



## EventTracker Agents Frequently Asked Questions

© Prism Microsystems, October 2009

### **Does EventTracker require an agent to monitor logs?**

EventTracker is an agent optional architecture and supports both agent and agent-less collection of logs. It is your decision to use either model.

Optional agents are available for Windows and Checkpoint.

No agent is needed for Cisco, AIX, HP-UX, Linux or generic Solaris.

No agent is needed for SNMP devices.

No agent is needed for any device generating events in the syslog format (UDP or TCP).

Agents are required for Trusted Solaris (BSM), IBM iSeries and z/OS Console, WTO messages and SMF records (Top Secret and RACF).

### **Why do certain platforms have agents and others don't?**

Agents may or may not exist for a number of reasons. In the Unix/Linux world, Syslog provides a real-time ability to collect logs. You can send Syslog via UDP or TCP to multiple listeners. On Microsoft and certain other technologies this capability is not provided. On Windows, for instance, the only way to collect the event logs is to poll the system on a periodic basis. This mechanism is generally not real-time, and often is more resource intensive (and potentially insecure) than the agent route. If multiple applications are polling the event log this can become a problem. The result is that on Unix/Linux Syslog generally obviates the need for agent technology; however on Windows it is far more common and beneficial.

An agent can also provide additional benefit through being capable of monitoring conditions that typically do not appear in the event log such as CPU or disk space usage. One particularly powerful feature that the EventTracker Agent provides on Windows is the capability to monitor USB storage devices. A simple insert or removal generates an event to the Windows event log, but the EventTracker Agent goes well beyond that and can apply rules disabling the device instantly to prevent unauthorized access, or it can catalog everything that is copied to and from the device. The information logged provides the device serial number and type, the user, time, and a complete history of every file copied to and from the device. EventTracker Windows Agents provide significant monitoring capability beyond simple log monitoring

Another reason for an agent is if the log format needs to be translated from the native format prior to transmission. On IBM z/OS or Trusted Solaris for example, EventTracker utilizes an agent to extract SMF data and format the entire event into a syslog compatible format.

### **Can I install agents on only selected machines with others agentless?**

Yes. You can install agents on selected Windows machines leaving others to be agentless. Any/all combination(s) is supported.

### **Isn't it always better to have no agents?**

Not really. The Agent model offers a number of outstanding benefits which are simply not available in any other way. These include:

- ✓ Reporting to multiple Consoles
- ✓ Granular at-the-source filtering
- ✓ SID translation
- ✓ Performance threshold monitoring
- ✓ Detection of install/uninstall of software
- ✓ Endpoint security monitoring of devices such as USB
- ✓ Service monitoring
- ✓ Native log backup
- ✓ Runaway process detection
- ✓ Network traffic monitoring
- ✓ Monitoring of application logs
- ✓ Change Auditing

On the other hand, agents must be deployed, configured and do take up some computing resources. You should decide based on your business requirements as opposed to accepting a single one-sized fits-all approach.

### **Why do some vendors insist that '*agents are evil*'?**

It is generally good to look deeper at blanket statements such as that. Perhaps their agent technology is not really theirs? Perhaps it's a weakly supported open-source project? Perhaps they have no agent distribution method – forcing you to manually distribute agents? Perhaps there is no central place to configure these agents?

Agent technology per-se is neither always desirable nor always bad. Like most other choices, they represent certain values/advantages at a price.

You should independently decide if they are worth it, in your situation.

### **In my organization, getting permission to install agents is very hard (politics). Am I not better off with an agentless solution?**

Perhaps. Only you can know the correct answer. According to Forrester Research, even if a solution does not require an installed agent, it usually requires a privileged account or configuration change. This is likely to be just as difficult.

## **Which is better for me, agent based or agent-less?**

It depends on your situation.

If the following requirements apply to you, then consider agent technology:

- Windows based but use distributed topology without Domains
- Requirement for real-time event collection
- Need to monitor application logs
- Need for performance/application/service/process monitoring
- Need for endpoint (USB, writeable CDROM) security monitoring
- Need for network traffic monitoring

The agent-less option may be better if:

- No requirement for real-time data collection
- Topology is all syslog or Windows Domain based
- No requirement for the other features described above

Here is a real-life example of the benefit of an Agent. You are using your Log Management solution for host-based intrusion detection. On Windows you set up a polling mechanism to access the Event Log on a 10 minute basis, if your system is hacked in the interim the first thing a hacker will generally try to do is compromise the event log to cover their tracks, With an agent, the events that indicate an intrusion has occurred are already gone to a secure control location before the hacker has any chance to tamper with them. In this case the polling mechanism increases your risk profile, and often increasing the polling frequency simply increases the performance impact on the monitored machine.

## **What is the impact of your Windows agent on my server?**

Virtually zero. Your servers are meant to serve their primary function not log management. Here are some measurements to consider:

Configuration (low end workstation): 1GHz CPU, 256MB RAM, 100 GB disk  
Total events: 10,000/day

CPU utilization: 0.0015% (2.2 mins in 24 hours)

Peak Memory: 6Mb

Network traffic: 15Mb/24 hours

## **Is your Windows agent logo certified?**

EventTracker v6 was tested with the WWT Tool provided by Microsoft (Works With Windows Vista). Prism Microsystems, Inc. is a Microsoft Gold Certified Partner.

## **How do I distribute and manage agents?**

The System Manager application (launched from the EventTracker Control Panel) is used to distribute Windows agents from a central location. It adheres to Microsoft requirements for security and requires the user to provide suitable credentials.

Agents can be installed, removed, upgraded and configured in either bulk (groups) or one-by-one. A scripting interface to distribute agents is also available.

The Trusted Solaris agent is packaged as a self contained pkg file and is installed traditionally.

### **How long has your agent technology been deployed?**

Our Windows agent has been in production since 2001. It is installed in more than 600 locations worldwide.

Our Trusted Solaris agent has been in production since 2003 and is in production at many US Department of Defense locations.

### **Who uses your agent technology?**

Since 2001 major corporations worldwide have deployed our software on mission critical servers. We can provide references in all vertical segments including Financial, Government/Military, Healthcare, Manufacturing and Education.

A Prism Representative will be happy to provide relevant references.