Malwarebytes

ENTERPRISE ENDPOINT PROTECTION **BUYER'S GUIDE**

TABLE OF CONTENTS

OVERVIEW

The threat landscape continues to innovate with increased volume and tenacity. In 2016, 53% of cybersecurity professionals reported an increase in attacks, and in 2017, 80% believe it is likely or very likely they will be attacked. We've seen successful attacks steal customer data and shut down business operations, in all industries in every region across the globe.

Whether it's a phishing email, malware, or advanced persistent threat (APT), the attacker's primary target is the endpoint. As a result, organizations have made great efforts to protect the corporate endpoints. As new threat techniques emerge, protection measures are challenged to keep up. Global ransomware attacks, such as WannaCry and Jaff, are good examples of this. In 2016, 62% of enterprises experienced a ransomware attack; and the world saw the WannaCry ransomware successfully lock up more than 200,000 computers across the globe. Only 53% of organizations have a formal process in place to deal with them.

Cybercriminals have moved to a multi-vector attack approach. For example, they combine elements like social engineering and phishing emails with malicious file attachments that exploit vulnerabilities on the endpoint system. Whether you decide to augment or replace your existing endpoint protection measures, your endpoint security needs to evolve to address this level of sophistication, as well as future tactics.

This guide details the core requirements to help you navigate your enterprise endpoint protection solution analysis, and it provides a solution questionnaire to help you with your evaluation process.

A MULTI-LAYER APPROACH TO ENDPOINT SECURITY

One successful malware infection provides the foothold cybercriminals need to steal your organization's sensitive data. Protecting the corporate endpoint is not achieved by a single "silver bullet" or next-generation technology. Anti-malware techniques each have their own capabilities that add value in detecting an infection attempt. But one technique, alone, does not deliver effective results.

Attackers use multiple vectors to deliver a successful attack; securing the endpoint requires multi-vector protection. Your endpoint security solution must have multiple layers of protection with a mix of static and dynamic approaches. Each layer has its positive attributes and shortcomings, which is why no individual layer is 100% effective on its own. Your endpoint solution must have a mix of layers that work together as a collaborative system. This approach delivers the most effective protection, and often detects and stops zero-day attacks.

Known Attack Detection

A solution's "known attack detection" layer blocks malware quickly and with low overhead. This is done with matching (i.e., signatures) and rules-based technologies. Despite some claims that signatures are outdated and ineffective, they have their place in a multi-layer process.

Signature-based detection is a lightweight method to protect against common attacks with minimal resource processing and administration requirements. Signatures are good at stopping the bulk of the less sophisticated attacks, and they do so with minimal processing and end user impact. While signatures provide low threat coverage, especially against zero-day attacks, they do have some advantages as part of a multi-layer protection solution:

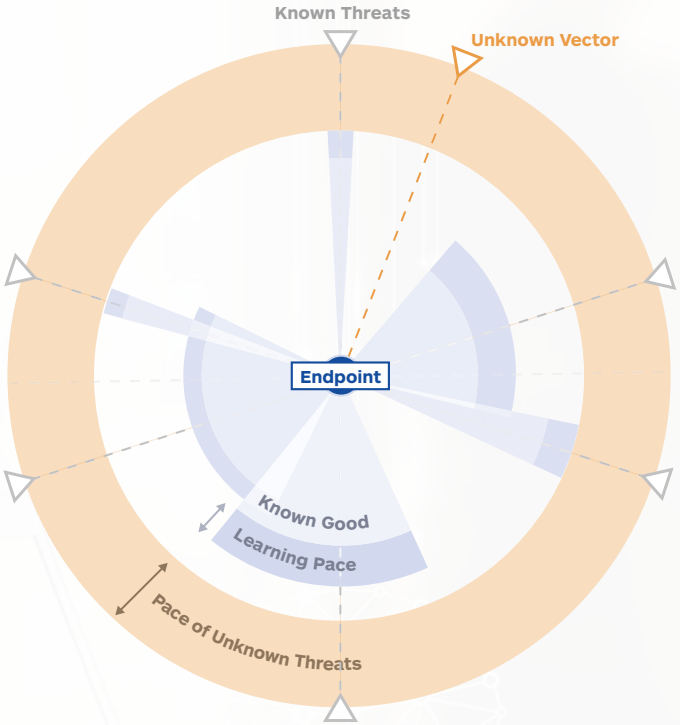
- Strong protection against known malware
- High accuracy – low false positive rates

Machine Learning

One anti-malware protection layer that has gained in popularity is machine learning. Machine learning is driving innovation across a wide range of industries, and it offers the cybersecurity industry a new way of dealing with the unknown. Machine learning in endpoint protection attempts to teach machines to recognize malware and distinguish it from legitimate software. In the anti-malware world, the intent is to apply detection technology that is more dynamic in nature than signature-based approaches.

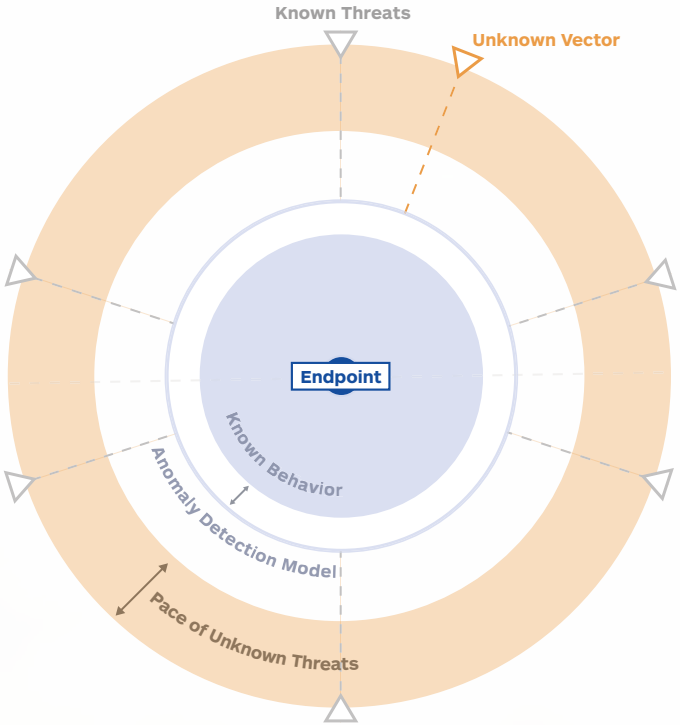
The accuracy and effectiveness of this layer varies depending on the vendor's training dataset and classification model. It's important to do some digging to understand the vendor's approach rather than simply ticking the machine learning feature box.

CLASSIC MACHINE LEARNING



Be cautious of a malware classification model that is trained on a dataset representative of, in all or in some part, malware. It produces a model prone to false positives and false negatives, as well as requires constant retraining on new files. The result is a machine learning model that is little more than a signature in disguise. Just like signature-based detection—it only knows what it knows.

ANOMALY DETECTION MODEL



Look for a machine learning approach that is an anomaly detection model built strictly on a dataset of good files. The anomaly detection model scores each file on how similar it is to the dataset of known good files. Highly dissimilar or anomalous files are considered suspicious and more likely to be malware. This provides a highly accurate and durable system that identifies zero-day viruses and newly emerging malware.

Behavioral Analysis

Behavioral analysis monitors applications and processes for indicators of ransomware and other intrusions to provide runtime protection against attack activity. This protection layer provides point-in-time detection, as well as monitors for suspicious processes over a period to build a greater contextual understanding of the behavior.

Applied to applications, behavior analysis prevents applications from being leveraged to infect the endpoint by ensuring they don't drop and execute malicious payloads. Application behavior analysis also protects against macro exploits that execute shell commands in MS Office and guards against non-secure Java operations that issue system commands.

Endpoint protection solutions using behavior analysis can also apply the capability to detect and block ransomware. This is done by deconstructing the phases of a ransomware attack and monitoring for behavior related to specific actions:

1. Back up points
2. Network file shares
3. Enumerating files
4. Encryption of those identified files

A risk score is applied to each and, with multiple detections, the score triggers a threshold and detects a ransomware risk.

Exploit Mitigation

As software vulnerabilities are discovered, most vendors focus on detection on a per attack or per vulnerability basis. It is easier to create signatures for something that is known and that can be studied in a lab. Unfortunately, this approach is reactive in nature.

A strong exploit mitigation layer makes it difficult for attackers to exploit software vulnerabilities. It proactively detects and blocks attempts to abuse vulnerabilities and remotely execute code on the endpoint. Exploit mitigation usually focuses on a small number of techniques that all exploit-based attacks use, which requires minimal resource processing. This provides the added benefit of low impact to the user as well as minimal management requirements.

For proactive protection against zero-day exploits, look for the following anti-exploit capabilities:

- Applies different techniques that harden applications to prevent malicious exploits from compromising endpoints through software vulnerabilities. Once an application is shielded, it cannot be exploited through any of its present or future zero-day vulnerabilities.
- Applies memory protection techniques that detect attempts to bypass built-in operating system protections.

Thorough Remediation

It's well understood that preventative measures are critical to your organization's security posture. However, no endpoint security solution will provide 100% detection effectiveness 100% of the time. Therefore, your best practice endpoint protection approach should include response capabilities. A solution that includes thorough and automated remediation will restore your endpoint to its pre-malware, trusted state.

Look for the following remediation capabilities:

ADVANCED REMEDIATION

Most solutions only remediate active malware components, which falls short of providing complete remediation. Your solution's remediation capabilities should also detect and remove dynamic and related artifacts. It should apply associated sequencing to ensure malware persistence mechanisms are removed in such a way that disinfection is permanent. Advanced remediation methodologies provide your organization with expedient malware identification and thorough removal.

PROACTIVE HUNTING

It's likely threats already exist in your environment. When an endpoint is successfully infected, attackers often initiate lateral movement to infect other endpoints. Your endpoint security solution should enable your incident responders to run scheduled scans that proactively hunt for recently reported indicators of compromise (IOCs). This capability makes it easy to adopt an assume-the-compromise process that greatly improves your security posture.

THREAT INTELLIGENCE

Threat intelligence has played a key roll in the evolution of cybersecurity. The quality of threat intelligence in todays mutli-vector attacks has never been more important. Cyber threat intelligence is the backbone to effective endpoint security protection.

To protect the endpoint, your security vendor needs to know what's succeeding for attackers. The single most critical factor of endpoint security threat intelligence is strong telemetry on landed malware—the malware that is getting past existing endpoint protection and resides on the machine.

Select a vendor with a strong threat feed based on endpoint remediation intelligence. Expertise in endpoint incident response provides a solid understanding of the "bad stuff"—the attacks that successfully execute on corporate devices. This footprint generates an informed threat intelligence telemetry of data on zero-day malware.

MANAGEABILITY & ENDUSER IMPACT

Your ideal endpoint protection solution must provide a strong blend of detection and response layers that run transparently and with low enduser impact. This means your vendor should have conducted rigorous testing on each layer to strike a balance between optimal effectiveness and minimal resource processing and false positive rates.

At the end of the day, you are protecting production systems that get a lot of daily use, so it's important that your endpoint solution doesn't interrupt business operations. Avoid a solution with techniques, such as application isolation, that provide minimal threat coverage and have significant impact on your enduser's resource requirements.

Your solution should also offer compelling manageability and low administrative overhead. Look for management capabilities that enable you to streamline the exception management process and to make the right decisions in the least amount of time. Likewise, ensure the solution provides flexible management, either on its own or as part of your existing endpoint systems management (ESM) solution.

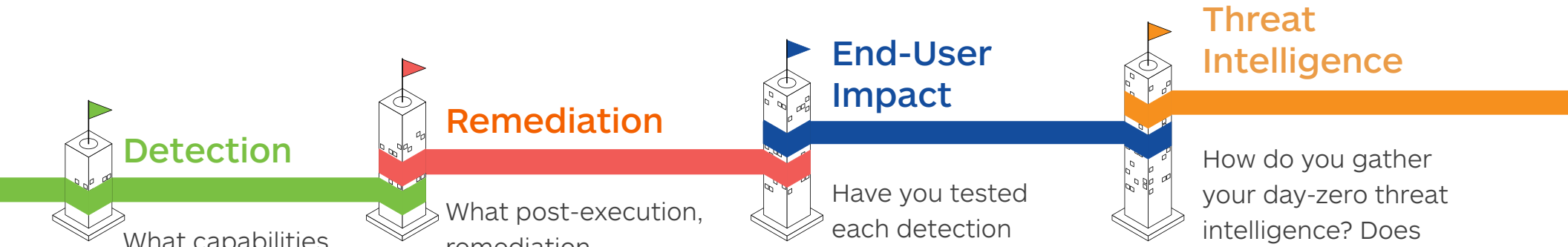
CONCLUSION

There's one thing organizations can count on: cybercriminals will continue to innovate and evolve their attack techniques. Your endpoint security solution needs to provide a strong combination of detection technologies that can keep pace with today's multi-vector attack techniques, as well as expected future advances. For the strongest endpoint security posture, you need to assume no solution will deliver 100% blocking detection all the time. Therefore, your solution of choice should offer advanced techniques that detect when a payload executes on the endpoint and deliver thorough remediation.

According to the U.S. government, more than 4,000 ransomware attacks happen across all industries daily. It's a safe bet the volume of all attack techniques will continue to soar in the coming months and years. The pressure is on to protect the endpoint. Organizations with limited IT staff resources should consider augmenting existing endpoint protection measures if a complete replacement effort is not feasible in the near-term.

EVALUATION QUESTIONS

These are evaluation questions to use in your vendor selection process. Selecting an endpoint security vendor with strong capabilities in these key areas will provide your organization with effective protection and remediation with minimal end user impact, for now and years to come.



Detection

What capabilities does the product use to detect attacks, including common and day-zero attacks?

Do your detection capabilities work together to share real-time intelligence on what they've detected?

What is the product's overall detection effectiveness?

Remediation

What post-execution, remediation capabilities does the product provide? Is remediation manual or automated?

Does remediation remove dynamic and related artifacts in addition to the active malware components?

Can I run scheduled scans that proactively hunt for recently reported indicators of compromise (IOCs)?

End-User Impact

Have you tested each detection technique for enduser impact and resource requirements? Can you share your findings?

What overall performance and usability impact will the product have on endusers?

Threat Intelligence

How do you gather your day-zero threat intelligence? Does it include telemetry on new, day-zero attacks?

Does your threat intelligence incorporate collaboration with third-party feeds?

Malwarebytes

WHY MALWAREBYTES?

Malwarebytes makes it easy for your security and risk management leaders to achieve effective endpoint protection. Our solution combines a blend of distinct and complementary technologies to deliver leading endpoint security with simplified management and minimal enduser impact. This creates an interlocking web of rules-based and behavior/AI-based technologies that work together to not only block malware execution but also its deployment on the endpoint.

At Malwarebytes, we have a strong history as the go-to vendor for endpoint malware remediation. Our expertise in endpoint incident response provides thorough remediation and generates the world's most informed threat intelligence telemetry of data on zero-day malware.

TAKE YOUR FIRST STEP IN PROACTIVE PREVENTION AGAINST RANSOMWARE.

For more information about
Malwarebytes Endpoint Protection visit:
malwarebytes.com/business/endpointprotection