Malwarebytes

SOLUTION BRIEF

The Value of **Multi-Vector Protection** on the Endpoint

The Need for a New Endpoint Security Approach

One successful malware infection provides the foothold cybercriminals need to steal an organization's sensitive data. As a result, organizations have made great efforts to protect the endpoint. As new threat techniques emerge, protection measures are challenged to keep up.

Ransomware attacks are good example of this. WannaCry successfully locked up more than 200,000 endpoints across the globe. Petya quickly followed, which impacted more than 300,000 endpoints across critical infrastructure entities, including energy, financial services, and transportation.

The question on everyone's mind: how are attacks getting past endpoint protection measures? Cybercriminals have moved to a multi-vector attack approach. It combines a mixture of social, malware, and hacking, which represent the triple threat in a cybercriminal's multi-vector attack technique. And it's working. According to Verizon, 51% of data breaches include malware, 62% include hacking, and 43% are social attacks.[i]

The proof is in the numbers: multi-vector attacks create a powerful arsenal to bypass signature-based endpoint detection measures. If organizations maintain their legacy endpoint protection, it's safe to assume cybercriminals will continue to exploit this technique. Protecting against multi-vector attacks requires multi-layered endpoint protection.

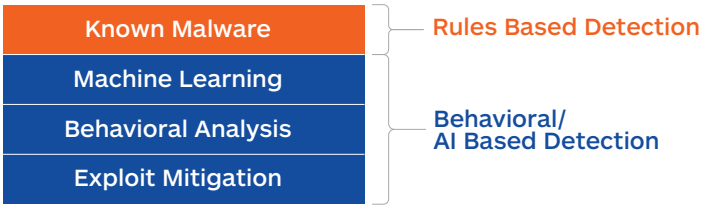
What is Multi-Vector Endpoint Protection?

Multi-vector endpoint protection provides the best practice approach to securing the corporate endpoints from unknown malware. That's why Gartner recommends organizations design "an endpoint protection strategy that consists of good security hygiene and layered protection and detection technologies."[ii]

What is multi-vector endpoint protection? It's an enterprise endpoint security platform that integrates multiple layers of protection with a combination of rules-based techniques (e.g., signatures and heuristics) and behavioral/artificial intelligence-based approaches, such as behavioral analysis.

Nonsignature-based methods that apply techniques like behavioral and anomaly detection are proactive in their prevention capabilities and provide higher threat coverage to protect against the majority of cyberattacks before they execute and cause damage. For example, 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.

For the best multi-vector protection coverage, your endpoint security should include the following layers:



The Business Impact of Your Adoption Approach

Whether you choose to augment or replace your organization's legacy antivirus solution, it's critical to increase your detection efficacy against multi-vector attacks. Some vendors will say that you can close the gap with a single "silver bullet" layer, such as AI or machine learning. But as noted by Gartner, each layer has its positive attributes and shortcomings. No individual layer is 100% effective on its own.

After conducting a gap analysis to determine which layers are missing from your existing endpoint security arsenal, the next focus should be on the best way to acquire them: piece-meal from separate vendors or integrated from a single vendor.

Protection Layers from Individual Vendors

When you acquire endpoint protection layers separately from multiple vendors, the approach creates many short and long term monetary and resource burdens for the organization.

Multi-Layered Protection from a Single Vendor

When you adopt your multiple endpoint protection layers from one vendor in a single solution you gain economies of scale by eliminating the monetary and operational burdens from the separate solutions approach. And your organization also optimizes the efficacy and performance of each detection technique.

It is for this reason that multi-vector protection in a single solution, a mix of layers that work together as a collaborative system, delivers the most efficient and effective endpoint protection against emerging and zero-day attacks.

Differences Between Multi-Vendor and Single Vendor Solutions

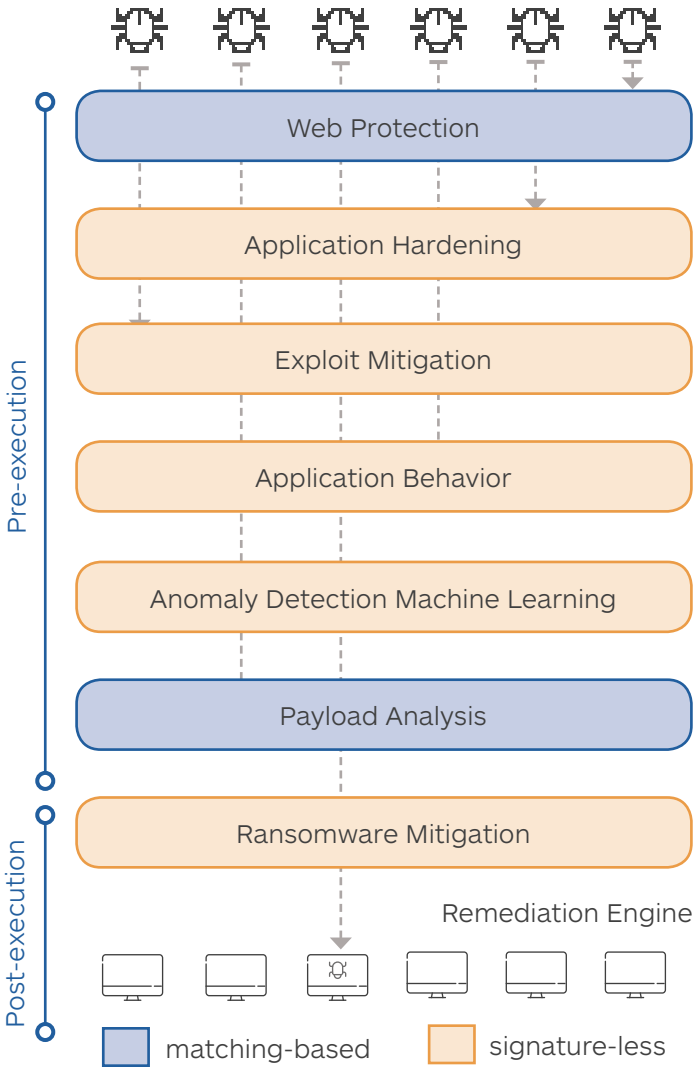
It becomes apparent that multi-layered protection from a single vendor is easier to manage, simpler to on-board, and can be more economical.

Multi-Vendor Solutions	VS.	Single Solution
Purchasing individual licenses for protection layers increases your total acquisition costs and eliminates opportunities for pricing economies of scale.	**ACQUISITION**	A single solution provides opportunities for pricing economies of scale.
Your security team will need to install and maintain each endpoint protection layer separately, as well as gain proficiency in each solution. Likewise, the team will need to create and maintain separate policy rulesets, which can inadvertently introduce policy exceptions and missing coverage for some endpoints.	**MAINTENANCE**	Your security team only needs to install and maintain one endpoint protection system that includes all the best practice protection layers.
Multiple Solutions installed on the endpoint may result in conflicts or impact system performance negatively.	**PERFORMANCE**	When your multiple detection techniques conduct analysis from a single system you maximize performance efficiency.
Management of multiple products not only includes the overhead of working with multiple vendors, it also includes contract negotiations, legal review cycles, and product training.	**MANAGEMENT**	Management is streamlined with one vendor relationship, a single contract and legal review, and one product to learn.
When a breakdown occurs, security teams need to investigate the different systems to uncover where it occurred. This often requires opening a support ticket with multiple vendors, and often, this can lead to a lack of clear ownership of an issue from a single vendor. Post event incident response activity would also require touchpoints to update and harden multiple products.	**ERROR INVESTIGATION**	A single endpoint system greatly simplifies your error investigation with one system to review and vendor support team that fully owns resolution of the issue.
Piece-meal threat detection from separate products eliminates the opportunity for your security to work together. Meaning, your individual layers don't gain information or intelligence from information another layer has learned.	**SILOED THREAT INTELLIGENCE**	Protection layers collaborate and share key findings in real time to provide a coordinated defense against zero-day threats

Malwarebytes: A Single Solution for Multi-Vector Protection

Malwarebytes makes it easy for your security and risk management leaders to achieve effective endpoint protection that optimizes your IT resources and cost efficiency. Our solution combines all the best practice detection layers to deliver leading endpoint security with simplified management and minimal end-user impact. This creates an interlocking web of rules- and behavior/AI-based techniques that work together to not only block malware execution but its deployment on the endpoint.

We have a strong history as the go-to vendor for endpoint malware remediation. This intelligence means we understand the "bad stuff"—the attacks that successfully execute on corporate devices. This provides customers with unmatched threat visibility of the latest threats. Powered by our big data analytics systems and expert research analysis, we process more than 3 million endpoint remediations each day.



Our platform applies the following real-time protection layers:

Protection Layers

Web Protection

1. Web protection protects users by preventing access to malicious websites, ad networks, scammer networks, and "bad neighborhoods."

Application Hardening

2. Application hardening reduces the vulnerability surface, making the computer more resilient, and proactively detects fingerprinting attempts by advanced attacks.

Exploit Mitigation

3. Exploit mitigations proactively detect and block attempts to abuse vulnerabilities and remotely execute code on the machine, which is one of the main infection vectors nowadays.

Application Behavior

4. Application behavior ensures that installed applications behave correctly and prevents them from being abused to infect the machine.

Anamoly Detection Machine Learning

5. Anomaly detection machine learning proactively identifies viruses and malware based on anomalies from known and good files.

Payload Analysis

6. Payload analysis is composed of heuristic and behavioral rules to identify entire families of known and relevant malware.

Ransomware Migitation

7. Ransomware mitigation is a behavior monitoring technology that detects and blocks ransomware from encrypting users' files.

Incident Response Layer

Thorough Remediation

8. In addition to real-time protection layers, our solution delivers automated, accurate, and thorough remediation. This provides your organization with critical coverage for the entire attack lifecycle – from initial infection attempts through an actual infection.

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 multi-vector attacks and future advances in the threat landscape.

Securing your endpoints with multi-layered techniques should not place undue efficiency or resource burdens on your operations or end users. For the strongest and most efficient endpoint security approach, pursue multi-vector protection from a single vendor. This provides a best practice approach that delivers the greatest efficiency advantage for your security team and strongest efficacy for your corporate endpoints.

LEARN MORE

To learn more about Malwarebytes Endpoint Protection visit: malwarebytes.com/business/

> "I CAN EASILY SAY THAT OF ALL OF OUR BUDGETED SECURITY PROJECTS FOR LAST YEAR, MALWAREBYTES HAD THE MOST IMPACT. IT HAS BEEN HUGELY BENEFICIAL TO OUR SECURITY STRATEGY. YOU GAVE MY TEAM MORE TIME AND MALWAREBYTES ALLOWS US TO FOCUS ON MORE STRATEGIC PROJECTS."
>
> KEVIN MEROLLA
> GLOBAL IT SECURITY ENGINEER, CHART INDUSTRIES

[i] Verizon. "2017 Data Breach Investigations Report."
[ii] Make Sense of Endpoint Malware Protection Technology, April 2017. Gartner, Ian McShane.

malwarebytes.com | corporate-sales@malwarebytes.com | 1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.