FTP/Auditor™

Find and mitigate hidden vulnerabilities

It has become common practice among end users to enable FTP on their desktops and department servers to share data with their coworkers. Freeware or shareware FTP servers can easily be downloaded from the internet if FTP is not already installed on the system. Most users have no idea of the security exposure they create when FTP is enabled without the knowledge of, or consent from, corporate IT..

Best practices for configuring and securing FTP are hardly ever followed, creating gaping holes in corporate security that will not be addressed unless IT staff happens to stumble across such a system.

Why are unauthorized FTP Servers a problem?

The very purpose of enabling FTP on a server is to serve all of the data it can access on a silver platter to anyone that connects to it. Many FTP variants by default allow full access to anyone (a feature called Anonymous FTP) regardless of who the user is or where the user is accessing the server from.

Anonymous FTP

Anonymous FTP is a very convenient way to make data available without having to maintain a burdensome list of user IDs and passwords. The trade-off, however, is that you need to keep a close eye on how it is being used and what data is available for download. Anyone with network access can log onto a server that supports anonymous FTP and download any of the files that are available on the server. In some cases, these same people can upload data to the server and the uploaded file will be available to anyone.

Any server that supports anonymous FTP requires a higher level of care and monitoring to ensure that no sensitive or protected data resides in the folders that are accessible by the server. If uploading is allowed, further monitoring must be performed to ensure that no sensitive or protected data is uploaded to the server's folders.

How FTP/Auditor Can Help

Few companies have any idea of which of their servers have FTP enabled, where they are located and what data they make available to users inside and outside of the company. The first step in getting control over FTP usage is to locate and evaluate the servers in your network that are running FTP.

FTP/Auditor enables you to:

- Locate and identify all FTP enabled servers in your network regardless of platform
- Determine how FTP on these servers is secured
- Evaluate their purpose and contribution of FTP usage to the business
- Ensure FTP usage that serves the business is properly secured
- Ensure FTP usage that does not contribute in a meaningful way to the business is disabled and stays disabled
- Protect your company from costly and embarrassing breaches of sensitive corporate or customer data.

Conduct regular, automated Scans

Maintaining network security requires constant vigilance. Many of our customers detect new FTP-enabled servers in their network every week.

To ensure consistent ongoing network security, FTP/Auditor can be set up to run at regular intervals and email the scan results.

New risks will be brought to your attention without any effort on your part. This allows you to evaluate them in seconds and decide whether to disable or secure FTP appropriately, depending upon business needs.

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