


Endpoint Security

SentinelOne Singularity for Endpoint With Reboot vs. Without Reboot

August 2023

EPS
PROTECTION





SE Labs tested **SentinelOne Singularity for Endpoint** to determine its threat detection and protection abilities. The test also assessed the security available on an endpoint running a newly deployed installation of **SentinelOne Singularity for Endpoint**, without rebooting the system. The goal was to judge the different levels of effectiveness between an established installation of endpoint protection and a completely new, fresh installation.

Both installations were tested against a comprehensive array of threats, ranging from targeted attacks using well-established techniques to public email- and web-based threats that were found to be live on the internet at the time of the test.

The results indicate how effectively the two deployments of the products were at detecting and/ or protecting against those threats in real time.

Management**Chief Executive Officer** Simon Edwards**Chief Operations Officer** Marc Briggs**Chief Human Resources Officer** Magdalena Jurenko**Chief Technical Officer** Stefan Dumitrascu**Testing Team**

Nikki Albesa

Thomas Bean

Solandra Brewster

Gia Gorbald

Anila Johny

Erica Marotta

Luca Menegazzo

Jeremiah Morgan

Julian Owusu-Abrokwa

Joseph Pike

Georgios Sakatzidi

Dimitrios Tsarouchas

Stephen Withey

Publication and Marketing

Colin Mackleworth

Sara Claridge

Janice Sheridan

IT Support

Danny King-Smith

Chris Short

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

SE Labs is ISO/IEC 27001 : 2013 certified and
BS EN ISO 9001 : 2015 certified for The Provision
of IT Security Product Testing.

SE Labs is a member of the Microsoft Virus Initiative (MVI);
the Anti-Malware Testing Standards Organization (AMTSO);
the Association of anti Virus Asia Researchers (AVAR); and
NetSecOPEN.

© 2023 SE Labs Ltd

Contents

Introduction	04
Executive Summary	04
1. Total Accuracy Ratings	05
Enterprise Endpoint Security Awards	05
2. Protection Ratings	06
3. Protection Scores	07
4. Protection Details	08
5. Legitimate Software Ratings	08
6. Conclusions	09
Appendicies	10
Appendix A: FAQs	10
Appendix B: Product Versions	10
Appendix C: Attack Types	10

Document version 1.0 Written 4th August 2023



Introduction

Protection starts with first installation

To reboot or not to reboot?

“Turn it off and on again.” This global IT support advice is known to everyone, from **Peppa Pig** (Mummy Pig at Work) to the **The IT Crowd** (every episode). But why? Why does rebooting a complex computer system solve so many problems? And why am I referring to British TV comedy in a serious report about computer security? We will answer one of those questions here.

Installing computer software can be as simple as copying a program file from an external source. However, complex software needs more attention. It needs to integrate more fully with the operating system and potentially other programs already installed. Some programs share code for efficiency's sake, for example.

When advanced applications need to embed into the operating system it's common to require the administrator to reboot the system after installation. This allows different components of the new program to play nicely with the rest of the system. However, there are good reasons why you may not wish to reboot a system. It might be busy doing something useful, but you still need the new application to operate. Or you might be investigating a live security incident.

SentinelOne Singularity for Endpoint claims to provide great protection, even before you reboot the system. We tested that claim in this report. Let's find out if you really need to turn it off and on again, to stay safe.

This report shows **SentinelOne Singularity's** performance in this test with and without a reboot after installation. The results are directly comparable with the public SE Labs Enterprise Endpoint Security (Q2 2023) report, available [here](#).

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

- **Both installations were effective at handling general threats from cyber criminals...**

SentinelOne Singularity for Endpoint provided comprehensive protection in the face of the public email- and web-based attacks. In both the established 'fresh installation (with reboot)' mode and 'fresh installation (without reboot)' it detected and protected against all of the general attacks, of the type that affect all internet users.

- **... while targeted attacks were handling well, as a whole.**

Both installations handled targeted attacks well. The rebooted version provided slightly better protection than the non-rebooted version. The 'with reboot' installation stopped all but one of the targeted attacks. The 'without reboot' version stopped all but two.

- **False positives were not an issue for the installations.**

Neither mode of operation caused any false positive alerts. The software did not mistake any legitimate applications as being malicious.

Executive Summary			
Products Tested	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Fresh installation (with reboot)	97%	100%	99%
Fresh installation (without reboot)	95%	100%	98%

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 5.

1. Total Accuracy Ratings

Judging the effectiveness of an endpoint security 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.

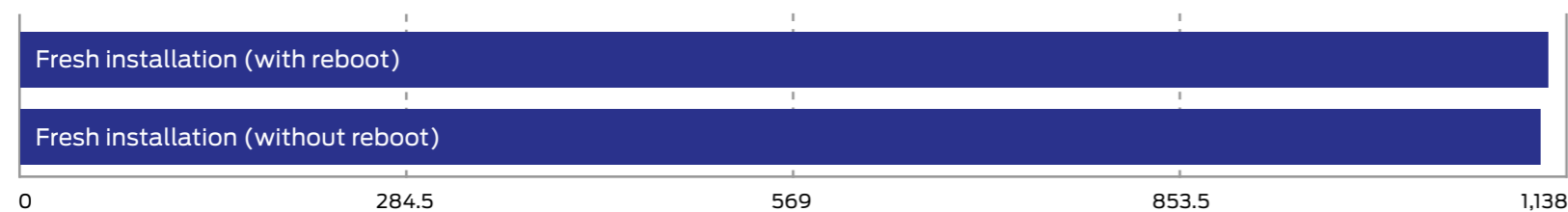
Not all protections, or detections for that matter, are equal. A product might completely block a URL, which stops the threat before it can even start its intended series of malicious events. Alternatively, the product might allow a web-based exploit to

execute but prevent it from downloading any further code to the target. In another case malware might run on the target for a short while before its behaviour is detected and its code is deleted or moved to a safe 'quarantine' area for future analysis. We take these outcomes into account when attributing points that form final ratings.

For example, a product that completely blocks a threat is rated more highly than one that allows a threat to run for a while before eventually evicting it. Products that allow all malware infections, or that block popular legitimate applications, are penalised heavily.

Categorising how a product handles legitimate objects is complex, and you can find out how we do it in **5. Legitimate Software Ratings** on page 8.

Total Accuracy Ratings			
Product	Total Accuracy Rating	Total Accuracy (%)	Award
Fresh installation (with reboot)	1,124	99%	AAA
Fresh installation (without reboot)	1,118	98%	AAA



Total Accuracy Ratings combine protection and false positives

Endpoint Security Award

The following product wins the SE Labs award:



**SentinelOne
Singularity
for Endpoint**

2. Protection Ratings

The results below indicate how effectively the products dealt with threats. Points are earned for detecting the threat and for either blocking or neutralising it.

■ Detected (+1)

If the product detects the threat with any degree of useful information, we award it one point.

■ Blocked (+2)

Threats that are disallowed from even starting their malicious activities are blocked. Blocking products score two points.

■ Complete Remediation (+1)

If, in addition to neutralising a threat, the product removes all significant traces of the attack, it gains an additional one point.

■ Neutralised (+1)

Products that kill all running malicious processes 'neutralise' the threat and win one point.

■ Persistent Neutralisation (-2)

This result occurs when a product continually blocks a persistent threat from achieving its aim, while not removing it from the system.

■ Compromised (-5)

If the threat compromises the system, the product loses five points. This loss may be reduced to four points if it manages to detect the threat (see Detected, above), as this at least

alerts the user, who may now take steps to secure the system.

Rating Calculations

We calculate the protection ratings using the following formula:

$$\begin{aligned} \text{Protection Rating} = & \\ & (1x \text{ number of Detected}) + \\ & (2x \text{ number of Blocked}) + \\ & (1x \text{ number of Neutralised}) + \\ & (1x \text{ number of Complete remediation}) + \\ & (-5x \text{ number of Compromised}) \end{aligned}$$

The 'Complete remediation' number relates to cases of neutralisation in which all significant traces of the attack were removed from the target.

These ratings are based on our opinion of how important these different outcomes are. You may have a different view on how seriously you treat a 'Compromise' or 'Neutralisation without complete remediation'. If you want to create your own rating system, you can use the raw data from **5. Protection Details** on page 8 to roll your own set of personalised ratings.

Targeted Attack Scoring

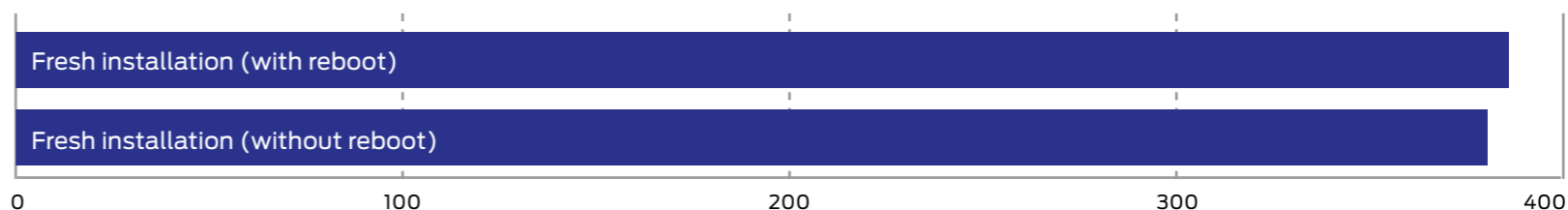
The following scores apply only to targeted attacks and are cumulative, ranging from -1 to -5.

■ Access (-1)

If any command that yields information about the target system is successful this score is applied. Examples of successful commands include listing

Protection Accuracy		
Product	Protection Accuracy	Protection Accuracy (%)
Fresh installation (with reboot)	386	97%
Fresh installation (without reboot)	380	95%

Average 96%



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

3. Protection Scores

current running processes, exploring the file system and so on. If the first command is attempted and the session is terminated by the product without the command being successful the score of Neutralised (see above) will be applied.

■ Action (-1)

If the attacker is able to exfiltrate a document from the target's Desktop of the currently logged in user then an 'action' has been successfully taken.

■ Escalation (-2)

The attacker attempts to escalate privileges to NT Authority/System. If successful, an additional two points are deducted.

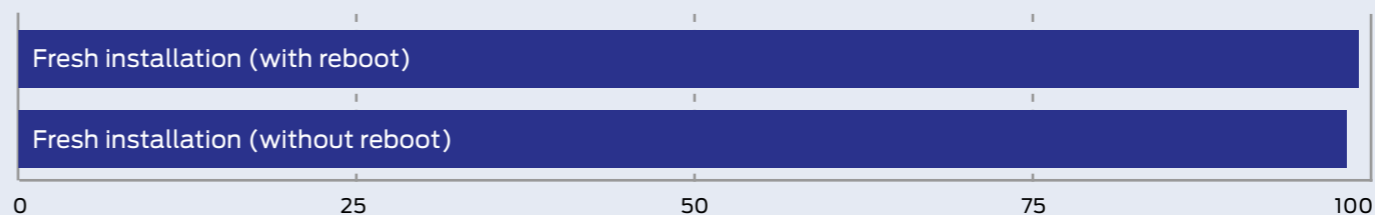
■ Post-Escalation Action (-1)

After escalation the attacker attempts actions that rely on escalated privileges. These include attempting to steal credentials, modifying the file system and recording keystrokes. If any of these actions are successful then a further penalty of one point deduction is applied.

This graph shows the overall level of protection, making no distinction between neutralised and blocked incidents.

For each product we add Blocked and Neutralised cases together to make one simple tally.

Protection Scores	
Product	Protection Score
Fresh installation (with reboot)	99
Fresh installation (without reboot)	98



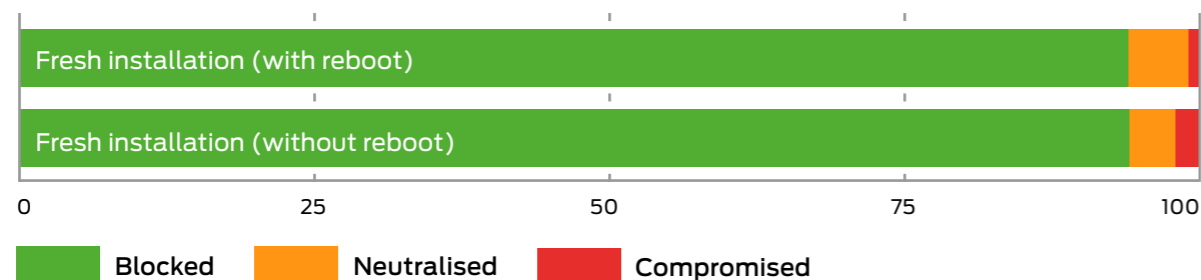
Protection Scores are a simple count of how many times a product protected the system.

4. Protection Details

These results break down how each product handled threats into some detail. You can see how many detected a threat and the levels of protection provided.

Products sometimes detect more threats than they protect against. This can happen when they recognise an element of the threat but aren't equipped to stop it. Products can also provide protection even if they don't detect certain threats. Some threats abort on detecting specific endpoint protection software.

Protection Details					
Product	Detected	Blocked	Neutralised	Compromised	Protected
Fresh installation (with reboot)	100	94	5	1	99
Fresh installation (without reboot)	100	94	4	2	98



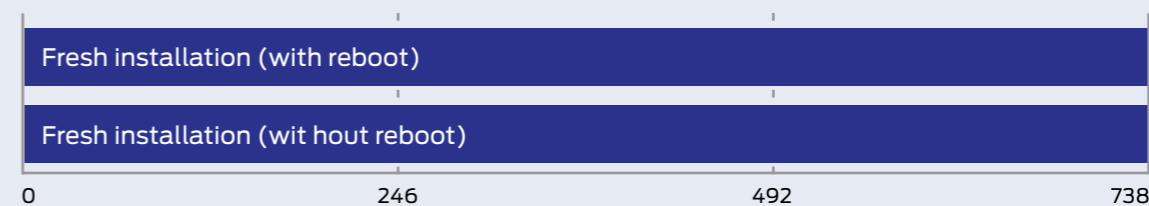
This data shows in detail how each product handled the threats used.

5. Legitimate Software Ratings

These ratings indicate how accurately the products classify legitimate applications and URLs, 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 applications and websites used in this part of the test, applying stricter penalties for when products misclassify very popular software and sites.

Legitimate Software Ratings		
Product	Legitimate Accuracy Rating	Legitimate Accuracy (%)
Fresh installation (without reboot)	738	100%
Fresh installation (with reboot)	738	100%



Legitimate Software Ratings can indicate how well a vendor has tuned its detection engine.

6. Conclusions

The two products under test are essentially the same, with one important distinction. One was installed in a traditional manner, which included updating itself and then rebooting the Windows system. The other, which we've called the 'without reboot' deployment, was installed but without the reboot step. This is what would happen if you wanted to protect a high availability system or decided to introduce protection to a computer that was experiencing a live security incident that you wanted to investigate without disturbing the attacker.

Attacks in this test included threats that affect the wider public and more closely targeted individuals and organisations. You could say that we tested the products with 'public' malware and full-on hacking attacks.

We introduced the threats in a realistic way such that threats seen in the wild on websites were downloaded from those same websites, while threats caught spreading through email were delivered to our target systems as emails.

A standard installation of **SentinelOne Singularity for Endpoint** should do well in this test. While we do 'create' threats by using publicly available free hacking tools, we do not write unique malware so there is no technical reason why any security vendor should do poorly in this part of the test.

As expected, the results were extremely strong, with the security product detecting and protecting against all of the public threats. The product did handle some of these threats differently, though. It blocked 70 of them perfectly but neutralised the remaining five. This is a good result, but slightly reduces the protection rating. We prefer security products to block, rather than stop and then delete threats.

The 'without reboot' deployment also did just as well in this part of the test. There was no difference at all.

The targeted attacks posed a harder challenge but both installations performed strongly. The standard deployment stopped all but one of the targeted attacks. The 'without reboot' version stopped all but two. We can observe that the performance between these two modes of deployment are near-identical, with a slight benefit to turning the computer off and on again following installation.

This report shows **SentinelOne Singularity's** performance in this test with and without a reboot after installation. The results are directly comparable with the public SE Labs Enterprise Endpoint Security (Q2 2023) report, available [here](#).

Annual Report 2023

**Our 4th Annual Report
is now available**

- **Threat Intelligence Special**
- **Ransomware Focus**
- **Security Awards**
- **Advanced Email Testing**



**DOWNLOAD THE
REPORT NOW!**
(free – no registration)

selabs.uk/ar2023

Appendices

Appendix A: FAQs

A **full methodology** for this test is available from our website.

- The products chosen for this test were selected by SE Labs.
- The test of the ‘without reboot’ deployment was commissioned by SentinelOne Inc.
- The test was conducted between 17th January and 21st March 2023.
- All products were configured according to the 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.

Appendix B: Product Versions

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)
SentinelOne	Singularity for Endpoint Fresh installation (with reboot)	22.3.4.612	22.3.4.612
SentinelOne	Singularity for Endpoint Fresh installation (without reboot)	22.3.4.612	22.3.4.612

Appendix C: Attack Types

The table below shows how each product protected against the different types of attacks used in the test.

Attack Types			
Product	General Attack	Targeted Attack	Protected (%)
Fresh installation (with reboot)	75	24	98%
Fresh installation (without reboot)	75	23	96%

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.