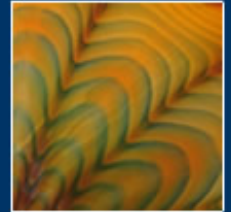




ADVANCED TOOLWARE
POWERFUL DOMAIN TOOLS



Lowering Operational Costs While Maintaining Network Integrity:

MONITORMAGIC – Network Monitoring

White Paper

INTRODUCTION

MonitorMagic delivers a comprehensive enterprise-class solution for centralized management of performance and availability of hardware, operating systems and applications. MonitorMagic enables system administrators to take full control of distributed environments by identifying and resolving potential problems before end users are affected. This results in increased end-user satisfaction together with a reduction of spent time and effort.

Lower TCO (Total Cost of Ownership) Using the effective combination of pro-active performance monitoring, event log archiving, application thresholds and graph trending, you can easily spot hardware and software weaknesses and act before your end users are affected. Not only will this drastically lower your TCO, you can also avoid unnecessary hardware investments based on performance trending predictions.

Hardware, Operating System and Application Monitoring MonitorMagic runs on all Windows 2003/XP/2000/NT workstation or server versions and can grab performance and status data from virtually every component on your network such as operating systems, SNMP compliant network components, Dell® and HP/Compaq® servers, printers, Active Directory, Exchange, SQL Server, Terminal Server and many more.

Centralized Agentless Monitoring and Collection

MonitorMagic's unique client-server architecture guarantees hassle-free client and agent deployment. Both MonitorMagic client and agent can be installed on any type of Windows 2003/XP/2000/NT server or workstation computer. A single MonitorMagic agent can monitor multiple other computers or devices remotely without installing any software or leaving a footprint. Each agent can be connected to a database to store monitoring data, and multiple agents can share a single, central database to consolidate trending data.

Scalable from One Server to WAN-LAN Hybrid Networks Whether you run a single server network or a multi-office WAN connected hybrid network, MonitorMagic will always deliver the performance needed to keep your environment up and running. MonitorMagic agents can be deployed locally on your central network or remotely at each office, and can be managed and configured from any location. For maximum performance, multiple agents can be deployed for monitoring load balancing.

Event Log Archiving and Reporting MonitorMagic includes a powerful report data collector which can be scheduled to visit all your servers at night and gather all Windows event logs. These logs are then recorded into a central Microsoft® Access, SQL Server or MSDE database. Using the included report data generator and template builder, MonitorMagic can produce company tailored reports real time on the screen for easy printing or HTML export, or email the reports automatically to the network support staff each week.

Unique Flexible Plug-in Architecture

If you have an application or device that is not directly supported by MonitorMagic's base set of Q&A monitors, but rather uses its own proprietary tools or scripts, simply plug these into MonitorMagic. The plug-in architecture allows the scheduled execution of any command and grabs the results from the screen. Based on these results, you can have MonitorMagic notify you or take appropriate actions.

System Requirements

	MonitorMagic client (required)	MonitorMagic client (recommended)	MonitorMagic service (required)	MonitorMagic service (recommended)
Operating system	Windows 2003(*), Windows NT 4.0(*), Windows 2000 (*), Windows 98, Windows ME, Windows XP	Windows 2003(*), Windows NT 4.0 (*), Windows 2000 (*), Windows 98, Windows ME, Windows XP	Windows 2003(*), Windows NT 4.0 (*), Windows 2000 (*), Windows XP (server)	Windows 2003(*), Windows NT 4.0, Windows 2000 (*), Windows XP (server)
Processor	Pentium, 133 MHz	Pentium III or higher, 266 MHz or higher	Pentium, 133 MHz	Pentium III or higher, 266 MHz or higher
Memory (RAM)	64 MB	128 MB or more	64 MB	128 MB or more
Free disk space	10 MB	16 MB	16 MB	32 MB

(*): Windows 2003 means all Microsoft Windows 2003 operating systems including Standard, Enterprise, and Small Business Server. Windows 2000 means all Microsoft Windows 2000 operating systems, including: Professional, Server, Advanced server, and Datacenter. Windows NT 4.0 means all Microsoft Windows NT 4.0 versions including workstation, server, and cluster server.

Feature Matrix

MonitorMagic gives IT administrators and managers the power to pro-actively control all software, hardware and operating system resources and components throughout the enterprise by combining the following core functions into a feature-packed, reliable, and scalable application.

Monitoring:

	MonitorMagic
Agentless monitoring	x
n-tier agent deployment	x
Built-in monitor policy editor	x
Drag-and-drop policy deployment	x
Pre-configured policies for popular applications	x
Control center for easy agent browsing	x
Customizable network browse tree	x
Extensive scheduling per monitor	x
Event log messages	x
Disk information	x
Directory information and statistics	x
Network share information	x
Performance counters	x
Service state information	x
System processes	x
TCP/IP devices/ports	x
SQL query response	x
URL response time and header check	x
REXEC remote command execution	x
SNMP Get	x
SNMP Trap	x
File analysis	x
File characteristics	x
Cluster resources	x
Command line plug-in support	

Notifications:

	MonitorMagic
Custom scheduling	x
Execution delay	x
Custom keywords	x
Escalation	x
Popup messages	x
E-mail messages	x
Pager and SMS messages	x
Log event	x
SNMP traps	x

Actions:

	MonitorMagic
Custom scheduling	x
Execution delay	x
Escalation	x
Command line, script and batch file execution	x
Start or Stop services with cascade	x
Terminate processes	x
Shutdown computers	x
Reboot computers	x

Reporting:

	MonitorMagic
Data collection	x
Scheduling	x
Customizable report profiles	x
Multiple computers	x
Data caching	x
Pre-defined reports	x
Advanced custom SQL queries	x
Built-in printing	x
Built-in HTML export	x
Built-in report template editor	x

Graphing and trending:

	MonitorMagic
Pinpoint potential problems	x
2D graphs	x
3D graphs, real-time rendering in OpenGL	x
Real-time values	x
Database link for historical values	x
Customizable time-line	x
Customizable graph colors and layout	x
Transparency	x
Rotation	x
Printing	x

Web interface:

	MonitorMagic
Integrated web server, no IIS needed	x
HTTPS access using SSL 128bit security	x
Integrated certificate creation	x
Configurable access levels	x
View global system statistics	x
View/manage event logs	x
View/manage service	x
View/manage processes	x
View/manage monitors and rules	x
Reboot computers	x
Shutdown computers	x

FEDERAL COMPLIANCE ACTS

Federal regulations such as the Health Insurance Portability Accountability Act, Sarbanes-Oxley Act, Family Educational Rights and Privacy Act, and the Gramm-Leach-Bliley Act, has added to the recognition that information security is a must for corporate responsibility and survival. Reasonable and appropriate administrative,

technical, and physical safeguards must be implemented to prevent intentional or unintentional use or disclosure of protected company data. For I.T., this means providing more frequent auditing and reporting information about their network.

This section is meant to be an overview of the government regulations and ways MonitorMagic can assist in maintaining compliance.

The Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act known as HIPAA, offers protections for millions of working Americans and their families. The goals and objectives of this legislation are to streamline industry inefficiencies, reduce paperwork, make it easier to detect and prosecute fraud and abuse, and enable workers of all professions to change jobs, even if they (or family members) had pre-existing medical conditions. Ultimately providing patients with confidence that their sensitive personal data is safeguarded from inappropriate use.

- To improve portability and continuity of health insurance coverage in the group and individual markets
- To combat waste, fraud, and abuse in health insurance and health care delivery
- To reduce costs and the administrative burdens of health care by improving efficiency and effectiveness of the health care system by standardizing the interchange of electronic data for specified administrative and financial transactions
- To ensure protecting the privacy of Americans' personal health records by protecting the security and confidentiality of health care information

HIPAA affects all healthcare organizations that maintain or transmit electronic health information. This includes health plans, healthcare clearing houses, and healthcare providers, from large integrated delivery networks to individual physician offices.

The Sarbanes-Oxley Act (SOA)

The Sarbanes-Oxley Act of 2002 legislates acceptable conduct regarding the retention of records; electronic and paper for public companies, executives and the general population. It establishes standards for corporate accountability as well as penalties for corporate wrongdoing. The legislation contains 11 titles, ranging from additional responsibilities for audit committees to tougher criminal penalties for white-collar crimes such as securities fraud.

Section 404 of the Act requires management to explicitly take responsibility for

establishing and maintaining an adequate internal control structure. There are four distinct phases to 404 compliance.

- First, companies should take an inventory of internal controls -- where are they sufficient and deficient -- and then assess those controls against a framework such as that of the Committee of Sponsoring Organizations (COSO).
- Second, companies should document how the controls have been assessed and what, if any, policies and procedures will be used to remedy any control deficiencies.
- Third, companies must test to ensure that the controls and any remedies work as intended.
- Fourth, management must pull the prior three phases of activities into a formal report.

Digital transactions and communication form the historical record of business operations and have become part of the financial and legal underpinning needed by auditors, regulators, and boards. Protecting these records minimizes financial risk and strengthens the integrity of the company.

“Sarbanes-Oxley requires public companies to have internal controls in place to ensure that pertinent company information is being properly managed and retained, Internal controls rely on secure IT systems that can manage the storage and flow of company information. In today’s regulatory environment, failure to have proper controls in place is tantamount to failure, which can and does result in the end of careers and fines in the millions of dollars.

Like any new business initiative, Compliance has a lifecycle of activities that are required to understand the issues, define the strategy and organization, assess current state, and then methodically close key gaps through a combination of new software acquisition, development, re-configuration or upgrades.

Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) is a Federal law designed to protect the privacy of a student's education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student, or former student, who has reached the age of 18 or is attending any school beyond the high school level. Students and former students to whom the rights have transferred are called eligible students." When an individual requests student information from a university, the university must respond in accordance with FERPA guidelines. The Department of Education's FERPA guidelines act as the foundation.

Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act requires each institution to implement a written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. The program should be designed to ensure the security and confidentiality of customer information, protect against unanticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. Each institution must assess risks to customer information and implement appropriate policies, procedures, training, and testing to manage and control these risks.

SOLUTION PREPARATION

Whether you're a large or small entity, one tool will not instantly bring your organization into compliance with these regulations. In fact, the concepts behind these regulations are as much to do with procedure as it is technology. In addition, compliance is not a one-time process; it's ongoing. One must constantly monitor your environment.

We now will discuss the implementation of MonitorMagic as a valuable component of not only compliance, but securing the functionality of your network in terms of data integrity and efficient use of equipment.

Planning MonitorMagic For Production

Before deploying your MonitorMagic Network Monitoring infrastructure, we recommend spending some time considering the following questions:

Do I want to monitor all events? You decide which events carry the most impact for your environment. For example, With MonitorMagic - Network Monitoring, you can monitor various objects like disks, services, performance counters, and so on. MonitorMagic uses monitors that correspond with these network devices. An administrator could monitor for a specific event in an event log or the status of a critical service. When this monitor meets certain criteria (Example: Event 5781 or IIS Service Stopped) MonitorMagic would send an alarm or automatically restart the service. In addition, the Windows Network environment provides extensive performance monitoring capabilities. The performance counter monitor is used to check the value and contents of performance counters. MonitorMagic uses a performance counter monitor for each performance counter. MonitorMagic supports all performance counters, including the counters that are part of the operating system, but also the counters that are installed by other applications. You can create performance counter

monitors directly or by using a monitor policy. It is recommended to create performance counter monitors by using monitor policies.

When and how would I know if there was a problem or failure? MonitorMagic uses both rules and monitor policies so you can achieve the level of checking you prefer. The main way of deciding what you're going to track is by setting up rules. Each monitor can have as many rules as you like, and each rule is designed to check on a particular event. You build rules by entering criteria such as 'available disk space is less than 20 percent. When a rule is triggered, MonitorMagic can execute alarm actions, for instance: send an E-mail, send an SNMP trap, or restart a service. Each rule can have any number of alarm actions. You can specify under what conditions alarm actions must be executed. **Custom scheduling and delay**-Every notification type supports custom scheduling and delay settings. These settings include trigger delay, trigger handling when actions fail and repetition. **Escalation**-All alarm actions can be escalated. MonitorMagic executes an alarm action, for instance an e-mail message. If the recipient doesn't respond within a set period of time, MonitorMagic can escalate the incident by executing other alarm actions, such as a e-mail message to management staff or an SMS message to the network administrator's mobile phone. **Custom keywords**-For flexible alarm action configuration, you can maintain your own set of keywords and define these globally per agent. Once the alarm action is processed, these keywords will be specified by the service. This will save you lots of configuration time when for instance email notifications should be sent to different staff every week. Just change one keyword and all email addresses in all your alarm actions will be updated automatically. **Popup messages**-Sends a standard popup message to a computer or a user notifying the status of the incident. The contents of popup messages can be configured using keywords containing status information. **E-mail messages**-Like the popup messages, e-mails can be configured to show relevant status information. **Pager and SMS messages**-MonitorMagic supports sending pager and/or SMS messages to all devices and operators worldwide. The contents of these messages can also be configured like the popup messages. MonitorMagic's pager support doesn't rely on email support by its provider, it has its own built-in protocols and connection software to directly communicate to any local provider worldwide. **Log event**-MonitorMagic can write an event to the event log of a computer, storing the status of an incident. When integrating MonitorMagic with other applications, these applications can receive status information through these log events. **SNMP traps** MonitorMagic can send messages to other computers in the form of an SNMP trap. These SNMP traps can be received by computers running operating systems other than Windows NT/2000. For instance, when integrating MonitorMagic with a central, enterprise management consoles (like HP OpenView, IBM Tivoli or CA UniCenter), MonitorMagic can send messages directly to that application.

How should I store my monitored events? Getting an immediate e-mail or message on your pager if things go wrong is a big improvement but it still means you have a problem. To help avoid this, MonitorMagic offers a range of reports based on your event logs that might alert you before problems occur. You can view reports for each MonitorMagic service that is connected, and all the possible reports can be viewed

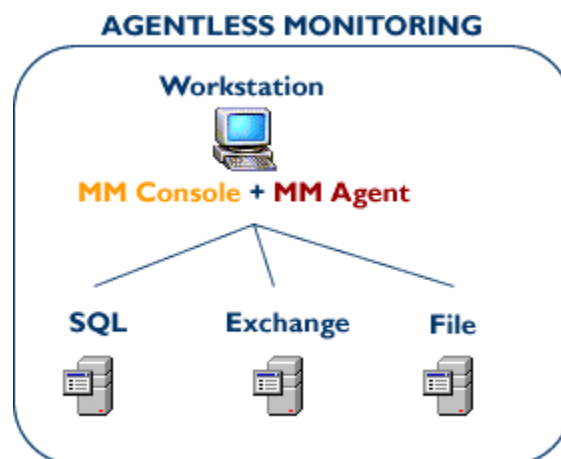
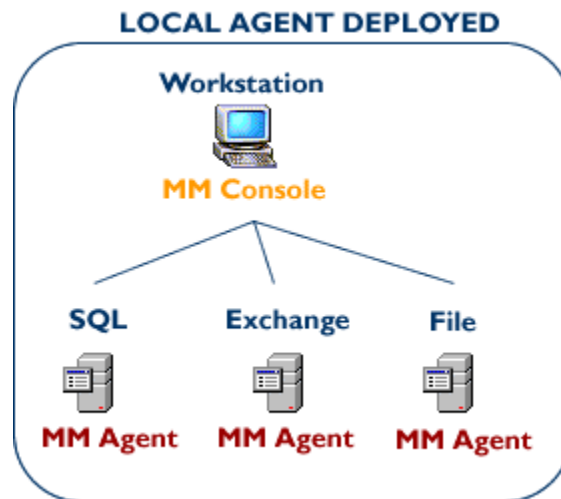
and configured from the main MonitorMagic window. Because the Windows Event log is stored locally on each computer, there is no consolidated source of status information. Windows itself has no method of replicating or synchronizing this information to a single, centrally available audit source. To resolve this, information from the reports is collected and stored in the MonitorMagic database according to the schedule you specify. Report management is easy enough – you can set up report profiles that apply to multiple computers or to a single machine, and where you're specifying a report profile for multiple computers, it doesn't matter if a particular computer isn't running all the MonitorMagic services for which you're asking for reports. This makes life a lot easier as you can ask for all the reports on all the computers and MonitorMagic will sort out exactly what information is realistic. The main problem with the reports, as with all reports collecting information from sources such as event logs, is that you end up with acres of data. All that data is usually stored in a database. You get the choice of using SQL Server, Access, or any ODBC compliant database manager, and the database can be local or remote. Whichever you go for, the database management software needs to be installed before a database can be created. It is treated as a system data source, and you can choose to connect to an existing database or create a new one. You can also choose to store your data locally then transfer it into the database according to a schedule. Once in the database, MonitorMagic can use the data for various purposes, including many of the reports and showing graphs of historical data, as well as predicting trends and carrying out analysis. One of the better ways to examine the health of your system is by viewing MonitorMagic's graphs. You can view both 2D and 3D graphs, and there are options to view either real time or historical data.

MONITORMAGIC IN ACTION

Real-time Monitoring

Agent/Agentless Support – One option is the deployment of agents on monitored servers which in return, reduces the load on the collecting server. Another alternative would be to take advantage of MonitorMagic's unique architecture enabling remote monitoring without the need to install an agent directly on the target computer. Without losing functionality, you can take advantage of all available monitoring capabilities using this concept.

- No software directly on your critical servers.
- Ideal for remote performance polling.
- Virtually unlimited scalability.
- No loss of functionality.
- Minimal network bandwidth usage.
- Minimal server load.
- Does not use memory on target system.
- No additional configuration; drag and drop to activate.
- Flexible agent deployment; use spare server or workstation.



Application Examples

Virus Detection - McAfee NetShield

As administrator, you are responsible for maximum uptime and application performance/stability. When using NetShield as your favorite anti-virus solution, you want the latest updates on virus detections, virus definition updates, and global application performance.

Critical issues - Did NetShield detect any viruses? Is NetShield conducting proper file system scans? Were all virus definition updates successful? Are all NetShield services running OK?

MonitorMagic - Using the "*McAfee NetShield NT/2000 4.5*" policy, MonitorMagic will continuously monitor for virus detection and scan operation events reported by NetShield. All virus definition updates performed by NetShield will be captured and the running state of all critical NetShield services is being scanned.

Norton AntiVirus

As administrator, you are responsible for maximum uptime and application performance/stability. When using Norton AntiVirus as your favorite anti-virus solution, you want the latest updates on virus detection, virus definition updates, and global application performance.

Critical issues - Did Norton AntiVirus detect any viruses? Is Norton AntiVirus conducting proper file system scans? Were all virus definition updates successful? Is the Norton AntiVirus scan engine running OK?

MonitorMagic - Using the "*Norton AntiVirus Corporate Edition 7.6*" policy, MonitorMagic will continuously monitor for virus detection and scan operation events reported by Norton AntiVirus. All virus definition updates performed by Norton AntiVirus will be captured and the running state of all critical Norton AntiVirus services is being scanned.

Backups -

Veritas Backup Exec - job/device monitoring, performance and stability

When you deploy a backup solution, you want to reach maximum data integrity while assuring that the backup actually runs, and that the tapes are correctly written.

Critical issues Does the backup actually start? Are there any tape/device errors reported by Backup Exec? Did Backup Exec encounter open files during backup? How many objects were skipped during backup? How long did the backup operation take? Are there any aborted/active jobs? Do my SQL and Exchange agents behave OK?

MonitorMagic Using the "*Veritas Backup Exec 8.x/9*" policy, MonitorMagic will scan all vulnerabilities of the Backup Exec application. The policy includes service monitoring, event log monitoring, and extensive performance and error characteristics.

ARCServe - backup job monitoring

Critical issues Does the backup actually start? Are there any tape/device errors reported by ARCServe? Did ARCServe encounter open files during backup? Does ARCServe's own log file indicate any issues?

MonitorMagic Using the "*BrightStor ARCServe Backup Windows 9*" policy, MonitorMagic will scan all vulnerabilities of the ARCServe application. The policy includes service monitoring, event log monitoring and log file analysis.

Database -

SQL Server 7.0/2000 - performance and stability

SQL Server is usually a critical component of your database driven website or application. Any possible downtime must be avoided.

Critical issues - Are all services like the SQL agent and the DTS agent still running OK? Are there any unusual SQL server event log entries? Are my databases using too much log space? How many users are currently connected to my database? How much lock memory is being used?

MonitorMagic - Using the "*SQL Server 7.0*" or "*SQL Server 2000*" policy, MonitorMagic will continuously scan the event log for any SQL alerts. This policy will also check the availability of all critical services and performance characteristics like cache ratio, lock memory, and user connections.

Event log reporting

MonitorMagic comes with several pre-configured monthly and weekly reports for computer overview and security analysis. Existing reports are fully configurable using graphic elements, text items, and sub-reports, tables and standard SQL Queries. Both SQL Server 7/2000 and Microsoft Access as a data source support MonitorMagic reports.

Network security - failed logons

HIPAA for example stipulates that you have "procedures for monitoring log-in attempts and reporting discrepancies."

Critical issues - Did a user try to guess a password? Do you need to reset a password? Are people with expired/disabled accounts trying to log in? Are people trying to ignore workstation logon times? Any locked user accounts? Any unusual NETLOGON errors?

MonitorMagic - Using the "*Security - User Logon Failures*" policy, MonitorMagic will continuously scan the event log for any issues regarding user accounts failing to logon to a domain. This includes disabled/locked/expired user accounts, unknown user accounts, NETLOGON errors, and workstation restrictions.

Network security - VPN Access

Due to the open nature of common consumer operating systems, some threats are quite difficult to protect against. For example, it is very difficult to assert with any level of certainty that a single user system, which permits the downloading, and running of arbitrary applications from the Internet has not been compromised. Also, that a covert application is not monitoring and interacting with the user's data at any point in time. Using MonitorMagic, one license allows for 10 workstation monitors. Scan for known trouble application services.

Archiving

Database storage

MonitorMagic includes a powerful event log archiver, which visits your computers at a scheduled time, (for example during the night), grabs all event logs and stores them into a central database. This database can be either Microsoft® Access, SQL Server or the MSDE.

Simple and automatic configuration

Each MonitorMagic agent can be connected to a database, which can either be a new database or an existing database used by another agent. MonitorMagic can create a new Access database file automatically or, when using SQL Server, create all appropriate tables and index on a specific SQL Server.

Duplicate checking - Reduced database space

The architecture for retrieving event logs is built to minimize server load, network traffic, and database space. MonitorMagic will first build up its own event log cache and when storing the event log data into a database, the descriptions will be checked for duplicates. Since the description of events can be long strings, these will consume lots of database space.

Data caching - Archive integrity

When retrieving event logs, MonitorMagic always creates cache files on the local computer to ensure optimum data integrity. For instance, the database connection fails due to a network outage or database failure, MonitorMagic will keep trying to connect to the database on regular intervals to store the cached data. No event data will be lost during the archive process.

Reporting

MonitorMagic comes with 10 pre-defined reports, containing performance characteristics over a set period of time. These reports contain all textual and graphical elements, as well as all the keywords and SQL queries. All reports can be modified and copied freely.

Each MonitorMagic report can contain a table with SQL information queried from the database. You can use any custom SQL query including keywords defined in each report. These keywords can also contain SQL queries, so you can build cascading queries, dependent on each other. Our pre-defined reports are all based on this principle and are available for editing.

Print high-resolution reports with integrated graphics and fully customized layout schemes. No additional software or special printer drivers need to be installed. MonitorMagic will automatically print on the standard available Windows printers using the highest possible resolution supported by the printer.

For portability, MonitorMagic can convert your reports into the industry standard HTML format. When converting a report to HTML, MonitorMagic will write the contents comparable to Internet Explorer, (i.e. HTML file in a root directory and all graphic files in its own sub-directory).

MonitorMagic uses templates to generate reports. Templates allow you to easily add new text or titles and include your company's logo into printed reports. All SQL queries are also contained within each template.

MonitorMagic can generate its own reports in real-time. There is no need for additional software such as Crystal Reports. However, you can integrate your reports with Crystal Reports if desired. All templates are completely open for modification, including all custom SQL queries.

Conclusion

While HIPAA, SOA, FERPA, and GLBA all focus on their respective industry, devising a public set of tough security standards can be valuable to any enterprise that needs to protect its most sensitive traffic.

One of the most irritating aspects of being a systems administrator is that by the time a problem is reported to you, it's already disrupting your smooth running network. What's worse is the knowledge that in many cases you could have limited the damage to a minor inconvenience if you'd seen it in time. In addition, not understanding the problem can cause one to incorrectly diagnose a problem by adding more hardware to a situation that just needs some internal adjustments. Monitoring, archiving, and reporting of server event logs, security logs and infrastructure device logs are a must in maintaining compliance and prudence. Let MonitorMagic do the hard work of gathering and analyzing the data, auditing for unwanted change, and re-aligning systems with policy. Adding automation to this routine but very complex and time-consuming task is the only way your I.T. staff will begin cultivating a more proactive environment while adding value to your network investment.