



Requirements for Virtualized Systems

Log Management RFP

Required Feature	Value of the Feature	Additional Explanation
End to end encryption-client to hypervisor	Transactions are encrypted from the client to the monitoring and logging software through to the hypervisor and during return	This feature insures there are no "holes" where an unencrypted transaction can be intercepted. In addition this feature must be automated so it is easy for an administrator to set up for hundreds of virtual machines. This is also required for complete forensic understanding of commands to power on, power off, reset, provision or otherwise configure a virtual Machine. Most regulatory requirements define logged and audited command, control, configuration and changes be completed as a compliance requirement. Without encrypted paths for information, passwords and other critical information might be intercepted producing serious security issues.
Ability of product to see every transaction and interaction with the virtual machine.	There is a requirement to know what anyone who touched a virtual machine did---powering off, on, creating events, etc.	This provides forensic understanding to potential production application outages, machine outages due to human error or intentional failure due to security breach. Additionally, logging and reporting on many of these transactions is required for regulatory compliance.
Ability of product to log virtual machine during "single user mode"	Virtual machines can be placed in single user mode to apply patches or updates. During that time, there may be access and intrusion that is unlogged. Such access must be recorded even through the operating system or network or security tools have been rendered inactive.	This is in direct response to the growing threat of the insider criminal who is stealing corporate information or inserting malicious software. For an outsourced services company, this insures that they can demonstrate that they did not insert malicious software or download information. This requirement also provides complete understanding of changes related to vendor software maintenance, patch installation and application or hardware configuration. Logging of this information is often required for complete regulatory compliance.
No agents on the hypervisor or virtual machines	There will be hundreds of virtual guest machines running and agents which are software programs will require massive amounts of physical updating, configuring and expense. In addition, agents are major performance hogs. They generally invalidate the warranty of the hypervisor vendor and are unsupported as well.	Agents by their very nature are invasive and may change the environment in which they are operating. They are to be avoided.
Direct connection to virtual console	The product is required to have direct connection to the virtual console port in order to be able to turn machine on/off when there is a problem with the O/S or hypervisor. Critical forensic understanding of root cause messages related to security events, application failures, operating system failures and other events are captured from the console of the virtual machine - much like the physical machine.	These messages are not generally sent over the network via SYSLOG or SNMP as they are generated after the network is inoperable and the source of the event or message is unable to rely on a functioning network or IP stack to transmit the message. Logging of transactions with the virtual console is part of a complete regulatory compliance solution.
Direct connection to the hypervisor	Hypervisor connection ensures closed loop log management--remediation of log related problems and real time log management	When a log event is detected, it may need to be remediated. In order to do so, one must have connection to the hypervisor in order to remediate it.
Hypervisor remediation after logging	When a problem is detected on a hypervisor, the product should be able to identify the problem, suggest remediation techniques consistent with vendor published standards and offer remediation.	This provides industry standard and business critical information relative to the quick and consistent resolution to a problem. As a part of identification and remediation - logging of the remediation activity is then associated to the event such that when it occurs again - the activity is also part of a resolution solution. Logging of remediation efforts including identification of the person performing remediation is often required for regulatory compliance.



Requirements for Virtualized Systems

Log Management RFP

Required Feature	Value of the Feature	Additional Explanation
Web based remote connectivity	Product must enable customer to log on from anywhere and see logs and events and remediate problems.	This capability also provides for secure, authenticated quick response to events detected in the IT infrastructure.
Role based security	Roles must be easily designated and easy to use	Separation of duties is often required for regulatory compliance. A clear separation of roles and associated privileges is required.
Move log files with virtual machine move	When a virtual machine moves from one physical location, the log files and all forensics must move with it.	
Central logging across enterprise	The logging system must log virtual systems, networks, infrastructure devices throughout enterprise and store data in central repository	
Logging of non IT environments	Telephone switches, Security, Power Distribution Units, Air Conditioning/Environmental, SCADA devices and other non IT devices must be logged at all times.	
Log files must contain sub-second timing with ability to interlace multiple log sources based on timestamp	The logging solution should allow the ability to interlace multiple log files for forensic study based on sub-second timing so that true forensic analysis of a business impact or outage can be understood across the infrastructure.	For instance - did a high humidity problem cause a power distribution unit to provide improper power to a device causing it to have power supply failures, resulting in the remaining power supply being overloaded which caused fan failures, improper temperatures and ultimate failure of a operating system, application and underlying hardware.
Log files must be searchable by third party applications and tools	Log files should be in a form easily usable by third party applications, for reporting, distribution and other solutions critical to business activity or compliance regulations	
Log files must be kept with a "Chain or Custody" requirement in mind.	Log files should be unable to be modified, proved they are original and kept in original form.	Compliance with regulations of course drives this, but should an event become part of litigation, proof that log files have not been modified can become even more important.
Log files should be stored in a manner that allows the log file to be digitally secured in a manner that identifies which parts of a log file are original and which parts were modified or not original.	This provides a true and easy understanding of what areas or lines in a log file were specifically changed or modified as well as what parts of a log file are still valid and accurate.	Compliance with regulations of course drives this, but should an event become part of litigation, proof that log files have not been modified can become even more important.
Fill virtualized logging gaps from traditional logging systems	Traditional log management systems do not log the virtual environment.	Must be able to offer all the functionality of leading log management systems for the virtual environment.