ThreatDown™
Powered by Malwarebytes

TOP 10 REASONS TO UPGRADE TO THREATDOWN EDR

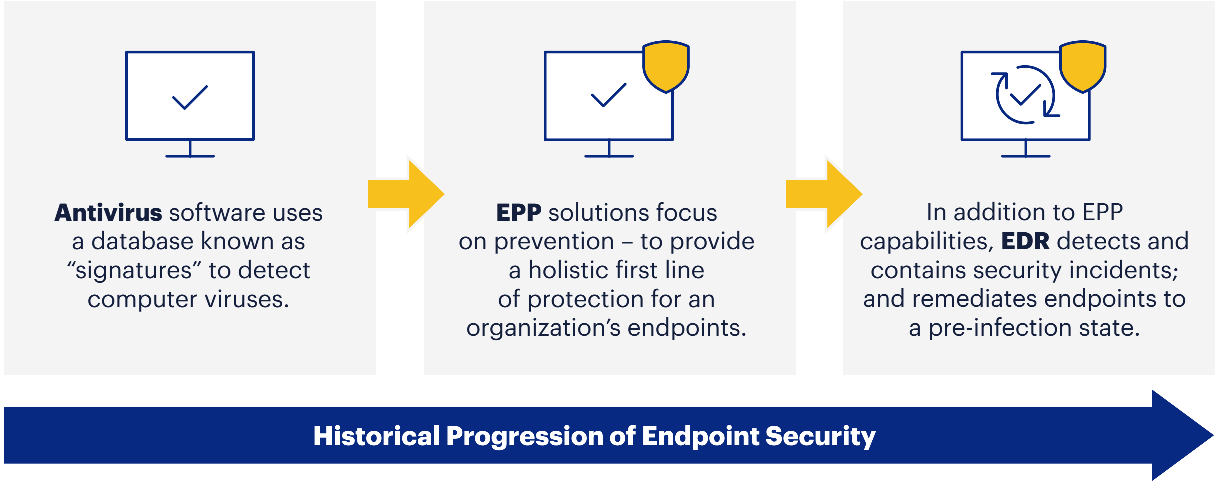
CONTENTS

INTRODUCTION

Cybercriminals are motivated and continue to develop new tactics in an attempt to bypass an organization's endpoint protection platform (EPP) solution. In a simpler time, having strong EPP was enough to safeguard the business against the dangers of cyber threats. Alas, those days have passed, which is why organizations are upgrading their defenses to endpoint detection and response (EDR) solutions.

To understand why organizations are upgrading to EDR, first, here's an overview on the difference between EPP and EDR solutions.

It's easiest to break the capabilities into three parts: prevention, detection, and response. EPP focuses on prevention. EDR includes prevention and adds detection and response capabilities.



Antivirus software uses a database known as "signatures" to detect computer viruses.

EPP solutions focus on prevention – to provide a holistic first line of protection for an organization's endpoints.

In addition to EPP capabilities, **EDR** detects and contains security incidents; and remediates endpoints to a pre-infection state.

Historical Progression of Endpoint Security

EPP (Prevention)

The goal of EPP is to focus on prevention – to provide the first line of defense against attacks on endpoints.

EDR (Prevention + Detection and Response)

When an attack gets past the prevention capabilities, EDR includes advanced threat detection capabilities that serve as a powerful safety net to capture and contain the threat. An EDR includes a range of more advanced capabilities for threat detection, isolation, investigating security incidents, and ability to remediate endpoints to pre-infection state.

INTRODUCTION (CONTINUED)

Why is EDR now considered the best practice security standard?

Well, a few reasons:

- **Expanding attack surface:** A key trend driving the need for EDR is the expanded corporate attack surface stemming from cloud adoption and device mobility where a remote and hybrid workforce place endpoints beyond the organization's traditional firewall perimeter.
- **Ever-evolving attacks techniques:** Since the dawn of the first cyberattack, threat actors have continually advanced their tactics to evade detection and gain access to corporate endpoints. The innovations in EDR were, and are continuously being, developed to provide organizations with security capabilities that outpace attacker techniques.
- **Endpoints are the target:** Regardless of how an attack begins, at the end of the day, cybercriminals are going after your endpoints: your servers, laptops, and other user devices. That's where your high-value data lives and it's also where the attacker can gain a foothold into your organization. In fact, 90% of security breaches originate at the endpoint, so it stands to reason that your endpoints need the best that security has to offer.[1]
- **Seismic business impact:** We've all heard the horror stories: just one successful attack can disrupt operations, occupy IT teams for weeks to successfully restore the network, and cost organizations significantly in lost revenue (and possible regulatory fines). If that's not worrisome enough, 31% of organizations end up closing down completely after falling victim to a ransomware attack.[2] Adopting EDR is the best endpoint security approach to avoid these troubling scenarios.

Why customers upgrade to ThreatDown EDR

As an existing ThreatDown Endpoint Protection customer, you've got the best in threat prevention capabilities. Because cybercriminals never sleep and are constantly looking for ways around EPP solutions, your organization will gain significant advantages by upgrading to ThreatDown EDR.

Customers have shared many reasons why they chose to upgrade from ThreatDown EP to EDR. The following pages list the top 10.

[1] Verizon. Data Breach Investigation Report. 2022.
[2] Security Boulevard. Dealing with a ransomware attack: How can firms spot and recover from these threats? August 2022.

#1 | THREATDOWN EDR IS A MUST-HAVE SECURITY BEST PRACTICE

Customers experience invaluable peace of mind

When the market first introduced EDR solutions a decade ago, it seemed like they were only suited for the largest organizations that had well-staffed security teams. Ten years later, that's not the case.

Today, every organization of every size should have an EDR solution in place. That's why cybersecurity frameworks like NIST and SANS recommend EDR as part of their best practice security frameworks, and cyber insurance companies require organizations to adopt EDR in order to obtain insurance coverage. ThreatDown EDR packs the full power that EDR has to offer and provides the ease of use that make it ideal for organizations of all sizes.

Most organizations know that even advanced prevention is not 100% effective: today's complex threats sneak past preventative measures.

ThreatDown EDR delivers a powerful security upgrade to address threats that bypass your current threat prevention capabilities.

> *"There are a lot of different, moving parts that go into our security ecosystem. ThreatDown EDR is probably our biggest and most important cog, and I would recommend it to all businesses."*
>
> **Andrew Jones**
> Senior IT Specialist
> City of Vidalia

#2 | ADVANCED THREAT DETECTION

Unlocks capabilities to stop zero-day attacks

ThreatDown EDR adds robust threat detection capabilities that advance your endpoint security posture by uncovering unknown (zero-day) and hidden threats.

Built on machine learning (ML) and behavioral analysis techniques, you'll gain leading-edge detection capabilities that monitor process, registry, file system, and network activity on your endpoints to swiftly detect anomalous patterns that might indicate malicious intent.

Zero-day threats account for 80% of successful breaches.[3]

> *"Put simply.... I'm thankful every night, weekend, and vacation day because ThreatDown EDR continues to run when I'm not watching. It keeps our organization safe."*
>
> **David Teston**
> Information Security Officer
> Georgia Public Library Service

[3] Dark Reading. Human Threat Hunters Are Essential to Thwarting Zero-Day Attacks. August 2022.

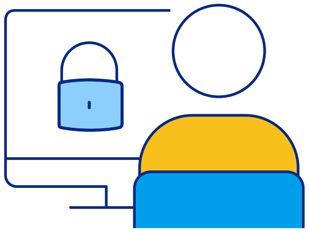
#3 | CONTAIN THREATS FROM SPREADING

Stops attackers in their tracks

When an endpoint is compromised, ThreatDown EDR's isolation capabilities help mitigate potential damage. Fast containment prevents the threat from spreading to other machines in your environment. Malware is stopped from phoning home, and remote attackers are locked-out, which prevents them from stealing your corporate and customer data.

Our granular isolation modes—per network segment, process, or endpoint—lock out remote attackers, stop malware from spawning new processes, and prevent users from initiating applications that might complicate response efforts.

> *"ThreatDown EDR is great to detect infections—but to also have a solution that isolates and disinfects the infection is huge. I believe Malwarebytes has a powerful solution, and no one currently has anything close to it."*
>
> **Joseph Sutorius**
> Chief Information Officer
> East Irondequoit Central School District



#4 | AUTOMATE ENDPOINT CLEAN UP

Delivers fast, thorough remediation

Fast clean up is essential when the inevitable incident occurs. Slow, manual efforts create long dwell times (the amount of time the attacker has to wreak havoc) that expose an organization to significant risk. With ThreatDown EDR, you can automate the disinfection effort with a single 'click.'

ThreatDown EDR is the trusted standard in automated endpoint disinfection and will expedite your response times with fast and complete remediation.

To prevent re-infection, our proprietary Linking Engine begins by eradicating active malware components; then, it seeks out and removes detected artifacts and config changes, which malware commonly leaves in its wake.

60% of attacks take organizations more than 9 hours to remediate.[4] This increases the likelihood of a successful data breach.

ThreatDown EDR accelerates your response time to minutes.

> *"ThreatDown EDR helped disinfect our network after a particularly nasty Emotet infection."*
>
> **Brian Maull**
> Network Administrator
> F.A. Davis Company

[4] Osterman Research. Understanding the Depth of the Global Ransomware Problem.

#5 | ROLLBACK RANSOMWARE

Facilitates ransomware recovery—no hefty ransom or lost data

Ransomware poses a significant risk. One successful attack can halt business operations and negatively impact your brand and customers.

Upgrading to ThreatDown EDR will protect your organization from ransomware by continually monitoring your endpoints for evidence of ransomware behaviors. When such behavior is detected, ThreatDown EDR activates the file backup process, encrypting and relocating data for later restoration. With one click, you can reverse ransomware damage by rolling back affected files to their pre-attack state up to 72 hours before the compromise.

11 seconds

$4.54 million

Businesses face a ransomware attack every 11 seconds.[5] The average cost if it's successful: $4.54 million.[6]

ThreatDown EDR: 100% guaranteed against ransomware attacks.

> *"ThreatDown EDR keeps us protected, and I'm blown away by the ransomware rollback feature. I sleep 10 times better knowing we have ThreatDown EDR on our infrastructure."*
>
> **Matthew O'Brien**
> Systems Administrator
> Finger Lakes Community Health

[5] DataProt. Ransomware Statistics in 2022. December 2022.
[6] IBM. Cost of a data breach 2022. 2022.

#6 | THREAT INVESTIGATIONS MADE EASY

Gives you an investigation wingman

Threat investigation is a cybersecurity technique where your team can proactively search your systems for indicators of compromise (IOC) and anomalies to find security risks. ThreatDown EDR simplifies your threat hunting with the visibility and guidance you need—at every step. You'll get the threat intelligence and research details to help you make the right decisions and to know what to do next with the following ThreatDown EDR features:

- **Rich threat hunting visibility:** Gain granular visibility with prioritized IOCs to quickly focus on endpoints that need further investigation.
- **Central search on event data:** Search on historical endpoint data (e.g., files, registry, processes, networking activity) with the Flight Recorder feature.
- **Guided investigation workflows:** Gain guided investigations with MITRE ATT&CK mapping that streamline your threat hunting and analysis.
- **Cloud sandbox:** Detonate potentially harmful malware within the cloud sandbox for evaluation and analysis.

> *"With the ThreatDown EDR cloud console, our IT team has the in-depth visibility required to always know the state of our company's security posture."*
>
> **Jon Debolt**
> Systems Administrator
> Meyer Tool

#7 | ENJOY AN EASY UPGRADE WITH NOTHING NEW TO DEPLOY

Provides a hassle-free upgrade to EDR

ThreatDown, powered by Malwarebytes, customers rave that the upgrade delivers all the added power, without requiring any time or effort to deploy new software. With ThreatDown's single, unified agent already deployed in your environment, upgrading your organization from ThreatDown EP to EDR couldn't be easier.

> *"The upgrade was so simple and didn't require deploying any new software."*
>
> *"It's so great we could move to ThreatDown EDR without any of the typical uplift new IT projects require."*
>
> *"With just a simple backend license change to EDR, we were off to the races."*
>
> **ThreatDown Customers**

#8 | INCREASE YOUR TEAM EFFICIENCY

Saves you time and resources

A common theme we hear from customers is that their IT team is stretched thin with so many responsibilities to manage and limited resources. This global trend is why we focus on providing our customers with business solutions that are easy to use, incorporate automation where appropriate, and enable IT teams to save time and resources.

ThreatDown EDR gives you the full culmination of these efficiency capabilities and benefits. With ThreatDown EDR, customers say they:

- **Reduce helpdesk tickets** related to malware by +25%
- **Save time** handling endpoint incident response and remediation tasks
- **Gain efficient capabilities** that streamline investigations

> *"ThreatDown EDR catches malware and deals with it straightaway. Done and dusted. It has given us back 20% of our work week by not having to restore infected machines, and our vendor experience is exceptional."*
>
> **Andrew Larner**
> Director of IT
> Trinity College

#9 | GAIN LESSONS LEARNED TO CLOSE SECURITY GAPS

Empowers you to know what's happening in your endpoint environment

As a company and as individuals, we all improve our security against cyber threats by sharing knowledge and obtaining helpful information about what's happening to our systems. At ThreatDown, powered by Malwarebytes, we prioritize this value.

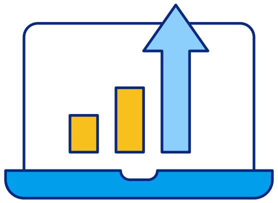
While some EDR and other security solutions hide the details or "smarts" behind their threat detections, ThreatDown EDR provides informative intelligence about your detected threats and details on the threat itself so you can understand how an attack happened and learn from it. Equipped with this insightful knowledge, you can proactively make appropriate improvements to your systems to stop the security issue from happening again.

> *"Personally, having ThreatDown EDR takes the stress out of being an IT manager in charge of all the computers that run the business. If something does crumble, I can simply click on the machine that's affected and remediate it. That takes the pressure off me, because I can just fix it as quickly as I can go into Malwarebytes and get it done."*
>
> **Chris Candy**
> Information Technology Manager
> Mike Carney Toyota

#10 | IMPROVE COST EFFICIENCY

Delivers a compelling ROI

When customers adopt ThreatDown EDR, they're delighted by the tangible and intangible savings they gain, as well as the costs they avoid by reducing the risks of a zero-day attack, data breach, or ransomware extortion.



Some examples include:

- Reduced helpdesk tickets by more than 25%
- Saved money on annual cyber insurance premium
- Recouped 8 hours per week (a full workday) no longer handling issues related to endpoint response
- Lowered risk of a security breach and avoided related costs
- Reduced potential and associated costs from ransomware attacks
- Gained 100% money-back guarantee against ransomware attacks

> *"At the end of the day, we've got ThreatDown EDR and ransomware remediation in place. If something does go pear shaped, we can roll back a PC and be fully operational again in minutes. Demonstrating ThreatDown EDR capabilities saved us money on our cyber insurance premium."*
>
> **Chris Candy**
> Information Technology Manager
> Mike Carney Toyota

LEARN MORE AND UPGRADE TO THREATDOWN EDR TODAY!

To experience, firsthand, the ten benefits of upgrading to ThreatDown EDR and learn how easy it is to upgrade, contact your ThreatDown, powered by Malwarebytes, Expert today.

www.malwarebytes.com/business ✉ corporate-sales@malwarebytes.com ☎ 1.800.520.2796