

Advanced Security Test Report

VMware

vDefend Advanced Threat Prevention



ONLINE REPORT

SE LABS ® tested **VMware vDefend Advanced Threat Prevention** against a range of hacking attacks designed to compromise systems and penetrate target networks in the same way criminals and other attackers breach systems and networks.

Full chains of attack were used, meaning that testers behaved as real attackers; probing targets using a variety of tools, techniques and vectors before attempting to gain lower-level and more powerful access. Finally, the testers/ attackers attempted to complete their missions, which might include stealing information, damaging systems and connecting to other systems on the network.

Contents

Introduction	04
Executive Summary	05
Advanced Security Test Award	05
1. How We Tested	06
Threat Responses	07
Attack Details	08
2. Total Accuracy Ratings	09
3. Response Details	10
4. Threat Intelligence	12
5. Legitimate Accuracy Rating	15
6. Conclusion	16
Appendices	17
Appendix A: Terms Used	17
Appendix B: FAQs	17
Appendix C: Attack Details	18
Appendix D: Product Version	21

Document version 1.0 Written 18th February 2025



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 Albasa
Thomas Bean
Solandra Brewster
Jarred Earlington
Gia Gorbald
Anila Johnny
Erica Marotta
Jeremiah Morgan
Julian Owusu-Abrokwa
Joseph Pike
Georgios Sakatzidi
Eneđja Torba
Dimitrios Tsarouchas
Stephen Withey

Marketing

Sara Claridge
Janice Sheridan

Publication

Rahat Hussain
Colin Mackleworth

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 : 2022 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.

© 2025 SE Labs Ltd

Introduction



CEO
Simon Edwards

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](#).

Early Protection Systems

Testing protection against fully featured attacks

There are many opportunities to spot and stop attackers. Products can detect them when attackers send phishing emails to targets. Or later, when other emails contain links to malicious code. Some kick into action when malware enters the system. Others sit up and notice when the attackers exhibit bad behaviour on the network.

Regardless of which stages your security takes effect, you probably want it to detect and prevent before the breach runs to its conclusion in the press.

Our Advanced Security test is unique, in that we test products by running a full attack. We follow every step of a breach attempt to ensure that the test is as realistic as possible.

This is important because different products can detect and prevent threats differently.

Ultimately you want your chosen security product to prevent a breach one way or another, but it's more ideal

to stop a threat early, rather than watch as it wreaks havoc before stopping it and trying to clean up. Some products are designed solely to watch and inform, while others can also get involved and remove threats either as soon as they appear or after they start causing damage.

For the 'watchers' we run the Advanced Security test in Detection mode. For 'stoppers' like **VMware vDefend Advanced Threat Prevention** we can demonstrate effectiveness by testing in Protection Mode.

In this report we look at how **VMware vDefend Advanced Threat Prevention** handled full breach attempts. At which stages did it detect and protect? And did it allow business as usual, or mis-handle legitimate applications?

Understanding the capabilities of different security products is always better achieved before you need to use them in a live scenario. SE Labs' Advanced Security test reports help you assess which are the best for your own organisation.

Executive Summary

VMware vDefend Advanced Threat Prevention was tested against a range of hacking attacks designed to compromise systems and penetrate target networks in the same way as criminals and other attackers breach systems and networks.

In this stand-alone test, we examined its abilities to:

- Detect the delivery of targeted attacks
- Track different elements of the attack chain ...
- ... including those that are compromised beyond the endpoint and into the wider network
- Handle legitimate applications and other objects

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

Executive Summary

Product Tested	Detection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
VMware vDefend Advanced Threat Prevention	94%	98%	97%

For exact percentages, see 2. Total Accuracy Ratings on page 9.

The product posted excellent results, detecting every targeted attack. It could also track almost all the hostile activities that occurred during the attacks. In most of the cases, **VMware vDefend Advanced Threat Prevention** also detected attackers moving from one target to another.

The product also proved adept at identifying legitimate applications. The penalty points it incurred for a very few sub-optimal interactions did not greatly detract from its Legitimate Accuracy Rating.

VMware vDefend Advanced Threat Prevention achieved a Total Accuracy Rating of 97% and won an AAA award for advanced security.

Advanced Security Test Award

The following product wins the SE Labs award:



VMware
vDefend Advanced
Threat Prevention

1. How We Tested

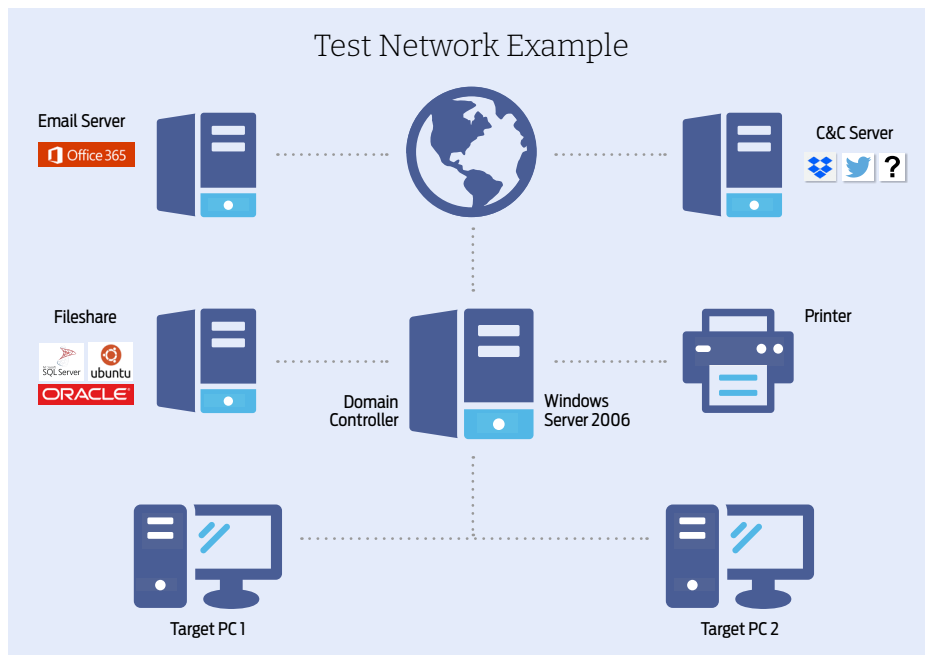
Testers can't assume that products will work a certain way, so running a realistic advanced security test means setting up real networks and hacking them in the same way that real adversaries behave.

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 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 **Attack Details** on page 8 and, for a really detailed drill down on the details, **4. Threat Intelligence** on pages 12-13 and **Appendix C: Attack Details** on pages 18-21.

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

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 that, 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 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 yet still 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 5-6).

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.

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 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.

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



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






Attack Details

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

Attacker/ APT Group	Method	Target	Details
Wizard Spider	Phishing Attachment		Credential harvesting, cryptomining and implementation of ransomware.
Sandworm	Phishing Link		Obtain sensitive network data via encryption and system data wiping.
Dragonfly & Dragonfly 2.0	Email Attachment		Phishing and supply chain methods used to gain access.

KEY					
	Education		Financial Industries		Gambling
	Government Espionage		Manufacturing		Natural Resources
	Private-sector Energy		Research Institutes		Travel Industries

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** on pages 12-14.

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 **2. Response Details** on page 10.

Total Accuracy Ratings



- Total Accuracy Ratings combine protection and false positives.

THE - C2

TUESDAY 25TH AND
WEDNESDAY 26TH MARCH 2025

Connecting business with cyber security

The-C2 is an exclusive, invite-only threat intelligence event that connects multinational business executives with the cutting edge of the cyber security industry. The event enables frank and open discussion of the developing digital threat landscape among global security leaders.

The-C2 is hosted by SE Labs, the world's leading security testing lab. Its unique position in the industry provides a route to understanding both the developing threat landscape and the evolving security measures for defending against attackers.

REGISTER AT
[THE - C2 . COM](https://www.the-c2.com)

2. Response Details

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. As mentioned in **2. Total Accuracy Ratings**, 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.

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 is detected. 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 below), 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.

Understanding Detection Groups

Incident No.	Detection	First Group		Second Group		Third Group		Fourth Group	
		Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action	
1	✓	✓	✓	—	✓	✓	✓	✓	✓
2	✓	—	✓	✓	✓	✓	✓	✓	✓
3	✓	—	✓	✓	✓	✓	✓	✓	✓
4	✓	✓	✓	—	✓	✓	✓	✓	✓

Attacker/ Apt Group	Number of Incidents	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/Action	Lateral Movement Action
Dragonfly & Dragonfly 2	4	4	4	2	4	4

Elements of the attack chain are put into groups. For example, the Delivery and Execution stages of an attack are in the same group. Similarly, we group the Post Escalation stage with the Post Escalation Action (PE Action) stage. When we count detections we look to see at least one detection (tick) in each group. One or two detections in a group is a success.

In this example we have four test cases, which we call 'incidents'. In Incident No. 1 there was a detection recorded for the delivery of the threat and when it was executed. These two results count as one detection. In Incident No. 2 the threat delivery was not detected, but its execution was. This also counts as one detection.

When no detection is registered in any part of a group the result will be a 'miss'. In Incident 1. there was no detection when the attacker performed the 'Action' stage of the attack. This is a miss for the product. In fact, this product only detected two of the four Action stages, which is why the Response Details table shows '2' in the Action column.

Wizard Spider

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
1	✓	N/A	✓	N/A	N/A	✓	✓	✓
2	✓	N/A	✓	N/A	N/A	N/A	—	✓
3	✓	N/A	✓	N/A	N/A	N/A	✓	✓
4	✓	N/A	✓	N/A	✓	N/A	✓	✓

Sandworm

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
5	✓	N/A	✓	✓	✓	N/A	✓	N/A
6	✓	N/A	✓	—	N/A	N/A	✓	✓
7	✓	N/A	✓	N/A	✓	✓	✓	N/A
8	✓	N/A	✓	N/A	✓	N/A	—	N/A

Dragonfly 8 & Dragonfly 2.0

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
9	✓	✓	✓	N/A	N/A	✓	—	✓
10	✓	✓	N/A	N/A	✓	N/A	✓	✓
11	✓	✓	N/A	N/A	✓	✓	✓	✓
12	✓	✓	N/A	N/A	✓	✓	✓	✓

Group Detections

We record detections in groups, as described above in Understanding Detection Groups. To get an overview of how a product handled the entire set of threats we then combine these detections into 'Group Detections'.

In a test with four incidents and four detection groups (Delivery/Execution; Action; Escalation/PE Action; and Lateral Movement/Lateral Action) the maximum score would be 16. This is because for each of the four threats a product that detects everything would score 4.

Our overall Detection Rating is based on the number of Detection Groups achieved.

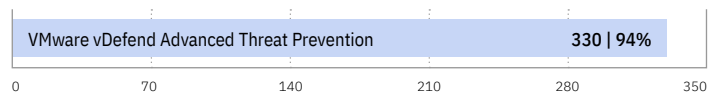
Response Details

Attacker/APT Group	Number of Incidents	Attacks Detected	Delivery/Execution	Action	Privilege Escalation/Action	Lateral Movement/Action
Wizard Spider	4	4	4	0	2	4
Sandworm	4	4	4	1	3	3
Dragonfly & Dragonfly 2.0	4	4	4	0	4	4
TOTAL	12	12	12	1	9	11

Detection Accuracy Rating Details

Attacker/APT Group	Number of Incidents	Attacks Detected	Group Detections	Detection Rating
Wizard Spider	4	4	10	100
Sandworm	4	4	11	110
Dragonfly & Dragonfly 2.0	4	4	12	120
TOTAL	12	12	33	330

Detection Accuracy Rating



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

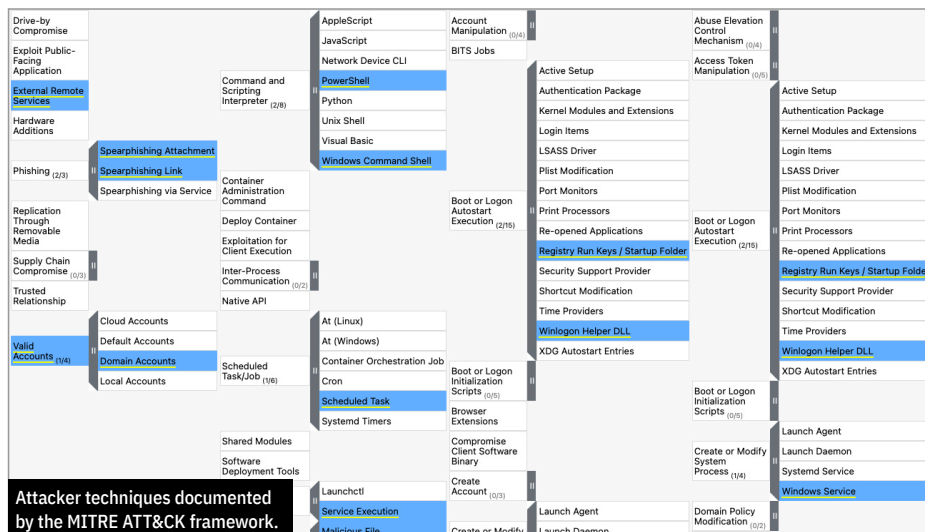
4. Threat Intelligence

Wizard Spider

The **Scattered Spider** group has been active since at least 2022 and focussed on targets that provided customer relationship and business process solutions. It also attacks telecommunication and high-tech businesses.

Reference:

<https://attack.mitre.org/groups/G0102/>



Example Wizard Spider Attack

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spear phishing link	Malicious link	System Information Discovery	Bypass User Account Control	Security Software Discovery	SSH	Archive Collected Data
	Web Protocols	System Owner/user Discovery	Valid Accounts	Masquerade Task or Service		Data staged
	Non standard port	Permission Group Discovery		Modify Registry		Data from Local System
	Windows Command Shell	File and directory Discovery		Process Discovery		Exfiltration Over C2 Channel

Sandworm

In operation since around 2009, Sandworm Team is threat group that has been connected to Russia's Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). It is believed to be the GRU's Unit 74455. Notable campaigns include a targeted attack on the 2017 French Presidential campaign, as well as the worldwide NotPetya ransomware attack in the same year.

Reference:
<https://attack.mitre.org/groups/G0034/>

Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques
Spearphishing Attachment	AppleScript	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)
Spearphishing Link	JavaScript	BITS Jobs	Access Token Manipulation (0/5)
Spearphishing via Service	Network Device CLI	Boot or Logon Autostart Execution (0/15)	Boot or Logon Autostart Execution (0/15)
	Command and Scripting Interpreter (3/8)	PowerShell	Boot or Logon Initialization Scripts (0/5)
		Python	Boot or Logon Initialization Scripts (0/5)
		Unix Shell	Browser Extensions
		Visual Basic	Compromise Client Software Binary
		Windows Command Shell	Cloud Account
	Container Administration Command	Create Account (1/3)	Domain Account
	Deploy Container		Local Account
	Exploitation for Client Execution		Escape to Host
Compromise Hardware Supply Chain	Inter-Process Communication (0/2)	Create or Modify System Process (0/4)	Event Triggered Execution (0/15)
Compromise Software Dependencies and Development Tools	Native API	Event Triggered Execution (0/15)	Exploitation for Privilege Escalation
Compromise Software Supply Chain	Scheduled Task/Job (0/6)	External Remote Services	Hijack Execution Flow (0/11)
	Shared Modules	Hijack Execution Flow (0/11)	Process Injection (0/11)
Cloud Accounts	Software Deployment Tools	Implant Internal Image	Scheduled Task/Job (0/6)
Default Accounts	System Services (0/2)	Malicious File	Valid Accounts (1/4)
Domain Accounts		Malicious Image	Default A
Local Accounts		Malicious Link	Domain
	Attacker techniques documented by the MITRE ATT&CK framework.		
	User Execution (2/3)		

Example Sandworm Attack

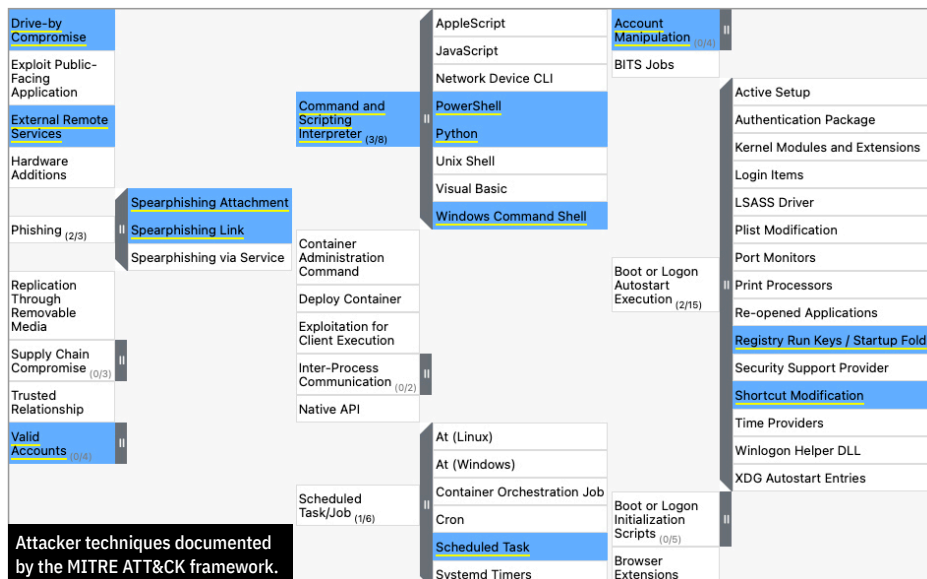
Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spear phishing Link	Windows Command Shell	File and Directory Discovery	Domain Accounts	Remote System Discovery	Lateral Tool Transfer	Data from Local System
	Powershell	System Information Discovery	Bypass User Account Control	LSASS Memory	SMB/Windows Admin Shares	Local Data Staging
	Malicious Link	System Owner/User Discovery				Exfiltration Over C2 Channel
	File Deletion	Data from Local System				Network Sniffing
	Obfuscated Files or Information	Local Data Staging				
		Exfiltration Over C2 Channel				

Dragonfly & Dragonfly 2.0

These two groups are sometimes tracked separately. Dragonfly has been active for approximately 10 years with their targets shifting from defense and aviation companies to the energy sector after 2013. Dragonfly 2.0 has kept the focus on the energy sector in its operations.

Reference:

<https://attack.mitre.org/groups/G0035/>



Example Dragonfly & Dragonfly Attack

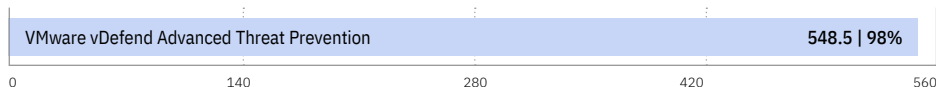
Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action	
Spear phishing Link	Command and Scripting Interpreter	Domain Groups	Valid Accounts	Modify Registry	Remote Desktop Protocol	Archive Collected Data	
Malicious Link	Windows Command Shell	Remote System Discovery		Query Registry		Registry Run Keys / Startup Folder	Data from Local System
	Powershell	System Information Discovery		Disable or Modify System Firewall		Forced Authentication	Local Data Staging
		Process Discovery					Screen Capture
		System Owner/User Discovery					Exfiltration Over C2 Channel

5. Legitimate Accuracy Rating

These ratings indicate how accurately the product classifies legitimate applications and URLs, while also taking into account the interactions that the 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 Accuracy Rating



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

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

6. Conclusion

The test exposed **VMware vDefend Advanced Threat Prevention** appliance to a diverse set of exploits, file-less attacks and malware attachments, comprising a wide range of realistic threats.

All these attack types have been witnessed in real-world attacks over the previous few years. They are representative of a real and present threat to business networks the world over.

The threats used in this test are similar or identical to those used by the threat groups listed in **Attack Details** on page 8 and **4. Threat Intelligence** on pages 12 – 14.

It is important to note that while this test used the same type of attacks, new files were used. This exercised the tested product's ability to detect and protect against certain approaches to attacking systems rather than simply detecting malicious files that have become well-known over the previous few years. The results are an indicator of potential future performance rather than just a compliance check that the product can detect old attacks.

The product detected all the threats on a basic level in that it detected at least some element of the

attack chain for each of the incidents. This was not immediately obvious and would have been a problem were it not for SELab's practice of awarding points based on group detection.

For example, detecting Spear phishing links and attachments is not applicable to the product. Since all of the attacks based on the Wizard Spider and Sandworm techniques were delivered this way, the product would have lost points had it not kicked into action when these Spear phishing attacks were being executed.

The obverse was true for the incidents based on the Dragonfly attack technique. Except for one instance when delivery and execution were both detected, alerts for the execution of malicious links and files were marked as "not applicable" since the delivery of these threats was already flagged.

Because SELabs takes into consideration the relevance of one part of an attack on another, **VMware vDefend Advanced Threat Prevention** received full marks for the group detection of the delivery/execution elements.

The product incurred some penalties as the tester/attacker advanced past the delivery/execution stage.

In one instance, the tester's attempts at discovery and exfiltration were not detected. Neither were some attempts to claim system privileges in order to inflict further damage.

It also failed to detect the movement of one threat from the endpoint to the other vulnerable systems in the network. Again, however, **VMware vDefend Advanced Threat Prevention** benefitted from scoring based on group detection rather than discrete attack elements. The product actually missed three instances of lateral movement but was awarded a full 10 points for each of the two other incidents. This was because it was able to detect the actions resulting from the missed movement.

In all, **VMware vDefend Advanced Threat Prevention** reached an impressive Detection Accuracy Rating of 94%. This, together with its excellent Legitimate Accuracy Rating of 98% enabled it to achieve a Total Accuracy Rating of 97% and win an AAA award for advanced security.

Appendices

Appendix A: Terms Used

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

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 for more information.

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

- The test was conducted between 22nd January and 4th February 2025.
- All products were configured according to each vendor's recommendations, when such recommendations were provided.
- Targeted attacks were selected and verified by SE Labs.
- Malicious emails, URLs, attachments and legitimate messages were independently located and verified by SE Labs.
- Malicious and legitimate data was provided to partner organisations once the test was complete.

Appendix C: Attack Details

Wizard Spider

Incident No.	Delivery	Execution	Action	Privilege Escalation	Post-Escalation	Lateral Movement	Lateral Action
1	Spear phishing Attachment	Windows Command Shell	Process Discovery	Bypass User Account Control	Scheduled Task	SMB/Windows Admin Shares	Data from Local System
		Malicious File	File and Directory Discovery	Valid Accounts	Winlogon Helper DLL	Remote Desktop Protocol	Data Staged
		Obfuscated Files or Information	System Network Configuration Discovery		Registry Run Keys / Startup Folder		Exfiltration Over C2 Channel
					Dynamic-Link Library Injection		
2	Spear phishing Link	Malicious Link	System Information Discovery	Bypass User Account Control	Security Software Discovery	SSH	Archive Collected Data
		Web Protocols	System Owner/user Discovery	Valid Accounts	Masquerade Task or Service	External Remote Services	Data Staged
		Non Standard Port	Permission Group Discovery		Modify Registry		Data from Local System
		Windows Command Shell	File and Directory Discovery	Process Discovery			Exfiltration Over C2 Channel
3	Spear phishing Link	Powershell	File and Directory Discovery	Bypass User Account Control	Remote System Discovery	Windows Remote Management	Archive Collected Data
		Malicious Link	System Network Configuration Discovery	Valid Accounts	Windows File and Directory Permission Modification		Data Staged
			Permission Group Discovery			Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	
4	Spear phishing Attachment	Powershell	Process Discovery	Bypass User Account Control	Remote System Discovery	Service Execution	Archive Collected Data
		Non Standard Port	System Information Discovery	Valid Accounts	LLMNR/NBT-NS Poisoning and SMB Relay	Domain Accounts	Data Staged
		Web Protocols	System Owner/User Discovery		NTDS		Data from Local System
		Obfuscated Files or Information	File and Directory Discovery	System Network Configuration Discovery	Security Account Manager	Kerboasting	Exfiltration Over C2 Channel

Sandworm

Incident No.	Delivery	Execution	Action	Privilege Escalation	Post-Escalation	Lateral Movement	Lateral Action
5	Spear phishing Attachment	Windows Command Shell	File and Directory Discovery	Domain Accounts	Keylogging	SSH	Cron
		Malicious File	System Information Discovery	Bypass User Account Control	Domain Account (Discovery)		Boot or Logon Initialization Scripts
		Non-Standard Port	System Owner/User Discovery				RC Scripts
			Data from Local System				Systemd Service
			Local Data Staging				
			Exfiltration Over C2 Channel				
Credentials from Web Browsers							
6	Spear phishing Link	Windows Command Shell	File and Directory Discovery	Domain Accounts	Remote System Discovery	Lateral Tool Transfer	Data from Local System
		Powershell	System Information Discovery	Bypass User Account Control	LSASS Memory	SMB/Windows Admin Shares	Local Data Staging
		Malicious Link	System Owner/User Discovery				Exfiltration Over C2 Channel
		File Deletion	Data from Local System				Network Sniffing
		Obfuscated Files or Information	Local Data Staging				
			Exfiltration Over C2 Channel				
7	Spear phishing Attachment	Windows Command Shell	File and Directory Discovery	Domain Accounts	Domain Account (Discovery)	SSH	Systemd Service
		Malicious File	System Information Discovery	Bypass User Account Control	Ingress Tool Transfer		Kernel Modules and Extensions
		Web Protocols	System Owner/User Discovery		LSASS Memory		SSH Authorized Keys
			System Network Configuration Discovery		Lateral Tool Transfer		
			System Network Connections Discovery				
8	Spear phishing Link	Windows Command Shell	File and Directory Discovery	Domain Accounts	Remote System Discovery	SSH	/etc/passwd and /etc/shadow
		Malicious Link	System Information Discovery	Bypass User Account Control	Security Software Discovery		Bash History
			System Owner/User Discovery				
			System Network Configuration Discovery				
			System Network Connections Discovery				Clear Linux or Mac System Logs

Dragonfly & Dragonfly 2.0

Incident No.	Delivery	Execution	Action	Privilege Escalation	Post-Escalation	Lateral Movement	Lateral Action
9	Spear phishing Attachment	Application Layer Protocol	System Information Discovery	Valid Accounts	Scheduled Task	Remote Desktop Protocol	Automated Exfiltration
	Malicious File	Command and Scripting Interpreter	Process Discovery		Clear Windows Event Logs		Screen Capture
		Windows Command Shell	System Owner/User Discovery		File deletion		Exfiltration Over C2 Channel
		Powershell			Ingress Tool Transfer		
					Local Account		
					Domain Account		
	Shortcut Modification						
10	Spear phishing Link	Command and Scripting Interpreter	Domain Groups	Valid Accounts	Modify Registry	Remote Desktop Protocol	Archive Collected Data
	Malicious Link	Windows Command Shell	Remote System Discovery		Query Registry		Data from Local System
		Powershell	System Information Discovery		Registry Run Keys / Startup Folder		Local Data Staging
			Process Discovery		Disable or Modify System Firewall		Screen Capture
			System Owner/User Discovery		Forced Authentication		Exfiltration Over C2 Channel
11	Spear phishing Link	Command and Scripting Interpreter	System Information Discovery	Valid Accounts	System Network Configuration Discovery	Remote Desktop Protocol	Archive Collected Data
	Malicious Link	PowerShell	Process Discovery		Archive Collected Data		Automated Exfiltration
			System Owner/User Discovery		Data from Local System		Exfiltration Over C2 Channel
			File and Directory Discovery		Local Data Staging		
			Network Share Discovery		Exfiltration Over C2 Channel		
					Credentials from Password Stores		
					LSA Secrets		
12	Spear phishing Attachment	Command and Scripting Interpreter	System Information Discovery	Valid Accounts	NTDS	Remote Desktop Protocol	Archive Collected Data
	Malicious File	Windows Command Shell	Process Discovery		Ingress Tool Transfer		Data from Local System
			System Owner/User Discovery		Security Account Manager		Local Data Staging
			Process Injection		Local Account		Screen Capture
			File and Directory Discovery		Domain Account		Exfiltration Over C2 Channel
					LSA Secrets		

Appendix D: Product Version

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

Vendor	Product	Build Version (start)	Build Version (end)
VMware	vDefend Advanced Threat Prevention	4.2.1.0.0.24304122	4.2.1.0.0.24304122
	NSX Application Platform	4.2.0-0.0-24124098	4.2.0-0.0-24124098

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.