How OKENA Is Positioned Favorably vs. Sandboxing Systems

Other content management and "sandboxing" technologies are designed to analyze active content while maintaining the access integrity of user privileges. Like OKENA, some vendors may offer products that are based on behavior and predefined rules for network applications. Vendors in this space are Finjan and Pelican Security.

Sandbox strengths:

?? Sandboxing will prevent damage from attacks that AV products cannot detect.

?? Sandboxing allows enterprises to replace AV products.

?? Sandboxing grants enterprises relief from the constant signature update process associated with the AV vendors.

Sandbox limitations:

?? Sandbox products only look at file access controls for selected network applications (typically IE, Outlook). They do not correlate network activity to recognize sophisticated attacks.

?? Sandboxing products have an inflexible definition of policy. Any new policy definitions will require a new release of the product.

?? Sandboxes have no defense if their controls miss an attack – the attack is free to propagate rapidly throughout the enterprise.

?? Sandboxing technology applies to desktops only.

OKENA StormWatch strengths:

?? OKENA detects attacks based on sequences of file and network activity. Sandboxing will miss these.

?? OKENA includes a general rules definition capability allowing IT to easily customize security to their specific policy. Behavior for Microsoft Office is included with StormWatch

Lifecycle of an Attack	*Okena*	*Sandbox*
Probe		
Ping Addresses	Yes	X
Scan Ports	Yes	X
Guess Passwords	X	X
Guess Mail Users	X	X
Penetrate		
Mail Attachments	Yes	Yes
Buffer Overflows	Yes	X
ActiveX Controls	Yes	Yes
Network Installs	Yes	X
Compressed Messages	Yes	Yes
Backdoors	Yes	X
Persist		
Create New Files	Yes	X
Modify Existing Files	Yes	X
Weaken Registry Security Settings	Yes	X
Install New Services	Yes	X
Register Trap Doors	Yes	X
Propagate		
Mail Copy of Attack	Yes	X
Web Connection	Yes	X
IRC	Yes	X
FTP	Yes	X
Infect File Shares	Yes	X
Paralyze		
Delete Files	Yes	X
Modify Files	Yes	X
Drill Security Hole	Yes	X
Crash Computer	Yes	X
Denial of Service	Yes	X
Steal Secrets	Yes	X

Preventative Security Provided During an Attack

?? OKENA protection applies to both servers and desktops.

?? OKENA includes protection that sandboxing cannot: email worm propagation, Trojan horse detection, buffer overflow hardening, port scan detection, SYN-flood prevention to name a few.

Bottom Line message:

OKENA's behavior enforcement technology goes well beyond the file-oriented sandboxing approach by proactively preventing damage for combinations of file and network attacks. The layered approach by OKENA protects the entire enterprise from the rapid spread of an attack as well as unapproved access. OKENA StormWatch also protects corporate servers.

71 Second Avenue, Waltham, MA 02451
Tel: 781-209-3200 Fax: 781-209-3199
E-mail:info@okena.com

www.okena.com

6905 Rockledge Drive, Suite 600
Bethesda, MD 20817
301-896-9388