Enhanced Malware Detection, Prevention, and Forensic Intelligence

Invincea end-user protection integrates with McAfee® ePolicy Orchestrator® software

Invincea helps stop the theft of intellectual property, government and commercial trade secrets, and financial fraud by protecting users against spear phishing, drive-by downloads, poisoned search results, and weaponized email attachments. Invincea's actionable, forensic malware intelligence is now integrated with McAfee ePolicy Orchestrator (McAfee ePO™) software. The joint solution provides better protection against zero-day malware and enhances the capabilities of the broader security infrastructure.

Your users may have become the unwitting accomplices in the breach of your network. Adversaries—from nation states to cybercriminals to hacktivists—who are savvy about human psychology can dupe your users into opening the door to your most sensitive information. Every user in your network is a potential target: users simultaneously are your first line of defense and your weakest link. Security awareness training alone may not be the answer to this problem. Asking users to make the correct security decision every time they access the Internet or open a legitimate-looking email attachment is not always easy or practical.

To protect your organization, you need a solution that does not impact productivity while it prevents users from unwittingly bringing malware into your network. The answer for many organizations has been to contain all untrusted content, so that users still have free reign to get their jobs done, but adversaries have no access to the systems connected to your network.

McAfee and Invincea Solution Benefits

McAfee has partnered with Invincea to bring additional user protection against zero-day and previously unknown malicious software. Invincea's innovative use of virtualization creates a protective “bubble” around browsers, PDF readers, Microsoft Office documents, ZIP files, and executables. These applications are the largest attack vectors used to deliver spear phishing exploits, distribute drive-by infections, mimic legitimate sites that have been compromised, offer fake antivirus, and propagate other online threats.

Containment

By placing all untrusted content coming through the browser or email attachments into a virtualized environment separate from the desktop operating system, Invincea has created an enterprise “airlock” that seals the potential attack vector off from infecting the desktop system and the network.

Detection

Using application behavioral-based detection, Invincea is able to spot malicious activity—including zero-day exploits—within this contained environment. By monitoring for abnormal application behaviors and actions, Invincea keeps pace with the exponentially growing malware landscape without needing previous identification of a malware strain.

Prevention

As soon as malicious behavior is identified, it is stopped in its tracks. An infection alert is then provided to the user, without asking the user to make a security decision, and an automatic restoration process is initiated, during which Invincea discards the tainted virtual environment and completely rebuilds one to a gold clean state. This process takes no longer than 20 seconds, and the user is up and running without a call to the help desk.
“Invincea effectively stops zero-day malware in its tracks.”
—Peter Stephenson
Technology Editor
SC Magazine

“Invincea is a shield that should not be left behind when working in today’s online wilderness.”
—John Breeden II
GCN Magazine

“You’ll put this on your test computer, aim some web-borne malware at it, and you’ll be sold.”
—Peter Stephenson
Technology Editor
SC Magazine

Forensic Intelligence
At the point of detection, Invincea automatically captures actionable, forensic malicious activity from the virtual machine and feeds that information directly to the McAfee ePO platform. McAfee ePO platform administrators can keep an eye on the most vulnerable users and strengthen defenses on their systems using new policies or additional endpoint security software.

The Invincea solution offers McAfee customers the following benefits:
• Comprehensive protection of every endpoint controlled by the enterprise—regardless of whether or not it is connected to the network
• Enhanced protection against zero-day attacks and advanced persistent threats (APTs) by protecting the primary target—users and their most targeted applications (web browser, PDF reader, Microsoft Office suite, and executables)

Complementary to McAfee Endpoint Protection and McAfee Host Intrusion Protection
Invincea’s innovative approach to malware blocking and intelligence collection provides an ideal complement to McAfee endpoint protection. McAfee protects against known malware using signature detection as well as unknown malware using behavioral detection. For certain types of threats, Invincea provides a complementary approach against unknown and zero-day malware using a virtual “bubble.” As users continue to be the primary target and vector of entry for adversaries into the enterprise, Invincea protects the enterprise by strengthening protection for users, performing attack behavior analytics, and informing the McAfee security management dashboard.

About Invincea, Inc.
Invincea is a leading innovator in malware threat detection, prevention and forensic intelligence via virtualization to protect enterprise networks from cyberthreats, including spear phishing. The company’s solutions offer a unique ability to protect networks against all types of threats directed at end users, including zero-day threats, by seamlessly moving applications that render untrusted content into controlled secure virtual environments that automatically detect and terminate threats in real time. For more information, visit http://www.invincea.com.