

Tembria White Paper

Agents vs. Agentless Monitoring

Abstract:

Many server monitoring solutions require that you install “agents” on the machines that are being monitored. This whitepaper explains why, in the current security environment, agents introduce unacceptable risks and how Tembria Server Monitor avoids them all with its 100% agentless monitoring approach.

Agents vs. Agentless Monitoring

We often get questions about how Tembria Server Monitor works, compared to other products in the same market. The primary difference has to do with our agentless monitoring engine whereas other products tend to rely on agents. Other vendors will try to coach you, telling you that agents are a necessary item for server monitoring. We strongly disagree. This whitepaper gives four good reasons why agents are a bad thing and explains how Tembria Server Monitor's agentless monitoring engine avoids of them.

What are Agents?

Some network and server monitoring solutions use what are called "agents" in order to get values from the machines they are monitoring. Agents are programs that run on the remote machines and communicate the main monitoring system. Some vendors try to hide the fact that they use agents. They'll say things like they "deploy" to remote systems or use other terminology but it all boils down to installing custom software on the remote machines.

Problem #1: Interference

The agent software runs on the remote machine and therefore affects its operation. In many environments, especially government and larger corporations, you simply can't go installing software on critical machines without going through an arduous evaluation and approval process. Even if you have complete control over your machines, before installing agents you need to verify that they don't conflict with other applications running on the system, use excessive memory, use excessive CPU, generate port conflicts, etc.

Problem #2: Shoddy Agents

Installing agents on remote machines has the potential to open them up to security vulnerabilities. The agent is running on each remote machine and needs to do things like read security logs, check files on disk, monitor processes, etc. It needs administrative privileges for many of its operations. Unless the agent software has been very carefully developed and is using high-grade security technology, there are serious security questions that need to answered.

Problem #3: Long Term Maintenance

Agents are hard to maintain. As the monitoring solution is updated, the agents will need to be updated from time to time. Vendors will tell you that it's an easy process but in practice it often is not. If you have a large number of systems, some of them might not be available when it's time to upgrade and then they're running outdated versions. Agents might be hiding on VM images that were down when the upgrade was done and only come to life days or weeks later. Over the course of few updates you end up with a mess of different agents on different machines.

Problem #4: Bypassing Network Security

This is the most severe problem with agents: Agents bypass your network security configuration. Vendors will often ask you to open up a particular port so that the monitoring system can communicate with the agents. Once the port is open, the information starts to flow. Data about CPU and disk usage may be innocent enough but when it comes to event log records, log file contents and security events, it's important to respect network security policies.

So Why Do So Many Vendors Use Agents?

So why do so many vendors use agents? They do it because it's easy. It gives them a clear pipeline right into the remote machines and they don't have to worry about security configuration, firewalls or any of the other rules that are in place.

The Benefits of Agentless Monitoring

So how is agentless monitoring different? We never install anything on the machines that we monitor.

Tembria Server Monitor uses standard protocols to do all of its monitoring and the big benefit is that when it comes to your security configuration, we're playing by the rules. You can be confident that nothing has circumvented your domain policies, firewall rules and other security measures.

Our commitment to agentless technology certainly makes for a lot more work for us, especially as each new version of Windows introduces enhanced security, but we think that the benefits to our customers are obvious.

For More Information

For more information about Tembria Server Monitor and agentless monitoring, visit our web site at <http://www.tembria.com> or give us a call at 1-866-552-0049.