

Going Beyond Standard Windows Auditing and Logging

As regulations regarding auditing and logging become increasingly complex, network activity monitoring – for both users and administrators – becomes even more business critical. With this innovative landscape, new requirements have become apparent:

- Auditing every single action performed in the computing environment provided by a company.
- Archiving all user actions for later playback and review.
- Assuring collected information is valid, complete, and securely stored.
- Solutions must be reliable to ensure all activity is captured.
- Solutions must be easy to deploy and cost effective.

Traditional tools may address some of the above requirements but in today's ever-changing landscape, such solutions have proved not to be adequate. In the wake of federal rule changes that clarify the requirements to produce electronic evidence in lawsuits, the demand for solutions that help companies track and search their electronic data is growing. In this whitepaper, we take a deeper look at auditing and logging, the current options, their drawbacks, and a new complementary way of addressing today's security issues.

Introduction to the Problem

Auditing and logging users and their activities has become extremely important, especially in lieu of regulations such as Sarbanes-Oxley, HIPAA, and others.

The benefits of having an auditing and logging solution in place are obvious but not always easy. Some benefits include assistance in abiding by industry regulations; offering a clear view of network activity; detecting and preventing intrusions; supplying evidence during litigations; and much more. Sarbanes-Oxley, HIPAA, and other regulations

Did you know?

On December 1, 2006, the US Supreme Court ruled that companies must keep all employee e-mails, instant messages, and other electronic documents as possible evidence to present in court if necessary.

impose stiff penalties on companies who fail to ensure the accuracy, security, and confidentiality of their data. In addition, companies can also be penalized for destroying or altering company data. These regulations continue to change and new ones arise, causing additional rules for companies to follow and add to their security policies.

On December 1, 2006, the US Supreme Court ruled that companies must now

It could be your company...

Some companies have paid a steep price for failure to preserve electronic information. In one high-profile case in 2005, former UBS AG equities trader Laura Zubulake won a \$29 million award in a federal gender discrimination suit. The presiding judge penalized UBS for failing to recognize that missing e-mails would end up being relevant to future litigation.

keep records of all electronic information generated by their employees. This is part of an amendment to federal regulations governing civil litigation and was approved by the Supreme Court's administrative arm in April 2006. This ruling makes it more important than ever, for companies to know what electronic information they have and where it is stored. In some cases in order for electronic files to hold up in court, companies may be required to assure the files have not been tampered with and that they were securely stored.

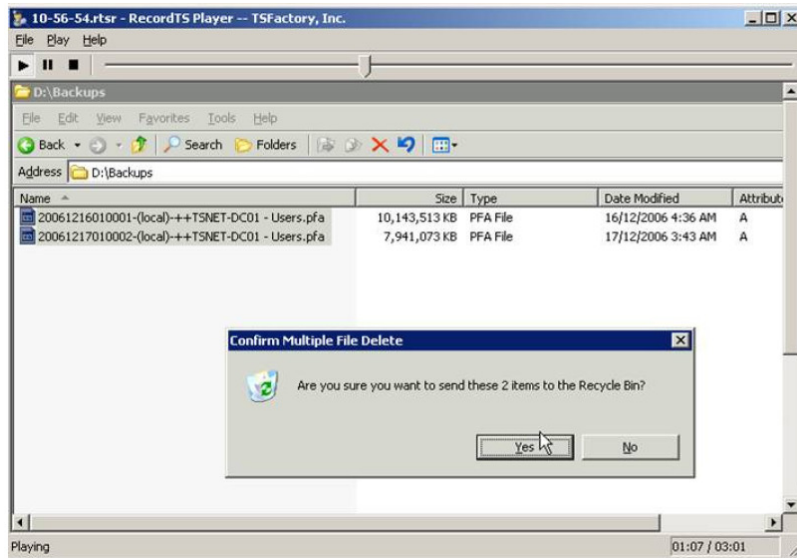
This illustrates how critical recording and auditing user activity has become and how companies now need a quick and easy method of retrieving all user activity.

A Preferred Solution

There are many solutions available to help network administrators with auditing, security, and compliancy. Some are even part of the standard Windows operating system. However, as the IT landscape becomes more and more complex, and regulations for companies rise, the traditional way of extracting the relevant information has become time consuming and complicated.

One novel solution now available is TSFactory's session recording tool called RecordTS. RecordTS acts as a Terminal Services or Remote Desktop "security camera", allowing network administrators, managers, or C-level executives to see exactly what happened on a company's server for a specific user. RecordTS can be used to monitor everything users and administrators are doing when connected to a Terminal Server or any Windows server accessed remotely using the Microsoft Remote Desktop Client. RecordTS shows the recorded information in a compact video file with options such as fast forward, rewind, and more. These individual 'video' files can be played back at any time or simply stored in a secure location (locally or externally) for auditing or security purposes. In

addition, the recorded files can be digitally signed to prevent tampering.



Problem Resolution

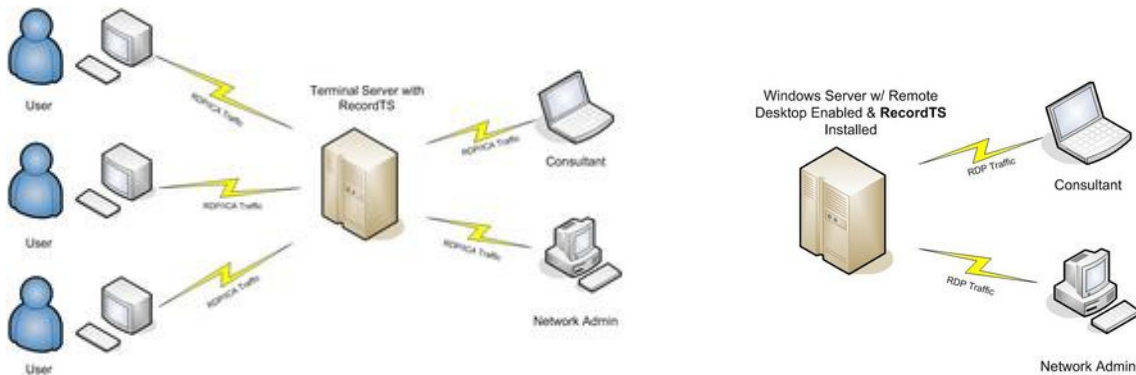
Instead of sorting through hundreds of entries in an event log, RecordTS allows network administrators to simply watch a video file illustrating exactly what a user saw on their screen, including mouse movements, errors, etc. This allows network administrators to see every action that lead up to a problem. Traditional tools require lengthy reviews of event logs to get this information, which does not always work since not all user actions produce event logs. With RecordTS, it is just a matter of locating the appropriate recorded file and playing it back. Administrators can also use RecordTS Event Stamps™ to show a timeline of events before watching the recorded session, therefore jumping directly to the relevant point in time when a specific action occurred.

TSFactory provides an application programming interface (API) that allows third party vendors and customers to integrate RecordTS with their existing solutions. This API can be used to trigger recording to take place only when needed. For example, RecordTS can be set to record once a user's phone is answered, providing great visual monitoring of the user's desktop and network activities while assisting a customer. This API makes it easy for companies to incorporate RecordTS with their existing infrastructure, allowing IT staff to focus on the business needs rather than technical issues.

Key Differences

Although there are many screen recording solutions available in the market, none of them were designed specifically for Terminal Services and its unique scalability requirements. Many of these tools were developed primarily for the desktop market. The issue here is when used on a Terminal Server running 50 user sessions, desktop solutions quickly overwhelm the system to the point where the server becomes unusable. This proves they are not a viable server based computing solution.

On the other hand, RecordTS runs as a Windows service, simultaneously recording any number of user sessions without affecting the end user's perceived performance. RecordTS is a unique server based solution because it works directly at the protocol level. It currently supports recording Microsoft RDP, Citrix ICA, and due to its modular design, it can be easily changed to support additional protocols such as VNC and others. When compared to other available screen recording solutions, RecordTS requires very little overhead and provides the performance necessary for an enterprise system. With the addition of Enterprise Manager, it is possible to manage 1000's of recording agents across a large network. Recording files can be automatically moved from the servers to back up storage for safe keeping and later session replay. A web console is also included to allow remote viewing of recorded sessions and provide advanced search and reporting features. It is also possible to record Windows servers and workstations to monitor what consultants are doing while remotely logged into your servers and employees that work from home or are on the road and remotely log into their office workstations.



Conclusion

Thanks to growing regulations regarding electronic evidence, auditing and logging user activity has become extremely important. Some reasons for this include confirmation that users are being ethical with company data, civil litigation protection, and assurance that information on a company's network is secure. Regardless of your company's size, and what your specific compliancy requirements are, it is critical to gather as much information as possible concerning the activities taking place on your network.

Solutions on the market today assist with auditing, security, and compliancy but individually do not provide the whole picture. Many only extract the information they feel is relevant and do so in a challenging way. This causes network administrators to spend valuable time piecing together information in order to see exactly what occurred. A new complementary way of addressing these issues is with a visual recording solution such as RecordTS. RecordTS is the only available solution that will easily allow you to gather information concerning users and their activities. The information gathered will assist in preserving critical electronic information that may prove to be invaluable should future litigations take place. RecordTS is extremely simple to install, use, and integrate with your current auditing and security tools. Given its affordable price, it provides an easily justifiable ROI (return on investment).

About TSFactory

TSFactory LLC is an established international software development company located in Raleigh, North Carolina. TSFactory has goals to develop easy to use and affordable solutions completely focused on Terminal Services and its add-ons. TSFactory products are used in production on thousands of servers around the world. For more information about TSFactory or their products, please visit their website at <http://www.tsfactory.com>.