Miercom

DR240329C

April 2024

Licensed for Distribution by:

Datto

EDR & AV Security and Features Summary

Miercom EDR Benchmark ™ 2024

Table of Contents

1.0 Executive Summary

In the current digital era, where cyber threats are evolving at an unprecedented rate, the significance of advanced cybersecurity measures has become paramount. Datto Endpoint Detection and Response (EDR) and Datto Antivirus (AV) are at the forefront of this battle, offering sophisticated tools and technologies to identify, prevent, and mitigate the impact of cyberattacks. These solutions are designed not only to deal with known threats but to uncover and respond to new, sophisticated attacks that evade traditional security measures. By incorporating these solutions into their security strategy, organizations can significantly enhance their resilience against cyber threats, ensuring the integrity and availability of their critical systems and data.

Datto engaged Miercom to conduct a private evaluation of the Datto Endpoint Detection and Response (EDR) and Datto Antivirus (AV) solutions as compared to competitive offerings. This study assesses and benchmarks the effectiveness of the products in protection and detecting actual threats with a focus on the latest malware strains and the most employed infection vectors.

Key Findings

- **Overall Malware Efficacy:** Datto EDR with Datto AV demonstrated an overall malware detection efficacy rate of **99.62%** in detecting and neutralizing malware threats, compared to the industry average of 73% of products in this class.
- **Zero-Day Threat Detection:** Our study revealed that both Datto EDR and Datto AV achieved a **98%** detection rate for zero-day threats, which is more than double the industry average for products in this class of **45%**.
- **Onboarding and Support:** Datto stands out with unparalleled support services characterized by fast response times and prompt follow-up actions. This high level of support ensures that customers can rely on timely assistance when needed.
- **Proven Advanced Threat Detection:** Datto exceeded our expectations for detecting fileless threats and ransomware while effectively isolating infected endpoints. Their solutions have proven effective in mitigating advanced evasive, advanced persistent, and polymorphic threats.

Datto is recognized as a leading vendor in the Miercom Endpoint Detection and Response Platform assessment, outperforming competitive products in a comprehensive evaluation focusing on Endpoint Detection and Response and Antivirus platforms. Datto’s overall malware efficacy, zero-threat detection and vendor support shows their commitment to providing a superior EDR and AV platform and has earned the **Miercom Certified Secure** award.

Robert Smithers

CEO, Miercom

2.0 EDR & AV Testing Summary

Datto EDR with Datto AV
Endpoint Detection and Response Platform Assessment Summary

Section	Evaluation Criteria	Rating
4.1	**Malware Detection Efficacy:** Datto EDR and AV proved in testing overall 99.62% efficacy rate in malware detection, 21% above the 73% industry average.	●
4.2	**Alert Correlation:** Datto EDR and AV boost security by prioritizing alerts based on threat level and identifying patterns of correlated events that may signal an emerging attack.	●
4.3	**Response and Remediation:** Datto EDR and AV enable the creation of policies for automated responses to threats, leveraging Datto's recommended actions.	◕
4.4	**Advanced Threat Protection:** Datto EDR and AV blocked 1,456 samples, demonstrating a 98% detection rate.	◕
4.5	**Zero Day Threat Prevention:** Datto excelled with a 98% detection rate for Zero-Day malware samples, far surpassing the industry average of 45%. (Combined achievement)	●
4.6	**Real-time and Historical Analysis:** Datto's portal showed remarkable accuracy, with the number of detected malware samples matching the alerts displayed including exact path.	●
4.7	**Performance:** Datto EDR and AV exhibited minimal resource consumption, using just 0.2% CPU in idle mode and approximately 8.5% during active scans, with overall system usage at 2% and 20%, respectively.	●
4.8	**Multi-Platform Support:** Datto EDR supports Windows, macOS, and Linux operating systems. Datto AV lacks current support for macOS and Linux, though plans to extend this support are anticipated this year.	◕
4.9	**Vendor Support:** Datto displayed exceptional responsiveness during testing, and swiftly and efficiently addressed all of Miercom's inquiries and concerns.	●
4.10	**Onboarding Experience:** Deployment of Datto AV and EDR, is achieved through online tutorials and live onboarding assistance to ensure the products were properly implemented.	◕
4.11	**Alerting and Reporting:** The Datto EDR and AV portals features a user-friendly dashboard with tabs for streamlined navigation which displays detected malware, with details like time, date, location, severity, and threat name.	◕
OVERALL RATING		●

Key				
●	◕	◑	◔	○
Excellent	**Good**	**Fair**	**Poor**	**Not Supported**

3.0 About Datto EDR and AV

In the dynamic landscape of cybersecurity, the importance of robust and effective security solutions cannot be overstated. This report explores two cutting-edge products: Datto EDR and Datto AV. These products represent a comprehensive approach to protecting endpoint devices and networks from a myriad of cyber threats.

Datto Endpoint Detection and Response (EDR)

Datto EDR is a layered, integrated endpoint security solution that provides continuous monitoring and automated responses to threats on end-user devices. Going beyond traditional antivirus, it records and analyzes endpoint behaviors, proactively identifying and responding to activities that signal potential threats, including zero-day threats, multi-staged attacks, and advanced persistent threats (APTs).

The Synergy of AV and EDR

Mainstream AV solutions, while effective against common threats, may not counter sophisticated cyberattacks due to their signature-based approach. Datto EDR complements AV by identifying suspicious behaviors and issuing actionable alerts, using behavioral analysis, heuristics, and machine learning to detect advanced threats that bypass traditional AV. This AV and EDR integration offer extensive protection against a wide array of threats.

Special Features and Integrations

Datto EDR offers features tailored for Managed Service Providers (MSPs), providing advanced endpoint detection and response in an affordable, user-friendly package. Highlights include rapid threat response capabilities, fileless attack detection via behavioral analysis, and integration with Datto RMM and the Kaseya IT Complete platform. Datto's EDR and AV solutions deliver critical protection against evolving cybersecurity threats, ensuring businesses have a comprehensive defense strategy for their digital assets.

Product Tested	Version
Datto Endpoint Detection and Response (EDR)	(Agent Version 3.3.1.1613) (Portal Version 8600)
Datto Antivirus (AV)	(Agent Version 3.3.1.1613) (Portal Version 8600)

4.0 Test Criteria Evaluation

4.1 Malware Efficacy

Malware Efficacy Rating	
●	Datto EDR and AV provides effective malware protection – 98% for Zero-Day threats which is 52 percentage points above the industry average for similar products. This excellence is part of an overall 99.62% efficacy rate in malware detection—21 points above the 73% industry average.

Description: The core mission of assessing malware efficacy is to evaluate the effectiveness of cybersecurity solutions in detecting, blocking, and mitigating malware to protect devices, networks, and data from unauthorized access or harm. This involves testing how well security tools can detect malware, including viruses, worms, trojans, ransomware, and more, to measure the reliability and robustness of these tools in real-world conditions to protect against cyber threats and maintain the integrity of information systems.

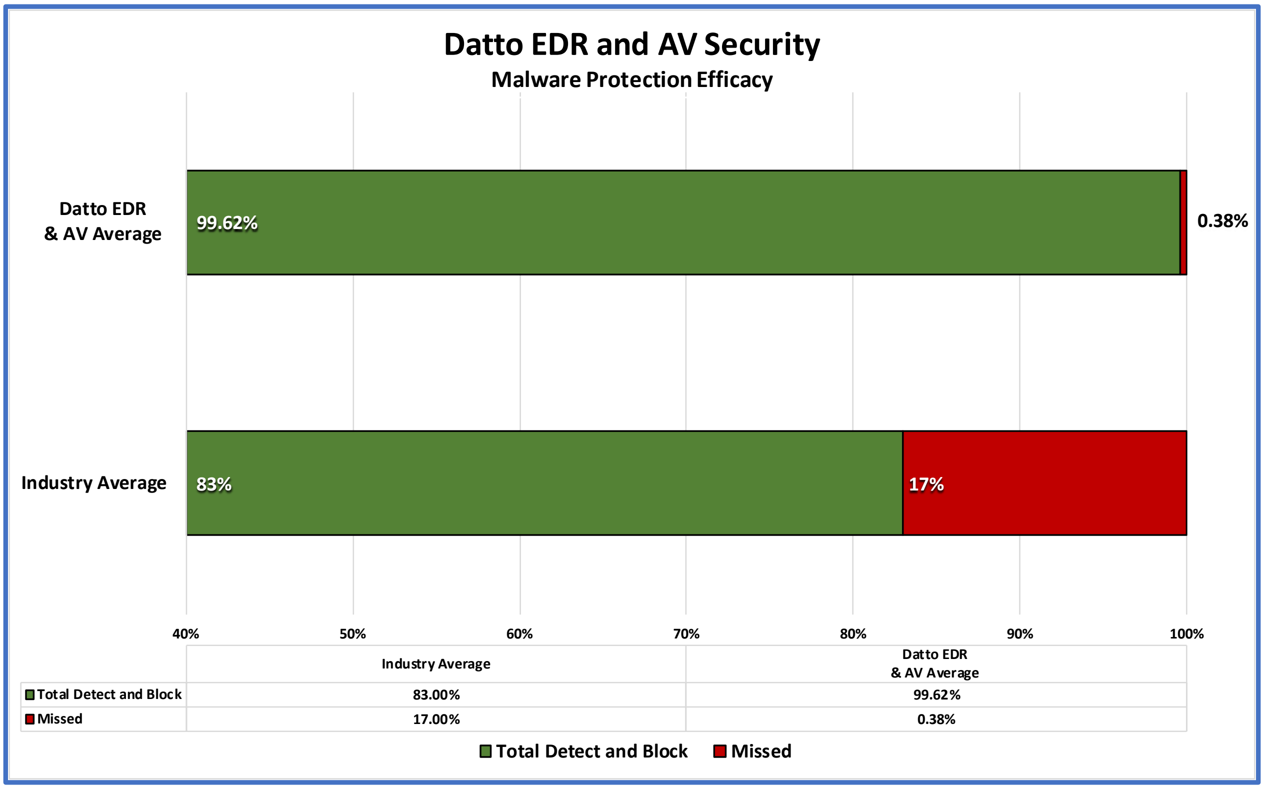
Impact: An effective EDR solution can detect abnormal behaviors or suspicious use of system tools. It should initiate countermeasures, provide information on the path of the malware for remediation, and provide reports detailing the attack's progression, the EDR's counteractions, and recommendations for enhancing endpoint security.

According to the 2023 Internet Security Threat Report by Symantec, malware attacks have evolved, with attackers increasingly using methods that evade traditional security measures. A 33% surge in ransomware attacks from the previous year stresses the urgency for robust EDR solutions. Furthermore, 1 in 4 organizations experienced at least one malicious email attack, demonstrating the prevalent risk and emphasizing the necessity for advanced EDR capabilities to detect, respond to, and mitigate these evolving threats effectively.

Procedure: Samples from the Miercom malware server are used in industry-wide studies of malware detection for network security devices. Common malware types are botnets and Remote Access Trojans (RATs). A particular emphasis is placed on active threats, advanced evasion techniques and advanced persistent threats. These represent the more complex and challenging categories for security solutions to identify. Detection results reveal individual approaches to malware detection, as well as its granularity.

The system under test (SUT) was an intermediary between untrusted and trusted zones of the simulated network. A simulated attack from the untrusted zone consisted of an attempted download of a malicious file. A successful block was logged when the simulated victim client cannot download the malware sample.

Observation: In reviewing Datto's malware protection efficacy by AV block and behavioral block across exploit types, the standout performance of its 100% interactive detection rate for categories including Legacy Malware, Modified Malware, and Mobile Threats. Particularly noteworthy is its response to Advanced Persistent Threats (APTs), Polymorphic, Ransomware, Botnet, and Backdoor malware where a 100% efficacy rate between AV and behavioral block was observed. Datto's proficiency in detecting Zero-Day threats at a 98% rate, 51 percentage points more than the industry average, proves its robustness in identifying and responding to the most elusive and emerging threats. This overall strong performance translates to a 99.61% malware detection efficacy rate between AV block and behavioral block, 17% higher than the industry average of 83%.



	Industry Average	Datto EDR & AV Average
🟩 Total Detect and Block	83.00%	99.62%
🟥 Missed	17.00%	0.38%

This chart compares the malware protection efficacy between Datto EDR & AV with the industry average. Datto proved a 99.62% success rate in detecting and blocking threats versus the industry's 83%, and only a .38% miss rate compared to the industry's 17%.

Miercom Malware Sample Definitions

Standard Malware

Active Threat

An active threat exploit is a term used to describe a situation where a malicious actor is actively exploiting a known vulnerability in a system or software. This means that the attacker has found a way to take advantage of a security flaw and use it for malicious purposes, such as installing malware, stealing data, or launching cyberattacks.

Backdoor

A backdoor exploit is a type of cyberattack that uses a hidden or unauthorized way to access a system, network, or software. A backdoor exploit can bypass the normal security measures and allow the attacker to control, spy on, or damage the target device or system.

Some common methods of creating or using backdoor exploits are installing malware such as trojans, rootkits, or keyloggers that can open a remote connection to the target, or exploiting a vulnerability in a software or hardware that can grant the attacker access to the target.

Botnets

Botnets are networks of devices or computers that have been infected by malicious software and are controlled by hackers. Botnets can be used for various cyberattacks, such as sending spam, stealing data, launching denial of service (DoS) attacks, or mining cryptocurrency.

Legacy

Legacy malware refers to malware that is mature and should be considered “well-known.” These are expected to be detected by most signature-based detection countermeasures. This malware set is the most extensive and is challenging to countermeasures with limited device memory for signature detection. Legacy malware may still pose a threat to systems and devices that are not updated or protected by modern security tools.

Legacy malware is relatively old malware and is expected to be detected; however, sometimes systems may disregard such antiquated threats, allowing them to still attack networks.

Malicious Documents

Malicious documents are files that contain harmful code or commands that can compromise the security of the system or software. Malicious documents can be used to infect systems with malware, steal data, launch cyberattacks, or perform other malicious actions.

Types of malicious documents include Microsoft Office files (.doc, .xls, .ppt, etc.) or PDF documents that contain macros, shellcode, JavaScript, embedded files, or objects that can exploit vulnerabilities or run malicious code.

This type of malware is often seemingly benign but contain malicious coding (“macros”) alongside plain-text data to seem legitimate while infecting the target device upon opening.

Remote Access Trojans (RATs)

A RAT exploit is a malicious attack that uses Remote Access Trojans to gain unauthorized access to a victim’s computer or network. RATs are a type of malware disguised as legitimate software that allows hackers to monitor and control the infected device or network remotely once activated and perform malicious activities such as stealing sensitive data, spying on user activities, manipulating files, installing additional malware, and launching attacks on other devices. RATs are often distributed through phishing emails, malicious downloads, or compromised websites, and they can be difficult to detect and remove.

Examples of Remote Access Trojans are DarkComet RATs, a popular RAT that was used by the Syrian government during the civil war. The DarkComet RAT allowed the attackers to capture keystrokes, screenshots, webcam feeds, passwords, and files from the infected computers.

A Ghost RAT is a RAT that was used by a cyberespionage campaign called OperationGhostNet to infiltrate and compromise high-profile targets such as embassies, ministries, and NGOs in over 100 countries. The Ghost RAT allowed the attackers to take full control of the infected computers including turning on the webcam and audio devices, logging keystrokes, stealing documents, and browsing files on the infected devices and networks.

The Onion Router (TOR)

A TOR Exploit is a type of cyberattack that uses a modified version of the TOR browser to compromise the security and anonymity of the users. The TOR browser is a software that allows users to browse the web anonymously by encrypting and routing requests through multiple layers or nodes, and it is often used to access hidden or otherwise inaccessible locations on the internet such as the dark web.

Hackers have created trojanized versions of the TOR browser that inject malicious codes or scripts into the visited websites or send the users' real IP address and other sensitive information to a remote server. These malicious TOR browsers are a form of malware with multi-layer encryption that collects personal data and sends it to a Command and Control (C&C) server.

Zero Day Malware

Zero Day refers to any threat that is not catalogued, and therefore not automatically recognized, by threat detection systems. Zero-day threats are particularly dangerous because they target vulnerabilities that are unknown to the victim, making them difficult to detect before any harm is done to the target system or network. Once a zero-day vulnerability is discovered, either the target system or protection solution must apply a patch to mitigate the threat and take measures to prevent future attacks.

Mobile Malware

Mobile malware is any file or software that exploits and attacks mobile devices such as smartphones and PDAs. Mobile devices have become substantially more complex and widespread in the modern world, greatly increasing the potential attack surface for any network or organization. Mobile threats exploit this by targeting vulnerabilities in such devices. Mobile malware has been a growing concern since it emerged in 2000 and continues to become more dangerous and more complex as technology evolves. Types of mobile malware include expanders, worms, trojans, spyware, backdoor attacks, and droppers.

Advanced Threats

Advanced Evasion Techniques (AETs)

Advanced Evasion Techniques (AETs) are methods of hiding malicious network traffic from security devices such as firewalls or intrusion detection systems. AETs can combine different evasion tactics that create multi-layer access, modify them during the attack, or use nonstandard protocols to avoid detection. AETs can enable attackers to deliver malware, steal data, or launch cyberattacks without being noticed.

Some examples of Advanced Evasion Malware are IP Fragmentation, which, splits a packet into smaller fragments that can bypass security filters; TCP segmentation which divides a TCP stream into smaller segments that can evade signature-based detection; Protocol Obfuscation, which alters or violates protocol specifications to confuse security systems; and Encryption or Encoding, which transforms the payload or header of a packet to make it unreadable by security devices.

Advanced Persistent Threats (APTs)

APT exploits are malicious attacks that use Advanced Persistent Threats (APTs) to gain unauthorized access to a victim's computer or network. APTs are cyberattacks that are carried out by well-funded and skilled actors, often sponsored by nation-states, over a long period of time and consist of continuous hacking with payloads opened at the administrative level. APT exploits aim to steal sensitive data, disrupt systems, extort random, or conduct cyber espionage on devices and networks.

One example is a DarkComet RAT, a remote access trojan that was used by the Syrian government during the civil war. Another example is CryptoWall, a ransomware strain that encrypts files on the victim's computer and demands a random for their decryption.

Modified Malware

Modified malware is based on original malware which has been modified with techniques that allow it to now evade detection. Modified malware can have enhanced capabilities such as evading detection, infecting multiple hosts, or performing complex attacks.

Some examples of modified malware include the Diamond Sleet supply chain compromise, which distributed a modified Cyberlink installer that contained malicious code to download and load a second-stage payload; and TOR trojan exploits, which use modified versions of the TOR browser to compromise the security and anonymity of the users.

Polymorphic, Zero-Day Malware

Polymorphic malware is a type of malware that constantly changes its identifiable features to evade detection and exploit known vulnerabilities. Many of the common forms of malware can be polymorphic including viruses, worms, bots, trojans, or keyloggers. Polymorphic malware can use various techniques to mutate its code such as encryption, compression, or obfuscation. These conditions make it difficult for traditional antivirus methods to detect since they rely on signature-based detection to detect and block the threat.

One example is Storm Worm, a spam email campaign that infected millions of computers with a trojan that turned them into bots. The malicious code changes approximately every thirty minutes. Another example is CryptoWall, a ransomware strain that encrypted files on the victim's computer and demanded a ransom for their decryption. The malware used a polymorphic builder to create a new variant for every potential victim. Another example is BeeBone, a malware that created a botnet to distribute banking activity through ransomware and spyware. It changed its signature up to 19 times a day.

5.0 About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including Certified Interoperable™, Certified Reliable™, Certified Secure™ and Certified Green™. Products may also be evaluated under the Performance Verified™ program, the industry's most thorough and most trusted assessment for product usability and performance.

6.0 Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report, but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation, or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness, or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading, or deceptive or in a manner that disparages us or our information, projects or developments.

Miercom's Fair Test Policy allows for any vendor evaluated to challenge or retest these results in accordance with Miercom Terms of Use Agreement if there are any disagreements in our findings presented here.

Miercom did not acquire products for this review, nor has Miercom agreed to any vendor's End User License Agreement (EULA) or any other overly restrictive agreements that limit free press, product evaluations, editorial works, or publishing product reviews. We believe in providing accurate objective information to assist customers make informed purchasing decisions.

By downloading, circulating, or using this report in any way you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit: https://miercom.com/tou.

© 2024 Miercom. All Rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the authors. Please email reviews@miercom.com for additional information.