eBook

ThreatDown™
Powered by Malwarebytes

Endpoint Security Evaluation Guide

Essential guide for evaluating corporate antivirus, Endpoint Protection, EDR, XDR, and MDR for MSPs and Resellers

Based on Q2 2024 MRG Effitas Assessment

How To Evaluate Endpoint Security Technology Today

Protecting laptops, desktops, mobile devices, and servers is the foundation of endpoint security, but the modern security stack behind that protection involves several, sometimes-overlapping and confusing technologies, including corporate antivirus, Endpoint Protection (EP), Endpoint Detection & Response (EDR), and Managed Detection & Response (MDR).

These technologies are vital, but the complexity behind terminology and products in this space often complicates the work of choosing the right solution.

While seemingly every other cybersecurity vendor touts that they "detect more of X" or "prevent more of Y," organizations are left with critical, unanswered questions: Will this product protect my organization from existing and emerging threats? Does the product have a low impact on system performance and a low number of false-positives?

This is where MRG's independent lab assessment comes in.

The 360° Assessment & Certification by MRG Effitas isn't like other tests that just evaluate traditional file-based attacks: They unleash real-world fileless cases and exploitation techniques, live botnets, and credit card skimming attacks on vendor products as well.

Centered around 11 rounds of rigorous testing, MRG's assessment criteria are the best way to evaluate endpoint security vendors today. The tests weed out all endpoint security products that can't crush modern threats—and only awards the ones that do.

MRG Effitas
CERTIFIED
360° ASSESSMENT

11 Criteria for Effective Endpoint Security

These 11 criteria by MRG Effitas are considered vital for evaluating endpoint protection for efficacy, performance, and reliability. MRG Effitas tests top vendors against these criteria as part of its 360° Assessment & Certification.

1. **In the Wild/Full Spectrum**
   Prevents zero-day malware and threats from spreading among real world computers.

2. **PUA/Adware**
   Blocks Potentially Unwanted Applications (PUAs) that are not malicious but considered unsuitable for most home or business networks.

3. **Exploit/Fileless**
   Prevents exploit and post-exploitation techniques.

4. **Banking Simulator/Magecart**
   Prevents against the Magecart credit card-skimming attack.

5. **Ransomware Simulator**
   Blocks in-house ransomware samples.

6. **Real Botnet**
   Prevents a Botnet designed to steal credentials.

7. **False Positive Ransomware**
   Correctly recognizes programs designed to mimic ransomware behavior as benign.

8. **False Positive**
   Correctly recognizes completely clean, recently created applications as benign.

9. **Performance**
   Measures a product's resource footprint and effect on the overall operating system performance.

10. **ITW Phishing**
    Blocks in-the-wild phishing URLs.

11. **Phishing Simulator**
    Blocks in-house phishing URLs with credential capturing capabilities.

New Certification: 360° Phishing Certification

Given the frequency of phishing attacks, and the risks they pose, it's clear that modern endpoint security solutions needs to protect against it.

According to Verizon, attackers used phishing for initial access in 15 percent of data breaches in 2022. CISA also showed that, within the first 10 minutes of receiving a phishing email, 84 percent of employees took the bait. After successfully compromising a system through phishing, threat actors can expand their attacks by dropping ransomware or stealing sensitive data, leading to costly financial and reputational damages.

To see if security products could address this persistent phishing threat, MRG Effitas added a new certification to its Q3 2023 tests: The 360° Phishing Certification.

To earn the certification, vendors need to automatically block every sample in one of two subtests: the ITW Phishing Test and Phishing Simulator Test.

In the ITW Phishing Test, MRG Effitas tried to identify the blocking ability of the security product's secure browser or browser extension. This quarter, they used five in-the-wild phishing URLs.

In the Phishing Simulator Test, MRG Effitas tested the proactive or heuristic anti-phishing capabilities of each security software against five crafted phishing URLs with credential capturing capabilities.

For the full Q2 2024 results on these tests, see the chart below.

100% phishing attempts blocked?	
ThreatDown	✓
Bitdefender	✗
ESET	✓
Microsoft	✗
Symantec	✗
Avast	✗
Avira	✗
Trend Micro	✗

MRG Effitas
CERTIFIED
PHISHING

5 Top-Tier Certifications Endpoint Security Must Have

Based on a product's performance on nine criteria, MRG Effitas awards the following five certifications:

1 **360° Level 1 Certification:**
The product blocked every in-the-wild sample and passed the Real Botnet Test.

2 **360° Exploit Certification:**
The product entirely blocked exploits in vulnerable applications from being used to deliver a malicious payload.

3 **360° Online Banking Certification:**
The product blocked every in-the-wild financial malware sample and passed the Reat Botnet Test and the Banking Simulator/Magecart Test.

4 **360° Ransomware Certification:**
The product blocked every in-the-wild ransomware sample, passed the Ransomware Simulator Test, and passed the False Positive Ransomware Test.

5 **360°Phishing Certification:**
The product automatically blocked all test samples in either the ITW Phishing or Phishing Simulator Test.

ThreatDown vs Avast Business

	Level 1	Online Banking	Exploit	Ransomware	Phishing
ThreatDown	✓	✓	✓	✓	✓
Avast Business	✗	✓	✓	✓	✓

Endpoint Protection Must Protect Against…

Botnets
Part of Level 1 Cert

Attackers can use Botnets to monitor keystrokes, steal login credentials, and take advantage of backdoors.

Zero-Day Threats
Part of Level 1 Cert

Zero-day malware that has never been seen before, allowing it to slip past traditional detection methods.

Exploits
Part of Exploit Cert

Attackers can use exploits in unpatched applications to enter a network and install malware in it.

Phishing
Part of Phishing Cert

Phishing is the #1 attack vector, with attackers using malicious URLs to gain initial access in a network.

The Risks of Inadequate Protection

- X Zero-day malware attacks account for 80% of successful breaches. The cost of a data breach was $4.88 million in 2024.

ThreatDown Delivers

ThreatDown, powered by Malwarebytes, leverages seven unique layers of detection techniques in what we call Multi-Vector Protection. These seven layers allowed ThreatDown to stop the threats Avast Business didn't.

ThreatDown is trusted by businesses large and small, VARs and MSPs, and institutions like schools, hospitals and governments.

ThreatDown vs ESET

	Level 1	Online Banking	Exploit	Ransomware	Phishing
ThreatDown	✓	✓	✓	✓	✓
ESET	✗	✓	✓	✓	✓

Endpoint Protection Must Protect Against...

Botnets Part of Level 1 Cert	Attackers can use Botnets to monitor keystrokes, steal login credentials, and take advantage of backdoors.
Zero-Day Threats Part of Level 1 Cert	Zero-day malware that has never been seen before, allowing it to slip past traditional detection methods.
Exploits Part of Exploit Cert	Attackers can use exploits in unpatched applications to enter a network and install malware in it.
Magecart credit card skimming Part of Online Banking Cert	Magecart is malware that infects websites and steals credit card information when it's entered into the site's checkout.
Phishing Part of Phishing Cert	Phishing is the #1 attack vector, with attackers using malicious URLs to gain initial access in a network.

The Risks of Inadequate Protection

- Zero-day malware attacks account for 80% of successful breaches. The cost of a data breach was $4.88 million in 2024.

ThreatDown Delivers

ThreatDown leverages seven unique layers of detection techniques in what we call Multi-Vector Protection. These seven layers allowed ThreatDown to stop the threats ESET didn't.

ThreatDown is trusted by businesses large and small, VARs and MSPs, and institutions like schools, hospitals and governments.

ThreatDown vs Avira Antivirus Pro

	Level 1	Online Banking	Exploit	Ransomware	Phishing
ThreatDown	✓	✓	✓	✓	✓
Avira Antivirus Pro	✗	✓	✗	✓	✓

Endpoint Protection Must Protect Against…

Botnets Part of Level 1 Cert	Attackers can use Botnets to monitor keystrokes, steal login credentials, and take advantage of backdoors.
Zero-Day Threats Part of Level 1 Cert	Zero-day malware that has never been seen before, allowing it to slip past traditional detection methods.
Exploits Part of Exploit Cert	Attackers can use exploits in unpatched applications to enter a network and install malware in it.
Magecart credit card skimming Part of Online Banking Cert	Magecart is malware that infects websites and steals credit card information when it's entered into the site's checkout.
Phishing Part of Phishing Cert	Phishing is the #1 attack vector, with attackers using malicious URLs to gain initial access in a network.

The Risks of Inadequate Protection

- Botnets have caused over $9 billion in losses to US victims and over $110 billion in losses globally.
- Zero-day malware attacks account for 80% of successful breaches. The cost of a data breach was $4.88 million in 2024.
- Exploits are involved in 60% of data breaches. The cost of a data breach was $4.35 million in 2022.

ThreatDown Delivers

ThreatDown leverages seven unique layers of detection techniques in what we call Multi-Vector Protection. These seven layers allowed ThreatDown to stop the threats Avira Antivirus Pro didn't.

ThreatDown is trusted by businesses large and small, VARs and MSPs, and institutions like schools, hospitals and governments.

ThreatDown vs Trend Micro

	Level 1	Online Banking	Exploit	Ransomware	Phishing
ThreatDown	✓	✓	✓	✓	✓
Trend Micro	✗	✗	✗	✓	✗

Endpoint Protection Must Protect Against…

Botnets Part of Level 1 Cert	Attackers can use Botnets to monitor keystrokes, steal login credentials, and take advantage of backdoors.
Zero-day Threats Part of Level 1 Cert	Zero-day malware that has never been seen before, allowing it to slip past traditional detection methods.
Exploits Part of Exploit Cert	Attackers can use exploits in unpatched applications to enter a network and install malware in it.
Magecart credit card skimming Part of Online Banking Cert	Magecart is malware that infects websites and steals credit card information when it's entered into the site's checkout.

The Risks of Inadequate Protection

- Botnets have caused over $9 billion in losses to US victims and over $110 billion in losses globally.
- Zero-day malware attacks account for 80% of successful breaches. The cost of a data breach was $4.88 million in 2024.
- Exploits are involved in 60% of data breaches. The cost of a data breach was $4.35 million in 2022.

ThreatDown Delivers

ThreatDown leverages seven unique layers of detection techniques in our Multi-Vector Protection. These seven layers allowed ThreatDown to stop the threats Trend Micro didn't. Read the whitepaper for more.

ThreatDown is trusted by businesses large and small, VARs and MSPs, and institutions like schools, hospitals and governments.

Evolving Threats Require Evolved Endpoint Security

Corporate antivirus, EP, EDR, XDR, and MDR, are the key technologies to achieving endpoint security.

But comparing the competing claims of different endpoint security vendors will only get you so far. The most objective measure of effective prevention technology can be found in the MRG Effitas 360° Assessment & Certification.

In MRG's testing, most vendors provided erratic results across the year—blocking threats one quarter but failing to block the same types of threats just three months later. Organizations cannot rely on endpoint security vendors that fail to keep up with modern threats.

Only when a vendor attains MRG's highest marks, for multiple quarters, should a company consider it as its first and only choice for endpoint security.

For the latest Q2 2024 results released by MRG, ThreatDown Endpoint Protection received certifications for Level 1, Exploit, Online Banking, Ransomware, and Phishing. This accomplishment makes us the only vendor to have obtained every certification for each quarter in 2023 and 2024.

For organizations that are concerned their current solution may not be up-to-par, the MRG Effitas assessment has demonstrated that ThreatDown EP—more consistently than anybody else—has what it takes to keep your business safe from today's most pressing

	Q1 (2023)				Q2 (2023)				Q3 (2023)					Q4 (2023)					Q1 (2024)					Q2 (2024)				
	LVL1	EXPL	BANK	RANS	LVL1	EXPL	BANK	RANS	LVL1	EXPL	BANK	RANS	PHISH	LVL1	EXPL	BANK	RANS	PHISH	LVL1	EXPL	BANK	RANS	PHISH	LVL1	EXPL	BANK	RANS	PHISH
ThreatDown	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Symantec	✗	✓	✗	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
Microsoft	✓	✗	✗	✓	✗	✓	✗	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓
Avast Business	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓
ESET	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓
Avira	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓	✓	✗	✗	✓	✓	✓
Trend Micro	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✓	✓	✗	✗	✓	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗

✓ Attained

✗ Failed

LVL 1 - 360 Assessment - Level 1 Certified

EXPL - Exploit - Certified

BANK - Online Banking Certified

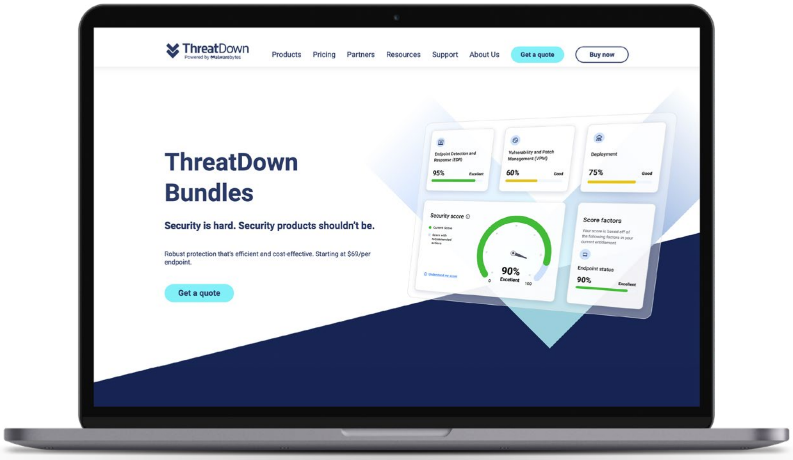
RANS - Ransomware Certified

PHISH - Phishing Certified

We get it—security is hard. Security products shouldn't be.

What you get	Core	Advanced	Elite	Ultimate
Incident response	✓	✓	✓	✓
Next-gen AV	✓	✓	✓	✓
Device control	✓	✓	✓	✓
Block unwarranted applications	✓	✓	✓	✓
Vulnerability Assessment	✓	✓	✓	✓
Ransomware Rollback		✓	✓	✓
Endpoint Detection & Response		✓	✓	✓
Patch Management		✓	✓	✓
Managed Threat Hunting		✓	✓	✓
Managed Detection & Response			✓	✓
Website Content Filtering				✓
Add-Ons	✓	✓	✓	✓

Learn More



ThreatDown Bundles

Security is hard. Security products shouldn't be.

Robust protection that's efficient and cost-effective. Starting at $69/per endpoint.

Try ThreatDown Bundles today!

Let us take care of your endpoint security. Deploy the solution that delivers superior defense, easiest to use management, and the best value for your security investment.

Get started

ThreatDown™
Powered by Malwarebytes

threatdown.com

sales@threatdown.com