

SECURITY AND COMPLIANCE GAPS IN TRADITIONAL LOGGING SYSTEMS

A whitepaper from:

TDI
1.800.695.1258
info@tditx.com
www.tditx.com



Executive Summary

TDI develops IT infrastructure management solutions for the commercial and government markets to manage monitor and remediate problems regardless of a device or system's operating state. TDI technology is also used to capture and log information related to the operation, command and control as well as application performance in aggregated digitally signed log files which are synchronized based on a common timestamp.

The TDI products grow from a patented set of facilities which enable TDI to secure and log both the virtual and physical environment in a manner beyond all known protection technologies.

The technology is used by the commercial and government sectors to capture remediation methods and IT best practices as well as provide vendor related intelligence associated with IT events.

Recently SANS Institute (www.sans.org) discovered a major security gap inherent in the computing infrastructure: the service processor. TDI has the only commercially available security and audit solution to close this gap.

TDI's products are setting a new standard for security in both the virtualized and physical world. The TDI product portfolio goes above all existing logging and access security measures and sets a new standard: Critical Infrastructure Protection (CIP) security.

CIP level security demands "gapless" logging and auditing: systems must be logged at all times, in all machine states regardless of whether the O/S or network is operational. The U.S. Government and other high security organizations are demanding CIP level security for both physical and virtual systems.

TDI has delivered patented, CIP level security for both the physical and virtual part of the enterprise. This CIP level security fills the security, logging and auditing gaps left by traditional systems.

Technical Overview

TDI's technology is based on a patented, purpose built web server used to maintain persistent connections to managed devices in the IT datacenter and network. The technology implements a closed loop logging capability which not only logs messages from applications, security and networks when the environment is operating properly, but it also captures events related to operating system failures, crash dumps, hardware failures like power supply outages, bus errors, memory errors and BIOS changes.

Because the product maintains a persistent connection to the device's baseboard management controller or serial console, it can provide a remediation path to correct any problems regardless of the state of the device.

The ability to manage a device throughout its life-cycle is due to technology being deployed throughout the datacenter as a result of the Distributed Management Task Force (WWW.DMTF.ORG). This device, generally called a Baseboard Management Controller (BMC) is present on virtually every computing, routing and switching device.

A baseboard management controller (BMC) is a specialized microcontroller embedded on the motherboard of most computers, especially servers.

Different types of sensors built into the computer system report to the BMC on parameters such as temperature, cooling fan speeds, power mode, operating system status, etc. The administrator can also remotely communicate with the BMC to take some corrective action such as system resetting or power cycling the system to get a hung O/S running again. This type of management is often referred to as “out-of-band management.”

Out-of-band management (sometimes called lights-out management or LOM) is the use of a dedicated management channel for device maintenance. It allows a system administrator to monitor and manage servers and other network equipment remotely regardless of whether the machine is powered on.

By contrast, in-band management is the use of regular data channels (usually through Ethernet) to manage devices. A significant limitation of in-band management is its vulnerability to problems from the very devices being managed. Periods of network problems are precisely when it would be most useful for IT administrators to remotely manage network servers and routers. However, the same problems that cause the network to go down also result in the loss of management access to those devices. Each of these periods constitutes a “gap” when systems are open to intrusion and traditional log management systems cannot log or audit them.

TDI’s technology utilizes out-of-band management which addresses this limitation by employing a management channel that is physically isolated from the data channel as a result allowing problems to be remediated regardless of machine state: running, hung, crashed, powered off or on. It is also the same technology and capability being used to deploy the “Green Datacenter” in emerging markets.

The advent of virtualization and its requirement for “agentless,” small footprint guest VM management demands outside-in management.

Log Files and Log Management

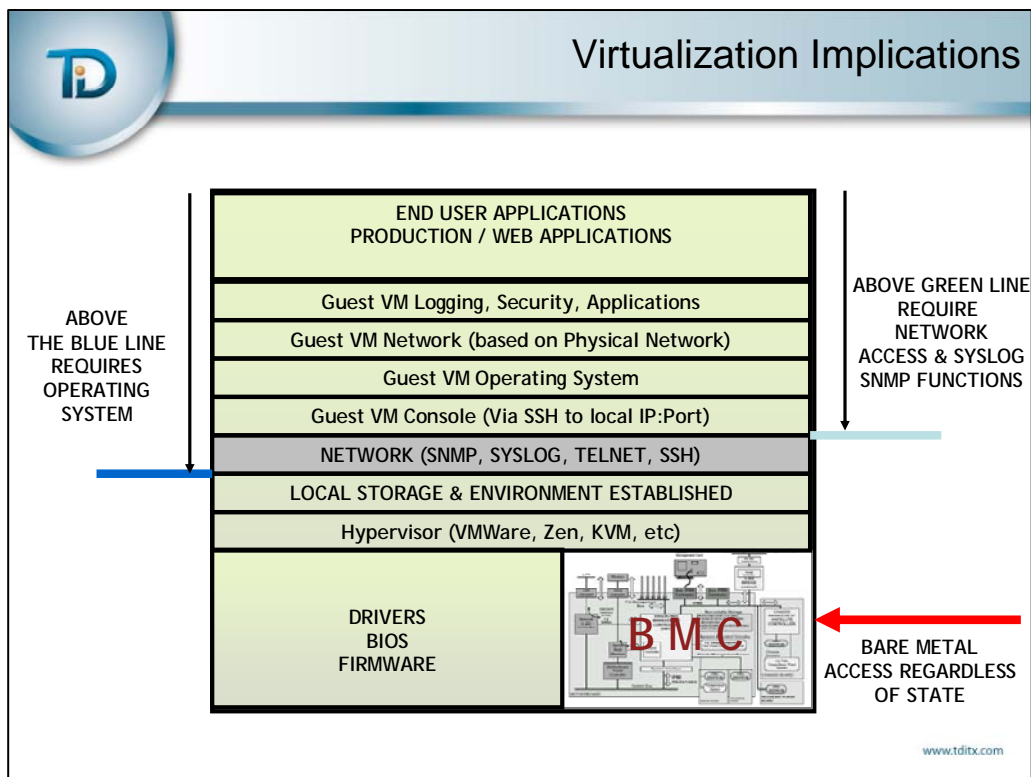
In order for traditional logging and security solutions to work, they actually require underlying infrastructure such as the network, operating system, hypervisor and hardware to be operational. As a result they require the actual environment they are responsible for monitoring to actually be available. Often it is not.

This issue becomes particularly important when one deals with the new issues of BMC security (baseboard management controller) and virtualization logging and management.

As the diagram below shows, the network and operating system must both be up and in perfect health for traditional log management systems to audit access. Often, the network, hypervisor or O/S is down thus causing security gaps where traditional log management systems are blind.

However, TDI's access is at the BMC level and TDI can provide secure, persistent protection and access to all devices, in all states, at all times, even when the hypervisor or O/S is not operational.

Such requirements are mandatory in new CIP (critical infrastructure protection) security environments. There can be no time, no machine state when a device is not being logged and audited.



LOG Management Gaps

Log management, aggregation and mining are the heart of both security and event management in the enterprise. Today, all log management systems are dependent on the SNMP protocol. Thus, they cannot log the critical data at the BIOS level which constitutes the root cause data necessary for remediation.

Nor can traditional log management systems protect the enterprise---corporate or government from intrusion at all times and under all conditions. For instance, when a machine is placed in single state to apply a patch, it is unlogged with all existing log management systems. It is at this time the clever insider criminal strikes.

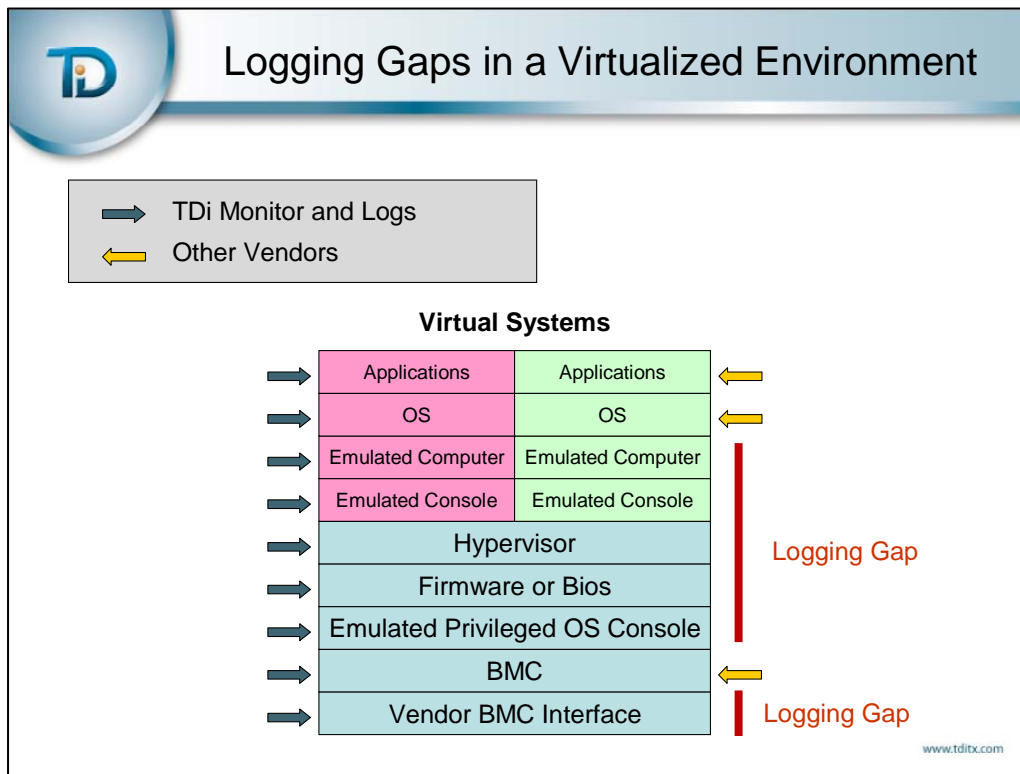
Virtualized systems are unlogged because it is impractical and cumbersome to place the agents required for them on these guest systems. Thus, virtualized systems can easily be hacked with no footprint or warning.

Operating systems and networks go down and at such times, there is no logging of these devices.

CIP level security requires that logging, auditing and protection occur:

- At All Times
- Under All Conditions
- In All Machine States
- Physical and Virtual

Below is a chart showing the logging gaps existing in today's data center:



Event Monitoring & Self-Healing Computing (Closed Loop Logging)

Events may be user defined or provided by TDI as part of its technology. TDI uses a packaged set of event definitions based on each vendor's error message and recovery procedures manual. This allows the technology to understand what to look for based on vendor defined message patterns which could occur vs. a customer defining what has occurred.

When an event is detected, the technology is able to provide the vendor's definition and recommendation of how to solve the problem. Because the technology also provides a remediation path for resolution of the problem which is logged, it also captures how the administrator resolves the event. This allows the administrators intelligence of solving the event to be associated with the event so that should it occur in the future the product can also provide examples of previous solutions.

As events are captured, a event life-cycle is created and managed within the product to include maintaining information such as where the event came from, when it happened, who solved it, what they did to solve it, how long it took to solve it. The technology manages three event "states" detection, acknowledgement, and completion. Based on the event being manually moved to each state, actions may be used to communicate with appropriate personnel or interface with other monitoring tools.

Compliance

Sarbanes Oxley, PCI, NERC-CIP, HIPAA and other regulations demand an organization secure, log and audit all access to critical information. Period.

These requirements cannot be met if there are known gaps in the logging, auditing and protecting of key infrastructure assets.

Thus, any logging system which does not explicitly resolve the BMC and virtualization gaps leaves the corporation open to fines, litigation and penalties.

Major public auditing firms, consulting firms, federal government auditors are aware of these problems and are taking steps to force compliance. A list of firms can be provided who can help with this matter.

TDI's logging and monitoring solutions fill the gaps left by traditional logging and security systems. TDI provides a real-time view of compliance risk events. After identifying an event, the technology can instantly associate a specific sentence or paragraph from a law, regulation, or standard with that event. Reporting on compliance events is equally easy since the technology can report by paragraph number rather than just by event. Digitally signed log files detect data modification, which satisfies compliance rules and regulations. TDI's technology integrates with other compliance solutions quickly and easily as well.

And with TDI, there are no compliance gaps.

Contact Information

The professionals at TDI look forward to engaging in a solution oriented discussion around your specific requirements. To engage in a technical demonstration, a live demonstration, address configuration or pricing questions, please call 1-800-695-1258 today or visit our web site at <http://www.TDItx.com/>.

About TDI

What We Do:

For 15 years TDI pioneered, patented, developed and deployed a family of technologies based on the "outside-in" infrastructure management paradigm for failure-intolerant customers such as The National Security Agency, The United States Army, Bank of America, Pfizer, Verizon, and the European Space Agency. TDI has over 280 customers with 3,200 installations.

How We Are Different:

The "outside-in" or "out-of-band" infrastructure management paradigm is not dependent on the infrastructure it is managing. If the O/S or hypervisor goes down, TDI still manages, monitors, finds the root problem cause and remediates the problem - all from a web browser. Virtualization and the advent of the baseboard management controller (BMC) have created a new paradigm for security, logging and event management that makes previous agent-based, polling technologies obsolete.

Why This Matters:

Whether it is virtualization, log management, or infrastructure management, the world is moving to a "self-healing" infrastructure. Human intervention is too expensive and prone to risk.

To heal, one must diagnose. To diagnose, one must see what is going on both at the lowest level of the device, and from a top down "holistic" perspective. With the advent of CIMOMs everywhere, a functional Alert Standards Format and SMASH deployment, TDI's technologies capture and interpret the data most relevant to healing a problem before it takes down the infrastructure.

TDI is located in Plano, Texas and has 40 employees. The company receives no venture funding and is profitable and growing. In each of the previous 3 years, TDI has been recognized as one of the Deloitte Fast 50 high tech firms in the region.

TDI Headquarters

1600 10th Street, Suite B

Plano, Texas 75074

(972) 881-1553

(972) 424-9181 (fax)

www.tditx.com

Copyrights and Trademarks

Copyright 2008 TDI

All Rights Reserved. This material is subject to copyright protection.

All other trademarks are acknowledged as the property of their respective owners.

This document and the products to which it pertains are distributed under licenses restricting their use, copying, distribution, and decompilation. No part of this document or of the associated products may be reproduced in any form by any means without prior written authorization of TDI.

MATERIAL IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.



TDI
1600 10th Street, Suite B
Plano, TX 75074
1.800.695.1258