Invincea

Advanced Endpoint Protection (AEP)

Advanced Endpoint Protection (AEP) is a very competent anti-malware tool that really focuses on the task at hand: protecting the endpoint from malware threats. It does this by encapsulating the endpoint application in a virtual environment and allowing malicious files to detonate, but containing the attack so that not even the most advanced zero-day can escape. That's a pretty strong statement, but Invincea lives up to it because the tool has no need for signatures or traditional heuristics.

The tool reduces the attack surface significantly through its use of "secure virtual containers." We really liked that the company did not try to convince us that it was sandboxing since sandboxes usually are a protective layer over the kernel that prevents the malware or its effects to escape. Sadly, it is possible to "go around" the sandbox layer and still infect.

Virtual containers are much different. They fully encapsulate the app in a secure environment, making it nearly impossible for a malware payload to do any damage. The container is Invincea's own virtual machine that is more lightweight than a typical type 2 hypervisor.

Invincea bases its approach on four elements: containment, detection, prevention and intelligence. Functionally, AEP contains and identifies the threat and controls it. The secure virtual container contains the threat. Threats are identified using several techniques, including OS monitoring, comparing to local knowledge, and sending to the cloud for further analysis, if necessary, and analyzing with a cool tool, developed under the DARPA-funded Cyber Genome project, called Cynomix. Control is achieved by checking across the enterprise for other examples of the threat found on a single endpoint.

AEP even works if the threat for some reason is outside of the container. It detects the threat due to its unknown behavior and analyzes it using advanced static analysis.

Setup is not at all difficult. The endpoint sensor is small and does not load down the endpoint. Setting up an AEP environment is pretty easy.

The management server also is easy to use and has a number of screens that help isolate functionality. When a threat is detected, AEP creates an alert with suspect activity details. Forensic information comes in the form of a map that shows exactly how a threat executed and the damage that it did. Additionally, a threat tree allows detailed analysis of the threat's dynamic functionality. Each infection vector is given a point value during analysis and that value determines the threat level of the event. Of course, the tool is vendor agnostic removing any vendor-specific restrictions. Once the sample is collected, it can be shipped to a partner such as VirusTotal for a full analysis.

– Peter Stephenson, technology editor

DETAILS

Vendor Invincea

Price $42/year per endpoint.

Contact invincea.com

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths The Cynomix engine is both cool and useful. Ease of deployment.

Weaknesses None that we found.

Verdict This is a significant anti-malware tool. It takes the position that by controlling malware at the endpoint you make the endpoint – and, thus the enterprise – more secure from today's sophisticated threats. We agree, and we make this our next generation Recommended product.

invincea®
3975 University Drive, Suite 330
Fairfax, VA 22030 USA
Tel: 1-855-511-5967
sales@invincea.com • www.invincea.com