Advanced Threat Endpoint Protection

Malwarebytes Endpoint Security (with anti-exploit) versus EMET, Palo Alto Traps, Invincea, and Bromium

There are several different exploit mitigation techniques. However, the primary difference between Malwarebytes Endpoint Security (which includes Malwarebytes Anti-Exploit for Business) and other products containing anti-exploit technology is that Malwarebytes Endpoint Security has been designed to work flawlessly in the vast majority of Windows configurations and third-party applications without any required advanced configuration, conflicts, false positives, or significant system resources.

Malwarebytes Endpoint Security includes:

- Award-winning remediation capabilities
- Real-time protection against zero-day malware
- Real-time protection against zero-day exploits

Malwarebytes Endpoint Security can be run alongside existing and traditional antivirus and endpoint security products to enhance and harden endpoint defenses. Implementing Microsoft's Enhanced Mitigation Experience Toolkit (EMET), Palo Alto Traps, or Bromium only adds one layer of defense while Malwarebytes Endpoint Security provides three additional layers of defense.

Let's take a closer look at the differences:

	Malwarebytes	Palo Alto Traps	Invincea	Bromium	Microsoft EMET
Remediation of unknown and advanced threats	Malwarebytes is renowned for its malware remediation capabilities, winning the "Best Disinfection 2014" award from AV-Test.org.	No malware remediation	No malware remediation of the host OS outside the sandbox	No malware remediation of the host OS	No malware remediation
Proactive detection of known and zero-day malware	Malwarebytes Endpoint Security includes the Malwarebytes Anti-Malware engine, which complements traditional endpoint security solutions. The engine is known for its ability to detect zero-day malware days, and sometimes weeks, ahead of top tier antivirus vendors.	No malware detection	No malware detection of the host OS outside the sandbox	No malware detection	No malware detection

Advanced Threat Endpoint Protection

Malwarebytes Endpoint Security (with anti-exploit) versus EMET, Palo Alto Traps, Invincea, and Bromium

	Malwarebytes	Palo Alto Traps	Invincea	Bromium	Microsoft EMET
Unobtrusive with Windows Updates and other third-party updates	Unobtrusive	Unknown	Invincea will block Windows Updates and end users have to allow and re-run Windows Updates	Unknown	Unobtrusive
Protects unsupported Windows XP	Yes	Unknown	Yes	No	Version 5.x of EMET does not support Windows XP
Market proven	Malwarebytes has an active policy of working with external and independent researchers and testers to continuously evaluate and improve the architecture and design of the product. Examples: The Hall of Fame, the results of independent tester @Kafeine, and the results of the independent testing lab PC Security Labs.	No independent verification of the efficacy of Palo Alto Traps available	No independent verification of the efficacy of Invincea available	No independent verification of the efficacy of Bromium available	EMET has been subject to a lot of scrutiny, and many bypasses have been documented.
Competitive pricing	Malwarebytes Endpoint Security is a competitively priced solution that includes remediation, anti-malware, and anti-exploit under the same Management Console.	Three times the price of Malwarebytes Endpoint Security for one-third of the protection offered by Malwarebytes Endpoint Security	Three times the price of Malwarebytes Endpoint Security for one-third of the protection offered by Malwarebytes Endpoint Security	Three times the price of Malwarebytes Endpoint Security for one-third of the protection offered by Malwarebytes Endpoint Security	Free, although due to the many reported conflicts and false positives, this is a clear case of "you get what you pay for"

Advanced Threat Endpoint Protection

Malwarebytes Endpoint Security (with anti-exploit) versus EMET, Palo Alto Traps, Invincea, and Bromium

	Malwarebytes	Palo Alto Traps	Invincea	Bromium	Microsoft EMET
Proactive detection of known and zero-day exploits	Included in the package Install and forget Compatible with Windows XP and later Compatible with traditional antivirus and endpoint security	Included in the package Requires installation and configuration by Palo Alto engineers Incompatible with Symantec and probably other major vendors	Included in the package, as long as running inside the sandbox Requires end-user training on sandbox operation Does not protect all popular applications Cannot add protection to non-protected applications Interferes with and blocks Windows Updates	Included in the package Minimum requirements Windows 7 and later Only for 64-bit Operating Systems	Included in the package Does not protect against Java exploits Does not protect against sandbox escapes Does not protect against explication flow design abuses Many reports of conflicts with third-party applications and false positives Many reports by users having to disable important exploit mitigations to “make it work”
Complementary to traditional antivirus and endpoint security	Complementary and recommended by security experts to be run alongside existing traditional antivirus and endpoint security Independent verification of complementary operation and negligible performance impact by Passmark	Reports from customers highlight incompatibility with at least Symantec Endpoint Protection More incompatibilities with other major vendors are likely	Unknown	Unknown	Complementary and recommended by security experts to be run alongside existing traditional antivirus and endpoint security No independent compatibility study available