BEST PRACTICES: EVENT LOG MANAGEMENT FOR SECURITY AND COMPLIANCE INITIATIVES

By Ipswitch, Inc.
Network Managment Division

www.whatsupgold.com
July 2010

Table of Contents

Executive Summary

Has someone made any unauthorized changes to your Active Directory policies or Access Control Lists (ACLs) for a directory on a server containing company Intellectual Property? Has someone gained unauthorized access to data that is regulated by law, such as HIPAA? Is somebody trying to hack into your internal systems? What if your compliance officer asks you for SOX-centric reports?

Every day, computer networks across the globe are generating records of the events that occur. Some are routine. Others are indicators of a decline in network health or attempted security breaches. Log files contain a wealth of information to reduce an organization's exposure to intruders, malware, damage, loss and legal liabilities. Log data needs to be collected, stored, analyzed and monitored to meet and report on regulatory compliance standards like Sarbanes Oxley, Basel II, HIPAA, GLB, FISMA, PCI DSS, NISPOM. This is a daunting task since log files come from many different sources, in different formats, and in massive volumes, and many organizations don't have a proper log management strategy in place to monitor and secure their network.

In response this white paper will discuss common Event and Log Management (ELM) requirements and best practices to decrease the potential for security breaches and reduce the possibility of legal or compliance issues. If you have downloaded this whitepaper and wish to view our recent "Best Practices: Security Log Management & Compliance" Webinar recording, you can access it through the following link: **http://www2.whatsupgold.com/l/1254/2010-07-28/ICE51 ?k_id=bestpract_wp**

Event and Log Management Best Practices

Here are some of the best practices that will help you build and maintain an effective ELM strategy:

- Define audit policy categories (in other words, configure which events to record)
- Automatically consolidate all event records centrally
  - ✔ Use both flat format & database records
- Event monitoring- Real-time alerts & notification policies
  - ✔ Define which events should trigger an alert, and define your poll intervals
- Generating reports for key stakeholders: auditors, security or compliance officers & management teams
- Auditing Log Data
  - ✔ Central Log Analysis
  - ✔ Ad-hoc forensics

Why Event and Log Management (ELM) is Important

Every system in your network generates some type of log file. In fact, a log entry is created for each event or transaction that takes place on any machine or piece of hardware--think of it as acting as your "journal of record". Microsoft-based systems generate Windows Event Log files, and UNIX-based servers and networking devices use the System Log or Syslog standard. Event Log Management is a key component of your compliance initiatives, since you can monitor, audit, and report on file access, unauthorized activity by users, policy changes, or even major changes in organizational roles via group membership.

Windows based systems have several different event logs that should be monitored consistently. Of these logs, the most important is the Security Log. It provides key information about who is on logged onto the network and what they are doing. Security logs are important to security personnel to understand if vulnerability exists in the security implementation.

Besides Security Event logs, some of other Windows event logs that should be regularly monitored include the:

- **Application events** – records application related events; application starts, failures
- **System events**– records system component events; driver failures and hardware issues
- **Directory Services events** – Domain controllers record any Active Directory changes
- **File Replication service events** – for File Replication service events; Sysvol changes
- **DNS events** – DNS servers record DNS specific events

By deploying an Event and Log Management solution, you can easily manage the frequently overwhelming amount of log information generated by your systems. Real-time access to log data will allow you to filter and locate that one "needle in a haystack" event that could be the cause of a security breach.

How Much Log Data is There?

Every day your servers and other network devices produce 10's of thousands of log entries. In fact, the average enterprise will accumulate up to **4GB of log data a day**. Over 95% of the data within the log files consists of detailed entries recording every successful event or transaction taking place on the system. For example; a server crash, user logins, start and stop of applications, and file access.

Many administrators are surprised to learn that "simple" log files can result in such a large amount of data that is collected and then stored. It is the perception of this mostly routine data that is at the heart of an organization's failure to capture, store and analyze the log data being generated constantly. You should never underestimate the importance of the data found within these files.

When manually collecting and reviewing log data, you need to be aware that the more servers you have producing log data, the potential for awareness and locating a security related or compliance issue decreases exponentially over time.

Security Inside the Perimeter

Security is always in the forefront of any size organization's IT strategy. Usually this strategy focuses on the perimeter of the network to prevent unauthorized access or attacks from malicious parties, that are not associated with the organization.

While external security is essential, what about the internal aspects? A nosy employee who wants to look at confidential company financial data and changes their access permissions? Or a disgruntled employee who has created a back door into a key server and is about to delete terabytes of customer data? While these may be extreme cases, are you prepared to counteract these possible events? The potential for a security breach is just as likely from an internal source as it is from the outside. In fact, it may even be higher. As we discussed in the Executive Summary, the potential for liability is considerable when some unauthorized individual accesses data that is considered protected by legislative act.

Through establishment of a comprehensive ELM strategy for security monitoring of Windows event logs for internal activities and changes that are out of the range of normal business activities, you can locate and prevent small events before they turn into a major catastrophe.

Compliance Initiatives: Prepare for the Worst

Your organization may or may not face regulatory compliance. If you are a private entity, most likely you do not. However, this should not prevent you from understanding what the regulatory standards have defined as requirements. Leveraging these standards can provide you with a blueprint for your own internal security plans and log management strategy.

If your organization is public, non-compliance with Sarbanes-Oxley, for example, can result in heavy fines and legal liability for the officers. Many of the requirements of the other legislative or industry specific initiatives for security and compliance, as they relate to log management, overlap with those of Sarbanes-Oxley. As a result, all public and many private companies look to that standard for guidance in building a log management strategy.

A quick review of each of the standards below will provide you with a high level overview to understand each of them and how they can affect your log management strategy.

Sarbanes-Oxley

In Sarbanes-Oxley, the phrase "internal controls" in section 404 of the act is central to compliance efforts. Public companies' annual reports must include:

[…] an internal control report, which shall –

1. state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

2. contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

Several misconceptions center on who and what is impacted by these requirements. First, Sarbanes-Oxley applies only to publicly traded organizations in excess of $75 million, or by extension, private firms to be acquired by public companies. Second, it isn't just the financial data itself or the reporting of that data with which Sarbanes-Oxley is concerned when it refers to "control structure failure;" this has been very broadly interpreted to include just about anything that could even affect the reliability of that data. More information on the specifics of Sarbanes-Oxley can be found at the SEC website:

http://www.sec.gov/about/laws/soa2002.pdf

Because of the inherent differences in network configurations, business models, markets, and the preferences of auditors,the best practices that are suggested later in this document should be viewed as a starting point. The below sidebar synthesizes some of the ELM requirements that should be included in your audit and compliance strategies.

While these suggestions are focused towards Sarbanes-Oxley, they can also be used in addressing the requirements of Basel II, GLBA, HIPAA, PCI, and other efforts.

In most cases, this will be part of a larger compliance strategy, so be sure to consult with your audit specialists for more detail relevant to compliance in your specific industry.

BASELINE ELM STRATEGY FOR SECURITY, COMPLIANCE AND AUDIT

Key Windows and Syslog Events to Monitor

- Any changes to File or Folder ACLs
- Registry Access – adds, changes, and deletions
- User account changes that provide administrator equivalent permissions
- Active Directory access and changes
- Changes to Groups – adds, changes or deletions
- Windows and SSH login failures and successes
- System events – process start and shutdown
- Application failure, start or shutdown
- IDS and anti-virus logs
- Interfaces for high TCP and UDP traffic
- Server offline or online and reboots
- Access to network infrastructure
- Changes to ACLs on switches, routers or firewalls
- DNS changes
- Web server access and permission changes
- HTTP "404" errors
- FTP server access and file transfers
- Server and workstation logs for intrusion incidents and policy changes
- Access and permission changes to Files, Folders, and Objects containing financial, customer or compliance data

Key Windows Event Logging Categories to Enable

- Logon Events - Success/Failure
- Account Logons - Success/Failure
- Object Access - Success/Failure
- Process Tracking - Success
- Policy Change - Success/Failure
- Account Management – Success
- Directory Service Access - Success/Failure
- System Events - Success/Failure

Basel II

Compared to Sarbanes–Oxley, Basel II is less well known and lacks its clout. The goal of Basel II is to promote greater stability in financial systems internationally. For our purposes here, the focus centers on Basel's concern with "operational risk," which is subject to interpretation. It is possible that a good starting point could also be those listed above for Sarbanes-Oxley compliance. Efforts will require interpretation of the Advanced Measurement Approach (AMA), a portion of the Basel II accord, by your group's management and audit teams.

Gramm-Leach-Bliley (GLBA)

Regarding IT compliance, the Gramm-Leach-Bliley Act focuses on the protection of customer data by financial institutions. Much of GLBA overlaps with Sarbanes-Oxley's requirements. Though sometimes regarded as just another collection of rules or mere guidelines, GLBA does have teeth. The consequences of failure to comply can include civil action brought by the U.S. Attorney General. The act can be access though the Federal Trade Commission's web site at: **http://www.ftc.gov/privacy/privacyinitiatives/glbact.html**

HIPAA

HIPAA's requirements are similar to GLBA's in that they stress the existence of a reliable audit trail to protect the personal data of medical patients. HIPAA is comprised of two major rules: the Privacy and Security Rules. Each of these has their own requirements for implementation and reporting. according to the Centers for Medicaid and Medicare, in addition to building IT infrastructure and strategies to protect against "threats or hazards to the security or integrity of the information," preparations must be in place for investigation of potential security breaches. An audit trail must be able to provide "sufficient information to establish what events occurred, when they occurred, and who (or what) caused them."

FISMA

The Federal Information Security Management Act (FISMA) is designed to protect critical information infrastructure of the United States Government. It sets minimum security standards for information and information systems and provides guidance on assessing and selecting the appropriate controls for their protection. Each Federal agency and its contractors are required to develop, document and implement policies that meet the FISMA standards.

The National Institute of Standards and Technology (NIST) has issued a Special Publication 800-53 to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government.

NISPOM

The requirements included in Chapter 8 of the National Industrial Security Program Operating Manual (NISPOM) are of interest to government agencies and private contractors with staff who have access to sensitive and classified data. The manual states that security auditing involves recognizing, recording, storing, and analyzing information related

to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.

PCI Data Security Standard (PCI-DSS)

Developed by MasterCard and Visa and being enforced by American Express, the Payment Card Industry (PCI) Data Security Standard provides IT shops that handle sensitive consumer credit card data with detailed requirements. Any entity that implements PCI-DSS must prove in an annual PCI-DSS audit report that they comply with the standard, or they can be denied the ability to process or store any credit card related information. Section 10 of the standard defines audit information and log files requirements. The standard can be accessed at: **http://www.pcisecuritystandards.org.**

Massachusetts Privacy Law – MA 201 CMR 17

The law defines that "every person that owns or licenses personal information about a resident of the Commonwealth" has a duty to design, document, and implement a system that protects that information. The affected person could be an employee or customer of the company. The effective date of the law was March 1, 2010. The specifics of the law can be found here: **http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf**

All of the legal or industry standards highlighted above reflect an ongoing need to not only ensure the protection and integrity of financial and personal data, but also prescribe that each and every transaction be auditable.

It is strongly recommended that IT and security professionals seek the input and feedback of their management and audit teams when structuring any compliance strategies based on ELM. There should be complete involvement from all disciplines within an organization to ensure the integrity of the entire process from gathering of event and log data to auditing and reporting.

Event and Log Management Best Practices

Best Practice #1: Define your Audit Policy Categories

The term audit policy, in Microsoft Windows lexicon, simply refers to the types of security events you want to be recorded in the security event logs of your servers and workstations. On Microsoft Windows NT® systems, you must set the audit policy by hand on individual servers and workstations, but in Windows 2000® or Windows 2003® Active Directory® domains, with Group Policy enabled, you can associate uniform audit policy settings for groups of servers or the entire domain. For a summary of key logging categories to enable, please refer to the "BASELINE ELM STRATEGY FOR SECURITY, COMPLIANCE AND AUDIT" table.

Best Practice #2: Automatically Consolidate All Log Records Centrally

By default, Windows event logs and Syslog files are decentralized, which each network device or system recording its own

event log activity. To obtain a broader picture of trends going on across the network, administrators tasked with security and compliance-centric initiatives must find a way to merge those records into a central data store for complete monitoring, analysis and reporting. Log data collection and storing is critical since some compliance standards mandate data retention for 7 years or more! Automation can really help here because it will save time and ensure the log data reliability. Remember:

1) **When the archived log files are retrieved, it must be a reliable copy of the data—there can be no debate as to the integrity of the data itself**. As the human element is removed with automation, the level of data reliability is increased.

2) The number of machines, users, and administrators in the enterprise; and considerations such as bandwidth and competing resources can complicate log collection so much that an automated solution is the only way to ensure that every event is collected. Can you ensure that each and every event has been successfully collected through a manual process?

In a typical setup, an administrator will configure an ELM tool to gather event log records nightly (or periodically) from servers and workstations throughout their network. This process involves saving and clearing the active event log files from each system, reading log entries out of the log files into a central database (e.g. Microsoft SQL or Oracle), and finally compressing the saved log files and storing them centrally on a secure server

Keeping your log data in two formats—as database records and as compressed flat files—offers a distinct auditing advantage. Event log data in flat files compresses extremely well, often down to 5% of the original size. Therefore, in terms of storage cost, it costs very little to keep archived log data for many years should an auditor ever need it. However, flat files are a very poor medium for analysis and reporting, so keeping an active working set of data (often 60 to 90 days) in a database allows ad hoc reporting as well as scheduled reporting to be available for recent events. **Look for an ELM tool that provides an easy mechanism for rapid re-import of older saved log files back into your database should they ever be needed.** It has been our experience that the majority of employee hours when facing an audit are dedicated to simply chasing flat files around and attempting to extract the same types of data from all of them. Having data at the ready in a central database greatly reduces the potential for lost hours when an auditor comes knocking.

Why log data collection automation is necessary:

1) **When the archived log files are retrieved, it must be a reliable copy of the data - there can be no debate as to the integrity of the data itself.** As the human element is removed with automation, the level of data reliability is increased.

2) The number of machines, users, and administrators in the enterprise; and considerations such as bandwidth and competing resources can complicate log collection so much **that an automated solution is the only way to ensure that every event is collected**. Can you ensure that each and every event has been successfully collected through a manual process?

Best Practice # 3: Event monitoring- Real-time alerts & notification policies

Most organizations have a heterogeneous IT environment, with a broad mix of operating systems, devices and systems. Even though your environment may trend towards Windows desktop and server OSs, you may also want the option of choosing **more than just Windows event log monitoring. Syslog support is important to have not only for routers, switches, IDS and firewalls, but also for UNIX or LINUX systems.**

Most software products require the use of agents to perform real time monitoring of log files. If any factor influences your choice of a solution this should be the one. I**f you can opt for a no-agents-required implementation of a monitoring solution, do it.** This will save a lot of headaches in the initial implementation, as your network grows, and in the ongoing maintenance of your monitoring solution.

When developing a log monitoring plan, every organization has different rules on what sorts of events they must monitor. IT departments will frequently focus on security events as the sole indicator of any issues. While monitoring the security event log is essential, other event logs can also indicate issues with applications, hardware issues or malicious software. **At a minimum, all monitored events should be traceable back their origination point.** The "BASELINE ELM STRATEGY FOR SECURITY, COMPLIANCE AND AUDIT" sidebar table in the above section provides the kick-off point for your log monitoring implementation.

Depending on your requirements and the flexibility of the ELM solution you deploy, you should define a methodology for **continuous monitoring based on how frequently you want to check logs for events of interest in real-time**. Each defined event is polled at a regular interval and will generate an alert or notification when an entry of interest is detected.

The number of events configured, number of target systems and polling frequency will dictate the amount of bandwidth consumed during a polling cycle. If you already know the events of interest on certain systems that you want to monitor, then configure away. **If you are establishing your event monitoring for the first time, it may better to start by enabling all events and configuring a higher polling frequency.** After your familiarity level increases, you can then pare down the number of events and decreasing the polling frequency.

Best Practice #4: Generating Reports for Key Stakeholders: Auditors, Security or Compliance Officers and Management Teams

Reporting is one area to which you should pay particular attention. It provides you with significant data on security trends and proves compliance. Reporting can help you substantiate the need to change security policies based on events that could result or have resulted in compromised security.

Any ELM solution that you implement needs to answer the following questions:

- What report formats are available?
- How much of your work is already done for you in prepackaged event log reports that ship with the event

- Are you tied to a particular format? Will HTML and the availability of that HTML report to multiple users play a role?
- Can customized filters be easily recalled for repeat use?
- From what data sources can reports be generated? Does it include EVT, text, Microsoft Access, and ODBC?
- Will the solution be compatible with your event archiving solution?

In general, reporting should be robust, have broad coverage, and provide rollup of data on a daily, weekly, monthly and yearly basis, along with the ability to define custom reports. Any compromise on reporting will negate all the other benefits of an ELM solution.

SARBANES - OXLEY	
Standard Requirements	**Suggested Reports**
Section 404 **Identification:** Log and report on all user identities and access privileges across all users and organizations, ensure all users are uniquely and irrefutably identified **Authentication:** log and report on all transactions from systems that provide an authentication mechanism **Policy-based access control:** log and report that only authorized business users have access to systems, data and network assets **Data Protection & Integrity:** log and report on access to data, who accessed data, how long and if data was changed, modified or copied, data integrity fed from upstream sources into the application system **Identity provisioning:** Log and report of access for all users including time-specific restrictions or access control based on the location of the originator	• Computer Account Management • Directory Service Access Attempts • Logon Failures – Active Directory • Logon Failures – Local Logons • Object Access Attempts – Success/Failure • Object Deletions • Password Reset Attempts by Users • Password Reset Attempts by Administrators or Account Operators • Process (Program) Usage • User Activity in Auditing Categories • Successful Network Logons – Workstations and Servers • Policy Change - Success/Failure • Account Management – Success/Failure • Directory Service Access - Success/Failure • System Events - Success/Failure

GRAMM-LEACH-BLILEY	
Legal Requirements	**Suggested Reports**
Section 501(b) • Log and report on systems containing customer information, including access to all systems and data by authorized individuals • Log and report on security of electronic customer information, including while in transit or in storage on networks or systems • Log and report of any customer information system modifications • Log and report on authentication and access control and segregation of duties • Monitor to detect actual and attempted attacks on or intrusions into information systems and log and report • Log and report destruction, loss, or damage of customer information due to technological failures	• Computer Account Management • Application Crashes • Printer Activity • User Account Lockouts • User Account Management • Object Deletions • Group Management • Password Reset Attempts by Users • Password Reset Attempts by Administrators or Account Operators • User Activity in Auditing Categories • Successful Network Logons – Workstations and Servers • Policy Change - Success/Failure • Account Management – Success/Failure • Directory Service Access - Success/Failure • System Events - Success/Failure

HIPAA	
Legal Requirements	**Suggested Reports**
Security Rule §164.306 and Privacy Rule §164.530(c) All of the following must be addressed for logging and reporting: • Password Aging • Consolidated Change Logs • User Privileges • NTFS Permissions • System Privileges • Role Permissions & Membership • Remote Access • User Access • Auditing Enabled	• Account Management – Success/Failure • Directory Service Access - Success/Failure • System Events - Success/Failure • Object Access Attempts – Success/Failure • Object Deletions • Group Management • Password Reset Attempts by Users • Password Reset Attempts by Administrators or Account Operators • Computer Account Management • Directory Service Access Attempts • Logon Failures – Active Directory • Logon Failures – Local Logons

FISMA	
Legal Requirements	**Suggested Reports**
8-602. Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them. • Individual accountability • Enough information to determine the date and time of action the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved • Successful and unsuccessful logons and logoffs • Successful and unsuccessful accesses to security-relevant objects and directories, including creation, open, close, modification, and deletion • Changes in user authenticators • The blocking or blacklisting of a user ID, terminal, or access port and the reason for the action • Denial of access resulting from an excessive number of unsuccessful logon attempts.	• Directory Service Access Attempts • Directory Service Access - Success/Failure • Logon Failures – Active Directory • Logon Failures – Local Logons • Object Access Attempts – Success/Failure • Object Deletions • Password Reset Attempts by Administrators or Account Operators • Process (Program) Usage • User Activity in Auditing Categories • Computer Account Management – Success/Failure • Successful Network Logons – Workstations and Servers • Policy Change - Success/Failure • Account Management – Success/Failure • Directory Service Access - Success/Failure • System Events - Success/Failure

PCI-DSS	
Standard Requirements	**Suggested Reports**
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user. **10.2** Implement automated audit trails for all system components to reconstruct the following events: • 10.2.1 All individual user accesses to cardholder data • 10.2.2 All actions taken by any individual with root or administrative privileges	• Directory Service Access Attempts • Directory Service Access - Success/Failure • Logon Failures – Active Directory • Logon Failures – Local Logons • Object Access Attempts – Success/Failure • Object Deletions • Password Reset Attempts by Administrators or Account Operators • Process (Program) Usage • User Activity in Auditing Categories

• **10.2.3** Access to all audit trails • **10.2.4** Invalid logical access attempts • **10.2.6** Initialization of the audit logs • **10.2.7** Creation and deletion of system-level objects **10.3** Record at least the following audit trail entries for all system components for each event: • **10.3.1** User identification • **10.3.2** Type of event • **10.3.3** Date and time • **10.3.4** Success or failure indication • **10.3.5** Origination of event • **10.3.6** Identity or name of affected data, system component, or resource	• Successful Network Logons – Workstations and Servers • Policy Change - Success/Failure • Account Management – Success/Failure • Directory Service Access - Success/Failure • System Events - Success/Failure

Best Practice #5: Auditing Log Data

The one portion of event log management that is perhaps the most intimidating is how to manually sift through and interpret vast amounts of everyday event data to locate the relevant information from log files that are archived. If careful steps have been taken in the planning of the actual log archive, this makes auditing and then reporting from event logs much easier. **A solution must provide predefined and configurable search and filtering capabilities. The ability to also define custom search and filtering parameters is another invaluable feature. Furthermore, log data should be automatically grouped into related sections, with event identifier codes translated into human readable explanations.**

Another point to consider is how to simplify routine or ad-hoc forensics activities. Previously, checking log files has required a lot of manual scanning and brings on eye and brain fatigue fast. The manual review and filtering of logs also creates opportunities for error. **The most important thing to keep in mind is that routine log review should be simple, quick, effective and error free.** The same old event viewer is no longer the most effective tool for spot checking log files. The best approach is to use a tree-view capability as opposed to the old-fashioned linear method to log scanning relied on for so long in the Windows event viewer. **A tree based capability allows for grouping of events, making on-the-spot discovery of individual events and trending across multiple log types and events more convenient and far more reliable.**

A final concern in this area that has cropped up in recent years is the shift from .EVT to .EVTX format. Because of API requirements, for example, the .EVTX logs generated from Windows Vista and later machines cannot be viewed on Windows XP and older machines. Complications caused by the format changes can be eliminated with your choice of a log viewing

tool. **Keep .EVTX compatibility in mind when selecting a solution for log viewing and formulating a routine log review strategy. Different field structures between logging formats and other transformations should be performed automatically to aid the administrator.**

Best Practices Summary

Preventing security breaches and ensuring compliance requirements are met requires real-time monitoring of all log files to rapidly detect specific events of interest, block offenders, and initiate rapid response processes. **ELM provides a more proactive approach to counteracting and resolving issues today, rather than tomorrow.** This translates into a faster return on investment as the results not only prove true with automation of everyday tasks, but also systems monitoring and troubleshooting.

Because the other goal of event log management is the ability to audit or perform forensics on log files, a robust collection system is critical. It ensures that a reliable audit trail exists when required in the future. With that reliable archive of event log files, comprehensive analysis and reporting is simplified. However, if a reliable mechanism for quickly sorting log files is not in place, the benefits of the strongest monitoring and archiving solutions will not be realized. A trusted event filtering and log report generation solution ensures maximum return on your investment as well as no additional finger pointing in the wake of a network crisis. An unprotected and unreliable IT infrastructure is not only a liability; it may even be a criminal offense.

What Should an Event and Log Management Solution Provide?

There are several schools of thought on ELM solutions and what is important to meet the both the needs of the organization and minimize the impact of issues. Based upon discussions with a broad spectrum of customers who are dealing with compliance regulations and industry standards on an ongoing basis, the requirements in the below sidebar table represent a general consensus of the most important features that a best fit solution would provide. Your industry, organizational structure, business model, IT infrastructure and policies and procedures will shape your direction and implementation of any ELM solution.

Only you can decide what best fits your situation and objectives. At a minimum, your evaluation checklist should reflect the features and functionality provided in the Event and Log Management Solution Requirements table.

Some additional factors that should also be considered when selecting an ELM product include:

- Scalability
- OS platform support
- Modularity
- Usability
- Licensing policies
- Technical support
- Maintenance cost
- Company reputation
- Customer references
- Product Documentation

EVENT AND LOG MANAGEMENT SOLUTION REQUIREMENTS	
Log Collection	**Log Archiving**
• Automated collection of log files • Supports Windows Event Logs – both .evt and .evtx formats • Supports Syslog log files • Configure to clear or not clear log files • Collects all generated events • Collects only certain types of events • Can export log data from one source to another	• Compression of log data • Can provide email notification of failed archive attempts • Can automatically retry failed archive attempts • Continues from last collected event • Scheduled time • Percent full (threshold) • Opens zipped event log files (.evt) for review
Log Consolidation and Storage	**Data Formats**
• Secure log aggregation and storage for Windows Event Logs and Syslog data from devices and OSs (UNIX, Linux) • Supports SQL databases for log data • Provides log normalization • Supports automated compression	• Syslog • SQL • MS Access • .evt Log Format • Comma Delimited Text File • HTML Report Format • Comma-Delimited Report Format

Monitoring	Alerts and Notifications

• Agentless monitoring
• Real-time monitoring
• Configurable polling
• Servers go offline/online
• System shutdowns/restarts
• Detect and track changes to users/ groups/ computers
• Detect and track unauthorized account usage
• Detect and track printer activity
• Detect policy changes
• Detect account lockouts
• Track logon activity
• Track errors and warnings
• Track changes/deletions on files/folders/registry keys
• Ability to create custom "alarms" for log monitoring
	• Define alerts for events of interest
	• Define alert for a single event
	• Configurable thresholds
	• Provides predefined alarms
	• Alerts on devices and OSs supporting Syslog
	• Define events as either: high risk, medium risk or low risk
	• Notification Support
	  • Network popups
	  • Email messages
	  • Pager
	  • Short email messages
	  • Syslog messages
	  • Database insertions
	  • NetBIOS broadcast notification
	• Supports regulation of notifications
	• Sends notifications to multiple email addresses

Reporting	**Log Analysis and Management**

• Provides out-of-the-box predefined reports
• Provides access to log reports via browser
• Can report daily, weekly, or monthly results for defined data
• Ability to create custom reports
• Configurable report formats
• HTML based reports
	• Provides a tree view of events and data for analysis
	• Supports extensive filtering options
	• Create custom filters for review
	• Provides predefined filters
	• Supports choice of log type to manage including:
	  • Application
	  • Security
	  • System
	  • DNS Server
	  • Directory Service
	  • File Replication Service

Conclusion

At Ipswitch, we frequently talk with people who are not fulfilling their own security and compliance requirements and policies – whether they are internal or external standards. Recently one customer had less than 12 hours to meet a crucial regulatory compliance deadline.

In the current environment of do more with less and budget restrictions, it is a question of weighing the risks and deciding as the Purolator commercial once stated; "You can pay me now or pay me more later."

Neither security nor compliance is easy or simple. They both require knowledge, planning and investment. In the end, the best place to start is to review the individual requirements you think apply and then take a look at some successes from other organizations. While this is in no way the complete answer to full compliance and an A+ score on an audit or security nirvana, it does represent the best information we've encountered in successful, real-world compliance efforts.

And, of course, it helps to get started on your effort more than 12 hours before the auditors arrive. We hope that this summary of best practices for both compliance and security initiatives has provided some real-world guidance, saved you valuable time and prevented any future headaches.

Introducing WhatsUp Event Log Management Suite

The WhatsUp Event Log Management Suite is a modular set of applications that can automatically collect store, analyze and report on both Windows Event and Syslog files for real-time security event detection and response, and historical compliance assurance and forensics.

- **Event Archiver:** Automate log collection, storing, backup and consolidation. It supports auditing, regulatory compliance and log forensics activities.
- **Event Alarm:** Monitor log files and receive real-time alerts and notifications. Quickly react and initiate rapid response processes to network outages or security threats.
- **Event Analyst:** Analyze and report on log data and trends. Automatically distribute reports to management, security officers, auditors and other key stakeholders.
- **Event Rover:** Single console to view and mine log all data across all servers and workstations. Supports ad-hoc forensics relying on patented Log Healer Technology, for handling and repairing potentially corrupt Microsoft EVTX log files.
- **Auditing Volume Analyzer** is a freeware utility offered to assist administrators in estimating the amount of event log data being generated on a given network.

Did you know that Ipswitch's **WhatsUp Event Archiver was awarded US's Army Certificate of Networthiness # 201004611?**

You can find out more about the WhatsUp Gold Event Log Management Suite at: **http://www.whatsupgold.com/products/event-log-management/**

About the Network Management Division of Ipswitch, Inc.

The Network Management Division of Ipswitch, Inc. is the developer of the WhatsUp Gold suite of innovative IT management software. WhatsUp Gold delivers comprehensive network, system, application and event log monitoring and management solutions for small and medium businesses and enterprises. Built on a modular, yet integrated architecture, the affordable and easy-to-use solutions scale with the size and complexity of any physical or virtual IT infrastructure. From a single console, WhatsUp Gold supports standard IT management tasks including automated discovery, mapping, real-time monitoring, alerting, troubleshooting and reporting. More than 100,000 networks worldwide use WhatsUp Gold solutions to assure the availability, health and security of their critical business infrastructure today.

Ipswitch, Inc.'s Network Management Division recently added to its product line complete, easy-to-use solutions for Windows Security Event Management (SEM) and Log Management for small businesses and enterprise-level organizations suite with the acquisition of Dorian Software Creations, Inc. WhatsUp Gold was named Network Management Product of 2010 by Network Computing Magazine and earned the Network Products Guide 2010 Product Innovation Award in Network Management. To learn more about WhatsUp Gold – the best value in IT Management software, download a free trial or to make a purchase, please visit: http://www.whatsupgold.com/products/download/.