Malwarebytes

TECH BRIEF

Best-Informed Telemetry: **Unmatched Threat Visibility**

The Gold Standard in Remediation Makes all the Difference

Through the evolution of cyber security, threat intelligence has played a key role. Attackers are focused and innovate at a fast pace. They collaborate and have established darknet marketplaces where cybercriminals can buy and sell exploit kits, malware, access to botnets, and even mentoring advice.

As a result, cyberthreat intelligence is the backbone to effective security protection. Threat intelligence makes it possible for your corporate security controls to detect and act upon indicators of attack and compromise as they occur. This is especially important at your corporate desktops because they are the main entry point into your internal network. One successful endpoint malware infection provides the foothold cybercriminals need to steal your organization's sensitive data. According to the Verizon 2017 Data Breach Investigations Report, 51% of corporate breaches included malware.

Remediation-Based Intelligence

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

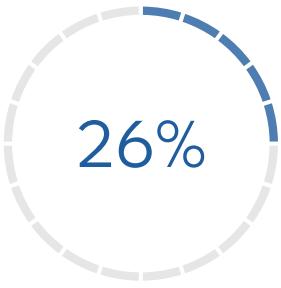
At Malwarebytes, we have a strong history as the go-to vendor for endpoint malware remediation. Our expertise in endpoint incident response means we understand the "bad stuff"—the attacks that successfully execute on corporate devices. This footprint generates the world's most informed threat intelligence telemetry of data on zero-day malware.

Powered by Malwarebytes big data analytics systems and expert research analysis, Malwarebytes endpoint disinfection has more than 500,000 daily downloads and processes more than three million endpoint remediations every day. The volume and breadth of endpoint remediations provide the highest quality, global data corpus for the threat intelligence behind Malwarebytes Endpoint Protection.

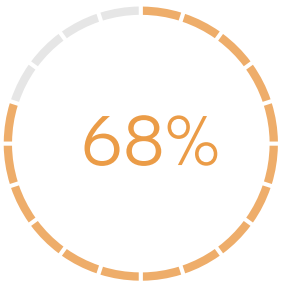
The Power of Remediation Telemetry

Let's look at the power of understanding landed malware. Malwarebytes remediation expertise provides deep insight into how current endpoint protection technologies fail to keep organizations safe. When Malwarebytes processes disinfections, we see which vendor's security controls the malware bypassed and details on the malware behavior and payload.

Looking at six vendors with the **largest endpoint protection market share**, on average:



of all infection attempts are successful *(i.e., infection rate)*



of successful infections are Trojan threats

For an organization with **1,000 endpoints**:

- **20 machines** are infected with Backdoor threats
- **10 machines** are infected with Rootkit threats
- **10 machines** are infected with Spyware threats

Malwarebytes is the "first responder" to clean up malware variants. This provides critical day-zero telemetry intelligence on how the attacker modified the malware's technique and payload to circumvent detection.

Mulit-Vector Endpoint Protection

Malwarebytes interpretation and analysis of the industry's most informed telemetry on landed malware drives our multi-vector protection engine. Attackers use multiple vectors to bypass antivirus products; securing the endpoint requires multi-vector protection that includes both static and dynamic protection layers.

We break the attack chain by combining a blend of advanced malware detection and remediation technologies in a single platform, which provides the ability to stop an attacker at every step.

Our system goes a step further to break down siloed security technologies with a shared intelligence security framework. The multi-protection layers collaborate and share key findings in real time to provide a coordinated defense against zero-day threats.

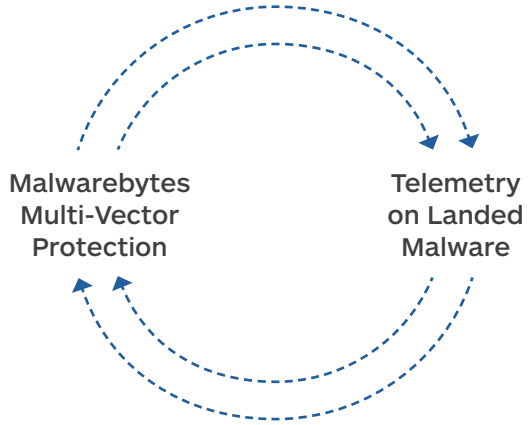
The Malwarebytes platform applies the following real-time protection layers:

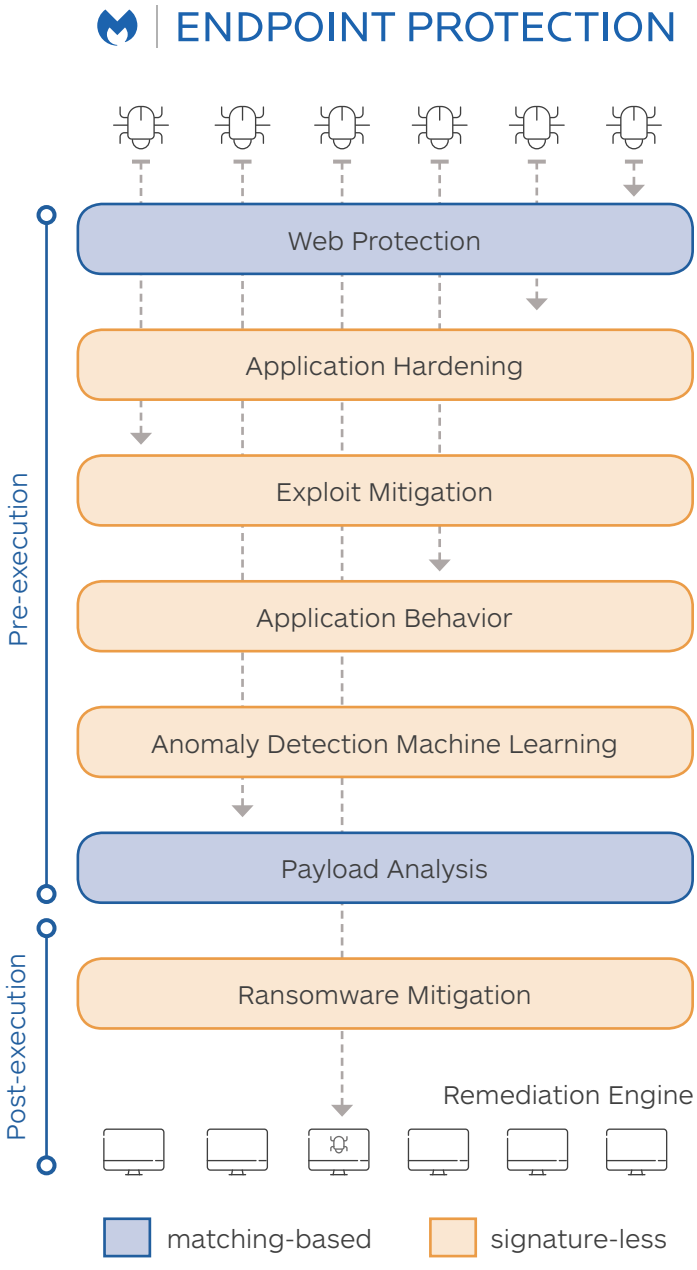
Web Protection
Prevents access to malicious websites, ad networks, scammer networks, and bad neighborhoods

Application Hardening
Reduces vulnerability exploit surface and proactively detects fingerprinting attempts used by advanced attacks

Exploit Mitigation
Proactively detects and blocks attempts to abuse vulnerabilities and remotely execute code on the endpoint

Application Behavior
Prevents applications from being leveraged to infect the endpoint





Anomaly Detection Machine Learning
Proactively identifies viruses and malware through machine learning techniques

Payload Analysis
Identifies entire families of known and relevant malware with heuristic and behavioral rules

Ransomware Mitigation
Detects and blocks ransomware via behavioral monitoring technology

> DURING WANNACRY, MALWAREBYTES BOUGHT US TIME TO STEP BACK AND MANAGE OUR PATCH PLANS AS A PROJECT. IT JUST WORKS.
>
> IT Manager
> *Large Manufacturing Company, Malwarebytes Customer*

Multi-Vector Protection in Action: WannaCry

To provide context on how multi-vector protection combined with remediation-based telemetry delivers reliable protection against zero-day attacks, let's look at how it responded to WannaCry. The WannaCry attack was a worldwide ransomware cyberattack that had a significant impact on consumers and businesses across the globe.

At the zero-hour of the attack, the Ransomware Mitigation layer identified WannaCry based on its malicious behavior and immediately halted the execution of the malware, preventing any files from becoming encrypted. As a signature-less technology, the Ransomware Mitigation layer proactively protected the endpoints without relying on prior knowledge of WannaCry.

Immediately following the initial detection by the Ransomware Mitigation layer, our telemetry informed the Payload Analysis layer, that then begins detecting the attack earlier in the infection chain.

From Scrambling to Managing

Malwarebytes empowers your organization to mature your response to security risks. With Malwarebytes providing endpoint protection, organizations can manage endpoint exploits and network vulnerabilities as a project rather than a crisis response.

When your organization adopts multi-vector endpoint protection from Malwarebytes you gain significant benefits:

Malwarebytes Endpoint Protection

- Stops zero-day malware and ransomware
- Simplifies endpoint security management and identifies vulnerable endpoints
- Deploys protection for every endpoint and scales as your company grows

Malwarebytes Breach Remediation

- Delivers automated, accurate, and thorough remediation
- Reduces malware dwell time
- Closes gap in personnel and skills shortage
- Eliminates cost and complexity of managing incident response

LEARN MORE

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

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.