ThreatDown
Powered by Malwarebytes

Endpoint Protection is Not Enough

ThreatDown vs Webroot

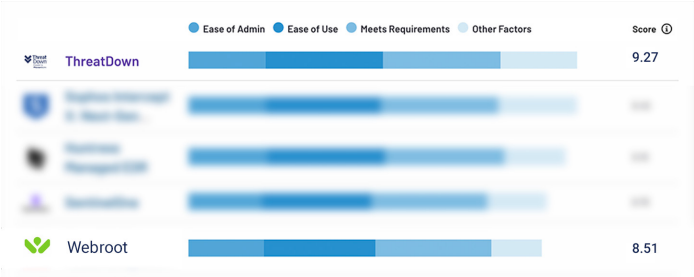
Today's zero-day and fileless threats require the threat monitoring, investigation, and remediation capabilities of a tested and proven endpoint detection & response (EDR) solution that can stop or rollback ransomware and guide security posture improvements.

Head-to-head comparison

	ThreatDown	Webroot
Attack surface coverage	✓ EDR, application block, vulnerability assessment, patch management, DNS filtering, etc.	✗ Only includes DNS filtering; very limited EDR features included in the Endpoint Protection product (no EDR product).
Automated deployment guidance	✓ Security Advisor (included for all customers) offers a security score that reflects the current state of deployment, guidance on improvements and provides the ability to make the changes.	✗ Does not offer any kind of automated guidance on the current effectiveness of a customer's deployment or how to improve
Ransomware rollback	✓ 7-day Ransomware Rollback included with EDR; which helps you return to a pre-ransomware state without reimaging machines or recreating encrypted files.	✗ Does not recover files attacked and encrypted by ransomware.
Broad OS and device support	✓ OS support includes Windows, macOS, Linux, iOS, Android, and ChromeOS.	✗ Does not support Linux and does not support mobile devices.

Take threats down

- ThreatDown received EVERY award, 52 out of 52 awards, since Q3 2021, from independent testing lab MRG Effitas
- Only vendor to consistently achieve 100% protection against ransomware, phishing, exploits, and every other real-world test
- ThreatDown was awarded "Product of the Year 2024" by AV Labs for blocking 459/459 of "in-the-wild" malware samples while in the latest Advanced In-the-wild Malware Test, Threatdown earned a 100% protection score whereas Webroot missed some malware.



ThreatDown ranked #1 in the G2 Endpoint Protection Suites Usability Index, with the highest score of all vendors. Webroot ranked 8.51 for usability, compared to ThreatDown's 9.27.

Take complexity down

Webroot

- Webroot only sells point products, not bundles or packages
- User interface is dated and difficult to navigate
- Webroot doesn't offer vulnerability assessment, patch management, mobile security or Linux support
- Limited EDR leads to layering multiple, complex solutions or lacking protection
- No security health check score to simplify optimizing security postures

ThreatDown

- Deployed in minutes, easy to navigate, no fine-tuning needed
- One, lightweight agent
- Includes Security Advisor score and prioritized actions
- G2 named ThreatDown EDR "Most Implementable," "Fastest Implementation," and "Easiest to Use"
- Protects your organization's mobile devices (including: iOS, Android, and ChromeOS) without adding management complexity.

Take costs down

Multiple tools cost budget and resources to manage. ThreatDown Bundles provide a single agent, single console, all-in-one solution that includes Application Block and Vulnerability Assessment for free.

A successful ransomware attack can have costly consequences. ThreatDown's 7-day ransomware rollback solution can restore files on workstations up to 7 days after a ransomware attack, saving valuable resources.

A former Webroot customer suffered $8M in losses from a ransomware attack before selecting ThreatDown for ransomware protection and peace-of-mind.

Read the case study on why **NELLO** turned to ThreatDown and book a demo to see **how ThreatDown can elevate your defenses against ransomware.**

Read case study | Book a demo

ThreatDown Powered by Malwarebytes | threatdown.com/contact-us | sales@threatdown.com