eBook

ThreatDown™
Powered by Malwarebytes

Endpoint Security Evaluation Guide for Education

Essential Guide for Evaluating Corporate Antivirus, Endpoint Protection, EDR, XDR, and MDR for educational institutions

May 2024

Based on Q4 2023 MRG Effitas Assessment

ThreatDown™ Powered by Malwarebytes

How To Evaluate Endpoint Security Technology Today

Protecting laptops, 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 and Response (EDR), Extended Detection and Response (XDR), and Managed Detection and Response (MDR).

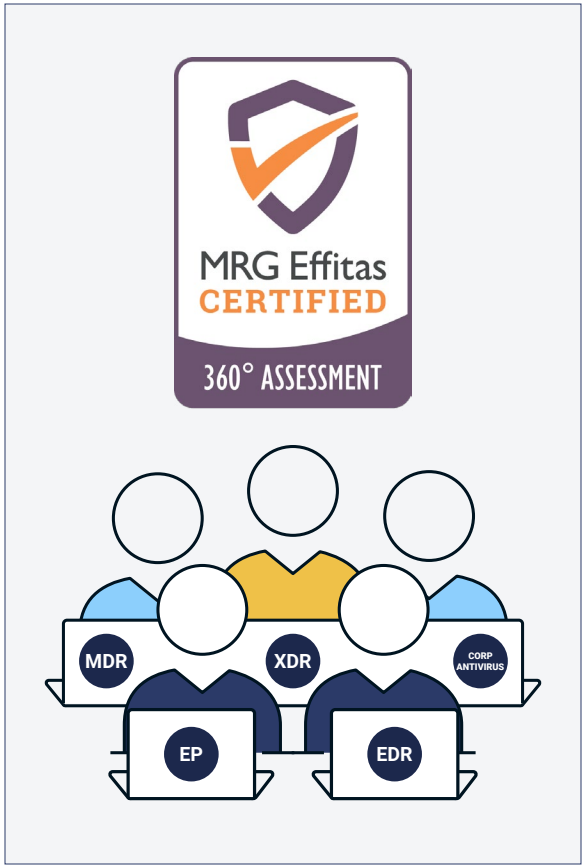
These technologies are vital, but the complexity behind terminology and products in this space often complicates the work of choosing the right solution.

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.



ThreatDown™ Powered by Malwarebytes

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 their 360° Assessment & Certification.

1. **In the Wild/Full Spectrum:** Prevents zero-day malware and threats from spreading among real world computers, also known as In the Wild (ITW) threats.
2. **PUA/Adware:** Blocks Potentially Unwanted Applications (PUA) 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:** Prevention 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:** Ability to correctly recognize programs designed to mimic ransomware behavior as benign.
8. **False Positive:** Ability to correctly recognize 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:** Ability to block ITW phishing URLs.
11. **Phishing Simulator:** Blocks in-house phishing URLs with credential capturing capabilities.

ThreatDown™ Powered by Malwarebytes

New Certification: 360° Phishing Certification

Given the frequency and risks associated with phishing attacks today, it's clear that modern endpoint security needs to protect against such attacks.

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 test: 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 security product's secure browser or its browser extension blocking abilities. This quarter, they used five ITW 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 Q4 2023 results on these tests, see chart below.

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

ThreatDown™ Powered by Malwarebytes

5 Top-Tier Certifications Endpoint Security Must Have

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

1 **360° Level 1 Certification:**
The product blocked every ITW 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 ITW financial malware sample and passed the Reat Botnet Test and the Banking Simulator/Magecart Test.

4 **360° Ransomware Certification:**
The product blocked every ITW 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 Test and Phishing Simulator Test.

ThreatDown™ Powered by Malwarebytes

ThreatDown vs Microsoft Defender

	Level 1	Online Banking	Exploit	Ransomware	Phishing
ThreatDown	✓	✓	✓	✓	✓
Microsoft Defender	✓	✓	✓	✓	✗

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.

In the Wild/Full Spectrum Threats
Part of Level 1 Cert

Attackers can use zero-day threats to infiltrate a network opportunistically, without any warning.

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

- Phishing as an attack vector is responsible for the second most expensive data breaches at USD 4.76 million

ThreatDown Delivers

ThreatDown, powered by Malwarebytes, leverages 7 unique layers of detection techniques in what we call Multi-Vector Protection. These 7 layers allowed ThreatDown to stop the threats Microsoft didn't.

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

ThreatDown Powered by Malwarebytes

ThreatDown vs Symantec

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

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.

In the Wild/Full Spectrum Threats
Part of Level 1 Cert

Attackers can use zero-day threats to infiltrate a network opportunistically, without any warning.

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 a web-skimmer—malware that is injected onto a vulnerable website so it can steal credit card information as 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

- Phishing as an attack vector is responsible for the second most expensive data breaches at USD 4.76 million
- It's estimated that Magecart attacks have cost businesses over $1 billion annually

ThreatDown Delivers

ThreatDown leverages 7 unique layers of detection techniques in what we call Multi-Vector Protection. These 7 layers allowed ThreatDown to stop the threats Symantec didn't.

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

ThreatDown Powered by Malwarebytes

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 malware
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 a web-skimmer—malware that is injected onto a vulnerable website so it can steal credit card information as 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 $4.35 million in 2022
- Exploits are involved in 60% of data breaches. The cost of a data breach was $4.35 million in 2022

ThreatDown Delivers

ThreatDown leverages 7 unique layers of detection techniques in our Multi-Vector Protection. These 7 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.

ThreatDown™ Powered by Malwarebytes

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 evolve past 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 Q4 2023 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 2022 and 2023.

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

	Q3 (2022)				Q4 (2022)				Q1 (2023)				Q2 (2023)				Q3 (2023)					Q4 (2023)				
	LVL1	EXPL	B ANK	RANS	LVL1	EXPL	BANK	RANS	LVL1	EXPL	BANK	RANS	LVL1	EXPL	BANK	RANS	LVL1	EXPL	BANK	RANS	PHISH	LVL1	EXPL	BANK	RANS	PHISH
ThreatDown	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Symantec	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗
Microsoft	✓	✓	✓	✓	✗	✗	✗	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✗
Avast Business	✗	✓	✗	✓	✗	✓	✗	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ESET	✗	✓	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Avira	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓
Trend Micro	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✓	✓	✗	✗	✓	✓	✗

✓ Attained

✗ Failed

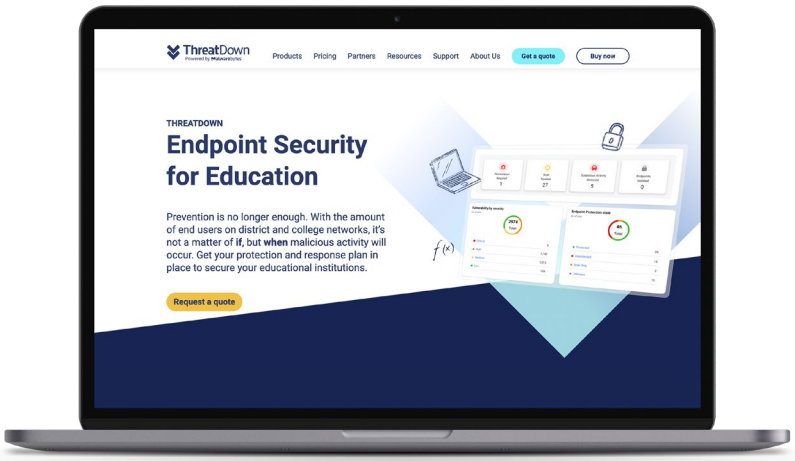
LVL 1 - 360 Assessment - Level 1 Certified

EXPL - Exploit - Certified

BANK - Online Banking Certified

RANS - Ransomware Certified

PHISH - Phishing Certified



Defend against tomorrow's threats!

Let us take care of your endpoint security for your educational institution. 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 | corporate-sales@malwarebytes.com | 1.800.520.2796