

# SELabs

INTELLIGENCE-LED TESTING

## Enterprise Advanced Security

# CrowdStrike Falcon

**EDR**  
RANSOMWARE

November 2023

SE Labs tested **CrowdStrike Falcon** against a range of ransomware attacks designed to extort victims. These attacks were realistic, using the same tactics and techniques as those used against victims in recent months.

Target systems, protected by **CrowdStrike Falcon**, were attacked by testers acting in the same way as we observe ransomware groups to behave.

Attacks were initiated from the start of the attack chain, using phishing email links and attachments, as just two examples. Each attack was run from the very start to its obvious conclusion, which means attempting to steal, encrypt and destroy sensitive data on the target systems.



# Contents

<b>Introduction</b>	<b>04</b>
<b>Executive Summary</b>	<b>05</b>
<b>Enterprise Advanced Security (Ransomware) Award</b>	<b>05</b>
<b>1. How We Tested</b>	<b>06</b>
Threat Responses	07
Hackers vs. Targets	09
<b>2. Total Accuracy Ratings</b>	<b>10</b>
<b>3. Response Details (Ransomware Deep Attacks)</b>	<b>11</b>
<b>4. Threat Intelligence (Ransomware Deep Attacks)</b>	<b>13</b>
Group 1	13
Group 2	14
<b>5. Protection Ratings (Ransomware Direct Attacks)</b>	<b>15</b>
<b>6. Protection Scores (Ransomware Direct Attacks)</b>	<b>16</b>
<b>7. Protection Details (Ransomware Direct Attacks)</b>	<b>16</b>
<b>8. Legitimate Software Rating</b>	<b>17</b>
8.1 Interaction Ratings	18
8.2 Prevalence Ratings	19
8.3 Accuracy Ratings	19
8.4 Distribution of Impact Categories	20
<b>9. Conclusions</b>	<b>20</b>
<b>Appendices</b>	<b>22</b>
Appendix A: Terms Used	22
Appendix B: FAQs	22
Appendix C: Product Versions	22
Appendix C: Ransomware Deep Attack Details	23

Document version 1.0 Written 31st October 2023

## 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 Sakatzidis  
 Dimitrios Tsarouchas  
 Stephen Withey

## Publication and Marketing

Colin Mackleworth  
 Sara Claridge  
 Janice Sheridan

## IT Support

Danny King-Smith  
 Chris Short

**Website** [selabs.uk](https://selabs.uk)

**Email** [info@SELabs.uk](mailto:info@SELabs.uk)

**LinkedIn** [www.linkedin.com/company/se-labs/](https://www.linkedin.com/company/se-labs/)

**Blog** [blog.selabs.uk](https://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



## Introduction

# Ransomware vs. Endpoint Security

## Results from the largest public ransomware test

Ransomware is the most visible, most easily understood cyber threat affecting businesses today. Paralysed computer systems mean stalled business and loss of earnings. On top of that, a ransom demand provides a clear, countable value to a threat. A demand for “one million dollars!” is easier to quantify than the possible leak of intellectual property to a competitor.

One reason why ransomware is so ‘popular’ is that the attackers don’t have to produce their own.

They outsource the production of ransomware to others, who provide Ransomware as a Service (RAAS). Attackers then usually trick targets into running it, or at least into providing a route for the attackers to run it for them. Artificial intelligence systems make the creation of such social engineering attacks easier, cheaper and more effective than ever before.

Given the global interest and terror around ransomware, we have created a comprehensive test that shows how effective security products are when faced with the whole range of threats posed by ransomware itself and the criminal groups operating in the shadows.

In this report we have taken two main approaches to assessing how well products can detect and protect against ransomware.

### Ransomware Deep Attacks

For the first part of this test, we analysed the common tactics of ransomware gangs and created two custom gangs that use a wider variety of methods. In all cases we run the attack from the very start, including attempting to access targets with stolen credentials or other means. We then move through the system and sometimes the network, before deploying the ransomware as the final payload.

In the first two attacks for each group, we gain access and deploy ransomware onto the target immediately. In the third, fourth and fifth attacks we move through the network and deploy ransomware on a target deeper into the network.

The ransomware payloads used in this part of the report were known files from all of the families listed in **Hackers vs. Targets** on page 9.

This test shows a product’s ability to track the movement of the attacker through the entire attack chain. We disable the product’s protection features and rely on its detection mode for this part of the test. The results demonstrate how incident response teams can use the product to gain visibility on ransomware attacks.

### Ransomware Direct Attacks

The second part of the test takes a wide distribution of known malware and adds variations designed to evade detection. We’ve listed the ransomware families used in **Hackers vs. Targets** on page 9. We sent each of these ransomware payloads directly to target systems using realistic techniques, such as through email social engineering attacks. This is a full but short attack chain. In this part of the test, we ensure any protection features are enabled in the product.

If products can detect and protect against the known version of each of these files, all well and good. But if they also detect and block each ransomware’s two variations then we can conclude that the protection available is more proactive than simply reacting to yesterday’s unlucky victims.

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

We tested **CrowdStrike Falcon** against direct attacks using known and unknown ransomware, as well as deeper hacking attacks that culminated in deployment of ransomware on target systems. All tests used live ransomware, delivered in a realistic fashion.

We examined its abilities to:

- Detect and protect against known ransomware
- Detect and protect against new ransomware variants
- Track full network breaches
- Detect deployment of ransomware on internal targets

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

**CrowdStrike Falcon** performed exceptionally well, providing complete detection and protection coverage against all direct ransomware attacks. It also provided thorough insight into the full network breaches that concluded with ransomware deployments. Only one misclassified legitimate application prevented it from achieving a perfect score. **CrowdStrike Falcon's** 99% Total Accuracy Rating is an excellent result in an extremely challenging test.

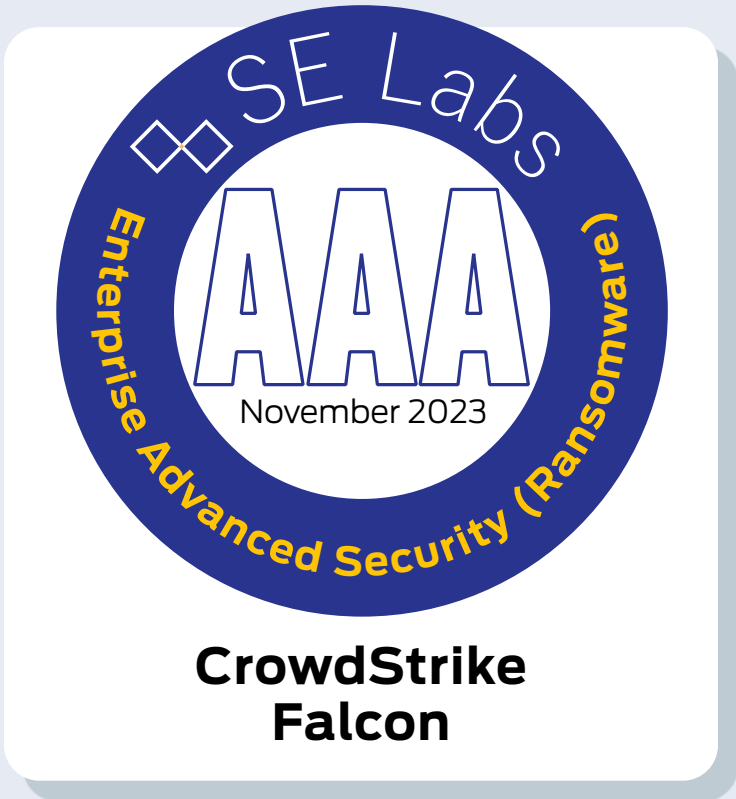
Executive Summary				
Product Tested	Protection Accuracy (%)	EDR Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
CrowdStrike Falcon	100%	100%	97%	99%

The Protection rating shows how effective the product was at preventing the ransomwares attacks from achieving their goals. The EDR rating reflects the level of detection at different stages of the attack.

For exact percentages, see **2. Total Accuracy Ratings** on page 10.

# Enterprise Advanced Security (Ransomware) Award

The following product wins the SE Labs award:



# 1. How we Tested

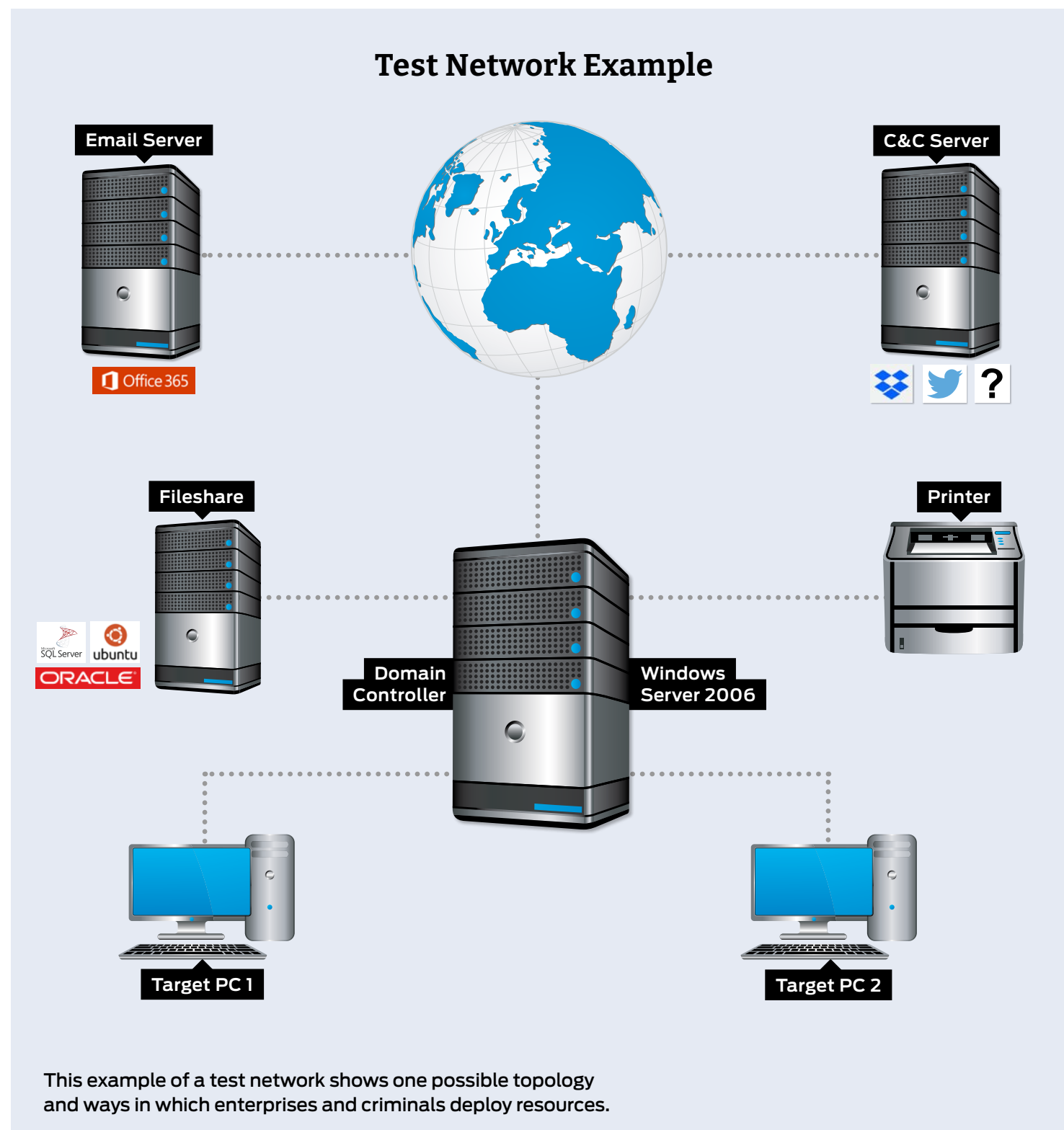
Testers can't assume that products will work a certain way, so running a realistic advanced security test means setting up real networks and hacking them in the same way that real adversaries behave.

In the diagram on the right you will see an example network that contains workstations, some basic infrastructure such as file servers and a domain controller, as well as cloud-based email and a malicious command and control (C&C) server, which may be a conventional computer or a service such as Dropbox, Twitter, Slack or something else more imaginative.

As you will see in the **Threat Responses** section on page 7, attackers often jump from one compromised system to another in so-called 'lateral movement'. To allow products to detect this type of behaviour the network needs to be built realistically, with systems available, vulnerable and worth compromising.

It is possible to compromise devices such as enterprise printers and other so-called 'IoT' (internet of things) machines, which is why we've included a representative printer in the diagram.

The techniques that we choose for each test case are largely dictated by the real-world behaviour of online criminals. We observe their tactics and replicate what they do in this test. To see more details about how the specific attackers behaved, and how we copied them, see **Hackers vs. Targets** on page 9 and, for a really detailed drill down on the details, **4. Threat Intelligence (Ransomware Deep Attacks)** on pages 13 to 14 and **Appendix C: Ransomware Deep Attack Details**.



# Threat Responses

## Full Attack Chain: Testing Every Layer of Detection and Protection

Attackers start from a certain point and don't stop until they have either achieved their goal or have reached the end of their resources (which could be a deadline or the limit of their abilities). This means, in a test, the tester needs to begin the attack from a realistic first position, such as sending a phishing email or setting up an infected website, and moving through many of the likely steps leading to actually stealing data or causing some other form of damage to the network.

If the test starts too far into the attack chain, such as executing malware on an endpoint, then many products will be denied opportunities to use the full extent of their protection and detection

abilities. If the test concludes before any 'useful' damage or theft has been achieved, then similarly the product may be denied a chance to demonstrate its abilities in behavioural detection and so on.

## Attack Stages

The illustration (below) shows some typical stages of an attack. In a test each of these should be attempted to determine the security solution's effectiveness. This test's results record detection and protection for each of these stages.

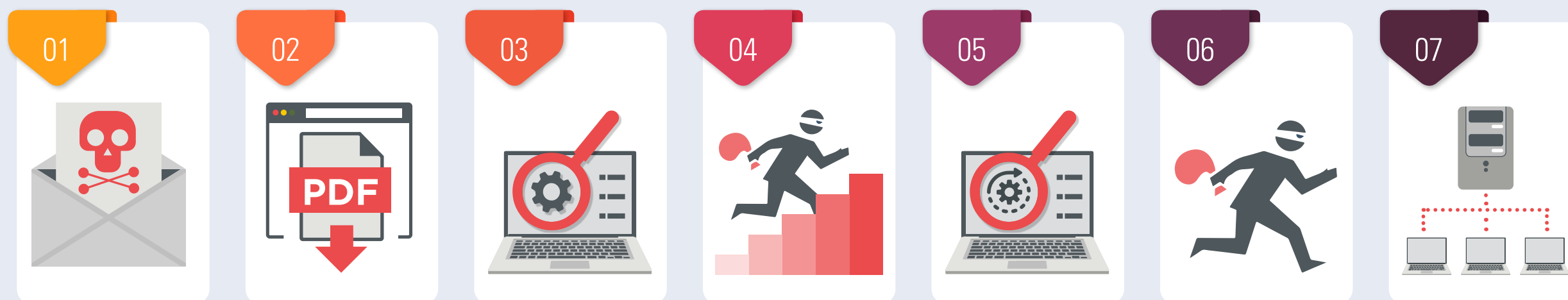
We measure how a product responds to the first stages of the attack with a detection and/or protection rating. Sometimes products allow threats to run but detect them. Other times they

might allow the threat to run briefly before neutralising it. Ideally they detect and block the threat before it has a chance to run. Products may delete threats or automatically contain them in a 'quarantine' or other safe holding mechanism for later analysis.

Should the initial attack phase succeed we then measure post-exploitation stages, which are represented by steps two through to seven below. We broadly categorise these stages as: Access (step 2); Action (step 3); Escalation (step 4); and Post-escalation (steps 5-7).

In **figure 1**, you can see a typical attack running from start to end, through various 'hacking' activities. This can be classified as a fully successful breach.

## Attack Chain Stages



**Figure 1.** A typical attack starts with an initial contact and progresses through various stages, including reconnaissance, stealing data and causing damage.



In **figure 2**, a product or service has interfered with the attack, allowing it to succeed only as far as stage 3, after which it was detected and neutralised. The attacker was unable to progress through stages 4 and onwards.

It is possible for an attack to run in a different order with, for example, the attacker attempting to connect to other systems without needing to escalate privileges. However, it is common for password theft (see step 5) to occur before using stolen credentials to move further through the network.

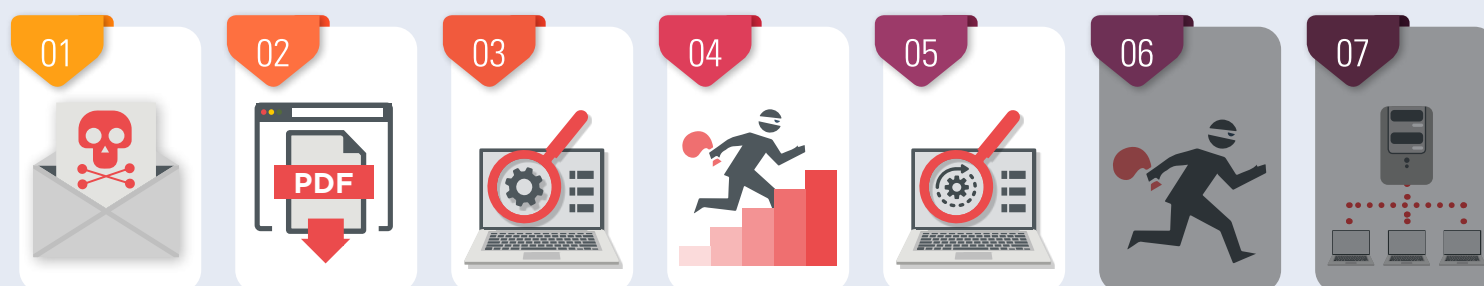
It is also possible that attackers will not cause noticeable damage during an attack. It may be that their goal is persistent presence on the systems to monitor for activities, slowly steal information and other more subtle missions.

In **figure 3**, the attacker has managed to progress as far as stage five. This means that the system has been seriously compromised. The attacker has a high level of access and has stolen passwords. However, attempts to exfiltrate data from the target were blocked, as were attempts to damage the system.

### Attack Chain: How Hackers Progress



**Figure 2.** This attack was initially successful but only able to progress as far as the reconnaissance phase.



**Figure 3.** A more successful attack manages to steal passwords but wholesale data theft and destruction was blocked.

# SE Labs

## INTELLIGENCE-LED TESTING

SE Labs helps advance the effectiveness of computer security through innovative, detailed and intelligence-led testing, run with integrity.



### Enterprises

Reports for enterprise-level products supporting businesses when researching, buying and employing security solutions.

**Download Now!**

### Small Businesses

Our product assessments help small businesses secure their assets without the purchasing budgets and manpower available to large corporations

**Download Now!**



### Consumers

Download free reports on internet security products and find out how you can secure yourself online as effectively as a large company

**Download Now!**

↓ **selabs.uk**



# Hackers vs. Targets



















When testing services against targeted attacks it is important to ensure that the attacks used are relevant. Anyone can run an attack randomly against someone else. It is the security vendor's challenge to identify common attack types and to protect against them. As testers, we need to generate threats that in some way relate to the real world.


















All of the attacks used in this test are valid ways to compromise an organisation. Without any security in place, all would succeed in attacking the target. Outcomes would include systems infected with ransomware, remote access to networks and data theft.

But we didn't just sit down and brainstorm how we would attack different companies. Instead we used current threat intelligence to look at what the bad guys have been doing over the last few years and copied them quite closely. This way we can test the services' abilities to handle similar threats to those faced by global governments, financial institutions and national infrastructure.

The graphic on this page shows a summary of the attack groups that inspired the targeted attacks used in this test. If a service was able to detect and protect against these then there's a good chance they are on track to blocking similar attacks in the real world. If they fail, then you might take their bold marketing claims about defeating hackers with a pinch of salt.

For more details about each APT group please see **4. Threat Intelligence (Ransomware Deep Attacks)** on page 13.

Hackers vs. Targets			
Attacker/ APT Group	Method	Target	Details
Avaddon			This group hires out ransomware as Ransomware as a Service (RaaS). It is used by multiple attackers against a wide range of targets.
Babuk			An RaaS threat that has targeted a wide range of industries. Notably, the developers have explicitly expressed hatred of certain communities, including Black Lives Matters and LGBT.
BadRabbit			Initially used against Russian targets, BadRabbit has also been used against Ukrainian infrastructure.
BlackBast			This threat is believed to acquire access to networks using information bought on the black market. It is highly targeted.
BlackCat			A prominent RaaS that was developed in the Rust programming language. It can target both Windows and Linux systems.
Diavol			Linked to the Trickbot gang, this ransomware is sometimes found alongside another ransomware malware called Conti.
Hello Kitty			A ransomware threat notable for an attack on the games developer CD Projekt Red. It stole games source code for the purposes of extortion.
RobbinHood			This threat was used to attack the city of Baltimore. It shut down the city's ability to take payment, costing the public \$18.2 million.
Lockbit			An RaaS threat used across a variety of industries and continues to be prolific in 2023.

Key					
 Aviation	 Banking and ATMs	 Defence	 Energy	 Education	 Entertainment
 Financial	 Gambling	 Generic RaaS	 Government Espionage	 Healthcare	 IT
 Law/ Legal	 Natural Resources	 Telecommunication	 Travel/ Transportation	 US Retail, Restaurant and Hospitality	

## 2. 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 chart.

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

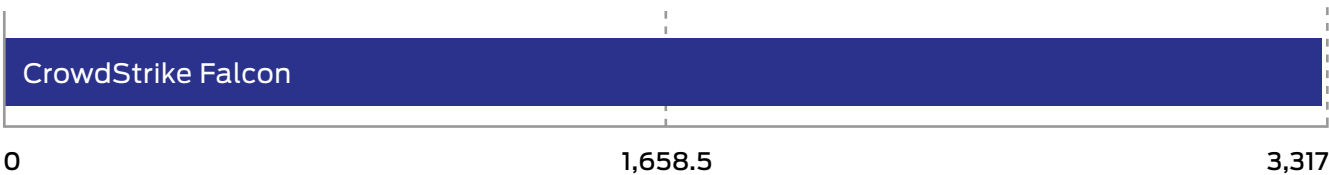
Not all protections, or detections for that matter, are equal. A product might completely block a URL, which stops the threat before it can even start its intended series of malicious events. Alternatively, the product might allow a web-based exploit to execute but prevent it from downloading any

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.

Scoring a product's response to a potential breach requires a granular method, which we outline in **3. Response Details (Ransomware Deep Attacks)** on page 11.

Total Accuracy Ratings			
Product	Total Accuracy Rating	Total Accuracy (%)	Award
CrowdStrike Falcon	3,302	99%	AAA



Total Accuracy Ratings combine protection and false positives.

# SE Labs Monthly Newsletter

Don't miss our security articles and reports

- Test reports announced
- Blog posts reviewed
- Security testing analysed
- **NEW:** Podcast episodes



**SUBSCRIBE NOW!**

### 3. Response Details (Ransomware Deep Attacks)

In this test security products are exposed to attacks, which comprise multiple stages. The perfect product will detect all relevant elements of an attack. The term 'relevant' is important, because sometimes detecting one part of an attack means it's not necessary to detect another.

For example, in the table below certain stages of the attack chain have been grouped together. These groups are as follows:

#### Delivery/ Execution (+10)

If the product detects either the delivery or execution of the initial attack stage then a detection for this stage is recorded.

#### Action (+10)

When the attack performs one or more actions, while remotely controlling the target, the product should detect at least one of those actions.

#### Privilege escalation/ action (+10)

As the attack progresses there will likely be an attempt to escalate system privileges and to perform more powerful and insidious actions. If the product can detect either the escalation process itself, or any resulting actions, then a detection is recorded.

#### Lateral movement/ action (+10)

The attacker may attempt to use the target as a launching system to other vulnerable systems.

Ransomware Deep Attack Group 1								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
1	✓	✓	✓	✓	✓	✓	N/A	N/A
2	✓	✓	✓	✓	✓	✓	N/A	N/A
3	✓	✓	✓	✓	✓	✓	✓	✓
4	✓	✓	✓	✓	✓	✓	✓	✓
5	✓	✓	✓	✓	✓	✓	✓	✓

Ransomware Deep Attack Group 2								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
6	✓	✓	✓	✓	✓	✓	N/A	N/A
7	✓	✓	✓	✓	✓	✓	N/A	N/A
8	✓	✓	✓	✓	✓	✓	✓	✓
9	✓	✓	✓	✓	✓	✓	✓	✓
10	✓	✓	✓	✓	✓	✓	✓	✓

If this attempt is discovered, or any subsequent action, a detection is reported.

The Detection Rating is calculated by adding points for each group in a threat chain that contains a detection. When at least one detection occurs in a single group, a 'group detection' is recorded and 10 points are awarded.

Each test round contains one threat chain, which itself contains four groups (as shown above),

meaning that complete visibility of each attack adds 40 points to the total value.

A product that detects the delivery of a threat, but nothing subsequently to that, wins only 10 points, while a product that detects delivery and action, but not privilege escalation or lateral behaviours, is rated at 20 for that test round.



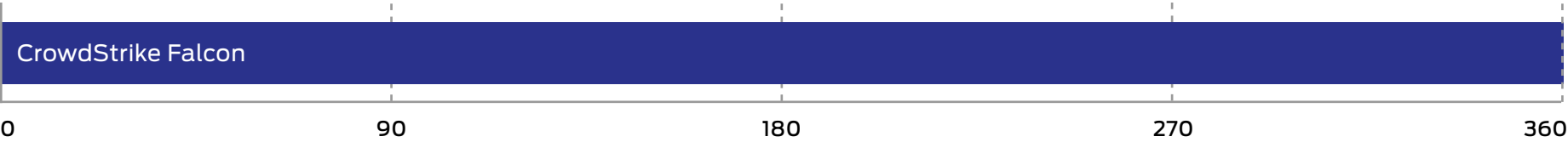
Response Details						
Ransomware Deep Attack	Number of Test Cases	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/Action	Lateral Movement/Action
Group 1	4	4	4	4	4	3
Group 2	4	4	4	4	4	3
Total	8	8	8	8	8	6

This data shows how the product handled different group stages of each APT. The Detection column shows the basic level of detection.

Detection Accuracy Rating Details				
Ransomware Deep Attack	Number of Test Cases	Attacks Detected	Group Detections	Detection Rating
Group 1	4	4	15	180
Group 2	4	4	15	180
Total	8	8	30	360

Different levels of detection, and failure to detect, are used to calculate the Detection Rating.

Detection Accuracy Ratings		
Product	Detection Accuracy Rating	Detection Accuracy Rating (%)
CrowdStrike Falcon	360	100%



Detection Ratings are weighted to show that how products detect threats can be subtler than just ‘win’ or ‘lose’.



## 4. Threat Intelligence (Ransomware Deep Attacks)

### Group 1

After the system was completely compromised, testers deployed ransomware from groups including Avaddon, BadRabbit and BlackCat.

How To Restore Your Files - Notepad

File Edit Format View Help

Hello! Your computer is locked and the data will be completely destroyed. To get an unlock key, you need to transfer \$100 to a bitcoin wallet bc1qqgylqg6yg88rhls33w6adtltdw8sac5j4jdvy After payment, do not hesitate to write to our contacts!) sorry\_bro\_zhalko@proton.me

The ransomware leaves instructions for victims to follow.



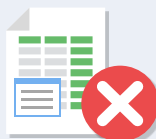


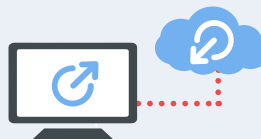

Process Explorer - Sysinternals: www.sysinternals.com [LILI\Administrator]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
fontdrvhost.exe		1,448 K	3,468 K	788	Usemode Font Driver Host	Microsoft Corporation
csrss.exe	0.05	1,824 K	5,268 K	500	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		2,480 K	11,104 K	556	Windows Log-on Application	Microsoft Corporation
fontdrvhost.exe		3,932 K	8,756 K	796	Usemode Font Driver Host	Microsoft Corporation
dwm.exe	0.57	34,440 K	63,744 K	348	Desktop Window Manager	Microsoft Corporation
explorer.exe	13.12	42,600 K	125,984 K	5140	Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe		1,732 K	9,276 K	7132	Windows Security notificatio...	Microsoft Corporation
Wireshark.exe	0.13	136,812 K	179,928 K	6828	Wireshark	The Wireshark developer ...
dumpcap.exe	0.01	2,944 K	9,924 K	2376	Dumpcap	The Wireshark developer ...
conhost.exe		6,668 K	14,236 K	2496	Console Window Host	Microsoft Corporation
procexp64.exe	3.13	19,016 K	39,944 K	2764	Sysinternals Process Explorer	Sysinternals - www.sysinter..
Tcpview.exe	30.83	4,888 K	16,376 K	2160	TCP/UDP endpoint viewer	Sysinternals - www.sysinter..
Procmon64.exe		2,296 K	13,584 K	3772	Process Monitor	Sysinternals - www.sysinter..
Procmon64.exe	3.50	42,480 K	57,776 K	4912	Process Monitor	Sysinternals - www.sysinter..
Microsoft.SharePoint.exe	0.09	7,308 K	18,636 K	4720	Microsoft SharePoint	Microsoft Corporation
f62f4261c914202f3445e122283...	32.94	6,312 K	17,468 K	5392	AnyDesk	AnyDesk Software GmbH

The line at the bottom shows the ransomware running. The line starting with SecurityHealthSystray.exe shows Microsoft Defender also running, but not helping.

### Example Ransomware Deep Attack Group 1

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Link	PowerShell	Query Registry	Access Token Manipulation - Create Process with Token	Modify Registry	External Remote Services	Exfiltration over C2 Channel
	Malicious File	System Information Discovery		Service Stop		Data Destruction
	Windows Command Shell	System Location Discovery - System Language Discovery				Data Encrypted for Impact
	Asymmetric Cryptography	File Deletion				Inhibit System Recovery
						Service Stop
 Spearphishing Link	 Malicious File	 File Deletion	 Access Token Manipulation - Create Process with Token	 Modify Registry	 External Remote Services	 Data Destruction

## Group 2

After the system was completely compromised, testers deployed ransomware from groups including Diavol, Lockbit and RobbinHood.

```
read=39019 kbytes, write=39501 kbytes, opened=8, encPS=246, totalFound=1241, TotalEncrypted=1203
(6888) [507] main: COINITIALIZE
(6888) [511] main: SET ERROR MODE
(6888) [515] main: STOP DOUBLE PROCESS RUN
(6888) [534] main: DO IOCP
(6888) [1257] DoIOCP: CPU AES +
(6888) [1268] DoIOCP: Number of threads 4
(7164) [712] ReadWritePoolThread: ReadWritePoolThread(7164) starting...
(6636) [712] ReadWritePoolThread: ReadWritePoolThread(6636) starting...
(4264) [712] ReadWritePoolThread: ReadWritePoolThread(4264) starting...
(1504) [712] ReadWritePoolThread: ReadWritePoolThread(1504) starting...
(2100) [1171] DriveSearchThread: Thread(2100): Looking for files in drive C:\
(6888) [1317] DoIOCP: Info: Waiting search threads job done
(1124) [1171] DriveSearchThread: Thread(1124): Looking for files in drive \\INDIA-DC\File Share
(376) [1171] DriveSearchThread: Thread(376): Looking for files in drive \\INDIA-DC\NETLOGON
(1528) [1171] DriveSearchThread: Thread(1528): Looking for files in drive \\INDIA-DC\SYSVOL
(1124) [1174] DriveSearchThread: Thread(1124): Search thread job done
(376) [1174] DriveSearchThread: Thread(376): Search thread job done
```


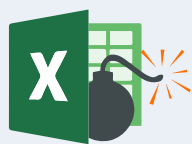





This is what ransomware looks like behind the scenes, when it's running. It is searching for and encrypting files on the target.

Process Explorer - Sysinternals: www.sysinternals.com [LIL\Administrator]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		3,700 K	21,324 K	5236	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,908 K	8,048 K	5308	Host Process for Windows S...	Microsoft Corporation
ctfmon.exe		3,576 K	15,000 K	5352	CTF Loader	Microsoft Corporation
svchost.exe		3,864 K	15,300 K	5516	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.01	1,960 K	7,488 K	5980	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,460 K	5,820 K	6080	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,188 K	10,140 K	6104	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.01	3,352 K	17,368 K	5336	Host Process for Windows S...	Microsoft Corporation
SearchIndexer.exe	0.80	21,420 K	26,372 K	6724	Microsoft Windows Search I...	Microsoft Corporation
SearchProtocolHost.exe		2,620 K	13,668 K	3840	Microsoft Windows Search P...	Microsoft Corporation
SearchFilterHost.exe		1,532 K	7,148 K	6692	Microsoft Windows Search F...	Microsoft Corporation
SecurityHealthService.exe		3,592 K	14,340 K	2980	Windows Security Health Se...	Microsoft Corporation
svchost.exe		1,320 K	6,232 K	6760	Host Process for Windows S...	Microsoft Corporation
SgmnBroker.exe		3,536 K	7,436 K	3248	System Guard Runtime Monit...	Microsoft Corporation
svchost.exe		2,700 K	11,564 K	2628	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,752 K	9,744 K	4848	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,964 K	12,188 K	4420	Host Process for Windows S...	Microsoft Corporation
lsass.exe	< 0.01	7,364 K	22,232 K	624	Local Security Authority Proc...	Microsoft Corporation
fontdrvhost.exe		1,440 K	3,440 K	788	Usemode Font Driver Host	Microsoft Corporation
csrss.exe	0.10	1,776 K	5,020 K	484	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		2,484 K	11,204 K	540	Windows Log-on Application	Microsoft Corporation
fontdrvhost.exe		3,100 K	6,656 K	780	Usemode Font Driver Host	Microsoft Corporation
dwm.exe	0.54	30,376 K	62,000 K	340	Desktop Window Manager	Microsoft Corporation
explorer.exe	3.42	43,528 K	119,676 K	5636	Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe	0.02	1,736 K	9,036 K	332	Windows Security notificatio...	Microsoft Corporation
procexp64.exe	2.03	19,036 K	40,080 K	2960	Sysinternals Process Explorer	Sysinternals - www.sysinter...
9a7daafc56300bd94ceef23...	81.94	52,440 K	62,316 K	1048		
conhost.exe	0.02	7,048 K	17,512 K	752	Console Window Host	Microsoft Corporation

The line highlighted in blue shows the ransomware executing on the target. Two lines above it Microsoft's anti-virus is shown to be running.

### Example Ransomware Deep Attack Group 2

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Attachment	Malicious File	Process Discovery	Bypass User Account Control	Credentials in Files	External Remote Services	Exfiltration Over Alternative Protocol
	Windows Command Shell	System Information Discovery	Valid Accounts	System Owner/ User Discovery		Data Destruction
	Software Packing	Credentials from Web Browsers		Modify Registry		Data Encrypted for Impact
	Masquerading			Windows Service		Inhibit System Recovery
						Service Stop
						
Spearphishing Attachment	Masquerading	System Information Discovery	Valid Accounts	System Owner/ User Discovery	External Remote Services	Data Encrypted for Impact



## 5. Protection Ratings (Ransomware Direct Attacks)

The following results relate to the direct ransomware attacks, in which ransomware payloads are sent directly to targets in realistic ways, such as via phishing emails.

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

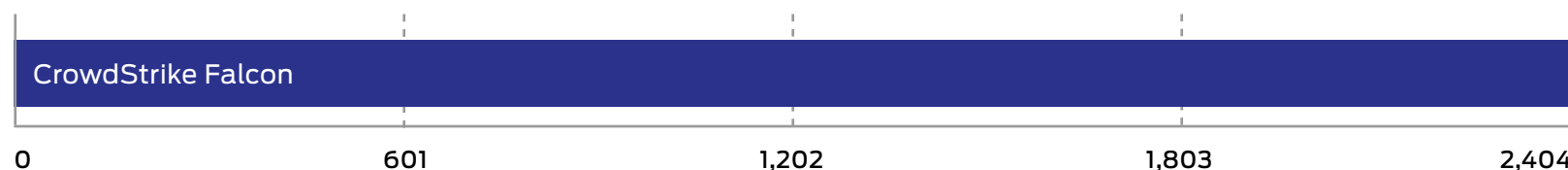
We calculate the protection ratings using the following formula:

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

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 **7. Protection Details (Ransomware Direct Attacks)** on page 16 to roll your own set of personalised ratings.

Protection Ratings		
Product	Protection Rating	Protection Rating (%)
CrowdStrike Falcon	2,404	100%

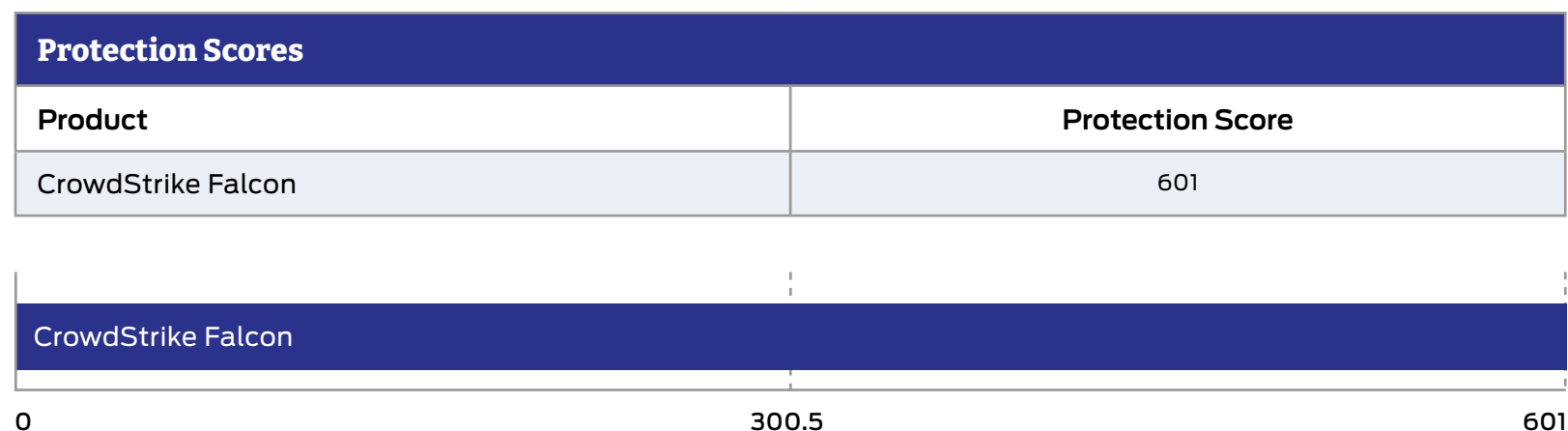


Protection Ratings are weighted to show that how products handle threats can be subtler than just 'win' or 'lose'

## 6. Protection Scores (Ransomware Direct Attacks)

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.

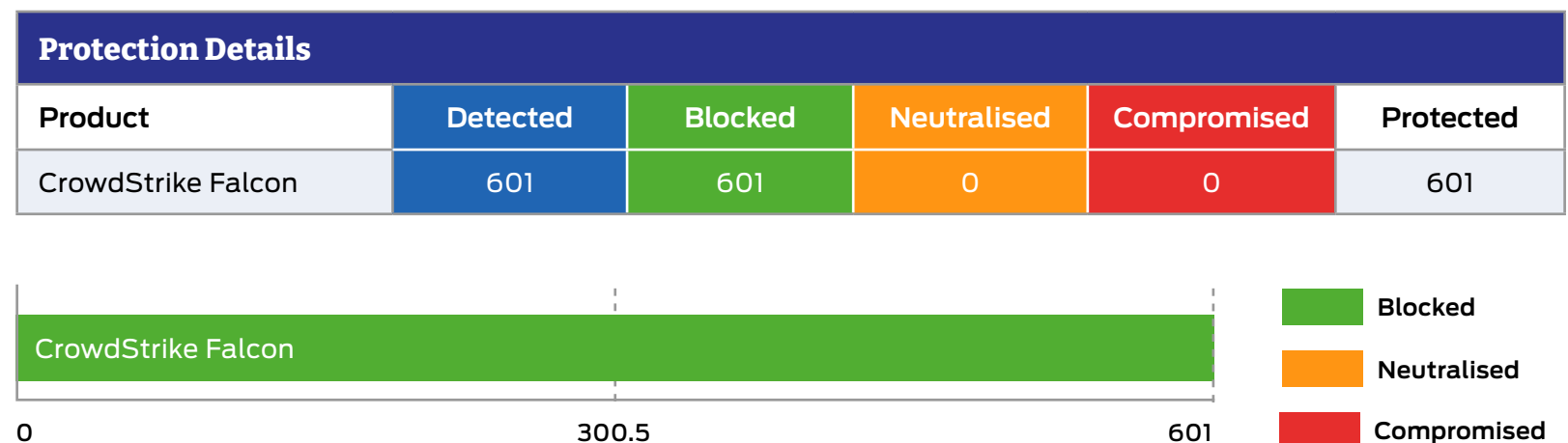


Protection Scores are a simple count of how many times a product protected the system.

## 7. Protection Details (Ransomware Direct Attacks)

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.



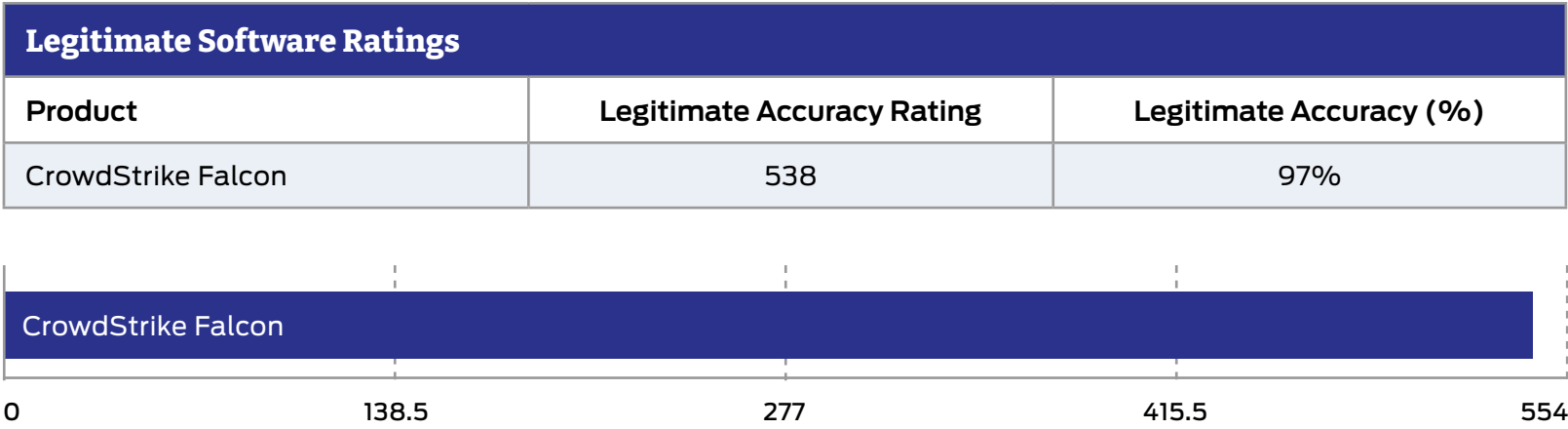
This data shows in detail how each product handled the threats used.

# 8. 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.

To understand how we calculate these ratings, see **8.3 Accuracy Ratings** on page 19.



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

# DE:CODED

## Deciphering Cyber Security

Understand cybersecurity and other security issues. Practical and insightful, our experts have experience in attacking and defending in the physical and digital worlds. Peek behind the curtain with the Cyber Security **DE:CODED** podcast.

# DE:CODED

SE Labs



## 8.1 Interaction Ratings

It is crucial that endpoint security products not only stop, or at least detect threats, but that they allow legitimate applications to install and run without misclassifying them as 'malware'. Such an error is known as a 'false positive' (FP).

In reality, genuine FPs are quite rare in testing. In our experience it is unusual for a legitimate application to be classified as 'malware'. More often it will be classified as 'unknown', 'suspicious' or 'unwanted' (or terms that mean much the same thing).

We use a subtle system of rating an Endpoint's approach to legitimate objects, which takes into account how it classifies the application and how it presents that information to the user. Sometimes the Endpoint software will pass the buck and demand that the user decide if the application is safe or not. In such cases the product may make a recommendation to allow or block. In other cases, the product will make no recommendation, which is possibly even less helpful.

If a product allows an application to install and run with no user interaction, or with simply a brief notification that the application is likely to be safe, it has achieved an optimum result. Anything else is a Non-Optimal Classification/Action (NOCA). We think that measuring NOCAs is more useful than counting the rarer FPs.

	None (allowed)	Click to Allow (default allow)	Click to Allow/Block (no recommendation)	Click to Block (default block)	None (blocked)	
Object is Safe	2	1.5	1			A
Object is Unknown	2	1	0.5	0	-0.5	B
Object is not Classified	2	0.5	0	-0.5	-1	C
Object is Suspicious	0.5	0	-0.5	-1	-1.5	D
Object is Unwanted	0	-0.5	-1	-1.5	-2	E
Object is Malicious				-2	-2	F
	1	2	3	4	5	

Interaction Ratings			
Product	None (allowed)	Click to allow/block (no recommendation)	None (blocked)
CrowdStrike Falcon	74	0	1

Products that do not bother users and classify most applications correctly earn more points than those that ask questions and condemn legitimate applications.

## 8.2 Prevalence Ratings

There is a significant difference between an Endpoint product blocking a popular application such as the latest version of Microsoft Word and condemning a rare Iranian dating toolbar for Internet Explorer 6. One is very popular all over the world and its detection as malware (or something less serious but still suspicious) is a big deal. Conversely, the outdated toolbar won't have had a comparably large user base even when it was new. Detecting this application as malware may be wrong, but it is less impactful in the overall scheme of things.

With this in mind, we collected applications of varying popularity and sorted them into five separate categories, as follows:

1. Very High Impact
2. High Impact
3. Medium Impact
4. Low Impact
5. Very Low Impact

Incorrectly handling any legitimate application will invoke penalties, but classifying Microsoft Word as malware and blocking it without any way for the user to override this will bring far greater penalties than doing the same for an ancient niche toolbar. In order to calculate these relative penalties, we assigned each impact category with a rating modifier, as shown in the table above.

Legitimate Software Prevalence Rating Modifiers	
Impact Category	Rating Modifier
Very High Impact	5
High Impact	4
Medium Impact	3
Low Impact	2
Very Low Impact	1

Applications were downloaded and installed during the test, but third-party download sites were avoided and original developers' URLs were used where possible. Download sites will sometimes bundle additional components into applications' install files, which may correctly cause anti-malware products to flag adware. We remove adware from the test set because it is often unclear how desirable this type of code is.

The prevalence for each application and URL is estimated using metrics such as third-party download sites and the data from Alexa.com's global traffic ranking system.

## 8.3 Accuracy Ratings

We calculate legitimate software accuracy ratings by multiplying together the interaction and prevalence ratings for each download and installation:

**Accuracy rating = Interaction rating x Prevalence rating**

If a product allowed one legitimate, Medium impact application to install with zero interaction with the user, then its Accuracy rating would be calculated like this:

**Accuracy rating = 2 x 3 = 6**

This same calculation is made for each legitimate application/site in the test and the results are summed and used to populate the graph and table shown under **8. Legitimate Software Ratings** on page 17.

## 8.4 Distribution of Impact Categories

Endpoint products that were most accurate in handling legitimate objects achieved the highest ratings. If all objects were of the highest prevalence, the maximum possible rating would be 500 (50 incidents x (2 interaction rating x 5 prevalence rating)).

In this test there was a range of applications with different levels of prevalence. The table below shows the frequency:

Legitimate Software Category Frequency	
Prevalence Rating	Frequency
Very High Impact	24
High Impact	25
Medium Impact	11
Low Impact	9
Very Low Impact	6

## 9. Conclusions

This report looks at how effectively a security product can protect against a wide range of ransomware attacks. It also investigates the product’s capabilities in tracking the behaviour of attackers that use ransomware as a final payload.

### Ransomware Deep Attacks

In the first part of the test, we ran full, advanced hacking attacks against the target systems and installed ransomware at the end of each attack. This accurately reflects how attackers breach large organisations.

We wanted to assess how well **CrowdStrike Falcon** could track the hacking attacks through the network, as well as registering the ransomware attacks at the end. For each test case we used 10 different payloads that led to ransomware. These were selected from the larger group of ransomware files used in the second part of the testing.

The methods of attacking the target systems were a combination of tactics used by a number of different ransomware groups. You can see a summary of these in **4. Threat Intelligence**, pages 13 and 14, and a full rundown of each in **Appendix D: Ransomware Deep Attack Details**.

**CrowdStrike Falcon** detected all 10 of the attacks and managed to generate alerts for all the attack

stages in each. Let’s look at what this means in terms of overall, useful detection.

We use a concept called ‘group detection’. For example, we expect a product to detect either the delivery or execution of a malicious file. While our scoring allows a product to achieve top marks if it detects one or the other, it’s worth noting that **CrowdStrike Falcon’s** exceptional performance derives from its ability to detect both events in this group.

We deployed ransomware at different stages in the attacks. For test cases 1, 2, 6 and 7, we installed ransomware on the main target systems. For the other test cases we jumped from these target systems to others on the internal network (moving laterally) and ran ransomware on these deeper targets. This is why the Lateral Movement and Lateral Action results for test cases 1, 2, 6 and 7 are not applicable (N/A).

The results show that **CrowdStrike Falcon** not only detected the ransomware in every case but had a thorough insight into the entire process of hacking the network. The product detected every stage of every attack from delivery onwards. It issued alerts when the attack performed an action and when the attack attempted to escalate system privileges. In the test cases where the internal network was targeted, **CrowdStrike Falcon** detected the lateral attacks against the deeper targets.



## Ransomware Direct Attacks

In the second part of the test, we used a large group of ransomware attack files. The files formed a combination of malicious software both known and unknown by security researchers. Our goal was to see how well a product could identify ransomware that has already been analysed by security experts, as well as new, never-before-seen variations that represent potential future attacks.

We identified nine prevalent families of ransomware and from each selected 10 malware files that attackers have used in the past. We then modified these files using techniques designed to make the malware look different (although the malware would perform the same malicious activities). These files represented malware that could reasonably be expected to appear now and in the near future. For each 'original' malware file we created a minimum of two variations. We discarded any samples that were broken by our modifications.

The test comprised 601 functional ransomware payloads, capable of damaging systems in the absence of protective software. This is the largest ransomware test published to date.

We exposed target systems to these ransomware files using very direct methods of attack, such as sending the malware (or links to the malware) via phishing emails.

**CrowdStrike Falcon** detected and blocked every single ransomware file, including all of the new variants. This is significant because our tweaks to make ransomware variants mimic how criminals launch ransomware in the wild. They deploy several variants to delay detection which allows the original ransomware to spread among many more victims. **CrowdStrike Falcon's** quick recognition of the ransomware's malicious behaviour, regardless of its disguise, allowed it to almost simultaneously repel the attack.

## Overall

**CrowdStrike Falcon** only missed a 100% Total Accuracy Rating by a single percentage point due to the misclassification of an application that was legitimate. Otherwise, it performed exceptionally well in difficult tests for both the detection of and protection against ransomware. **CrowdStrike Falcon** achieved an AAA rating because of this excellent result.

# Enterprise Security Testing Services for CISOs

**Elevate your cyber security strategy with SE Labs, the world's leading security testing organisation.**

SE Labs works with large organisations to support CISOs and their security teams:

- Validate existing combination of security products and services.
- Provide expert partnership when choosing and deploying new security technologies.

SE Labs provides in-depth evaluations of the cyber security that you are considering, tailored to the exact, unique requirements of your business.

**For an honest, objective and well-informed view of the cyber security industry contact us now at**

**[selabs.uk/contact](https://selabs.uk/contact)**

# Appendices

## Appendix A: Terms Used

Term	Meaning
Compromised	The attack succeeded, resulting in malware running unhindered on the target. In the case of a targeted attack, the attacker was able to take remote control of the system and carry out a variety of tasks without hindrance.
Blocked	The attack was prevented from making any changes to the target.
False positive	When a security product misclassifies a legitimate application or website as being malicious, it generates a 'false positive'.
Neutralised	The exploit or malware payload ran on the target but was subsequently removed.
Complete Remediation	If a security product removes all significant traces of an attack, it has achieved complete remediation.
Target	The test system that is protected by a security product.
Threat	A program or sequence of interactions with the target that is designed to take some level of unauthorised control of that target.
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.

## Appendix B: FAQs

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

- The test was conducted between 25th August to 18th September 2023.
- The product was configured according to its vendor's recommendations.
- Targeted attacks were selected and verified by SE Labs.
- Malicious and legitimate data was provided to partner organisations once the test was complete.
- SE Labs conducted this endpoint security testing on physical PCs, not virtual machines.

### 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 We are a customer considering buying or changing our endpoint protection and/ or endpoint detection and response (EDR) product. Can you help?

**A** Yes, we frequently run private testing for organisations that are considering changing their security products. Please contact us at [info@selabs.uk](mailto:info@selabs.uk) for more information.

## Appendix C: 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)
CrowdStrike	Falcon	6.58.17210.0	7.01.17311.0

## Appendix D: Ransomware Deep Attack Details

Ransomware Deep Attack Group 1							
Test Case	Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
1	Spear phishing Attachment	Powershell	Process Injection	Access Token Manipulation - Create Process with Token	Disable or Modify Tools	N/A	N/A
		Obfuscated Files or Information	System Information Discovery		File Deletion		
		Malicious File	System Service Discovery		Exfiltration Over C2 Channel		
		Windows Command Shell			Data Destruction		
		Asymmetric Cryptography			Data Encrypted for Impact		
					Inhibit System Recovery		
					Service Stop		
2	Spear phishing Link	Windows Command Shell	System Location Discovery - System Language Discovery	Access Token Manipulation - Token Impersonation/Theft Process Injection	Ingress Tool Transfer	N/A	N/A
		Malicious File	Permission Groups Discovery - Domain Groups		Data Destruction		
		Native API	Query Registry		Data Encrypted for Impact		
		Match Legitimate Name or Location			Inhibit System Recovery		
					Service Stop		
3	Spear phishing Link	Powershell	Query Registry	Access Token Manipulation - Create Process with Token	Modify Registry	External Remote Services	Exfiltration over C2 Channel
		Malicious File	System Information Discovery		Service Stop		Data Destruction
		Windows Command Shell	System Location Discovery - System Language Discovery				Data Encrypted for Impact
		Asymmetric Cryptography	File Deletion				Inhibit System Recovery
			Service Stop				
4	Spear phising Attachment	Windows Command Shell	System Information Discovery	Access Token Manipulation - Token Impersonation/Theft Process Injection	Disable or Modify Tools	Lateral Tool Transfer	Exfiltration over C2 Channel
		Malicious File	Permission Groups Discovery - Domain Groups		Inhibit System Recovery	Remote Desktop Protocol	Data Destruction
		Visual Basic	Process Injection				Data Encrypted for Impact
			File Deletion				Inhibit System Recovery
5	Spear phishing Attachment	Windows Command Shell	System Information Discovery	Access Token Manipulation - Token Impersonation/Theft Process Injection	Ingress Tool Transfer		External Remove Services
		Malicious File	Query Registry		Modify Registry	Domain Accounts	Data Destruction
		Native API					Data Encrypted for Impact
		Match Legitimate Name or Location					Inhibit System Recovery

## Ransomware Deep Attack Group 2

Test Case	Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action	
1	Spear phishing Attachment	Malicious File	Process Discovery	Bypass User Account Control	Data From Local System	N/A	N/A	
		Windows Command Shell	System Information Discovery	Valid Accounts	Exfiltration Over C2 Channel			
		PowerShell	Permission Groups Discovery		System Owner/User Discovery			
		Deobfuscate/Decode Files or Information	System Network Configuration Discovery		Data Destruction			
		Obfuscated Files or Information			Data Encrypted for Impact			
					Inhibit System Recovery			
					Service Stop			
2	Spear phishing Link	Malicious File	Process Discovery	Bypass User Account Control	Data From Local System	N/A	N/A	
		Windows Command Shell	System Information Discovery	Valid Accounts	Exfiltration Over C2 Channel			
		Masquerading	Account discovery - Local Account		Credentials from Web Browsers			
		Software Packing	System Network Configuration Discovery		Data Destruction			
		Native API			Data Encrypted for Impact			
		Symmetric Cryptography			Inhibit System Recovery			
					Service Stop			
3	Spear phishing Link	Malicious File	Process Discovery	Bypass User Account Control	Data From Local System	External Remote Services	Exfiltration Over Alternative Protocol	
		Windows Command Shell	System Information Discovery	Valid Accounts	Exfiltration Over C2 Channel		Automated Collection	
		Software Packing	Network Share Discovery		Modify Registry		Data Destruction	
		Obfuscated Files or Information	System Service Discovery				Data Encrypted for Impact	
							Inhibit System Recovery	
							Service Stop	
4	Spear phishing Attachment			Malicious File		Process Discovery	Bypass User Account Control	Credentials in Files
		Windows Command Shell		System Information Discovery	Valid Accounts	System Owner/User Discovery	Data Destruction	
		Software Packing	Credentials from Web Browsers	Modify Registry		Data Encrypted for Impact		
		Masquerading		Windows Service		Inhibit System Recovery		
				Service Stop				
5	Spear phishing Link	Malicious File	Process Discovery	Bypass User Account Control	Scheduled Task	Lateral Tool Transfer	Exfiltration Over C2 Channel	
		Windows Command Shell	System Information Discovery	Valid Accounts	Registry Run Keys / Startup Folder		Automated Collection	
		Obfuscated Files or Information	Credentials from Web Browsers				Data Destruction	
			System Owner/User Discovery				Data Encrypted for Impact	
							Inhibit System Recovery	
		Service Stop						



## 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.