SOLUTION BRIEF

Malwarebytes for Business

4 REASONS WHY MALWAREBYTES MDR CAN TRANSFORM YOUR SECURITY PROGRAM

THE TIME IS RIPE FOR 24/7 CYBERSECURITY

For every business around the world (despite size or industry), 2021 was a record-breaking cyberattack year,[1] with 2022 exhibiting no signs of slowing. Cyber criminals are ever more persistent, as evidenced by the staggering **76% of ransomware attacks that occur on weeknights or weekends.**[2]

Statistics like these point to today's reality: **having a security operation center (SOC) that operates eight to ten hours a day Monday through Friday** is akin to locking your house only on weekdays: it's **not a viable option**, particularly in light of the potential cost.

Up 10% from 2020, the **average cost of a breach in 2021 for attacks of all sorts was US $4.24 million.**[3] You can lower that potential cost by literally millions—assuming you catch and contain malware quickly, which naturally requires having eyes on the threat landscape around the clock.

The time is clearly ripe for a 24/7 SOC—but is this relatively new and arguably essential paradigm within reach for your organization?

OUR ONE-TWO COMBO

Purpose-built for resource-constrained teams, Malwarebytes MDR provides alert monitoring and threat prioritization with flexible options for remediation—at a cost that makes sense.

Our highly-effective, easy-to-deploy EDR technology coupled with our team of security experts creates the perfect one-two combo for fighting cybercrime.

Dedicated Experts & Precise Technology

Underpinned by our proven EDR technology, Malwarebytes MDR provides powerful and affordable threat prevention and remediation services. Our team of experienced cybersecurity experts remotely monitors your network 24/7 to

- Detect,
- Analyze,
- Prioritize,
- Investigate,
- Triage,
- Remediate, and
- Hunt for threats.

Malwarebytes MDR defends your network every day and all night, safeguarding your data, reputation, and finances with always-on dedicated protection.

- **An MDR solution is only as good as the technology stack it's built on**—and as recent independent research attests, Malwarebytes EDR provides a rock-solid foundation:[4]

  – Replaces or easily augments other endpoint security solutions
  – Deploys within minutes and is lightweight and non-disruptive
  – Detects known *and* unknown threats
  – Removes artifacts, executables, and modifications associated with threat incidents
  – Includes 72-hour ransomware rollback for Windows workstations

- Each MDR provider offers different degrees of collective experience—**our MDR analysts have decades of experience in threat hunting and incident response:**

  – Monitors & analyzes log data & alerts that Malwarebytes EDR generates in near real time
  – Investigates and validates alerts
  – Escalates and reports validated security incidents to customers
  – Communicates clearly with customers on detected threats with guidance for remediation steps

FOUR REASONS WHY:

1 SAFEGUARD YOUR NETWORK 24/7

Lacking sufficient qualified staff is the primary barrier to meeting organizations' security needs.[5] But given the global shortage of cybersecurity professionals, hiring and retaining skilled staff to operate the 24/7 SOC you need proves difficult. With Malwarebytes MDR, you clear this hurdle with ease.

Our experts are your experts: with Malwarebytes MDR, our team of cybersecurity professionals acts as an extension to your security team, ensuring that you have the staff, skill, and experience you need to maximize your cybersecurity posture on a 24/7 basis.

With our MDR analysts monitoring your network around the clock, your security team is free to turn its attention toward other pressing projects, such as conducting digital forensics, creating (and training on) security policies, and fine-tuning procedures that affirm ongoing compliance.

2 MONITOR AND TRIAGES CRITICAL THREATS

Cybercriminals' persistence generates a preponderance of threat alerts that can overwhelm any security team but particularly resource-constrained teams. While estimates vary, some suggest that organizations experience as many as 11,000 alerts every day.[6]

With Malwarebytes MDR, our experts analyze and prioritize threats; they triage the critical ones while sharing clear guidelines that empower your team—whatever its skill level—to swiftly remediate those threats.

Through this process, Malwarebytes MDR reduces the number of daily alerts, which in turn reduces the risk of alert fatigue. With our team prioritizing alerts, your team gains back time spent investigating lower-level or false-positive alerts so it can focus instead on responding appropriately to threats that matter.

3 REDUCE DWELL-AND-RESPONSE TIMES

When your network is breached, the race is on to find and contain the threat: the longer it takes to contain, the costlier its effect. In fact, according to Ponemon, breaches that take longer than 200 days to identify and contain cost $1.26 million more than breaches that take fewer than 200 days to identify and contain.[7]

Malwarebytes MDR helps reduce dwell-and-response times from hundreds of days to only a few hours or, in some cases, only minutes. Our platform actualizes this apparent magic: applying data from past incidents of compromise and near real-time threat intelligence to effectively hunt for threats, identifying both the known and unknown.

But active hunting that merely detects threats, would help very little; Malwarebytes MDR helps a lot by remediating the hidden threats it uncovers—quashing them before they cause infection or continue to spread. By thus reducing dwell times, Malwarebytes MDR saves your organization potentially millions of dollars.

4 MITIGATE RISK OF REGULATORY COMPLIANCE VIOLATIONS

IndustryARC cites the need for compliance as one of the top three drivers of the MDR market.[8] And the likely driver of compliance is the substantial costs associated with non-compliance: reputational damage and financial penalties.

Malwarebytes MDR helps you comply with data protection regulations by performing many of the critical steps required for doing so. For example, Malwarebytes MDR analyzes and responds to security alerts in near real time and logs suspected threat events.

HERE TO BRING CYBER PROTECTION TO EVERY ONE

At Malwarebytes, we believe that you're only free to thrive when you're free from threats—so we're on a mission to rid the world of malware. To do that, we must be accessible, which is why we design our products to be as intuitive to use as they are tech effective—all the while ensuring they remain bandwidth friendly.

- **Home users**—from geeks to grandmas—love us.
- **Businesses**—large and small—trust us.
- **Public institutions**—schools, hospitals, and governments—rely on us.

Why? Because our products are easy to use, based on the latest and greatest technologies, and as highly effective as they are efficient.

Malwarebytes MDR is built on our industry-tested and -proven Malwarebytes EDR and backed by our team of dedicated, experienced cybersecurity experts. Armed with this one-two combo—threat prevention and remediation services managed by our highly-skilled team—Malwarebytes MDR delivers round-the-clock protection for your network environment.

[1] J. Greig, "Cybersecurity: Last year was a record year for attacks," 11 January 2022. [Online].
[2] C. Cimpanu, "Most Ransomware Attacks Take Place During the Night or Over the Weekend," 16 May 2020. [Online].
[3] "Cost of a Data Breach 2021," IBM Security and Ponemon Institute, 2021.
[4] https://www.malwarebytes.com/blog/news/2022/04/malwarebytes-evaluation-of-the-mitre-engenuity-attck-round-4-emulations/amp
[5] "A Resilient Cybersecurity Profession Charts the Path Forward," (ISC)2, 2021.
[6] "Cutting Through the Noise from Daily Alerts," 9 August 2021. [Online]..
[7] "Cost of a Data Breach 2021," IBM Security and Ponemon Institute, 2021.
[8] "Managed Detection and Response Market - Industry Analysis, Market Size, Share, Trends, Growth & Forecast," IndustryARC, 2021.