STORMWATCH

OKENA protects the integrity of software applications and operating systems. Our innovative intrusion prevention software, StormWatch™, proactively protects enterprises against known and unknown security risks.

Unlike existing security solutions that are attack-centric and reliant on databases of known attack signatures, StormWatch is application-centric, focusing on the behavior of mission-critical applications.

Key Benefits:

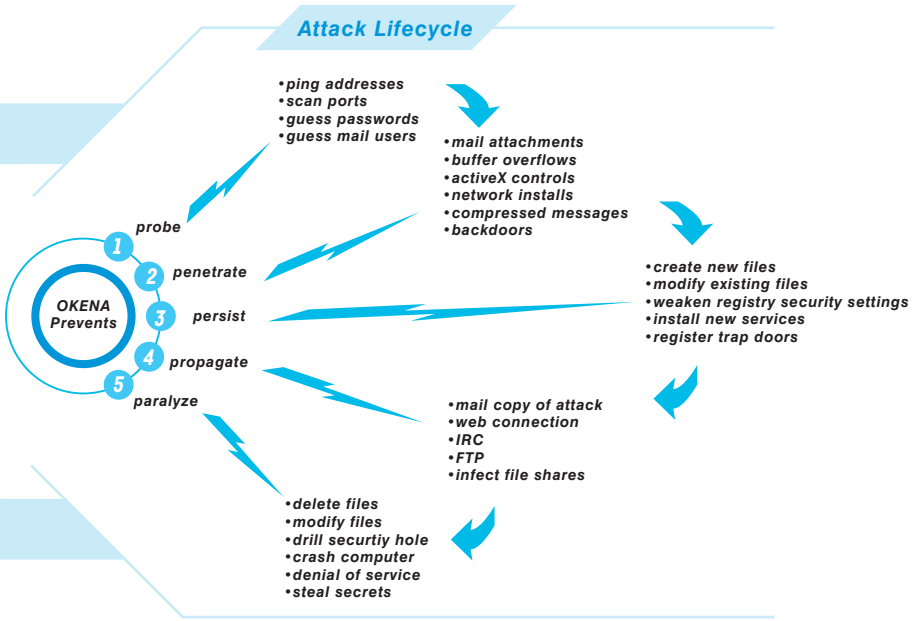
- ***Proactive security customized to your corporate environment***
- ***Ability to define and enforce security according to corporate policy***
- ***Intrusion prevention for current and future innovative attacks***
- ***Reduces downtime of network resources***
- ***Preventive protection against classes of attacks including Port Scans, Buffer Overflows, Trojan Horses, Malformed Packets, E-mail worms***

01 The Limitations of Traditional Security Technologies

Prevailing defensive measures – firewalls, AV software, vulnerability scanners, and IDS systems – are reactive and focus on barriers, or on known antidotes to threats. As recent high-visibility attacks like Nimda and Code Red have shown, these traditional technologies are unable to combat the effects of a new and evolving attack. Corporations who merely rely on a database of known signatures for protection leave their mission critical applications open to damage from indiscriminate attacks such as Code Red or, perhaps more significantly, targeted attacks or insider configuration abuse. Companies and their applications require security that protects through all stages of an attack.

02 The Attack Lifecycle

Assaults on network systems typically go through stages. OKENA recognizes that only a layered approach is effective against security breaches that can occur at any stage, from beyond the perimeter, to the server, or at the file level. StormWatch proactively defends against damage to a host, throughout all stages of the attack whereas other technologies provide early-stage protection and only then, when a signature is known. StormWatch is specifically designed to protect against new attacks where there is no known signature.

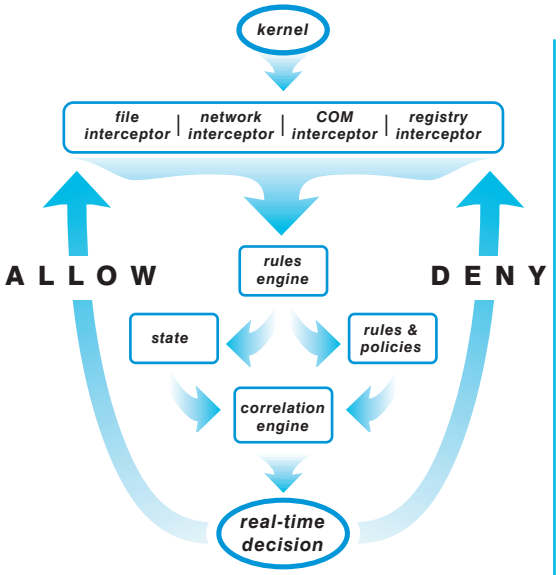


03 The StormWatch Solution

StormWatch consists of a management console resident on a Win2K server and host-based agents that are deployed on mission-critical desktops and servers.

StormWatch has application visibility because it resides at the kernel level within the OS. StormWatch's unique INCORE (Intercept Correlate Rules Engine) architecture intercepts all system calls to file, network, COM and registry sources. StormWatch applies unique intelligence to correlate behaviors of such system calls, based on rules that define appropriate or acceptable behavior for a specific application. This correlation and subsequent understanding of an application's behavior is what allows the software - as directed by the security staff - to truly prevent new intrusions.

When an application attempts an operation, StormWatch checks the operation against the application's security policy and makes a real-time allow or deny decision on its continuation. The StormWatch security policy is a collection of rules that IT and/or security administrators assign to each server and desktop to be protected. These rules provide safe application access to required resources.



StormWatch Security Policies for:

* Corporate desktops
* File Servers
* Application Servers
* IIS Web Servers
* Microsoft SQL Server
* DNS, DHCP
* Microsoft Office
* Server and Desktop Network Access (personal firewall)
* Corporate Web sites
* Instant Messenger
* Policies can be created for any application

Key Features of StormWatch:

* Browser based UI
* Remote installation of server and desktop agents
* One StormWatch console manages up to 2500 agents
* Agent-to-agent correlation for prevention of network-wide events
* Buffer overflow protection
* Real time file integrity monitoring
* Integration with desktop AV solutions for global virus correlation
* Application monitoring and control - control of which applications and versions can run on a host

OKENA

For more information about how OKENA StormWatch proactively prevents intrusions from executing, please visit us at www.okena.com. Or call us at (781) 209-3200.

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

Sales Information:
Tel: (301) 896-9388 FAX: (301) 896-9476 E-mail: Sales@okena.com