STORMFRONT

OKENA protects the integrity of software applications and operating systems. Our innovative intrusion prevention software proactively protects enterprises against known and unknown security risks. OKENA's new StormFront™ product works in tandem with StormWatch software: unique, industry-leading intrusion prevention software that prevents intrusions from executing malicious code within an enterprise environment.

By making it simple to create new StormWatch policies, StormFront allows customers or partners to easily protect any application. Because StormFront creates protective solutions for even highly customized, business-critical applications, IT organizations can quickly and easily eliminate substantial risk exposure.

Key Benefits:

- *Protect all new and legacy corporate applications – easily retrofit security for all applications*
- *Automated security policy generation for any application*
- *Enables the faster roll-out of secure applications to the environment*
- *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*
- *Installs as a snap-in to the StormWatch management console*

Working with StormWatch to Secure the Enterprise

StormFront works with the StormWatch Management Console and StormWatch Intelligent Agent, serving as a data analysis and policy creation tool for administrators who are deploying StormWatch policies across systems and networks.

StormFront protects any business application by analyzing its actual operation and automatically creating a StormWatch protective policy to secure it. Because this analysis is based on actual, observed behavior, it allows protection of any application, even extremely complex ones that have been highly customized to an individual customer's environment.
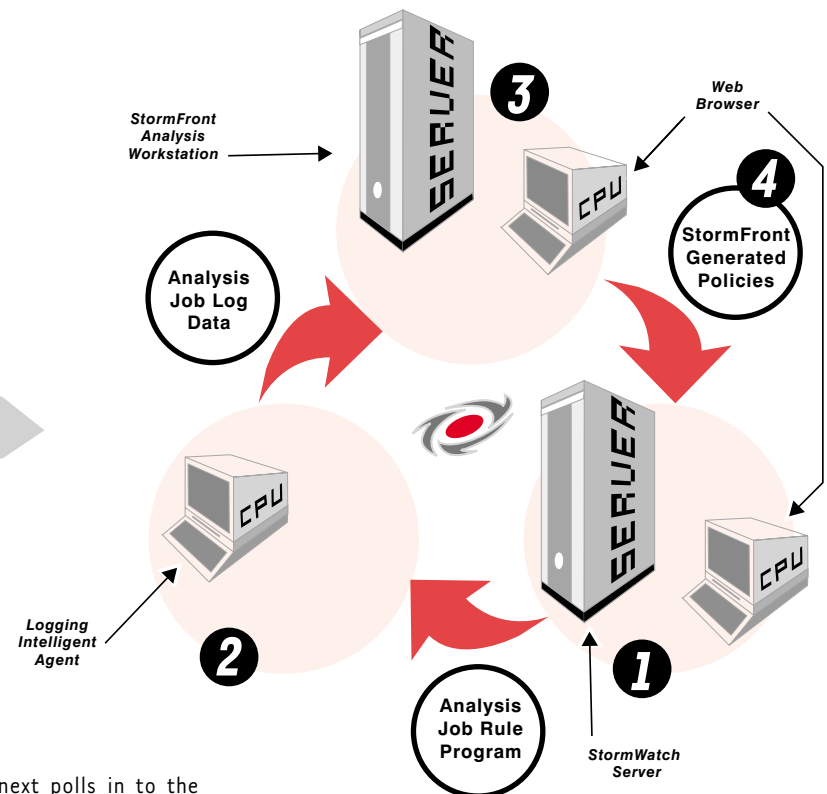
02 How it works

StormWatch secures enterprises primarily through the protection of applications. Because the rules that comprise StormWatch policies are application centric, understanding the resources applications require for normal operations is integral to building effective StormWatch policies. OKENA StormFront does that by analyzing applications as they operate in a normal environment and generating proactive security policies based on that analysis.

When deployed on a system running a StormWatch Intelligent Agent, StormFront monitors the actions of designated applications on that system, logging all network and operating system resource access attempts made by the application. StormFront then analyzes the logging data it collects and develops a StormWatch policy for the application in question. This policy enforces what is determined to be normal application behavior, while restricting all other behaviors.

03 Application Analysis in Detail

The application analysis and policy creation process is performed by three different contributing components: the StormWatch Management Console, the StormWatch Intelligent Agent (logging agent), and the StormFront Analysis Workstation.

1. Through the StormWatch Management Console, you designate which application you want to analyze. You also select an intelligent agent host on which the analysis is to take place and a time frame within which the analysis will be completed. This analysis configuration is then sent to the intelligent agent on the selected host in the same way new policies are delivered to agents.

2. The StormWatch Intelligent Agent receives the analysis configuration information when it next polls in to the management console. This intelligent agent now becomes the "recording agent" in this process. It analyzes and records all operations performed by the designated application. When the analysis is complete, the recorded data is sent to the StormFront Analysis Workstation.

3. The StormFront Analysis Workstation examines all the recorded data it receives from the recording agent. When the analysis is complete, it creates a policy for the application. This policy enforces the normal operations seen in the record file and will deny any operation attempts by the application that do not align with this normal behavior.

4. The StormWatch Management Console then imports the policy created by the analysis workstation.

StormFront Analysis Workstation

Web Browser

3

4

StormFront Generated Policies

Analysis Job Log Data

SERVER

CPU

SERVER

CPU

CPU

Logging Intelligent Agent

2

1

Analysis Job Rule Program

StormWatch Server

OKENA

For additional information about OKENA's innovative intrusion prevention solutions, please visit www.okena.com. Be sure and review the information on StormWatch' intrusion prevention software for a through understanding of how intrusion prevention goes beyond traditional scanning and signature technologies in preventing damage from new and evolving attacks.