Chapter 1

StormFront Product Overview

What is StormFront

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

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's StormFront product does that by analyzing applications as they operate in a normal environment and generating useful policies based on that analysis.

When deployed on a system running a StormWatch Agent, StormFront monitors the actions of designated applications on that system, logging all 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. These other behaviors could now be construed as abnormal or suspicious based on the analysis.

The Analysis Process

The application analysis and policy creation process is performed by three different contributing components: the StormWatch Management Console, the StormWatch Agent (logging agent), and the StormFront Analysis Workstation. (See Figure 1-1.)

- Through the *StormWatch Management Console*, you designate which application you want to analyze. You also select an 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 agent on the selected host in the same way policies are sent to agents.

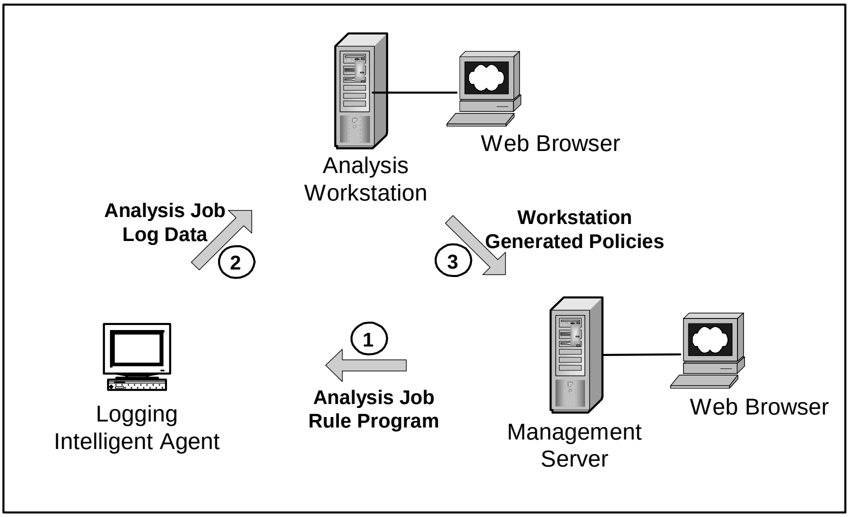
- The *StormWatch Agent* receives the analysis configuration information when it next polls in to the management console. This agent now becomes the "logging agent" in this process. It logs all operations performed by the designated application. As this logging takes place, it is assumed that the application is being thoroughly exercised in a normal operating environment. When the analysis is complete, the logged data is sent to the StormFront Analysis Workstation.

  Note: When the logging agent receives an analysis job, any policies relevant to the application being analyzed are disabled on the agent until the job is completed.

- The *StormFront Analysis Workstation* examines all the logged data it receives from the logging agent. When the analysis is complete, it creates a policy for the application and generates reports containing information on all resources accessed by the application. The policy enforces the normal operations seen in the log file and will deny any operation attempts by the application that do not align with this normal behavior.

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

Figure 1-1: Analysis Information Flow



StormFront Analysis Jobs

When the StormFront Analysis Workstation software is installed (see Chapter 2 for installation instructions), it automatically contacts the StormWatch Management Console. When the StormWatch Management Console detects the analysis workstation on the network, it adds a new category to its **Configuration** menu. This category is called **Analysis Jobs**. It is by accessing this Analysis Jobs window from the management console that you can configure parameters for analyzing a particular application.

Note: The StormFront Analysis Workstation can be installed on the StormWatch Management Console. However, if you're collecting a great deal of data, it is suggested you use a separate dedicated server system for data collection and analysis. See Figure 1-1.

Preparing to Install

Before installing the StormFront Analysis Workstation software, read the system requirements listed in this chapter. You should also refer to the *release notes* for the latest product information. Not doing so can result in the misconfiguration of your system.

Caution: Before installing the StormFront Analysis Workstation, you must have the **StormWatch Management Console** installed on either the same server system or on a separate server system on the network. If you have not installed the StormWatch Management Console, see the *StormWatch Getting Started Guide* provided as a PDF file on the StormWatch distribution CD.

You MUST also have a **StormWatch Agent** running on the server system to which you are installing the StormFront Analysis Workstation. If you are not running an agent on that system, install an agent kit before beginning the StormFront installation. The StormFront Analysis Workstation requires a StormWatch Agent running on the same system in order to operate. OKENA recommends that you apply the **Server Module** or the **StormWatch Manager Module** to the agent installed on the analysis workstation.

Hardware Requirements

To run the StormFront Analysis Workstation on your Windows 2000 server system, the requirements are as follows:

Component	System Requirements	Comments
CPU	Intel Pentium 500 MHz or higher	Uni-processor and dual processor systems are supported.
Memory	Windows 2000 - 256 MB minimum	
Disk Space	1 GB or higher	If you are running several analysis jobs, disk space requirements may vary.
Network	Single NIC interface	Multihomed systems are not supported.

Note: If you are installing the StormFront Analysis Workstation on the StormWatch Management Console system, all hardware requirements remain the same, except for the disk space required. A system running both products would require at least 2 GB's of disk space.

Software Requirements

- **StormFront Analysis Workstation** requires - Windows 2000 Server or Advanced Server with Service Pack 3 loaded
  (The StormFront Analysis Workstation is not supported on Windows NT, Windows XP, or UNIX systems. However, logging agents sending data to the StormFront Analysis Workstation can be installed on Windows 2000, Windows NT, and Windows XP.)

Note: At this time, StormFront logging agents are not supported on UNIX platforms.