SENTINEL: z/OS and Enterprise Wide FTP Management
An All Encompassing & Secure Real-Time FTP Management Solution

SENTINEL Introduction

SENTINEL is a z/OS-based software product that enables companies to actively manage and monitor Enterprise-wide FTP activity. It enables companies to regulate z/OS FTP server usage and block unauthorized and unwanted activity. SENTINEL also enables companies to monitor FTP usage real-time throughout the Enterprise and enhance Data Centre automation efforts by integrating FTP usage into the automation plan.

Why is SENTINEL Required?

Most companies have insufficient control over and knowledge of the FTP activity taking place on their network, what data is moving in and out of the enterprise and who (or what) is initiating the FTP activity. Knowing where FTP servers are, what they are being used for and stopping unwanted FTP activity enables you to address concerns and exposures to sensitive (privacy) data before they harm your organization. You can't make FTP go away but you can get it under control.

How Does SENTINEL Work?

SENTINEL enables companies to police z/OS FTP server usage using existing security facilities (ACF2, RACF, Etc.), stopping all unwanted FTP activity before it results in a problem or exposure. SENTINEL also reduces the complexity of managing FTP by merging and reporting on all of the FTP servers in an enterprise (Distributed Systems, z/OS). SENTINEL provides real-time monitoring of FTP usage, ISPF and Windows-based interactive analysis and consolidated reporting of FTP activity, failures, exceptions, throughout the entire enterprise. With SENTINEL, compliance comes through controlling access and managing exceptions. The primary functions of SENTINEL are:

- Polices FTP usage on z/OS FTP servers
- Enforces compliance
- Prevents expensive data security breaches which can damage company reputation
- Monitors cross-platform and cross-application FTP activity
- Helps perform FTP Audits in minutes
- Helps ensure Service Level Agreements are met
- Answers auditor's questions
- Integrates FTP activity into automation efforts
- Provides on-line reporting for problem resolution
- Helps improve network utilization with on-line analysis of FTP usage
- Invokes corrective action when FTP transmissions fail
- Provides exception reporting for Managers and Auditors

The primary components of SENTINEL are:

SAF Security Interface

IBM's z/OS FTP server provides few internal controls for managing FTP usage and protecting sensitive data. SENTINEL's SAF interface enables you to write SAF rules (RACF, ACF2, TopSecret) to inspect every FTP server connection request and command, determining authorization suitability to permit the request. Connections to the FTP server can be restricted to authorized locations. File transmission requests can be approved or denied based on the request originator, where data is coming from or where the data is going to (inside or outside the firewall) and what data is involved (file name). All FTP activity can be under SENTINEL control, including file transmissions, file deletion/renaming, allocations, batch job submission, job output retrieval and HFS file access. ***No longer will read-access to a file be all that is necessary for file transmission!***

A Real-Time FTP Usage Monitor

The Real-Time Monitor runs as a started task and monitors FTP usage throughout the Enterprise, working with z/OS TCP/IP to monitor z/OS FTP usage. It works with SENTINEL remote agents monitoring FTP usage for Distributed System platforms. All FTP usage activity is archived into the SENTINEL History File to meet regulatory compliance requirements.

All FTP activity is analyzed by the Real-Time Monitor and alerts to existing Data Centre automation tools can be generated based on criteria that are meaningful to you. The alert information can be used to further automate processes dependant on FTP usage, such as triggering production jobs, et al. The Real-Time Monitor started task also maintains active reports showing all FTP activity, sensitive data transmissions, exceptions, failed FTP transactions and FTP security checking results. Anyone with access to the started task output can see everything they need to know about what FTP activity has been taking place.

SENTINEL: z/OS and Enterprise Wide FTP Management
An All Encompassing & Secure Real-Time FTP Management Solution

FTP Auditor - Network Discovery Tool

SENTINEL's FTP Auditor is a Windows "discovery" tool that scans the network looking for active FTP servers. It identifies and assesses all of the FTP servers that it locates on the network. It reports on where the FTP servers are and whether they accept anonymous logon (not recommended). Double-clicking an FTP server enables you to log onto the server and display the list of files that are accessible to the server users. The first step toward managing FTP usage is to identify what FTP servers are running on your network so you can start the process of auditing their usage. Running FTP Auditor regularly makes it possible to identify when new FTP servers are added to the network and keep abreast of what they are being used for.

Remote Agent

SENTINEL's Remote Agent is a Java program that runs on distributed system platforms (Windows, UNIX, Linux, etc.), monitors FTP usage and feeds it back to the SENTINEL Real-Time Monitor. The Remote Agent currently supports FTP servers that log in IIS, W3C, SFTP and XFERLOG formats. Most third-party FTP servers support one of these log formats. Remote Agents enable SENTINEL to consolidate Enterprise-wide FTP activity into a single location for monitoring, automation and exception handling.

Interactive FTP Audits

In many companies, the volume of daily FTP activity is too large to effectively monitor using manual processes, especially where FTP servers reside on disparate platforms and log activity in different formats. z/OS FTP activity, in binary SMF format, is difficult to review without writing custom programs to format the data. SENTINEL makes quick work of analyzing FTP usage by presenting both summary and detail information in an interactive analysis application (Windows and ISPF). Drill-down capabilities from summary to detail data enable you to focus your attention on the FTP activity that requires further attention and skip over the rest. A built-in custom Exceptions view highlights FTP activity that you determine needs further attention.

ISPF Interface

SENTINEL incorporates a comprehensive ISPF interface for maintaining the SENTINEL software environment, submitting batch reporting and analysis jobs and performing interactive FTP usage audits. Reusable analysis specifications are stored for quick access to repeatable batch reporting and interactive analysis. All batch JCL is generated automatically from specifications made in ISPF panels. SENTINEL's ISPF interface dramatically increases the productivity of personnel responsible for auditing FTP usage to ensure compliance with company policy and external regulations.

Windows Interface

SENTINEL's Windows GUI facility simplifies interactive FTP usage data analysis. Summary and detail information can easily be filtered, sorted, interactively analyzed and printed. SENTINEL's Windows interface dramatically increases the productivity of personnel responsible for auditing FTP usage, safeguarding compliance with company policy and external regulations.

Custom Reporting

SENTINEL enables you to create custom report formats, focusing on FTP activity of particular interest to you. Custom reports can select and display filtered FTP activity in detail and summary format.

What are the Benefits Associated With SENTINEL?

Managing FTP resources efficiently, automatically and securely is a mandatory requirement for any Data Centre. SENTINEL facilitates this objective, and is a product that seamlessly and automatically delivers the following benefits:

- Monitors FTP usage throughout the entire Enterprise
- Integrates FTP activity throughout the Enterprise and associated automation efforts
- Provides sophisticated and interactive Windows based auditing of historical FTP usage
- Provides comprehensive user-defined escalation of FTP exceptions for existing automation solutions

Additionally, the dynamic SENTINEL Network Discovery tool provides an easy-to-use starting point for any Enterprise reviewing FTP usage, identifying environment size, assessing associated risk, and thus a "quick wins" based implementation plan!

Value-4IT Limited
7 Wright Road, Long Buckby
Northampton, NN6 7GG
United Kingdom
Tel: +44 (0) 845 0579386
sales@value-4it.com
www.value-4it.com

Dino-Software Corporation
P.O. Box 7105
Alexandria, VA 22307
United States of America
Tel: +1 703 768 2610
sales@dino-software.com
www.dino-software.com