

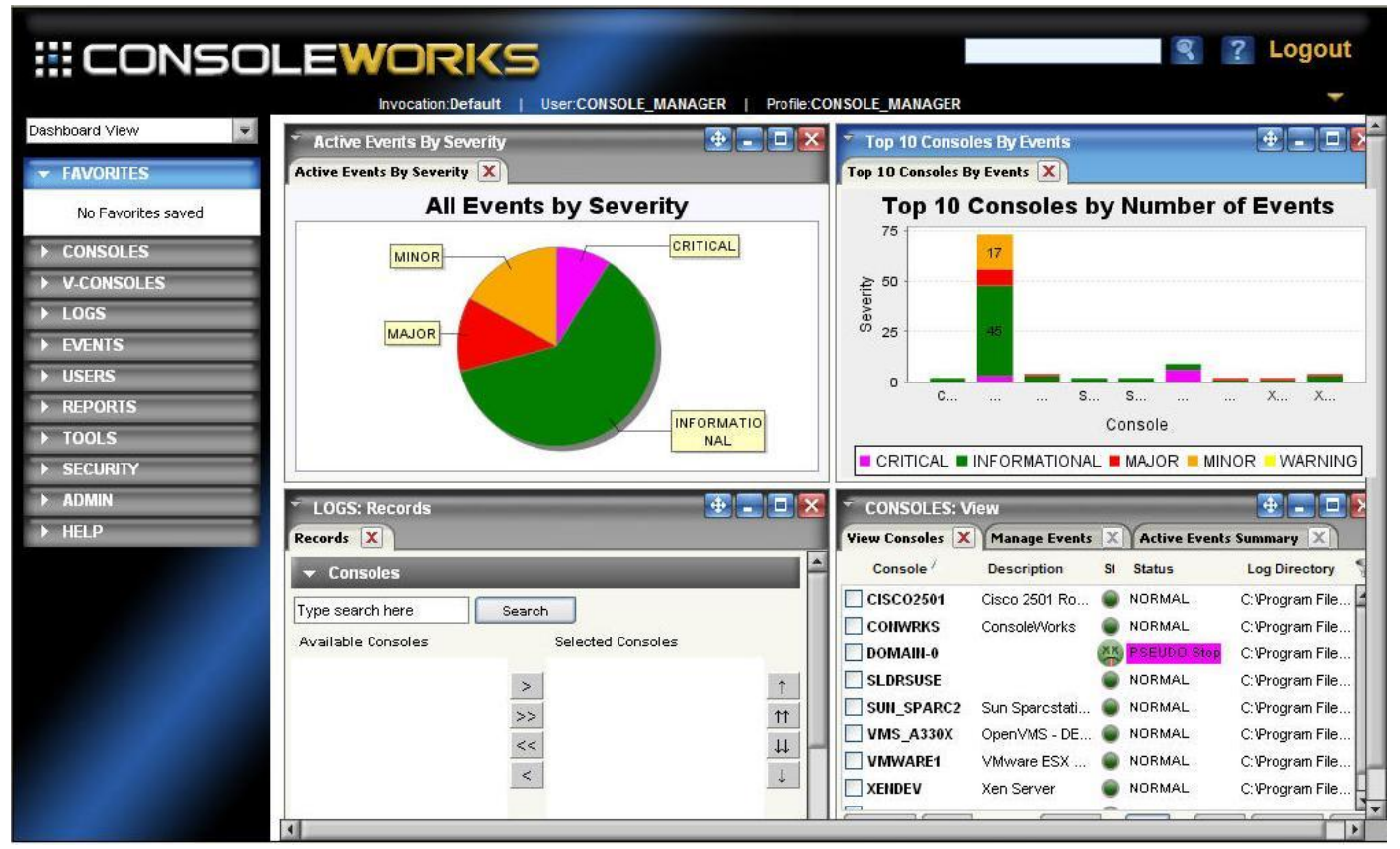


Automated Virtualized Systems Management Product Description

VIRTUALfx

TDI's VIRTUALfx technology logs, monitors, manages and remediates problems in a virtualized infrastructure. It does so for VMware or XEN hypervisor systems today and will add more vendor technologies as they are more generally accepted.

ConsoleWorks Dashboard View



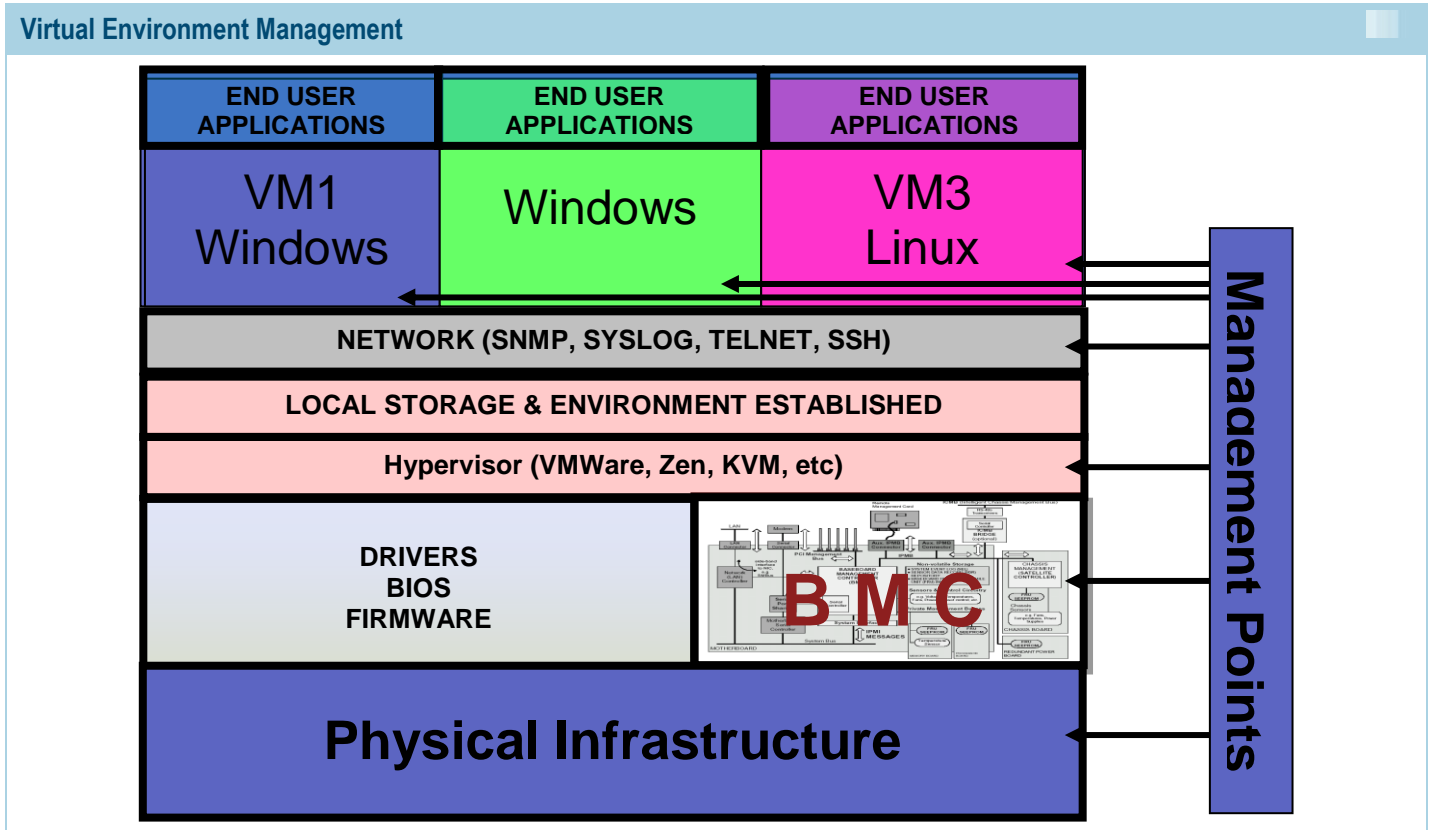
VIRTUALfx is built on TDI's Consoleworks' well proven, mature business critical infrastructure management technology which provides well understood management and remediation of physical infrastructure. Combining these technologies provides the user with a mature, single solution to monitor, manage, log and remediate the virtual and physical environment within the same solution.

Management of a virtual environment consists of four primary disciplines:

1. One must consider the virtual guest machine
2. Underlying hypervisor
3. The physical machine the hypervisor runs on and
4. The physical infrastructure the physical devices to which the machine is connected and dependent.



VIRTUALfx interfaces with, understands and controls all four disciplines so a virtual machine can be managed, logged, monitored and remediated enterprise-wide. Having well understood logging, management and remediation capabilities across the total environment is critical to providing security, logging, management, remediation and visibility to the virtualized environment.



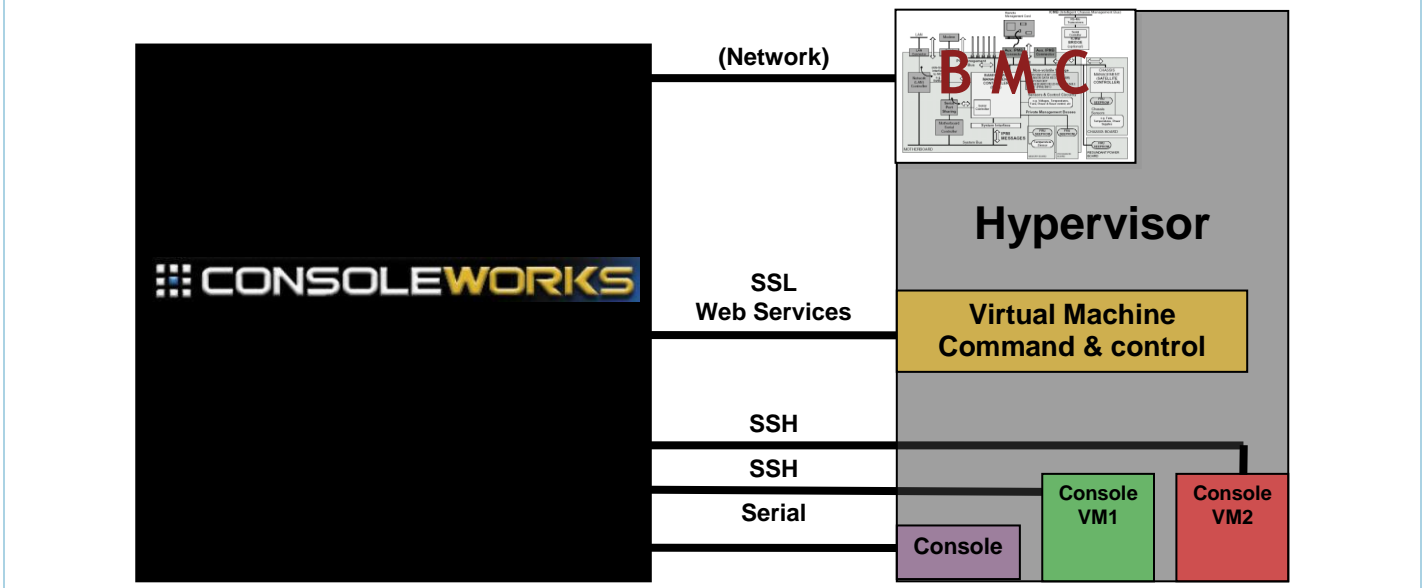
AGENTLESS MONITORING

Problem: In a virtualized paradigm it is often difficult to determine if someone has modified the virtual environment because virtual machines are like black boxes. There is limited monitoring and managing capability and no logging solutions. Users wishing to install third party solutions for security, logging and monitoring often void their performance and availability guarantees.

Solution: VIRTUALfx connects to the virtual console, the physical console and to the hypervisor with an agentless, low footprint connection to gather information such as machine state, power on/off process messages, operating system boot process messages and operating system console messages thus providing a complete record of all events surrounding the creation and operation of a guest virtual machine and its physical environment.

Thus Virtualfx installs quickly, requires no ongoing management as do agents, and requires no specialized agent skills and none of the costly maintenance for specific agents.

Hypervisor Monitoring



HYPERVERSOR MONITORING

Problem: In a virtual environment the hypervisor is the underlying life support system for all running virtual machines. If the hypervisor goes down, is hacked or has a problem, many virtual systems and associated applications are impacted. Thus, one must know and understand what is happening on the hypervisor at all times, see when it may fail, monitor its associated resources like storage and remediate a failure when one happens. It's also important to understand, log and potentially control all hypervisor command and control messages.

Solution: VIRTUALfx monitors the hypervisor directly and each of its guest operating system instances as well. VIRTUALfx understands and monitors the hypervisor, each guest and all associated devices like storage. Understanding and logging hypervisor control commands, guest machine operating states, security and other event messages is critical to virtualized infrastructure management. VIRTUALfx collects events such as:

- Who connected to where
- What commands were issued
- Password changes, security events
- State changes, stop, start and restart
- Machines added or removed

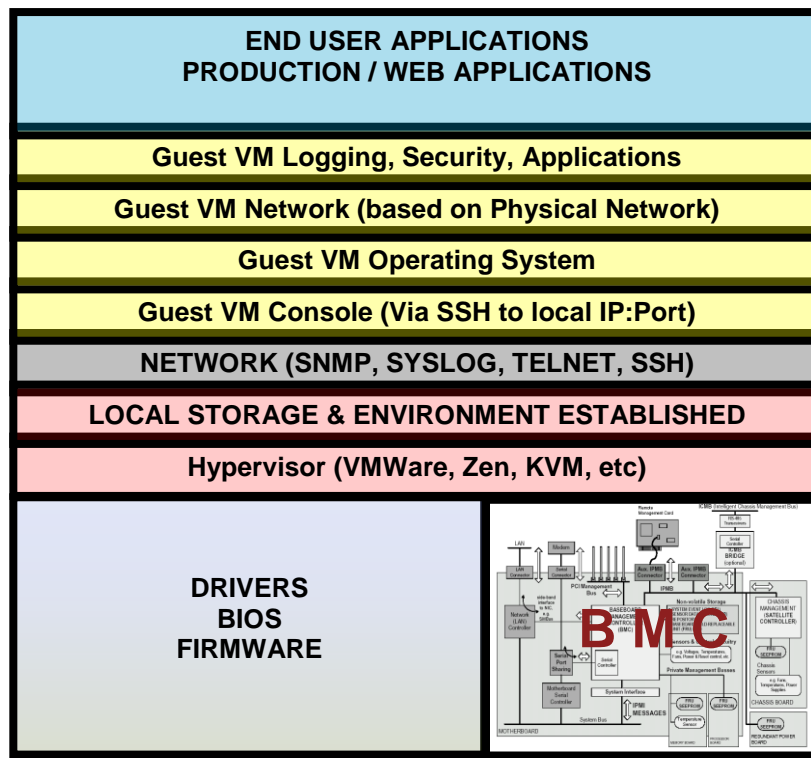
VIRTUAL GUEST MONITORING

Problem: Virtual machine guest systems often live in groups of hundreds or thousands. Managing them from a central location, across multiple virtual architectures (VMware, XEN) is difficult at best – never mind the physical infrastructure environment it takes to support all the virtual machines.

Solution: VIRTUALfx actively manages a guest virtual machines' life cycle from a central window. Common tasks can be centralized for all virtual systems, regardless of their vendor (VMware or XEN). VIRTUALfx enables the user to:

- Provision
- Power off
- Power on
- Restart
- Virtual machine console connections

Virtualization Implications – VM Monitoring



VIRTUAL LOG MANAGEMENT

Problem: While a virtual machine may contain traditional logging solutions within it, they are often impacted negatively in the virtual world as their ability to understand logging messages around performance is often broken creating multiple false alerts.



This is because the physical environment is often changed and impacted as virtual machines are moved; additional virtual machines are added to the same physical machine and as other virtual machines' applications place demand on the physical CPU, memory and network resources.

Compliance regulations demand the underlying heart of virtualization must also be logged because it is often impacted by administrators as they make changes to accommodate physical load requirements in the virtualized world. When an administrator moves virtual machines, stops or starts virtual machines, all the command and control as well as configuration messages occur at the hypervisor level – which is not seen from within the virtual machine environment by the traditional logging solutions.

As a result, security, compliance and root cause forensic understanding of environmental impacts is missed by traditional solutions. There are compliance gaps.

Virtualized systems often move from one physical machine to another. What happens to their underlying status log files generally kept by the hypervisor itself? They are left behind. Thus there is no continuous log file related to the health, configuration and changes related to the specific virtual machine. This creates problems with compliance, security, configuration, performance and forensic understanding of events related to the virtual machine.

Solution: VIRTUALfx not only logs virtual systems, applications and other traditional logging tasks without any agents: it also logs the underlying hypervisor activity relative to the virtual machine as well as the physical machine the hypervisor runs on. It connects directly to the virtual console and to the hypervisor and collects information not available to traditional logging systems.

As an example:

```
sldrsuse on vmware.eng.tditx.com in ha-datacenter is powered on
vmkernel: 13:22:19:09.131 cpu3:1036)World: vm 1171: 895: Starting world vmware-vmx with flags 4
vmkernel: 13:22:19:10.014 cpu3:1171)World: vm 1172: 895: Starting world vmm0:sldrsuse with flags 8
vmkernel: 13:22:19:10.014 cpu3:1171)Sched: vm 1172: 5352: renamed group 31 to vm.1171
vmkernel: 13:22:19:10.014 cpu3:1171)Sched: vm 1172: 5366: moved group 31 to be under group 15
vmkernel: 13:22:19:10.016 cpu3:1171)Swap: vm 1172: 2169: extending swap to 2097152 KB

vmkernel: 13:22:19:10.025 cpu3:1171)World: vm 1173: 895: Starting world vmm1:sldrsuse with flags 8
vmkernel: 13:22:19:12.227 cpu1:1171)VSCSI: 4059: Creating Virtual Device for world 1172 vscsi0:0 (handle 8206)
vmkernel: 13:22:19:31.029 cpu2:1173)VSCSI: 2803: Reset request on handle 8206 (0 outstanding commands)
vmkernel: 13:22:19:31.030 cpu2:1056)VSCSI: 3019: Resetting handle 8206 [0/0]
vmkernel: 13:22:19:31.030 cpu2:1056)VSCSI: 2871: Completing reset on handle 8206 (0 outstanding commands)
```

The example above shows the results of starting, renaming and moving a guest VM and powering it off again. It also demonstrates the underlying information about the VM not being captured by traditional logging solutions limited to only the guest VM.

When virtual guests move, VIRTUALfx maintains a single log file for a specific virtual machine/guest operating system instance. As it moves from one physical environment to another, it is tracked by VIRTUALfx resulting in a continuous single log file maintained through the Guest Virtual Machine. One of the many benefits of a continuous log file for the guest VM is compliance. However, should something happen to the application in the Guest VM, a set of log files related to the application, Guest Operating System in the VM, the Guest VM itself, the hypervisor and the other physical infrastructure supporting the application, can be quickly and easily accessed, reviewed, integrated and interlaced for forensic analysis.

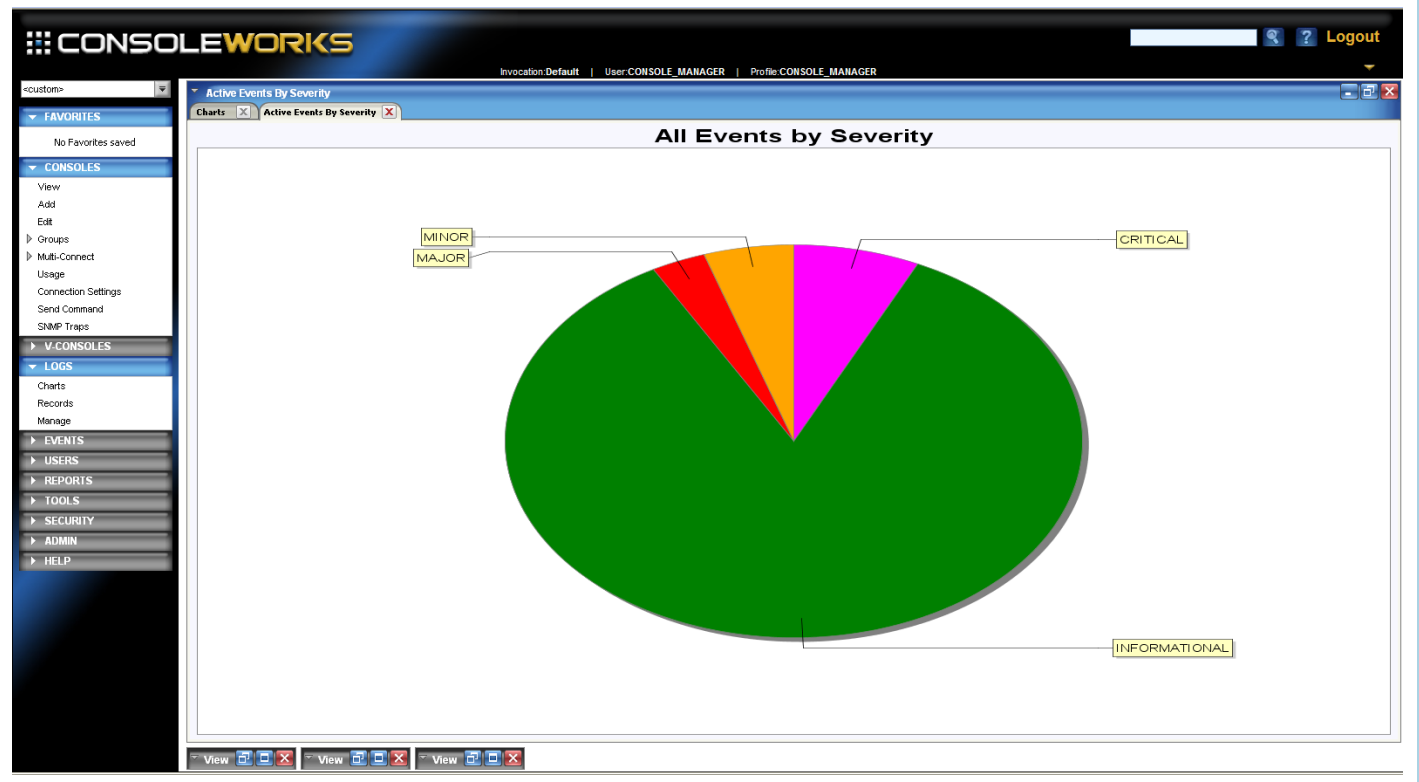
HISTORICAL REPORTING

Problem: Because there is not generally a good solution to provide aggregation and integration of all environments supporting virtualized computing, there is not a good method of reporting what commands were issued to the VM, its operating system, applications and the resulting status. When a firm has 500-1000 virtual machines running, such information takes on added significance as it relates to business risk, security of information, compliance and forensics of an outage or business impact.

Solution: VIRTUALfx collects information from the hypervisor, the virtual machine guests and the hardware and reports at the lowest granular level. It aggregates information such as:

- Disk error
- Disk running out
- Bad hardware
- Network card failure
- Security issues
- Environmental warnings – CPU/GPU/case/disk temperature, fan speed, power supply under/over voltage

Graphic of Active Events





VIRTUAL SYSTEMS PROBLEM REMEDIATION

Problem: Physical machines running a hypervisor with multiple virtual systems increase risk when they fail because multiple applications or environments are affected. Thus, understanding a problem before it becomes critical or remediating it with little or no human intervention has high benefits. Visibility and understanding of the physical infrastructure around the virtualized environment is paramount to understanding why it may have been impacted.

Solution: VIRTUALfx manages and logs the hypervisor and each of the guests. It is also capable of monitoring the entire business infrastructure---routers, switches, servers to determine a problem and recommend a solution.

VIRTUALfx detects hypervisor or guest problems, compares the problem codes with vendor recommended procedures and actions called Intelligent Event Modules (IEM). VIRTUALfx also captures a company's senior engineers' best practices for virtualization remediation down to keystroke. Thus, in the event the same problem occurs in the future, any VIRTUALfx user can solve the problem the same way it was solved before yielding consistency and complete resolution. Simply using the technology builds the business's data warehouse of intellectual property related to problem resolution.

PERFORMANCE MANAGEMENT

Problem: In a virtualized environment with hundreds of virtual guests running information on performance of hard drives, SAN systems, running threads and other physical or network resources needs to be shown in a single place.

Solution: VIRTUALfx directly connects to a machines' service processors for each of these services and devices. It also uses the latest in technology standards that provide agentless information about performance and configuration of the virtual or physical environment. VIRTUALfx then reports on the usage of each of these services in a graphical form.

Multi-log

The screenshot displays the CONSOLEWORKS web interface. The top navigation bar includes the logo, a search field, and a 'Logout' button. Below the navigation, the user is logged in as 'User: CONSOLE_MANAGER' with the profile 'Profile: CONSOLE_MANAGER'. The main content area is titled '2008/06/04 Logs for 2 Consoles' and shows a list of log records with columns for 'Date Time', 'Console', and 'Message'. The logs include events like 'VmPoweredOnEvent' and 'suse login'. A left-hand sidebar contains a navigation menu with categories like 'FAVORITES', 'CONSOLES', 'LOGS', 'EVENTS', and 'USERS'. The bottom of the interface features a toolbar with various icons for viewing and managing logs.

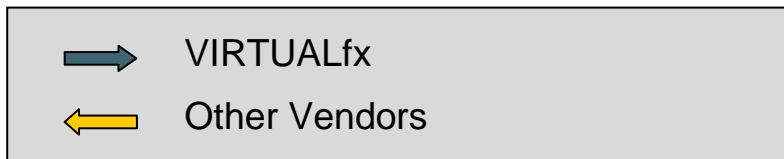


COMPLIANCE REPORTING

Problem: Virtualized systems often fail to meet compliance requirements. They have the same compliance monitoring and reporting requirements as non-virtualized system. Virtual systems are not easily logged and audited. Traditional log systems have compliance gaps because they do not log virtualized systems.

Solution: The VIRTUALfx logs, audits all access to the guests, hypervisors and physical equipment with a persistent connection such that the same information is available for them as with non-virtual systems. Thus, there are no compliance gaps.

VIRTUALfx VS Other Vendors



Virtual Systems

