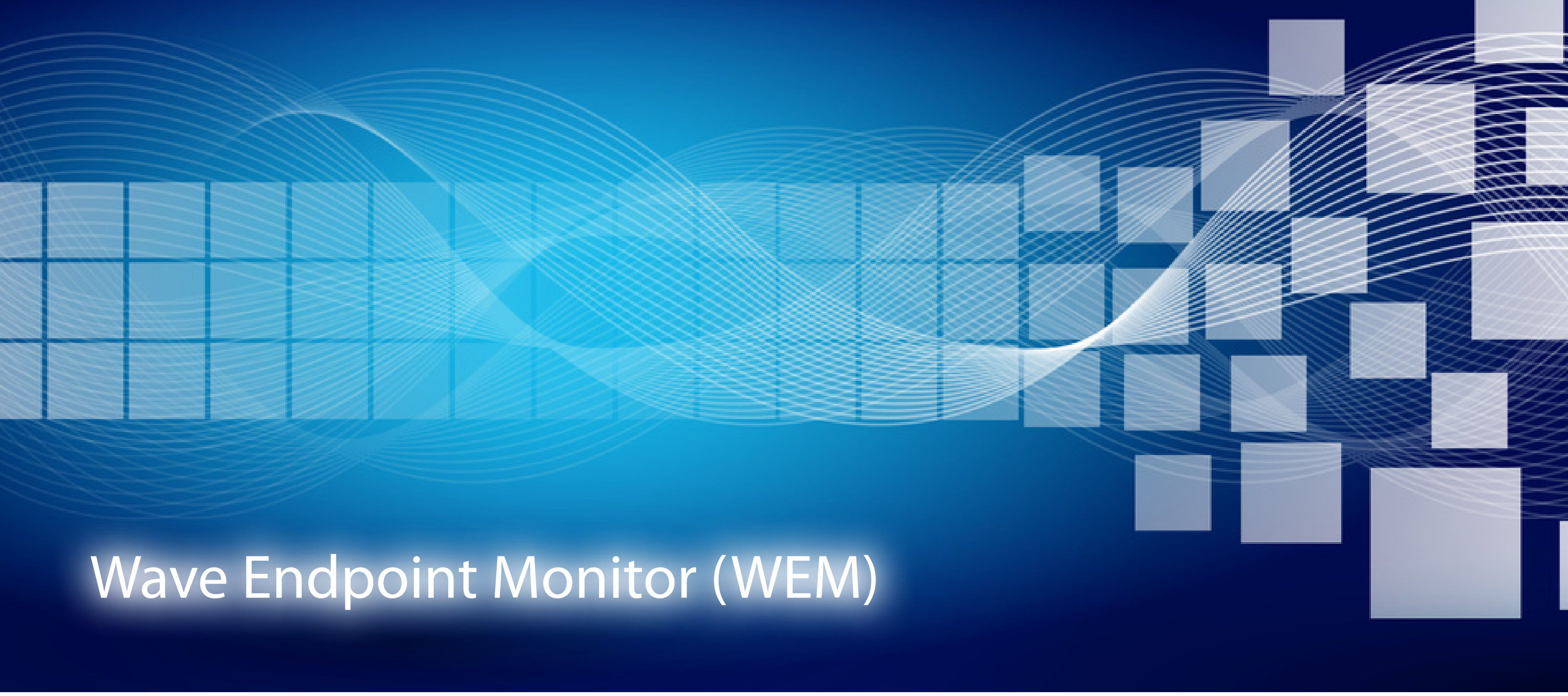
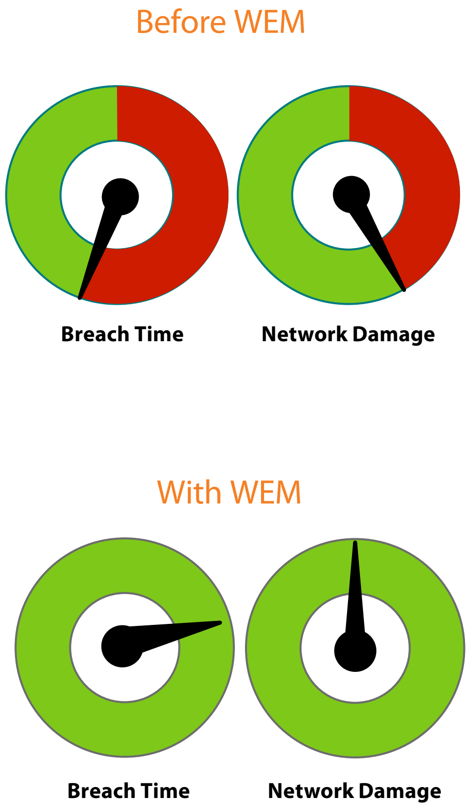


Wave Endpoint Monitor (WEM)

What is malware?

Malware is a general name for software that installs on your organization's computers and creates damage. It includes computer viruses, worms, Trojan horses, spyware, adware, rootkits, and more. These malicious programs could be created by a tenacious adversary, or by financially motivated criminals, and inserted into your organization's computers. These programs may lie down there undetected for months or secretly do things like log your keystrokes, steal your passwords, harvest your address book, observe where you go on the Internet, report sensitive data to distant servers, or even wipe or encrypt your data. Recent high profile malware attacks on utilities and countries even introduced altered software reported to affect the functioning of physical devices, like uranium enrichment centrifuges, oil rig equipment and water pumps. Malware can be introduced through a web download, an email attachment or even a USB external device for networks that are not connected to the Internet.



Software-only model can't reliably detect malware

The big problem with malware is that antivirus software doesn't always detect it. Anti-malware software is based on signatures of known bad software. However, there always needs to be a patient 0 that discovers he is infected, for

Solution Brief

An APT (or rootkit) is not detected by traditional malware scanners since these run in the Operating System

the rest of the world to benefit from it. In the case of APTs (Advanced Persistent Threats) your organization may be the only target for the specific strand of malware. In that case, you will not gain any protection from the signature detection process. Modern anti-malware and other software packages that promise cyber security or protection from APTs would use various heuristics and "AI" (Artificial Intelligence) to detect malware based on a predefined set of behavioral parameters. A sophisticated attacker is able to fine tune the behavior of the malware he is writing for various known anti-malware software, so that it can evade detection for long periods of time.

A further challenge for anti-malware software is that it commonly works at the operating system (OS) level. It isn't very good at seeing deeper into the system, where some malware lives. Malware can hide from anti-malware software by starting earlier in the stack and then feeding anti-malware software false results when it asks the OS questions. APT's extent seems wider each week. News stories about targeted attacks on organizations appear weekly. Even more stories do not appear, as malware is not detected for very long periods of time. Some malware described as "cutting edge" has code components that have been available for 3 to 4 years, thus dating their undetected time of life in the wild. With online tools, even a nontechnical person can create an APT easily. And there are more ways than ever for malware to spread: the Internet, personal computing devices, downloads, email, social media sites. Government agencies recognize it as a growing threat. Early detection is the highest priority in this Cyberwar. In 2011 NIST published guidelines for establishing a chain of trust for the basic input/output system (BIOS), which initializes a computer when it boots up. This critical system is one of malware's more consequential targets and an area specifically protected by Wave Systems in its products and in its thinking.

Wave's solution: start with the device

If anti-malware doesn't work, what does? The Wave alternative relies not on superficial layers of software but on standards-based hardware: self-encrypting drives (SEDs) and Trusted Platform Modules (TPMs), security chips that are already embedded in many of your devices. When you turn them on and manage them with Wave software you suddenly have a broad, deep view into the devices on your network. Among other things, you'll know immediately whether any one of your devices—desktops, laptops, tablets—has been tampered with. But Wave is proactive too: you can block the kinds of behaviors that invite malware in. Wave Endpoint Monitor provides early detection for attacks originating in the low level stack of your devices.

Which other attack vector should you watch? One common vector that is used to attack even the most secure networks is physical devices - connected to USB, FireWire or Secure Digital (SD). Our Data Protection Suite (DPS) AV scanner allows you to block any unscreened device from connecting to any machine in the organization, until it has been scanned for known malware.

Heads-up: Wave supports Windows 8

Windows 8 will be offering new protections against malware. You'll upgrade eventually. With Wave you can start taking advantage of the security hardware you already have, and when you make the transition to Windows 8, it will be seamless.

Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238
(877) 228-WAVE · fax (413) 243-0045
www.wave.com