Malwarebytes

eBOOK

Threat hunting made easy

Keep your organization running and your employees productive

Table of contents

Introduction

Threat hunting has become a popular cybersecurity buzzword in recent years, but many don't know what it really means. In a nutshell, threat hunting is about being proactive, seeking out indicators of compromise (IOCs), malware, and other threats that may be hiding within your organization's network. Threat hunting arrived on scene as an important security practice with the increased prevalence of unidentifiable or highly-obfuscated threats—those that quietly lurk in the network, siphoning off confidential data and searching for credentials to access the "keys to the kingdom."

Manually intensive and costly threat-hunting tools have historically restricted this practice to larger organizations with an advanced cybersecurity model and a well-staffed security operations center (SOC). The good news: tools have advanced, making threat hunting easy for organizations of all sizes and security skill levels.

5-minute read

Grab a coffee, spend a few minutes reading this, and you'll be on your way to saving hours every month on threat investigation and response.

Learn how response-driven investigations can deliver recovery in minutes with a solution that automates and guides you through these essential steps:

- **Isolate:** quickly contain the suspicious activity
- **Investigate:** quickly determine if the threat is malicious or benign
- **Respond:** remediate in one click

Indeed, hunting for threats is no longer a luxury, it's a necessity. That's because even the strongest organizational defenses are not able to prevent all the attacks that businesses, schools, governments, and other organizations face every day. The increasing sophistication of attack methods and threat forms aimed at organizations have challenged security teams, especially since infection rates in organizations grew by 79 percent in 2018[1], and an additional 13 percent in 2019.[2]

To stay ahead of the curve, organizations must have:

- Server and workstation endpoint security that can be managed by a lean staff with any skill level
- Better investigation methods to shorten the mean time to respond (MTTR)
- Automation that increases the capacity of your security staff

1. Malwarebytes. 2019 State of Malware. 2019.
2. Malwarebytes. 2020 State of Malware. 2020.

By doing this, your security team can drown out the noise and focus on the needle—not the haystack. They'll be empowered to move from reactionary to champions, pivoting from performing "dark room" SOC investigation to response-driven investigation where active response is measured in minutes, not days. In fact, nearly 25 percent of companies report threat hunting provides a 21 to 30 percent improvement to their company's security posture.[3]

We're here to help you turn threat hunting into a reality. Invest five minutes to read this paper, and you'll learn the essential requirements for a threat hunting program that ensures your servers and workstations are always productive—making your security team revenue-enabling heroes that help the business grow.

3. Malwarebytes. Cybersecurity Resiliency Survey. 2019.

Ready for threat hunting season?

Great! But first, let’s address the elephant in the room.

Chances are, you've already thought about threat hunting and how it applies to your company's security operations. If you haven't suited up in your threat hunting gear yet, maybe you're thinking you need a PhD in analytics to conduct a manual investigation of IOCs and then hole up in a bunker to research root causes.

Does that sound doable anytime soon? Definitely not.

And, it's not the practical threat hunting companies need to prioritize, anyway.

Your threat hunting should focus on your organization's first line of defense: endpoints including servers. And, your threat hunting tool should provide guided threat response; one that tells you the next, best steps to take when there is suspicious activity—from isolation to investigation and response.

Empowered by guided threat response, you can accelerate your threat hunting efforts and make hunting achievable by team members of all skill levels.

Successful, essential threat hunting

Priority #1

Keep your organization productive and running 24x7.

How?

Endpoint threat hunting powered by guided threat response from your endpoint security solution.

Skill level required?

Doable by IT generalist or Level 1 analyst.

Guided threat response, automated for success

Ready to get started and achieve positive gains from threat hunting? The good news is that with the right endpoint security solution, you can easily implement a strong program. In fact, 90 percent of organizations use an infrastructure tool, such as endpoint detection and response, to perform hunting.[4]

4. Ibid.

Without question, your solution must have superpower sorting hat capabilities to conduct threat hunting. It should analyze volumes of data to:

1. Identify the clearly malicious threats, automate remediation, and restore your systems

2. Accurately cull the data set to uncover the *potentially malicious* threats that require threat hunting attention

Once your solution hunts down threats that are potentially malicious, it should make the next steps fast and easy with automated guided threat response, delivering actionable information and recommendations on what to do next.

The goal here is to make threat hunting powerful and accessible, without requiring advanced security training, programming skills, or long stretches of time wasted on manual search and analysis.

To tighten up reaction time to suspicious activity on servers and workstations, your response should cover the following three steps:

1 Isolate

2 Investigate

3 Respond

1

Isolate

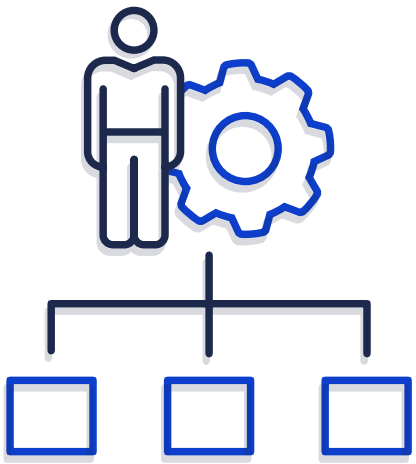
Contain the suspicious activity

Whether an attack does a fast “smash and grab” or moves slow and low while it searches your network for valuable data, successful breaches can do a lot of damage.

Your threat hunting mission: isolate the threat; stop the damage.

Containing an attack while you are investigating suspicious threats creates an air gap between the compromised endpoint and the other systems within your organization. This gives you breathing room to plan out and prioritize your response efforts.

Isolate



Solution requirements

Automation here is essential for an easy and powerful threat hunting program. For this reason, 47 percent of security managers have automated infected endpoint isolation.[3]

Your solution should reduce east-west propagation through software-driven capabilities and enable you to granularly isolate a potential threat—without physically disconnecting machines or ports. It should also help you contain a threat through network, device, and process isolation. These containment mechanisms restrict the malware from taking further actions, such as phoning home to receive command-and-control communication or moving laterally to infect other systems in your network.

3. Malwarebytes. Cybersecurity Resiliency Survey. 2019.

Isolate

Malwarebytes sets you up for “Threat isolation success”

Malwarebytes quickly locks down the affected endpoints including servers, preventing lateral movement, so you can conduct your investigation confidently knowing the suspicious threat can’t do further damage.

We arm you for threat hunting success by automating your endpoint isolation with the following capabilities:

- Network isolation that restricts which endpoint-initiated processes can communicate
- Device isolation that stops further interaction to limit damage
- Process isolation that controls which endpoint processes are permitted to continue functioning

Investigate

Quickly make a decision

With your suspicious activity safely isolated, it's time to get on with the hunt. Priority one: your solution should automate your investigation, so you can quickly triage and decide if the activity is malicious or benign.

Historically, this stage has been fraught with challenges. Security professionals have a hard time getting the right data and visibility to identify and map a threat's attack sequence. For instance, 59 percent of security professionals say they need better investigation functions to manage threat hunting. And, the same group point to endpoint data (including event logs) as the best source of hunting telemetry to identify malicious behavior.[5]

Your endpoint security solution must address these challenges head on, so they become nothing more than a distant memory.

5. SANS 2018 Threat Hunting Survey

2

Investigate

Solution requirements

The solution should guide your investigations to quickly narrow in on the prioritized IoCs and trace the attack chain. This visibility is so essential for your guided hunting investigations that you should conduct a detailed walkthrough during your solution evaluation.

To succeed with investigation, your solution should provide:

Broad visibility

Your solution should let you see across your servers and workstations to identify which and how many systems are affected.

Attack chain drill down

Your solution must support your efforts in investigating an attack's execution chain. What processes were initiated, what applications were launched, and which other systems were infected through lateral movement?

Guided response options

Threat hunting shouldn't require a PhD in security analysis. Your solution must support security staff of all levels by guiding them with the suggested response options along with the recommended best, next steps.

Malwarebytes:
Your investigation wingman

Malwarebytes simplifies your security management and threat hunting with the visibility and guidance you need—at every step. Our solution provides the threat intelligence and research details needed to help you make the right decisions and makes it easy to know what to do next. When you're ready to investigate suspicious activity, our solution supports you at every step with the following capabilities:

- Threat analysis from broad data sources and threat intelligence telemetry that provides the latest information to analyze IOCs and offer guidance on response.
- Cloud-based console provides a single pane of glass and guided, automated threat hunting with prioritized IOCs across your organization, enabling security team members to quickly focus on server and workstation endpoints that need further investigation.
- Process graph gives a visual representation to trace the malware's execution chain, mapping the chain with nodes and connecting edges that show each of the applications or processes the original malware spawned. You can click on each node to obtain details on the processes and execution parameters.

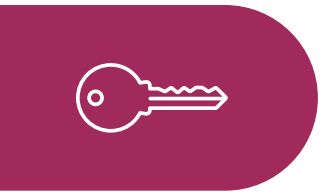
3

Respond

...Like a security superstar

A quick refresher: your endpoint security solution should automatically remediate the attacks it has identified as clearly malicious.

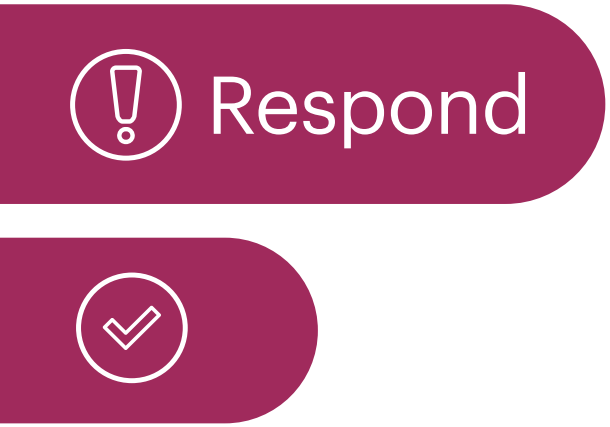
For the suspicious threats you've investigated, your solution should empower you to actively respond in an orchestrated manner to remediate servers and workstations at scale. With automated remediation, your organization will be well on the way to a record-breaking fast Mean Time to Recover (MTTR).



Solution requirements

Your investigation results fall into two buckets: confirmed threat and benign activity. For your confirmed threats, your solution must automate remediation. It must also provide complete and thorough malware removal with a single click. Your server and workstation remediation capabilities should include detection and removal of dynamic and related artifacts to ensure malware persistence mechanisms are permanently removed.

If you determine the activity is benign, your product should allow you to update the exclusions list. This ensures similar activity will not be flagged in the future. It should go without saying, but we'll say it anyway: The exclusions list should work. Don't settle for a product that can take the exclusion but cannot *perform* the exclusion when called on to do so.



Your response efforts are “in the bag” with Malwarebytes

Forget the days of server and workstation endpoint re-imaging and time-consuming manual remediation. Malwarebytes helps you achieve a new response paradigm with active response capabilities. You can immediately respond—across all endpoints—with a solution that combines power and simplicity when remediation is required. Our single, unified agent eliminates the complexity and provides both your server and workstation endpoints with complete and thorough remediation.

Respond

Malwarebytes supports your threat hunting response with the following capabilities:

Response for malicious threats

- Initiate remediation on all endpoints, including servers, with one click. From there, remediation is fully automated, the threat is fully removed, and files are restored to their previous healthy state.
- Sequencing identifies and thoroughly removes threat artifacts associated with the primary payload.
- Ransomware rollback remove the remaining threats and restore files that the threat removed, modified, or encrypted.

Response for benign threats

- Once the process is added to your global exclusions list, Malwarebytes will not flag future behavior from this process as suspicious activity.

Conclusion

For companies big and small, threat hunting is an essential security practice. If you haven't yet, it's time to jump into the game. Your efforts will prove fruitful. In fact, 27 percent of security professionals report finding one to three threats from their hunting efforts, and another 21 percent find four to 10 threats over a twelve-month period.[5]

But beware: you need the right endpoint security tool to maximize your threat hunting efforts and minimize your resource requirements.

Your solution should help you focus on your organization's security front line: all endpoints including servers. If your endpoints fall prey to an unidentified threat, it could halt your business operations. Threat hunting focused on your endpoints will keep your employees' fingers buzzing on their keyboards and keep your business productive.

5. Ibid

The right technology will be your best threat hunting ally. It should automate key functions and guide you through your investigation and response efforts. This ensures your organization can adopt a powerful and accelerated threat hunting program that doesn't require a cot, food rations, or advanced security training.

As you embark on your solution evaluations, take a close look at the products' capabilities that support your ability to quickly isolate, investigate, and actively respond to persistent attacks, rather than waiting for the payload to activate. Your solution should be intelligence-driven to allow you to quickly isolate and investigate IOCs and suspicious threats. In addition, for the activity you deem malicious, the solution should guide you through the response process, as well as automate endpoint remediation functions.

Selecting a vendor with strengths across these areas should provide your organization with the best fit now and years to come.

Evaluation checklist

Threat containment

- ☐ Provides automated containment functions that quarantine the threat during hunting investigations
- ☐ Network isolation that restricts which endpoint-initiated processes can communicate
- ☐ Server and workstation isolation that stops further interaction to limit damage
- ☐ Process isolation that controls which endpoint processes are permitted to continue functioning

Suspicious threat investigation

- ☐ Provides broad visibility to see across your endpoint systems to identify which and how many servers and workstations were affected
- ☐ Supports your efforts in investigating an attack's execution chain to see which processes were initiated, applications launched, and if other systems were infected
- ☐ Provides built-in threat intelligence that guides response with suggested options and recommended next steps

Suspicious threat response

- ☐ Provides automated and complete malware removal, with a single click
- ☐ Applies associated sequencing to ensure malware persistence mechanisms are permanently removed
- ☐ Allows you to update the exclusions list to ensure this type of activity is not flagged in the future

Threat hunting season is open

For more information about how Malwarebytes makes threat hunting easy, visit:

www.malwarebytes.com/business/solutions/enterprise/