

Malwarebytes Endpoint Protection

Advanced threat prevention

TECHNICAL FEATURES

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 Protection

Prevents applications from being leveraged to infect the endpoint

Anomaly Detection

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

The most effective protection strategy starts with proactive prevention, but the best prevention approach won't be found with a silver bullet. In fact, security experts advise against relying solely on a single technology or technique to protect business endpoints. Effective prevention requires a layered approach capable of addressing not only today's threats, but preventing tomorrow's as well.

Malwarebytes Endpoint Protection is an advanced threat prevention solution for endpoints that uses a layered approach with multiple detection techniques. This provides businesses with full attack chain protection against both known and unknown malware, ransomware, and zero-hour threats. Unified onto a single agent, Malwarebytes Endpoint Protection reduces the complexity and costs often associated with deploying multiple individual solutions.

The industry's best-informed telemetry drives the efficacy of Malwarebytes Endpoint Protection detection techniques. Malwarebytes is the gold standard for providing complete and thorough remediation of threats when existing security solutions fail, evidenced by 500,000 consumers and businesses downloading Malwarebytes technology daily. Malwarebytes finds and remediates 3 million infections every day. This unique telemetry provides insight into the threats and techniques that are succeeding in the wild and offers a better understanding of what makes these attacks effective and how to best counter them.

Threat	Category	Status	Type	Location	Endpoint	Detection Time
PUP.Optional.Dadfish	PUP	Quarantined	File	06/05/2017 - 10:51:17 AM
Trojan.Killbox	Malware	Quarantined	File	06/05/2017 - 10:51:13 AM
PUP.Optional.Amazon1Bus...	PUP	Quarantined	File	06/05/2017 - 10:18:16 AM
Spyware.Zeus	Malware	Quarantined	File	06/05/2017 - 07:41:40 AM
PUP.Optional.Amazon1Bus...	PUP	Quarantined	File	06/05/2017 - 07:41:34 AM
Malware.Exploit.Agent.Gen...	Exploit	Blocked	Exploit	-	...	06/02/2017 - 03:10:57 PM
Malware.Exploit.Agent.Gen...	Exploit	Blocked	Exploit	-	...	06/02/2017 - 03:08:08 PM
Trojan.Killbox	Malware	Quarantined	File	06/02/2017 - 02:32:46 PM
PUP.Optional.AdvancedT...	PUP	Quarantined	File	06/02/2017 - 02:32:43 PM
Ransom.Carber	Ransomware	Quarantined	File	06/02/2017 - 02:31:26 PM
Malware.Exploit.Agent.Gen...	Exploit	Blocked	Exploit	-	...	06/02/2017 - 02:30:07 PM
Malware.Exploit.Agent.Gen...	Exploit	Blocked	Exploit	-	...	06/02/2017 - 02:29:42 PM
Ransom.Filecoder	Ransomware	Quarantined	File	06/02/2017 - 02:28:11 PM
Ransom.WannaCrypt	Ransomware	Quarantined	File	06/02/2017 - 02:17:23 PM
web	Website	Blocked	OutboundConnection	06/02/2017 - 02:16:29 PM
web	Website	Blocked	OutboundConnection	06/02/2017 - 02:16:29 PM
web	Website	Blocked	OutboundConnection	06/02/2017 - 02:16:29 PM

Malwarebytes cloud console Real-Time Protection

Key benefits

Layered detection techniques

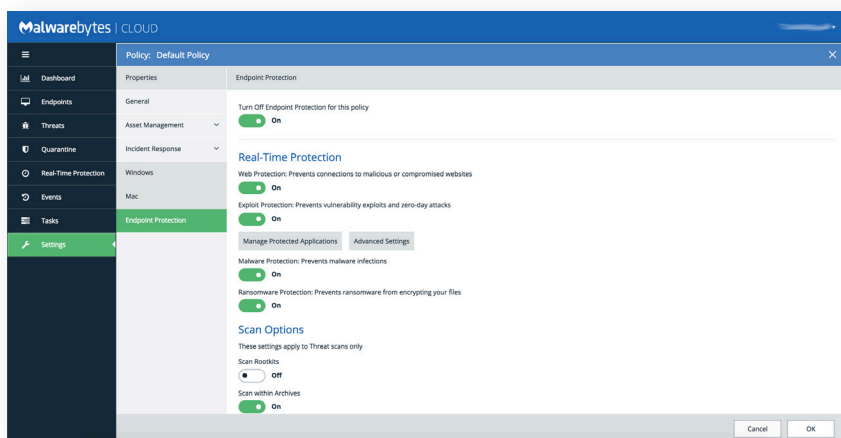
Malwarebytes Endpoint Protection employs multiple techniques to identify and defend against attacks at all stages of the attack chain using a highly effective mix of signature-less and matching-technology layers working both pre- and post-execution. Leveraging the best-informed telemetry, the pre-execution techniques are updated to continually drive toward earlier detection in the infection chain.

Complete and thorough remediation

Malwarebytes Endpoint Protection leverages our Linking Engine technology to remove all traces of infections and related artifacts—not just the primary threat payload. This signature-less approach speeds up threat scans and saves time normally spent wiping and re-imaging endpoints.

Cloud-enabled management

Malwarebytes Endpoint Protection is delivered via our Malwarebytes cloud-based endpoint management platform. This cloud platform reduces complexity, making it easy to deploy and manage Malwarebytes Endpoint Protection and other Malwarebytes solutions, regardless of the number of endpoints. This centralized cloud-console eliminates the need to acquire and maintain on-premises hardware.



Malwarebytes Endpoint Protection security policy settings

SYSTEM REQUIREMENTS

Included Components

- Malwarebytes cloud platform
- Malwarebytes Endpoint Protection (persistent Windows agent)
- Email and phone support

Hardware Requirements

Windows

CPU: 1 GHz

RAM: 1 GB (clients); 2 GB (servers)

Disk space: 100 MB (program + logs)

Active Internet connection

Supported Operating Systems

Windows 10® (32-bit, 64-bit)

Windows 8.1® (32-bit, 64-bit)

Windows 8® (32-bit, 64-bit)

Windows 7® (32-bit, 64-bit)

Windows Vista® (32-bit, 64-bit)

Windows XP® with SP3 (32-bit only)

* Windows Server 2016® (32-bit, 64-bit)

* Windows Server 2012/2012R2® (32-bit, 64-bit)

* Windows Small Business Server 2011

* Windows Server 2008/2008R2® (32-bit, 64-bit)

* Windows Server 2003® (32-bit only)

Please note that Windows servers using the Server Core installation process are specifically excluded.

** Windows Action Center integration not supported for Windows Server operating systems.*



malwarebytes.com



corporate-sales@malwarebytes.com



1.800.520.2796

Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company's flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts.

Copyright © 2017, Malwarebytes. All rights reserved. Malwarebytes and the Malwarebytes logo are trademarks of Malwarebytes. Other marks and brands may be claimed as the property of others. All descriptions and specifications herein are subject to change without notice and are provided without warranty of any kind.