Malwarebytes + Windows Defender

The most cost-effective way to protect your organization

THREATS ORGANIZATIONS FACE

Email phishing
- End users redirected to malicious websites

Botnet attacks
- Organization computing resources infected and hijacked

Fileless infections
- Attacks that do not write any files to the infected system's hard drive, bypassing traditional AV detection

Malvertising
- Malware and scams delivered via infected ads on popular sites (e.g., msn.com, nytimes.com, bbc.com)

Ransomware
- Files and systems encrypted and held for ransom

PUPs and PUMs
- Potentially unwanted programs and modifiers downloaded, slowing down computer performance

Every organization is looking to strengthen its security posture. And most are constrained by lean IT budgets. Layering Malwarebytes Endpoint Security with Microsoft's Windows Defender and Microsoft Security Essentials provides businesses with the most cost effective method of bringing next-generation endpoint protection to bear against the most malicious threat landscape that we have ever seen.

Budgets tighten, breaches increase

Information security is a top IT issue faced by organizations and businesses. According to Osterman Research (*Understanding the Depth of the Global Ransomware Problem*, published August 2016), 79 percent of the businesses surveyed suffered a security-related breach in the previous twelve months. Most organizations have seen the failure of their current AV solutions first hand. There is no doubt that traditional security solutions using legacy techniques regularly fail to identify modern threats. Malware techniques have evolved so rapidly that to keep pace, so does the technology to protect against these threats.

While most of organizations recognize the need to upgrade their security solutions to better address advanced threats, it is in direct conflict with budgetary constraints. As much as a next-generation antivirus solution may be desired, it often cannot conform to today's budget realities.

Microsoft Windows Defender and Microsoft Security Essentials

Depending on which operating system is running, Microsoft provides either Windows Defender or Microsoft Security Essentials (MSE) at no cost to protect systems against malware and viruses. Systems running Windows 8 or Windows 10 can leverage built-in Windows Defender. On older systems running Windows XP, Windows Vista, or Windows 7, Windows Defender can only protect against spyware, so MSE can be added at no additional cost to address known malware and viruses.

Strengthening Windows Defender with Malwarebytes Endpoint Security

Microsoft's solutions alone, however, cannot protect against the advanced threats that organizations face daily. By adding Malwarebytes Endpoint Security to Microsoft's free basic products, IT admins get next-gen

protection that is not only affordable but also catches threats that get by traditional antivirus programs. Malwarebytes Endpoint Security combines three key technologies into one solution, and with one of the Microsoft's solutions, creates four powerful security layers. This is the layered security strategy experts recommend.

Malwarebytes Endpoint Security

With more than 200,000,000 downloads over the past 10 years, Malwarebytes detection technology is powered by the world's most informed telemetry. The key technologies included in Malwarebytes Endpoint Security are:

Anti-malware technology detects and blocks malicious software. It monitors and stops malicious processes before they can do damage. Leveraging advanced heuristic scanning, this module provides protection against the latest malware threats.

Anti-exploit technology protects the system with application-shielding code that prevents exploits from compromising endpoints through software vulnerabilities. The shielded application cannot be exploited through any zero-day vulnerabilities.

Anti-ransomware technology provides real-time detection and blocking of ransomware. Based on proprietary behavioral technology, this signature-less engine protects against not only all variants of known ransomware but also unknown (zero-hour) ransomware.

Additional Malwarebytes solutions

Malwarebytes Breach Remediation
Rapid, lightweight solution detects and removes advanced threats from Windows and Mac endpoints. Scans and cleans infected endpoints remotely using an extensible platform. Forensic Timeliner gathers system events surrounding breaches so the security team can address security gaps and reduce malware dwell-time.

What organizations and businesses say

"
Malwarebytes is a critical part of the layered security needed in today's environments. It's doing a great job of protecting us.

—John Major, IT Operations Manager,
Sun Products

"
Malwarebytes is a very effective tool. It's enabling us to enhance our overall endpoint security strategy with much better protection. It's easy to deploy and manage. Best of all, our users don't have to do anything, except continue to work without interruption.

—Gareld Rodriquez, Group IT and Data Security,
Sagicor Financial Corporation

Organizations everywhere trust Malwarebytes

Vermeer®   **Dole**   **SAMSUNG**   **Stanford** University

---

malwarebytes.com/business   business@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.