OKENA

Intrusion Prevention: Security Without Signatures

OKENA protects the integrity of software applications and operating systems in an environment where threats to that integrity are constantly changing.

OKENA offers unique, innovative solutions for your desktops and servers that go beyond today's host-based intrusion detection systems, anti-virus and distributed firewall solutions. A free OKENA StormWatch evaluation will show you:

- *Why traditional reactive security technologies can't help you against modern attacks*

- *Why StormWatch meets and exceeds the requirements for other security solutions you're considering for desktops and servers*

- *Why proactive security solutions like OKENA StormWatch actually protect you from as yet unknown e-mail worms, Trojan Horses, Buffer Overflows, hackers and other high-profile, crippling attacks*

- *How to reduce security management/administration and improve ROI for your security infrastructure*

These are just a few of the reasons why Secure Computing and Network Computing Magazine selected OKENA as one of the companies to watch in 2002.
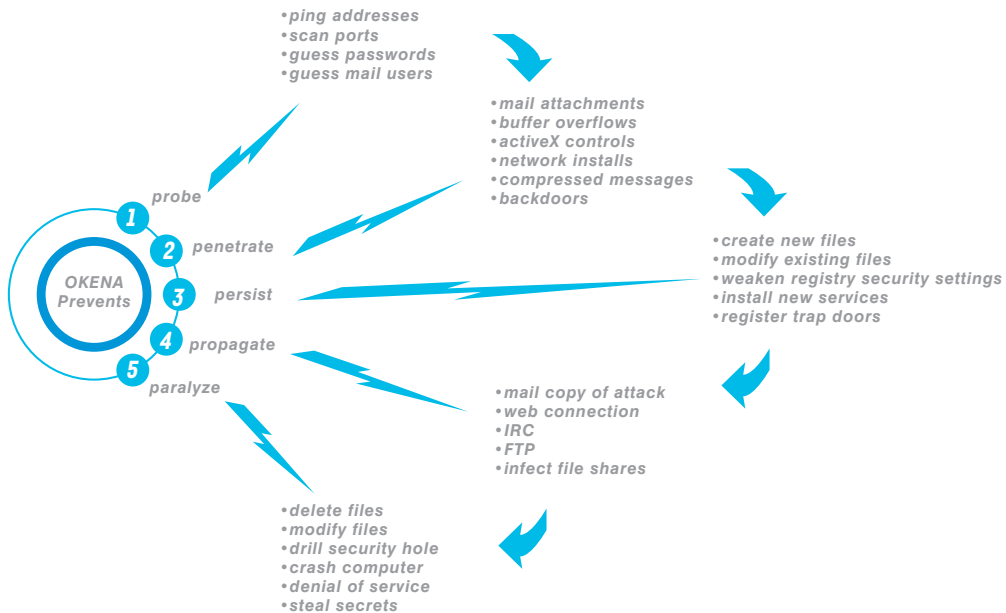
Limitations of Existing Security Technology

Today's attacks are increasingly sophisticated, with the emergence of rapidly-released poly-morphic attacks and content-based attacks targeted at specific applications.

Traditional intrusion detection and virus scanning security technologies focus on identifying and removing known threats through the use of signatures, requiring extensive administrative time and effort. However, today's attacks infiltrate servers and desktops and cause damage before signatures are known and developed by product vendors.

Assaults on networks typically go through stages (see diagram at right). OKENA recognizes that only a layered approach is effective against security breaches that can occur at any stage. OKENA StormWatch security software proactively defends against damage to a host, through-out all stages of the attack, while other technologies provide early-stage *detection* only when a signature is known. StormWatch provides application–specific policies within an intelligent agent architecture residing on servers *and* desktops. By defining and enforcing the behavior of applications, StormWatch protects against known *and* unknown security risks.

- *ping addresses
- *scan ports
- *guess passwords
- *guess mail users

- *mail attachments
- *buffer overflows
- *activeX controls
- *network installs
- *compressed messages
- *backdoors

- *create new files
- *modify existing files
- *weaken registry security settings
- *install new services
- *register trap doors

OKENA Prevents

1. probe
2. penetrate
3. persist
4. propagate
5. paralyze

- *mail copy of attack
- *web connection
- *IRC
- *FTP
- *infect file shares

- *delete files
- *modify files
- *drill security hole
- *crash computer
- *denial of service
- *steal secrets

OKENA Intrusion Prevention: Security Without Signatures

StormWatch, the cornerstone of OKENA's ongoing StormSystem enterprise security strategy, combines previously undelivered features of host-based intrusion detection systems and personal firewall solutions for desktops and servers . . . with prevention in mind.

StormWatch application security policies can be implemented out of the box or can be customized to meet unique corporate environments. The results are more secure networks and less administrative burden in managing the security environment.

"The security landscape continues to evolve and enterprises now realize that they must do more to protect themselves from the constant cycle of attack and respond. StormSystem, from OKENA, delivers on proactive intrusion prevention.. . . OKENA took a stand-alone intrusion prevention solution to the next level by creating a strong framework that prevents enterprise-wide intrusions."

- Charles Kolodgy, Internet Security Software Research Manager, IDC

"How will this save me money as opposed to all the other security we bought in the past . . . which didn't stop us from getting whacked by Code Red and Nimda?"

When your security solutions require you to spend valuable administrative time shutting down networks for repairs, patching systems, updating signatures and wading through an endless sea of log files, your IT resources are significantly impacted. In addition to preventing damage from known and unknown attacks, OKENA intrusion prevention products will reduce the administrative burden of staying on top of the latest attack on your network, as well as the attacks that are yet to come.

StormWatch Allows You To:

- Consolidate multiple security products with one solution

- Move away from the constant cycle of patch/scan/patch

- Alleviate the burden of deploying and managing signatures

- Drastically reduce the number of alerts and false positives that are generated

OKENA also works with leading, strategic solution and service alliance partners as part of our overall Global Alliance Network. Visit www.okena.com for an up-to-date listing of our growing network of partners.

Founded in 1999, OKENA provides break-through Intrusion Prevention Security software products that proactively preserve the operational integrity of applications and host systems.

OKENA, Inc. 71 Second Avenue Waltham, MA 02451
Tel: 781.209.3200 FAX: 781.209.3199
E-mail: info@okena.com

Sales: Tel: 301.896.9388 FAX: 301.896-9476
E-mail: sales@okena.com

OKENA, StormSystem, StormWatch and StormFront are trademarks of OKENA, Inc. Other trademarks used in this document are the properties of their respective owners.