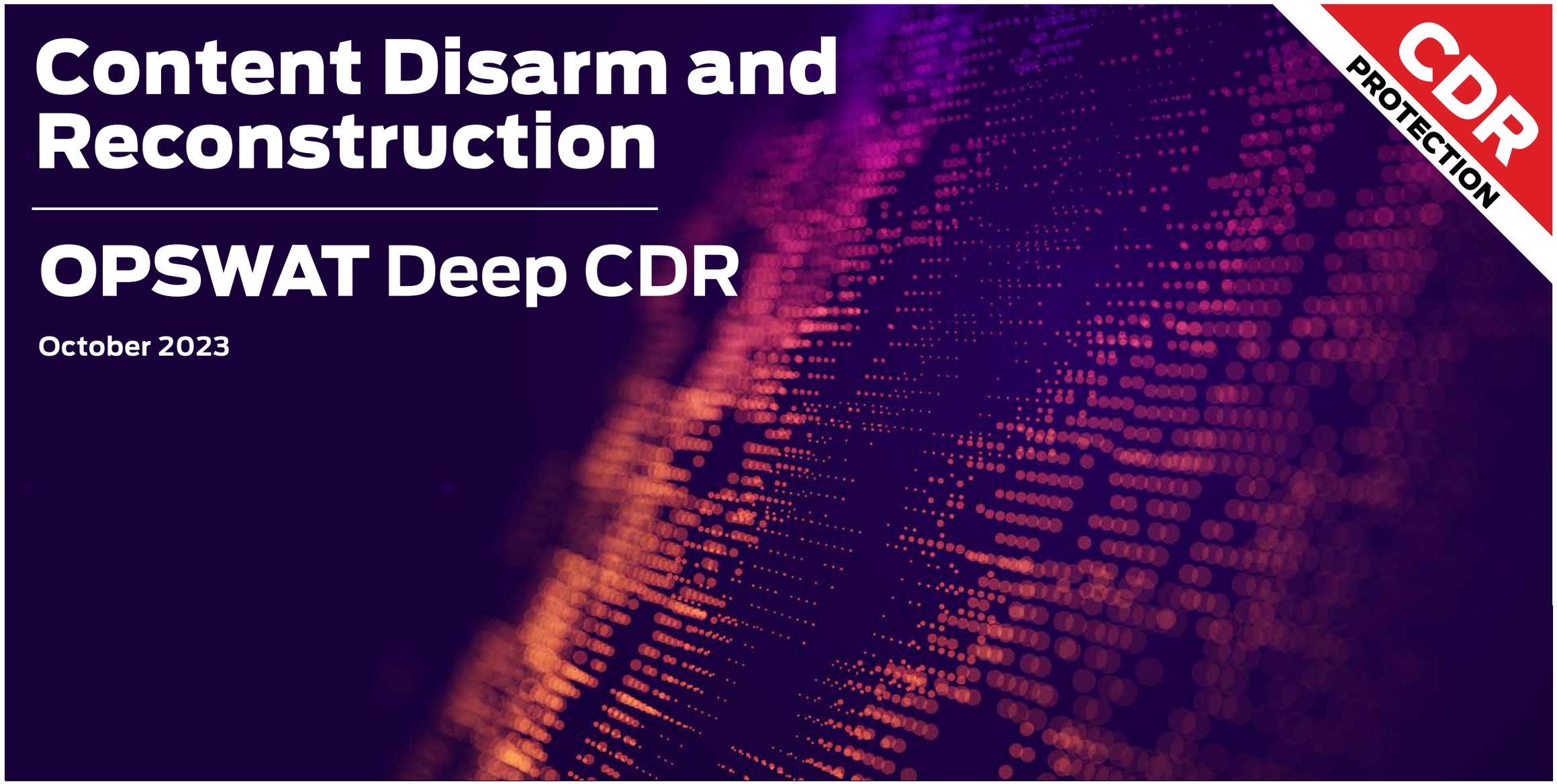
SE Labs

INTELLIGENCE-LED TESTING

Content Disarm and Reconstruction

OPSWAT Deep CDR

October 2023



SE Labs tested **OPSWAT Deep CDR** against targeted attacks using file-based threats. These attacks are designed to compromise systems and penetrate target networks by hiding threats inside files that appear to be innocent.

Testers hid threats inside a variety of common file formats, such as office documents, web pages and archive files.

These files were assessed by the CDR system, which attempted to remove known and unknown threats. The results show the extent to which the threat prevention system achieved that goal accurately.

Contents

Introduction	**04**
Executive Summary	**05**
Enterprise Endpoint Security Awards	**05**
1. Total Accuracy Ratings	**06**
2. Protection Ratings	**07**
3. Protection Scores	**08**
4. Legitimate Object Ratings	**08**
5. Conclusions	**09**
Appendicies	**10**
Appendix A: Terms Used	**10**
Appendix B: FAQs	**10**
Appendix C: Product Version	**10**
Appendix D: Detailed Threat Results	**11**
Appendix E: Detailed Legitimate Results	**12**

Document version 1.0 Written 18th October 2023

Website selabs.uk
Email info@SELabs.uk
LinkedIn www.linkedin.com/company/se-labs/
Blog blog.selabs.uk
Post SE Labs Ltd,
55A High Street, Wimbledon, SW19 5BA, UK

Introduction

Attacker in the Middle?

Content Disarm and Reconstruction targets Trojans

Content Disarm and Reconstruction (CDR) security solutions take a different approach than many others. Instead of detecting threats, they pull files apart and put them back together again. The idea is that anything bad gets dropped by the wayside, and only good things can pass through.

This approach is particularly appropriate when considering the risk of man-in-the-middle attacks. You might send a useful file to a colleague, but an attacker intercepts it and adds a little extra something, like a remote access tool. When you open it, you see what you would expect, while the attacker gains access to your system.

Trojan files are a common way for attackers to gain access to a target. Just as the classical story describes how the Greeks offered a seemingly harmless gift to the city of Troy, computer Trojans appear to be something you want, but contain a nasty surprise. You are even more likely to believe that the gift is legitimate if it comes from someone you work with.

CDR aims to permit users to keep working, while stripping out threats that somehow make it into the communications.

In this test we looked at three general types of files:

1. **Office documents, such as PDFs, PowerPoint presentations and Excel spreadsheets.**
2. **Archives, such as Zip and RAR files.**
3. **Various others, such as image files, web pages and LNK link files.**

In each case we created a legitimate file that the recipient should expect to receive. Then, acting as an attacker, we added a Trojan component that would give us remote access to the victim should they open the file. Finally, we sent the file through the CDR solution to see what would happen.

Common outcomes might be that it allowed the file through, complete with the threat. This would be a disastrous failure. Or it might remove the threat completely, leaving a perfect copy of the original legitimate file, which would be awesome. Or something else in-between might happen. There could be some corruption, with the threat dying while taking the legitimate content with it. Or part of the threat might be removed, but not the sum total.

We looked at all of the possibilities and you can find the results in this report.

If you spot a detail in this report that you don't understand, or would like to discuss, please **contact us**. SE Labs uses current threat intelligence to make our tests as realistic as possible. To learn more about how we test, how we define 'threat intelligence' and how we use it to improve our tests please visit our **website** and follow us on **LinkedIn**.

Executive Summary

SE Labs tested **OPSWAT Deep CDR** against targeted file-based attacks concealed within legitimate files.

The threats themselves were designed to provide attackers with remote access to the victim's systems. These were hidden inside a range of useful files such as office documents, web pages and archive files, such as Zip and RAR files.

We examined its abilities to:

- **Deconstruct files and reconstruct only the useful parts, in a usable form.**
- **Remove threats during this process of reconstruction.**
- **Reconstruct files with the minimum of corruption.**
- **Handle legitimate files without damaging them in the process.**

Legitimate files were used alongside the threats to measure any false positive detections or other sub-optimal interactions.

OPSWAT Deep CDR scored 100% overall, demonstrating 100% accuracy when handling entirely legitimate applications and 100% accuracy when handling files that contained Trojan threats designed to provide attackers with remote access.

For specific build numbers, see **Appendix C: Product Versions** on page 10.

Executive Summary			
Products Tested	**Protection Accuracy Rating (%)**	**Legitimate Accuracy Rating (%)**	**Total Accuracy Rating (%)**
OPSWAT Deep CDR	100%	100%	100%

Products highlighted in green were the most accurate, scoring 85 per cent or more for Total Accuracy. Those in yellow scored less than 85 but 75 or more. Products shown in red scored less than 75 per cent.

For exact percentages, see **1. Total Accuracy Ratings** on page 6.

Content Disarm and Reconstruction Award

The following product wins the SE Labs award:

OPSWAT Deep CDR

1. Total Accuracy Ratings

Judging the effectiveness of a product is a subtle art, and many factors are at play when assessing how well it performs. To make things easier we've combined all the different results from this report into one easy-to-understand graph.

The graph below takes into account not only each product's ability to detect and protect against threats, but also its handling of non-malicious objects such as web addresses (URLs) and applications.

Not all protections, or detections for that matter, are equal. A product might completely remove all threats from a file and leave the file in a perfectly usable state. Alternatively, the product might remove some threats from a file but leave other actively dangerous elements in place. Or it might destroy all good and bad parts of the file! We take these outcomes into account when attributing points that form final ratings.

For example, a product that completely removes a threat and leaves the file usable is rated more highly than one that removes parts of threats or damages the good parts of files.

Categorising how a product handles legitimate objects is complex, and you can find out how we do it in **4. Legitimate Object Ratings** on page 8.

Total Accuracy Ratings			
Product	**Total Accuracy Rating**	**Total Accuracy (%)**	**Award**
OPSWAT Deep CDR	270	100%	**AAA**

Total Accuracy Ratings combine protection and false positives

2. Protection Ratings

Detected – Cleaned (+1)
The product has successfully cleaned and removed malicious elements. The file doesn't present any harm to the user and is in a usable/readable state.

Detected – Corrupted (+1)
The product has successfully cleaned and removed the malicious elements. The file has been corrupted and is not usable, but it doesn't present harm to the user.

Detected – Invalid (+1)
The product detects invalid files and rejects them.

Detected – Partial Clean (-0.5)
In case of multiples malicious elements, the product removes some elements but a threat is still present.

Missed (-1)
The product fails to remove or destroy the malicious elements of the file.

Protection Accuracy		
Product	**Protection Accuracy**	**Protection Accuracy (%)**
OPSWAT Deep CDR	135	100%

Protection Ratings are weighted to show that how products handle threats can be subtler than just 'win' or 'lose'.

3. Protection Scores

The table below shows the overall level of protection per category, making no distinction between clean, corrupted or invalid verdicts.

Protection Scores		
Product	**Protection Score**	**Protection Score %**
Office	65	100%
Archives	25	100%
Miscellanous	40	100%

4. Legitimate Object Ratings

These ratings indicate how accurately the products classify legitimate objects, while also taking into account the interactions that each product has with the user. Ideally a product will either not classify a legitimate object or will classify it as safe. In neither case should it bother the user.

We also take into account the prevalence (popularity) of the legitimate objects used in this part of the test, applying stricter penalties for when products misclassify very popular legitimate objects.

Legitimate Object Ratings		
Product	**Legitimate Accuracy Rating**	**Legitimate Accuracy (%)**
OPSWAT Deep CDR	135	100%

5. Conclusion

This test challenged **OPSWAT Deep CDR** to a range of file-based attacks that our testers concealed within legitimate files. The threats themselves were designed to provide attackers with remote access to the victim's systems. These were hidden inside a range of useful files such as office documents, web pages and archive files, such as Zip and RAR files.

Content Disarm and Reconstruction (CDR) technology uses an unusual approach to cleaning threats. Rather than identifying the bad parts of a file and removing them, it identifies the good (or at least, policy-compliant) parts and throws away everything else. A good CDR defence would only throw away the bad, non-compliant parts. The good, compliant parts would remain intact and in a usable state.

What can happen is that only some of the non-compliant parts are removed. Or some of the compliant parts could be destroyed. Or both. Businesses would no doubt prefer the compliant parts to be destroyed if that also meant the threats were mitigated. The worst case scenario would be the destruction or corruption of useful files and the preservation of one or more threats. Arguably the removal of one threat (and an alert about that) but leaving another viable threat in place is even worse, as it leaves victims both vulnerable and with a false sense of security!

In all cases we recorded what happened when **OPSWAT Deep CDR** encountered the files containing both malicious and useful components.

We also assessed the product with purely useful files. If it allowed these to pass through to users unmolested then that's an ideal situation. If it corrupted files to any extent, then the security measures are unnecessarily disrupting business, which is suboptimal.

In this test, which is the first of its kind, **OPSWAT Deep CDR** handled the legitimate files perfectly. In this respect it scored 100%. When it came to handling the threats it was also very effective. Overall we awarded it a Protection Score of 100%. This breaks down as follows: It handled office files and miscellaneous files perfectly (100% in each set of files), removing all elements of the threats while leaving the useful parts of the files intact. It was excellent at handling Trojanised archive files too, handling all correctly.

Taking it handling of threats and legitimate files into full account, **OPSWAT Deep CDR** achieves a AAA award for its excellent performance.

Appendices

Appendix A: Terms Used

Term	Meaning
Threat	A program or sequence of interactions with the target that is designed to take some level of unauthorised control of that target.
False Positive	When a security product misclassifies a legitimate application or website as being malicious it generates a “false positive”.
Target	The test system that is protected by a security product.
Update	Security vendors provide information to their products in an effort to keep abreast of the latest threats. These updates may be downloaded in bulk as one or more files, or requested individually and live over the internet.
Disarm	Malicious elements of the threats have been removed.

Appendix B: FAQs

- The products chosen for this test were selected by SE Labs.
- The test was sponsored by OPSWAT, Inc.
- The test was conducted between 11th May and 14th September 2023.
- All products were configured according to each vendor’s recommendations, when such recommendations were provided.
- Malicious URLs and legitimate applications and URLs were independently located and verified by SE Labs.
- Targeted attacks were selected and verified by SE Labs.
- Malicious and legitimate data was provided to partner organisations once the test was complete.
- The web browser used in this test was Google Chrome. When testing Microsoft products Chrome was equipped with the Windows Defender Browser Protection browser extension (**https://browserprotection.microsoft.com**). We allow other browser extensions when a tested product requests a user install one or more.

Q What is a partner organisation? Can I become one to gain access to the threat data used in your tests?

A Partner organisations benefit from our consultancy services after a test has been run. Partners may gain access to low-level data that can be useful in product improvement initiatives and have permission to use award logos, where appropriate, for marketing purposes. We do not share data on one partner with other partners. We do not partner with organisations that do not engage in our testing.

Q I am a security vendor and you tested my product without permission. May I access the threat data to verify that your results are accurate?

A We are willing to share a certain level of test data with non-partner participants for free. The intention is to provide sufficient data to demonstrate that the results are accurate. For more in-depth data suitable for product improvement purposes we recommend becoming a partner.

Appendix C: Product Version

The table below shows the service’s name as it was being marketed at the time of the test.

Product Versions			
Vendor	**Product**	**Build Version (start)**	**Build Version (end)**
OPSWAT	Deep CDR	6.6.2	6.6.2

Appendix D: Detailed Threat Results

The Detailed Threat Results show how the product handled each file containing a threat.

Office Files	Detected				Missed
Format	Cleaned	Corrupted	Invalid	Partial Clean	
PDF	10	0	0	0	0
Word	30	0	0	0	0
Excel	20	0	0	0	0
OneNote	2	0	0	0	0
Powerpoint	3	0	0	0	0
Total	**65**	**0**	**0**	**0**	**0**

Archives	Detected				Missed
Format	Cleaned	Corrupted	Invalid	Partial Clean	
7z	5	0	0	0	0
zip	10	0	0	0	0
iso	0	0	5	0	0
rar	5	0	0	0	0
cab	5	0	0	0	0
Total	25	0	5	0	0

Miscellanous	Detected				Missed
Format	Cleaned	Corrupted	Invalid	Partial Clean	
hta	15	0	0	0	0
html	10	0	0	0	0
lnk	10	0	0	0	0
Image	5	0	0	0	0
Total	**40**	**0**	**0**	**0**	**0**

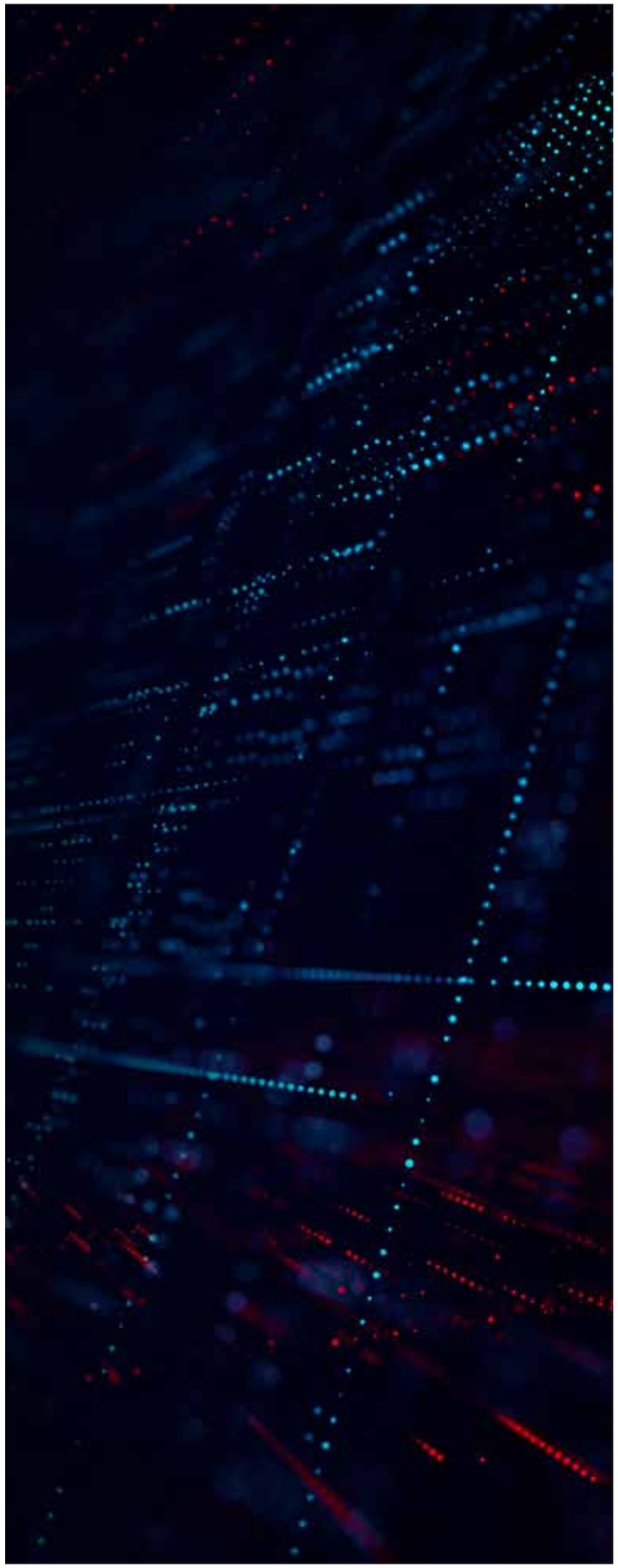
Appendix E: Detailed Legitimate Results

The Detailed Legitimate Results show how the product handled each wholly legitimate file used in the test.

Office Files	Detected				Missed
Format	Cleaned	Corrupted	Invalid	Partial Clean	
PDF	10	0	0	0	0
Word	30	0	0	0	0
Excel	20	0	0	0	0
OneNote	2	0	0	0	0
Powerpoint	3	0	0	0	0
Total	**65**	**0**	**0**	**0**	**0**

Archives	Detected				Missed
Format	Cleaned	Corrupted	Invalid	Partial Clean	
7z	5	0	0	0	0
zip	10	0	0	0	0
iso	5	0	0	0	0
rar	5	0	0	0	0
cab	5	0	0	0	0
Total	30	0	0	0	0

Miscellanous	Detected				Missed
Format	Cleaned	Corrupted	Invalid	Partial Clean	
hta	15	0	0	0	0
html	5	0	0	0	0
lnk	5	0	0	0	0
Image	5	0	0	0	0
Total	**40**	**0**	**0**	**0**	**0**



SE Labs Report Disclaimer

1. The information contained in this report is subject to change and revision by SE Labs without notice.
2. SE Labs is under no obligation to update this report at any time.
3. SE Labs believes that the information contained within this report is accurate and reliable at the time of its publication, which can be found at the bottom of the contents page, but SE Labs does not guarantee this in any way.
4. All use of and any reliance on this report, or any information contained within this report, is solely at your own risk. SE Labs shall not be liable or responsible for any loss of profit (whether incurred directly or indirectly), any loss of goodwill or business reputation, any loss of data suffered, pure economic loss, cost of procurement of substitute goods or services, or other intangible loss, or any indirect, incidental, special or consequential loss, costs, damages, charges or expenses or exemplary damages arising his report in any way whatsoever.
5. The contents of this report does not constitute a recommendation, guarantee, endorsement or otherwise of any of the products listed, mentioned or tested.
6. The testing and subsequent results do not guarantee that there are no errors in the products, or that you will achieve the same or similar results. SE Labs does not guarantee in any way that the products will meet your expectations, requirements, specifications or needs.
7. Any trade marks, trade names, logos or images used in this report are the trade marks, trade names, logos or images of their respective owners.
8. The contents of this report are provided on an “AS IS” basis and accordingly SE Labs does not make any express or implied warranty or representation concerning its accuracy or completeness.