SE Labs

INTELLIGENCE-LED TESTING

CPU DETECTION

Enterprise Advanced Security (Ransomware)

Intel

Threat Detection Technology

February 2023

selabs.uk

info@SELabs.uk

selabs.uk/newsletter

blog.selabs.uk

SE Labs tested Intel's hardware approach to ransomware detection, using a wide 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 included Windows PCs, both Intel vPro-based hardware and alternative AMD platforms. All were attacked in the same way by testers acting as we observe ransomware groups to behave.

Attacks used original ransomware malware, as seen in the wild during recent months, as well as more advanced variations designed to evade detection. In all cases the ransomware's goal was to steal, encrypt and destroy sensitive data on the target systems.

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 Gorbold
Anila Johny
Erica Marotta
Luca Menegazzo
Jeremiah Morgan
Julian Owusu-Abrokwa
Joseph Pike
Georgios Sakatzidi
Dimitrios Tsarouchas
Stephen Withey

IT SUPPORT
Danny King-Smith
Chris Short

PUBLICATION
Sara Claridge
Colin Mackleworth

Website selabs.uk
Email info@SELabs.uk
LinkedIn linkedin.com/company/se-labs/
Blog blog.selabs.uk
Phone +44 (0)203 875 5000
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 Information Alliance (VIA); the Anti-Malware Testing Standards Organization (AMTSO); and NetSecOPEN.

Contents

Introduction 04
Executive Summary 05
Enterprise Advanced Security (Ransomware) Award 05
1. How We Tested 06
Hackers vs. Targets 07
2. Total Accuracy Ratings 08
3. Detection Scores 09
4. Legitimate Software Ratings 10
4.1 Interaction Ratings 11
4.2 Prevalence Ratings 12
4.3 Accuracy Ratings 12
4.4 Distribution of Impact Categories 12
5. Conclusions 13
Appendicies 14
Appendix A: Terms Used 14
Appendix B: FAQs 14
Appendix C: Original and Evasive Detections 15
Appendix D: Ransomware Family Detections 15
Appendix E: Tested System Details 15

Document version 1.0 Written 9th February 2023
1.1 Updated 24th April 2023: Score Corrections and Clarifications

INTRODUCTION

Ransomware Detection Using Hardware

Computer processors get the final word when running programs. Can they judge bad code from good?

All malware has to run on a target to achieve its goal. Whether it's a remote access Trojan, a wild internet worm or devastating ransomware, malware is most likely software that has to run on a PC of some sort. The anti-virus software industry tries to detect and stop these threats, but news headlines suggest it's not winning the war.

Part of the problem is that attackers can disguise malware. In the same way you might try to slip past a security guard in thick glasses and a wig, hackers can take their regular code and make it look different. There are many ways to do this, but before it can achieve its ultimate goal, malware has to run, or execute. And at that stage it drops its disguise, at least as far as the hardware it runs on is concerned. As the code runs, its intentions become clear.

Security on a Chip

And this presents an opportunity for defenders - detect malware at the very last moment, just as it reveals itself while executing. The concept of 'security on a chip' has been around for a long time and when Intel bought McAfee in 2010 the world waited for anti-virus processors. They didn't really appear and seven years later McAfee and Intel separated.

But now Intel claims that it has introduced anti-malware to its vPro hardware platform. By monitoring code as it executes, it hopes to detect malware and inform compatible security software when it does. It claims to do this by using pattern matching, via machine learning, to spot suspicious behaviour. The goal is to have a combination of security software and hardware working together to prevent infections.

Ransomware

Ransomware is a prevalent, damaging and expensive threat that can cripple the largest organisations and completely destroy smaller ones. But it's just code that you don't want to run on your computer. It's not even that unpredictable. In most cases it will encrypt data, delete files and steal information.

This presents another opportunity for detection. Regardless of how a file 'looks', if it starts doing the usual bad things you'd expect from ransomware, it's probably safe to identify it as a threat. Intel's claim is that its Threat Detection Technology is capable of spotting malicious trends with the help of machine learning.

Origin Story

When detection happens at the hardware level, it doesn't matter if the malware appears in a Zip file, is downloaded from Dropbox or is a script that hides inside an Office document. The malware doesn't even need to land on the hard disk. File-less and other threats all need to run on the processor.

In this report we test Intel's claims that the Threat Detection Technology built into its vPro platform can detect known ransomware and disguised variations.

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 Intel's CPU-based approach to detecting ransomware, namely the Threat Detection Technology (TDT) built into the Intel vPro hardware platform. The test exposed computer systems running both Intel vPro hardware and AMD Ryzen Pro systems to a wide range of ransomware attacks. These included recent, prevalent ransomware payloads alongside new, never-before-seen variations.

Intel claims that TDT uses machine learning to detect patterns of malicious behaviour, as it appears to the CPU

We examined the different hardware platforms' abilities to:

- **Detect known ransomware**
- **Detect unknown ransomware**
- **Detect intentionally evasive ransomware**

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

Intel vPro's Intel Threat Detection performed very well, providing 93% detection against all of the known and unknown threats without assistance from software security solutions. Combined with EDR, the detection increased to 97%.

In some cases the EDR product detected threats that Intel Threat Detection Technology (TDT) did not, and in others TDT detected threats that the EDR solution missed. There were no false positive results produced by any combination of hardware and software options.

Executive Summary

Product Tested	Detection Score (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Intel TDT (with EDR)	97%	100%	99%
Intel TDT (no EDR)	93%	100%	97%
Intel TDT (inactive EDR)	90%	100%	96%
AMD (with EDR)	73%	100%	88%

The Detection Score shows how effective each product was at detecting the ransomware samples. The Total Accuracy Rating combines detection ability with the products' accuracy when handling legitimate files.

For exact percentages, see **2. Total Accuracy Ratings** on page 8.

Enterprise Advanced Security (Ransomware) Award

The following product wins the SE Labs award:

SE Labs

AAA

February 2023

Enterprise Advanced Security (Ransomware)

Intel
Threat Detection Technology

1. How we Tested

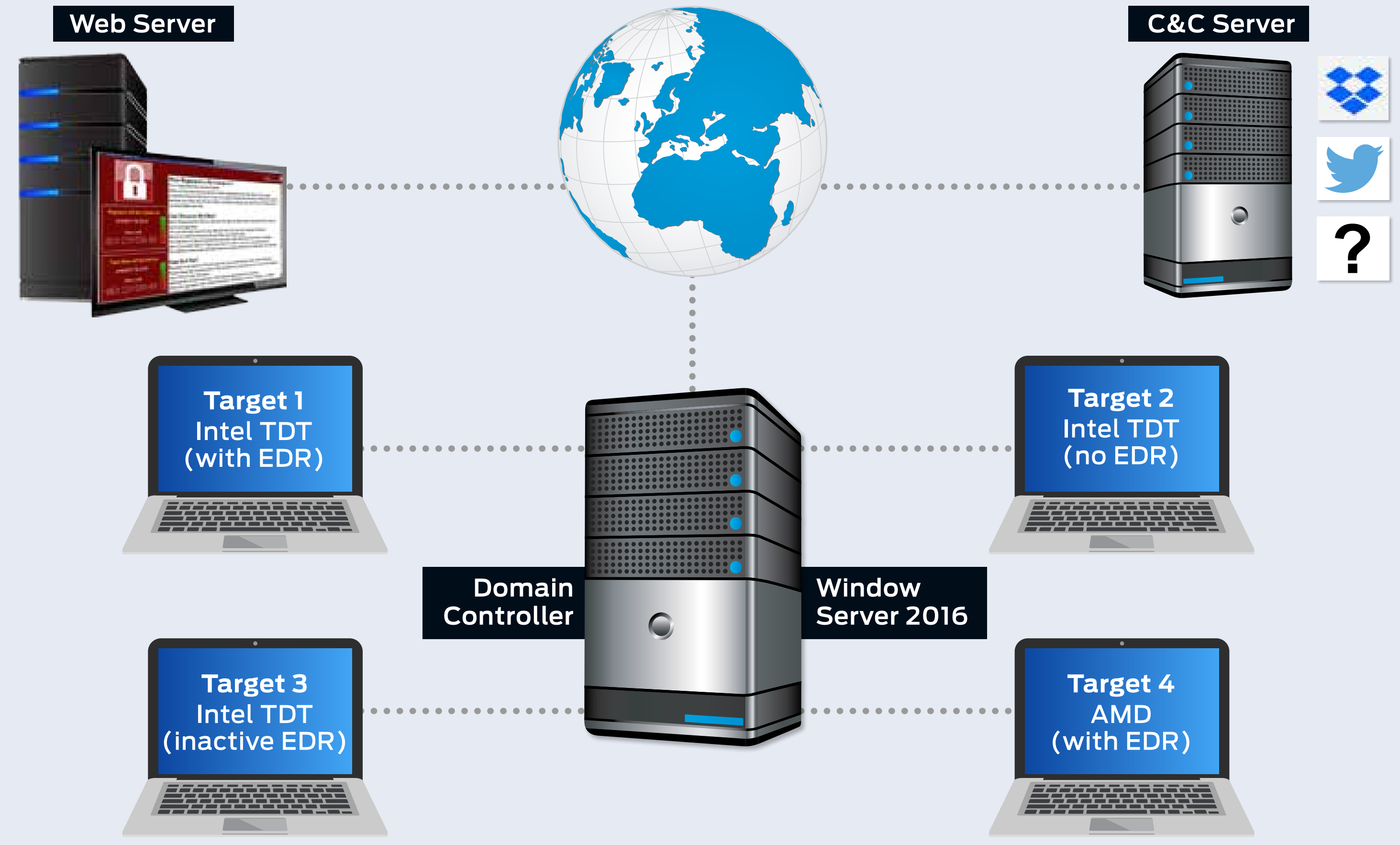
For this scientific security test of hardware security we used laptops that were available to businesses and consumers at the time of testing. Each contained the latest processors from Intel and AMD. They were equipped with Endpoint Detection and Response (EDR) software and we then attacked each system using a variety of ransomware attacks. The attacks were launched in a realistic way, giving the security products full opportunities to detect the attacks at all stages.

The testers recorded the detections made by the EDR products in each situation, as well as detections made by Intel Threat Detection Technology (TDT), which Intel claims uses machine learning to determine malicious behaviour as code executes, but acting as a standalone hardware sensor. To access this data we used an application with the capability of reporting TDT's detections independently (i.e. not through the EDR software).

The test included an Intel TDT system that ran inactive EDR software. The purpose for this was to determine if the very presence of EDR on the system hampered Intel TDT, aided it or made no difference.

The attacks were made using the most prevalent ransomware from nine different groups, or 'families'. We used 10 ransomware attacks from each family, all of which we verified were capable of working when used on a system without protection.

Test Network Example



This example of a test network shows one possible topology and ways in which enterprises and criminals deploy resources

Cyber criminals frequently use evasive tactics to bypass EDR and other endpoint 'anti-virus' products. We replicated this by making two additional versions of each attack. In each case the files were just as capable of causing problems for victims, but appeared to be different. We used the same obfuscation approaches and tools that cyber criminals use on a routine basis.

By disguising the files, we put more pressure on the security solutions to detect the threats, many of which are already known to the security industry. While not strictly 'zero day' threats, we created unknown malware variants. Security products need to be sufficiently advanced to detect these.

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.

Hackers vs. Targets

Attacker/APT Group	Method	Target	Details
AvosLocker	@	$	Hired out as 'Ramsomware as a Service (RaaS)' and used against a wide range of targets.
Conti	@	🏛	Affects all versions of Windows. Attackers known to leak stolen data.
DarkSide	****	◎	An RaaS operation that focusses on large, well resourced organisations.
Dharma	RDP	◎ 🇬🇧	Installed on target systems over remote desktop connections (RDP).
Maze	SPAM	◎ 🇺🇸	Often installed using stolen or guessed credentials.
NetWalker	SPAM >_	◎	File-less ransomware that uses DLL injection in memory.
Ragnar Locker	RDP ✊	🏭	Highly customised. Attackers known to leak stolen data.
REvil (Sodinokibi)	✊	◎ 💀	Considered the 4th most used ransomware globally.
Ryuk	@	◎	Focussed on businesses. Attackers known to leak stolen data.

Key

✈ Aviation	🏛 Banking and ATMs	🏭 Energy	🎭 Entertainment
$ Financial	🃏 Gambling	◎ Generic	◎ 💀 Generic RaaS
◎ 🇬🇧 Generic/ UK	◎ 🇺🇸 Generic/ US	🏛 Government Espionage	⊕ Healthcare
⚖ Law	⛽ Natural Resources	🛒 US Retail, Restaurant and Hospitality	

2. Total Accuracy Ratings

Judging the effectiveness of endpoint security, hardware or otherwise, is a subtle art. There are many factors at play when assessing how well products, or combinations of products, perform. To make things easier we've combined all of our results into one easy-to-understand chart.

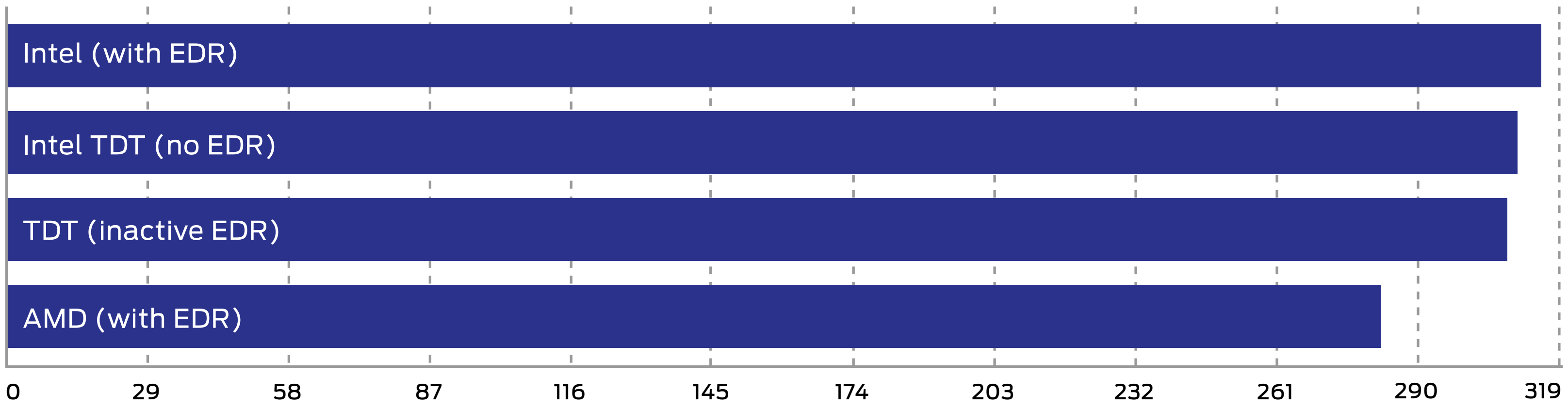
The chart below takes into account not only the products' abilities to detect ransomware, but also their handling of non-malicious objects such as useful website addresses (URLs) and legitimate, harmless applications.

Combining these two types of results is important because a security product that detects everything (both good and bad) as malware isn't much use. Neither is one that fails to alert on any software (evil and useful). Balancing the aggression of detections, so that most malware is flagged up and users can run their favourite apps without alarming, false alerts is ideal.

The Total Accuracy Ratings show how well each of the combinations of products handle the balance of security. For more information about threat details, see **3. Detection Scores** on page 9.

Total Accuracy Ratings

Product	Total Accuracy Rating	Total Accuracy (%)
Intel TDT (with EDR)	315	99%
Intel TDT (no EDR)	310	97%
Intel TDT (inactive EDR)	305	96%
AMD (with EDR)	282	88%



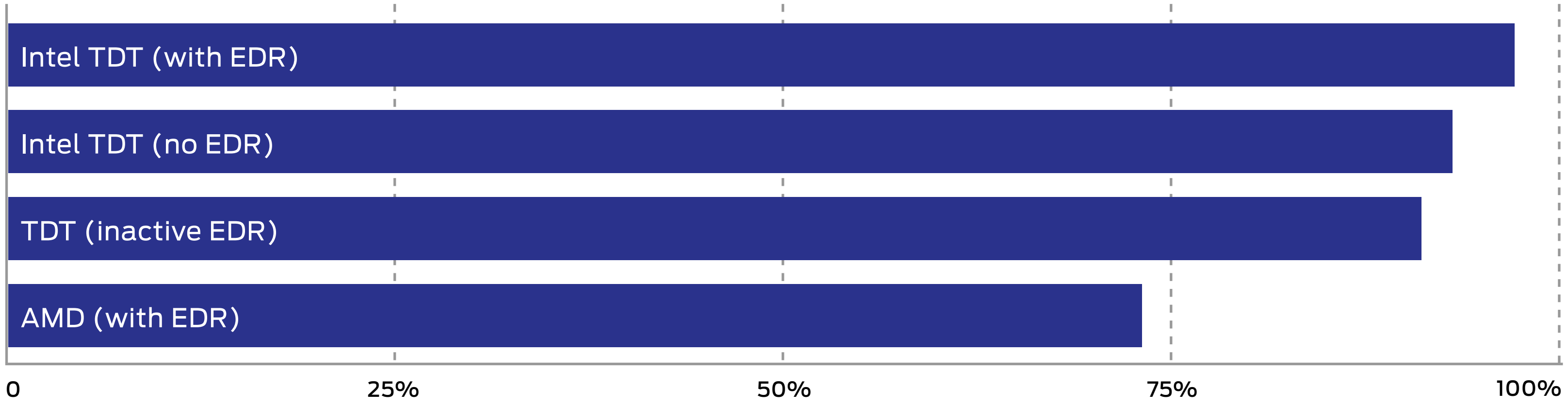
The Total Accuracy Ratings show how well each of the combinations of products handle the balance of security

3. Detection Scores

This graph shows the overall level of detection available with each of the products, or combinations of solutions. This includes all of the original ransomware attacks, as well as the evasive variations produced to replicate attackers actively trying to avoid detection by anti-malware solutions.

For more details, including which products detected which types of threat, see **Appendix C: Original and Evasive Detections** on page 15 and **Appendix D: Ransomware Family Detections** on page 15.

Detection Scores	
Product	**Detection Score (%)**
Intel TDT (with EDR)	97%
Intel TDT (no EDR)	93%
Intel TDT (inactive EDR)	90%
AMD (with EDR)	73%



The Detection Scores show how effective each solution, or combination of solutions, was at identifying each ransomware attack.

Subscribe
Past issues
Translate
RSS
SE Labs
INTELLIGENCE-LED TESTING
News from the security lab
FREE
Security opportunities for Managed Service Providers
Most popular reports of 2022
Your favourite blog posts and podcast episodes

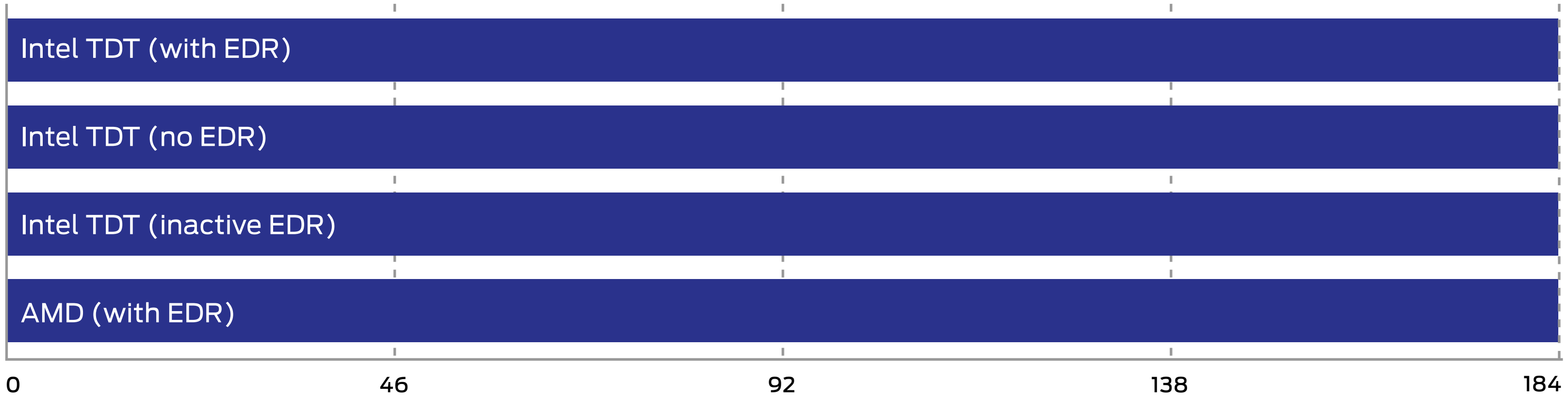
4. Legitimate Software Ratings

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 **4.3 Accuracy Ratings** on page 12**.**

Legitimate Software Ratings

Product	Legitimate Accuracy Rating	Legitimate Accuracy (%)
Intel TDT (with EDR)	184	100%
Intel TDT (no EDR)	184	100%
Intel TDT (inactive EDR)	184	100%
AMD (with EDR)	184	100%



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

4.1 Interaction Ratings

It's crucial that anti-malware Endpoint 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)
Intel TDT (with EDR)	184	0	0
Intel TDT (no EDR)	184	0	0
Intel TDT (inactive EDR)	184	0	0
AMD (with EDR)	184	0	0

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

4.2 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.

4.3 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 **4. Legitimate Software Ratings** on page 10.

4.4 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	8
High Impact	8
Medium Impact	4
Low Impact	3
Very Low Impact	2

5. Conclusions

This report examines how effectively hardware-level security measures can detect attackers attempting to run ransomware on a target. It also measures the combined strengths of Endpoint Detection and Response (EDR) software and hardware-based detection.

We tested the effectiveness of Intel's Threat Detection Technology (TDT) in a number of ways. First, and most realistically, we tested using systems equipped with Intel Threat Detection and an active EDR product. Then we disabled the EDR software and retested to determine how well TDT detected threats without help from an 'anti-virus' product. We also tested without the EDR software installed at all, which produced an unexpected and interesting result that we'll discuss below.

At the same time we ran the same tests against the EDR software running on AMD-based systems, which do not claim to offer similar hardware-based detection. The final results give a good indication of how effectively Intel's Threat Detection Technology works in isolation and in partnership with 3rd-party EDR products.

Intel claims that TDT uses machine learning to spot patterns of malicious behaviour, as it appears to the CPU.

Our ransomware attacks included original, known files and disguised variants. Detecting new threats is both challenging but necessary to combat the ever-developing threat landscape.

The most effective outcome involved the combination of Intel TDT and the EDR software (a compatible enterprise endpoint security product from one of the top-tier vendors). Between them, and often with overlapping abilities, this combination detected 97% of the ransomware threats.

There was a close similarity in the effectiveness when handling both known and unknown ransomware threats. This combination detected 98% of known ransomware and 96% of unknown ransomware.

Intel TDT in isolation, running Windows with a inactive EDR product installed, detected 90% of the threats whereas with EDR it detected 97%. We can deduce that the EDR product adds a further 7% benefit. That said, in the real world you'd need that software installed and active to be able to use Intel's TDT detections in a meaningful way. This is because Intel TDT feeds its detections to compatible EDR software. You can't just run a vPro-based system and expect it to stop ransomware on its own.

To look at it another way, the same EDR product running on another hardware platform (AMD) achieved a detection score of 73%. Intel's TDT would have added a further 24% of ransomware detection for a total of 97%.

So you can say that the hardware detection adds 24% or that the software detection adds 6%. There is a lot of overlap.

We also ran the ransomware tests without any EDR software at all, and monitored Intel TDT's detections using a terminal that could read directly from the hardware. Interestingly, we found that the detection rate rose from 90% (TDT with an inactive EDR) to 93%. This suggests that the Intel TDT system can be even more effective when there is better integration between its output and the EDR software in play.

Ransomware is an ever-present, expensive and challenging threat. These results show that hardware-assisted ransomware detection is not only a reality but a very effective one at that.

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 commissioned by Intel.
- The test was conducted between 30th September 2022 and 13th February 2023.
- Products were configured to detect malware using default settings.
- 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 ransomware test 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 security protection and/ or detection solutions. 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** for more information.

Appendix C:
Original and Evasive Detections

Attack Types					
Product	**Original Detections**	**Obfuscated Detections**	**Original Detections (%)**	**Obfuscated Detections (%)**	**Attacks Used Original/ Obfuscated (Total)**
Intel TDT (with EDR)	49	82	98%	96%	50/85 (135)
Intel TDT (no EDR)	28	48	93%	92%	30/52 (82)
Intel TDT (inactive EDR)	44	77	90%	90%	50/85 (135)
AMD (with EDR)	30	68	60%	80%	50/85 (135)

Appendix E:Tested
System Details

System Details	
Vendor	**Processor**
Intel	i7-1185G7
Ryzen Pro	5675U
Ryzen Pro	5875U
Ryzen Pro	6650U
Ryzen Pro	6850U

Appendix D:
Ransomware Family Detections

Ransomware Families												
Family	**Intel TDT (with EDR)**			**Intel TDT (no EDR)***			**Intel TDT (inactive EDR)**			**AMD (with EDR)**		
	Original	Obfuscated	Total Attacks Used	Original	Obfuscated	Total Attacks Used	Original	Obfuscated	Total Attacks Used	Original	Obfuscated	Total Attacks Used
Avoslocker	4 / 4	12 / 13	17	3 / 3	11 / 11	14	3 / 4	10 / 13	17	2 / 4	10 / 13	17
Conti	8 / 8	14 / 14	22	4 / 4	10 / 10	14	8 / 8	14 / 14	22	6 / 8	12 / 14	22
Darkside	7 / 7	10 / 10	17	2 / 2	4 / 4	6	7 / 7	10 / 10	17	6 / 7	7 / 10	17
Dharma	4 / 5	12 / 12	17	3 / 3	6 / 6	9	4 / 5	12 / 12	17	3 / 5	11 / 12	17
Maze	4 / 4	5 / 5	9	4 / 4	3 / 3	7	4 / 4	5 / 5	9	4 / 4	4 / 5	9
Netwalker	3 / 3	6 / 8	11	1 / 2	1 / 4	6	2 / 3	3 / 8	11	2 / 3	4 / 8	11
Ragnarlocker	4 / 4	2 / 2	6	2 / 2	-	2	4 / 4	2 / 2	6	3 / 4	2 / 2	6
Revil_Sodinokibi	8 / 8	10 / 10	18	4 / 4	8 / 8	12	8 / 8	10 / 10	18	3 / 8	8 / 10	18
Ryuk	7 / 7	11 / 11	18	5 / 6	5 / 6	12	4 / 7	11 / 11	18	1 / 7	10 / 11	18

* The test of Intel TDT (no EDR) used fewer ransomware attacks than the other tests. This is because, without an EDR in place, the ransomware was able to render some test systems completely unrecoverable.

SE Labs

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.