FTP/Sentry™
FTP Auditing, Alerting and Automation

Lack of Breach Detection Tools

Many corporations would not even notice they have been breached because they do not have the tools or the processes to detect a breach.

In addition, even if they should become aware of a breach they would not be able to reliably determine exactly what information had been accessed.

Log Management Challenges

As few corporations have an enterprise-wide access log management policy, logs of data accesses are often not kept long enough to aid in a breach investigation.

Logs kept on individual systems are often worthless, as it is common practice for skilled intruders to cover their tracks by deleting or altering access logs.

Furthermore, having to scan through potentially hundreds of log files on each individual server for signs of a breach makes an investigation time-consuming, expensive and error-prone.

Management of Sensitive Data

The exposure to breaches is magnified exponentially when sensitive files remain exposed on servers longer than they need to.

As users often forget to delete their files, many breaches happen long time after a file was uploaded.

Most enterprises lack the FTP automation capabilities to determine which files do not belong on an FTP server and manage the file retention for files that have been successfully downloaded by the recipient.

Security and Controls

FTP/Sentry provides the controls to audit FTP activity as well as detect and investigate suspicious activity. FTP/Sentry ensures Audits and Breach investigations can be performed instantly and are accurate, comprehensive, timely and cost effective.

In addition, FTP/Sentry prevents breaches by detecting sensitive files not belonging on exposed servers and minimizing the time frame legitimate files reside on a server by removing them after a successful transfer.

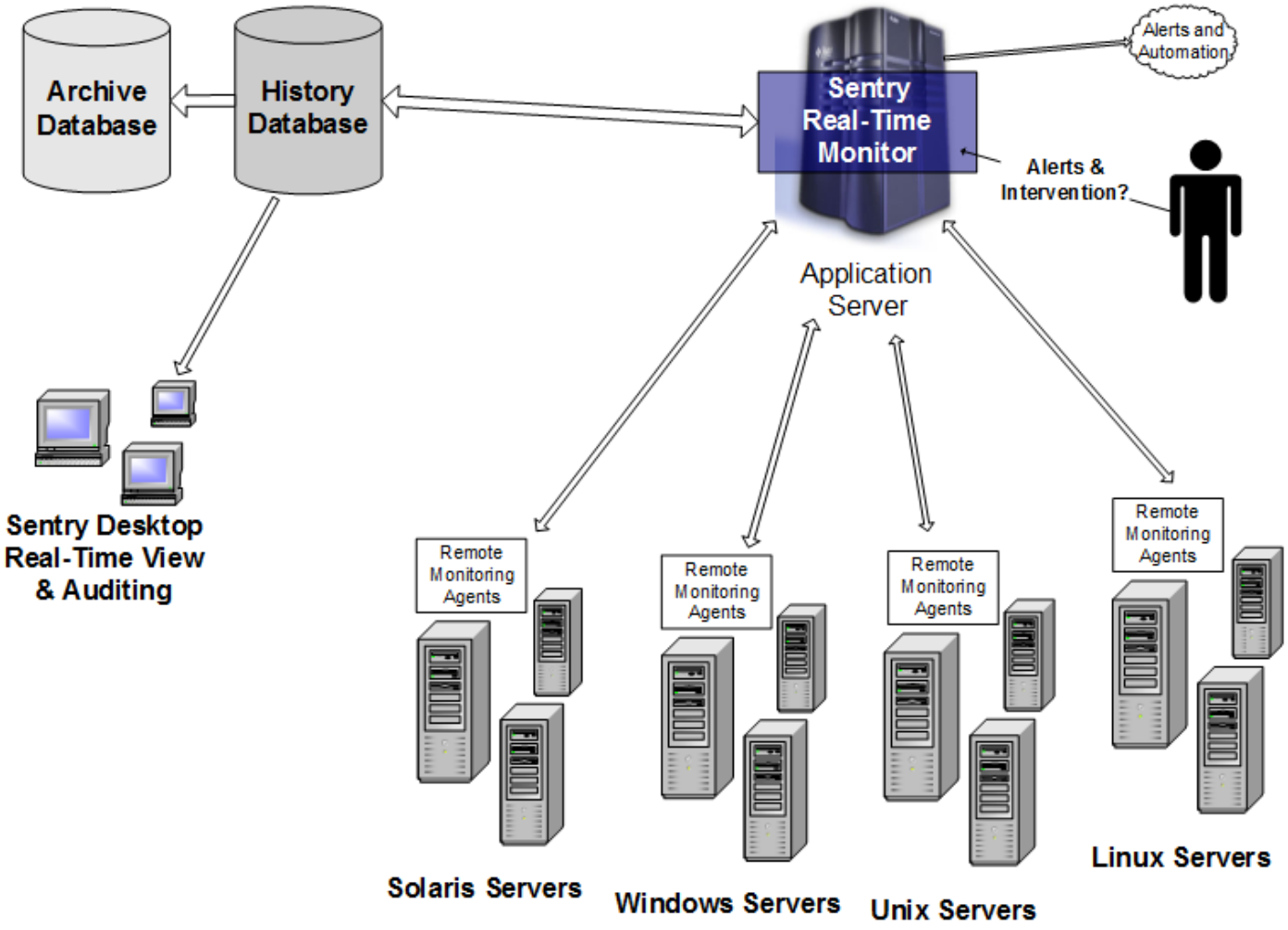
Breach Investigation

Breach investigations can be difficult, as often very little information is available. FTP/Sentry allows you to investigate a breach in several possible ways:

- **By Filename:** If you know that a given file has been accessed, FTP/Sentry will show you which ID accessed it when and from which IP address.
- **By IP address:** If you know an attack originated from a given IP address, FTP/Sentry will show you what files on which servers were accessed and when they were accessed.
- **By FTP Server:** If you know a given FTP server was breached, FTP/Sentry will show what files were accessed when, under which ID and from which IP address.
- **By Time Period:** If you know when an attack happened, FTP/Sentry will show you what files on which servers were accessed as well as which IDs were used and from which IP addresses they were accessed.

Phone: (678) 965 0885 · **Email: sales@ftpsentry.com** · **Web: http://www.ftpsentry.com**

FTP/Sentry™
FTP Auditing, Alerting and Automation



Remote Monitoring Agents are deployed on distributed platforms (Linux, Unix, Windows, Solaris, etc. as well as IBM z/OS Mainframes and provide real-time FTP usage data to the Real-Time Monitor.

FTP/Sentry's **Real-Time Monitor** interfaces with Remote Monitoring Agents to monitor FTP activity across the enterprise and records the activity in a secure location. It also monitors the health of the Remote Monitoring Agents and can generate an alert when an agent becomes unresponsive.

FTP/Sentry Desktop, a Windows application, can tell you **who** accessed **what** information **when** and **from where**.

The **Alert Center** allows you to define alerts for a variety of events including uploads of sensitive data, transfers to external, unknown destinations etc.

The **Automation Framework** enables you to initiate actions based upon events such as deleting files after successful download, notifying business partners of failed or interrupted file transfers etc.

Phone: (678) 965 0885 · **Email: sales@ftpsentry.com** · **Web: http://www.ftpsentry.com**

FTP/Sentry™
FTP Auditing, Alerting and Automation

Alerts

The Real-Time Monitor can generate alerts for any circumstance. For example:

- Alerts can be generated for uploads of sensitive data (identified by file name using pattern matching). This can be used to alert IT personnel of a potential exposure to prevent a breach.
- Alerts can be generated for transmissions of sensitive data. The criteria can be narrowed down to e.g. issue an alert when sensitive data is being transferred out of the corporate network.
- Alerts can be generated for failed FTP transactions (failed file transfers, logon failures, etc.).
- Alerts can be generated for specific FTP transactions, based on user-provided selection criteria .

Alert emails contain critical information about the FTP transaction, thereby enabling the email recipient to determine whether further action is required.

On z/OS platforms, alerts can also be generated in the form of WTO messages which can be monitored by a data center's console monitoring solution to integrate with data center automation efforts.

The alert for sensitive data transmissions contains the date and time the transaction started, the FTP action (upload, download, etc.), the User ID used to initiate the transaction, the file name of the file involved in the transaction, the local and remote IP addresses and an indication whether a secured connection was used for the transaction.

Benefits

FTP/Sentry ensures Audits and Breach investigations are:

Accurate: Performed using data stored in a secure location, so intruders cannot manipulate log files.

Comprehensive: They encompass all FTP Servers in the enterprise - including those which otherwise might not be included.

Performed Instantly: Audits and Breach investigations are easily performed without advance planning or notice to collect data and can therefore be performed instantly when suspicion of abuse arises.

Timely: In an Active Attack Scenario, seconds count. FTP/Sentry provides all information instantly.

Cost effective: Ensures Auditors and Breach Investigators do not waste costly time gathering data and sifting through endless log files.

FTP/Sentry helps reduce exposure and prevent data breaches by providing an automation framework capable of detecting uploads of sensitive files and removing files automatically after successful transfer.

More Information

Software Assist Corporation specializes in providing Security and Controls for responsible FTP usage to large and medium-sized enterprises. Our range of innovative software products helps customers worldwide become more secure, more compliant and more efficient.

For more information please contact us or visit our website.

Phone: (678) 965 0885 · **Email: sales@ftpsentry.com** · **Web: http://www.ftpsentry.com**