Dell Software

Best Practices Guide for IT Governance & Compliance

Assess, Audit/Alert and Remediate

Summary

Federal regulations, such as the Sarbanes-Oxley Act (SOX), the Health Insurance Portability Accountability Act (HIPAA), and the more recent Payment Card Industry (PCI) initiative, require businesses to know exactly what changes are being made to structured and unstructured data in their corporate networks. As a result, IT organizations need to provide more detailed monitoring, analysis, auditing, and reporting on the changes being made to this protected data. In fact, auditing of changes made to structured and unstructured data has become a standard business practice for most companies.

This white paper details three critical steps for maintaining compliance with external regulations and internal security policies: assess the environment and controls; audit and alert on unapproved user activity; and develop remediation procedures. Then we discuss four key external regulations that are driving companies to prepare for an IT compliance audit. Finally, we discuss best practices for implementing a compliance solution that will minimize stress during an organization's next IT compliance audit.

While this paper is focused primarily on external regulations that apply to organizations based in the United States or conducting business in the United States, many international regulations have similar auditing requirements that make a compelling case for implementing a comprehensive data protection compliance solution.

Key steps to maintaining compliance

Once an organization has met initial regulatory requirements, it must continue to comply on an ongoing basis. But most companies find that the time and manual effort required to maintain compliance with data protection laws are cost-prohibitive. Thus, automating at least some internal controls is no longer optional; it is necessary to maintain compliance.

As the demands on IT organizations become increasingly complex due to regulatory requirements and other compliance mandates, IT must implement solutions and processes to minimize risk and complexity.

When evaluating the automation of their compliance initiatives, organizations need to focus on three key tasks:

- Assess
- Audit/alert
- Remediate

Assess

To give management visibility into compliance, an organization must assess the internal controls in its IT environment. This assessment process includes comparing the organization's processes and policies to industry standards and recommendations, such as security frameworks like COBIT or ISO 17799 as they relate to specific regulations. Such an analysis often results in a well—scoped compliance program that is officially recognized by management.

The organization also needs to perform a risk analysis to evaluate which controls it considers essential and locate gaps in implementing those controls. This control identification and prioritization process establishes a baseline of controls and aligns it with the organization's compliance objectives as set forth by the compliance program.

Organizations should evaluate the following areas:

- User rights throughout the network
- Group memberships and the access privileges they provide
- Permissions to access files and folders
- Alternative locations of files, such as Exchange or SharePoint
- Configuration settings of systems

Assessment should be an ongoing process for any organization since the baseline of internal controls will change and require maintenance to meet ever-evolving IT requirements. As the demands on IT organizations become increasingly complex due to regulatory requirements and other compliance mandates, IT must implement solutions and processes to minimize risk and complexity. This strategy enables IT to function as a viable business unit, ensure fewer outages, and demonstrate greater control over IT infrastructure and services.

Audit/alert

Once the baseline for internal controls has been established, IT organizations must continually audit the environment and alert stakeholders to changes from the baseline, including violations of corporate policy and security breaches. Alerting provides immediate notification about business-critical offenses and helps mitigate exposure and risk.

Verizon's *2012 Data Breach Investigations Report* shows that 97 percent of breaches were avoidable through simple or intermediate controls and that 92 percent of incidents were discovered by a third party. Therefore, to mitigate risk, organizations must track both user and administrator activity from logon to logoff, including the files accessed, the changes made to permissions, and the changes made to established security policies. Auditors look for evidence that a company has processes and procedures in place to audit its users and their activities. Often auditors will include "spot checks" in their audits that require the ability to find specific data or data from a specific point in time. Forensic analysis enables organizations to replay a violation as it occurred, which helps the organization learn how to prevent the violation from being repeated in the future.

Audit log management

Audit log management is about making sense of the multiple, separate audit logs generated within an organization's infrastructure. An effective audit log management strategy includes managing event logs from servers, workstations, network devices, and applications to collect, store, and report on event data.

Many companies struggle to glean meaningful information from their event logs that can support auditing efforts. In most cases, the system administrator must sift through the multitude of event log files using native operating system tools, which is an extremely time-consuming task usually performed on a reactive, ad-hoc basis. These native event viewers are insufficient and not intended to be used as true event log management solutions because they provide no means of:

- Collecting event data from multiple systems and applications
- Generating reports to support an audit
- Generating alerts on critical violations to organizational policies

Effective audit log management solutions do exist, however, and they will be discussed later.

Remediate

Many regulations require an organization to have a written remediation policy that specifies the actions that will be taken in the event of a corporate policy violation. Informing all internal users of the consequences of a violation can help deter them from committing violations, and specifying the steps to take in the event of a violation can help minimize its impact. Auditors often look at remediation policies very closely; they are a key component of any external audit.

At least two forms of remediation are available: proactive and reactive.

- Most organizations are reactive. Organizations achieve reactive remediation by de-provisioning accounts in the event of a violation or inappropriate activity, automatically disabling an account after a pre-defined action has occurred, or shutting down a server due to an unapproved change. This type of policy normally passes an audit because no IT department can effectively control everything.
- Proactive remediation techniques, which more organizations are beginning to implement, prevent unauthorized or unapproved changes. For example, an organization can prevent the modification of business-critical objects in Active Directory, applications, or systems.

  Proactive remediation can also include pre-defined role management, as well as provisioning and de-provisioning of accounts, which helps to separate duties among administrators.

Regulations and corporate compliance

Many government regulations are designed to govern the practices of corporations, protect individual's rights to privacy, and spur adherence to standard best practices. The following sections provide a general working knowledge of four key regulations that affect IT departments in the United States and, to a lesser extent, international organizations doing business in the Unites States:

- The Health Insurance Portability and Accountability Act (HIPAA)
- The Gramm-Leach-Bliley Act (GLBA)
- The Sarbanes-Oxley Act (SOX)
- The Payment Card Industry Data Security Standard (PCI DSS)

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act was signed into law on August 31, 1996. Virtually all health care organizations, including health care providers, are affected by HIPAA requirements. The intention of HIPAA is to enforce standards for privacy, security, and electronic interchange of health information. In particular, HIPAA requires health care organizations to:

- Ensure the confidentially, integrity, and availability of all electronically protected health information that organizations create, receive, maintain, or transmit
- Regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports
- Establish, document, review, and modify a user's right to access a workstation, transaction, program, or process
- Monitor login attempts and report discrepancies
- Identify, respond to, and document security incidents

> An effective audit log management strategy includes managing event logs from servers, workstations, network devices, and applications to collect, store, and report on event data.

SOX provides additional oversight to the audit process and eliminates conflicts of interest by creating a standard set of criteria that all publicly held corporations must adhere to in managing their financial data.

HIPAA dictates the use of security standards, privacy standards, electronic transaction and code sets, and unique employer identifiers when managing and maintaining critical data. While compliance is federally mandated, compliance also benefits health care organizations by providing patients with confidence that their sensitive personal data is safeguarded from inappropriate use.

With stiff penalties for non-compliance, health care organizations are aggressively working toward demonstrating HIPAA compliance. Meeting these challenges requires that IT departments have systems and processes in place to collect, store, and report on the events occurring within their networks, thus creating the required audit trail.

Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act was signed into law in November of 1999. To comply with GLBA, all organizations in the financial services industry must implement a comprehensive security program specifying how their customer information is protected. In particular, these organizations must implement:

- Dual control procedures, separation of duties (SoD), and employee background checks for employees with responsibilities for or access to customer information
- Monitoring systems and procedures to detect actual and attempted attacks on, or intrusions into, customer information systems

Compliance with GLBA is regulated by federal banking agencies, such as the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation. Because many organizations have already been audited and found to be out of compliance, GLBA was expanded with detailed instructions for deploying an information security program. In clarifying the new guidance, the Federal Financial Institutions Examination Council (FFIEC) states: "Security is an ongoing process, whereby the condition of a financial institution's controls is just one indicator of its overall security posture. Other indicators include the ability of the institution to continually assess its posture and react appropriately in the face of rapidly changing threats, technologies, and other business conditions." Institutions must prove their readiness by conducting regular self-audits of their enterprises and documenting the results.

Sarbanes-Oxley Act (SOX)

The Sarbanes-Oxley Act was passed in July of 2002 as a direct reaction by the U.S. Congress to the accounting scandals of late 2001 and early 2002. SOX provides additional oversight to the audit process and eliminates conflicts of interest by creating a standard set of criteria that all publicly held corporations must adhere to in managing their financial data. It also seeks to advance the standards for corporate governance. Record retention is central to SOX. In particular, companies and their auditors are required to retain more records than before, including all documents and data that relate to an audit. Fines and jail terms are imposed for the deliberate and willful destruction of audit-related data, and an auditor is responsible for oversight of the enterprise's internal documentation surrounding the audit. In addition, the Retention of Records Relevant to Audits and Reviews as directed by Section 802 of the act states that the Securities and Exchange Commission (SEC) will dictate rules and regulations concerning "the retention of records such as work papers, documents that form the basis of an audit or review, memoranda, correspondence, communications, other documents and records (including electronic records) which are created, sent, or received in connection with an audit or review and contain conclusions, opinions, analysis, or financial data relating to such an audit or review."

Companies with a market capitalization greater than $75 million were required to comply with these new rules for fiscal years ending on or after November 15, 2004; other companies have received extensions. Under the law, the retention time for records is generally five years; however, retention periods vary according to a number of variables. IT executives need to formulate and formalize an enterprise-wide strategy to best manage such data now and into the future to reduce the enterprise's large exposure and ensure future data integrity.

Payment Card Industry Data Security Standard (PCI DSS)

What Is the PCI DSS?

In September of 2006, five payment card brands (Visa Inc., MasterCard Worldwide, American Express, Discover Financial Services, and JCB International) formed the PCI Security Standards Council to develop a new standard for securing their customers' payment card data. The members of the council jointly require all merchants who process payment card transactions with their brands (credit cards and signature debit cards embossed with a council member's logo) to comply with the new standard, the Payment Card Industry Data Security Standard (PCI DSS). All banks that process payment transactions associated with these cards are responsible for ensuring their merchants meet the standard, and penalties for failing to comply with the standard can be severe.

Who Is subject to the PCI DSS?

PCI DSS has broad applicability. In order to determine whether a company is subject to the PCI DSS compliance, answer the following questions:

- Is the business any of the following?
- Card acquirer
- Merchant
- Processing agency
- Does the organization store, exchange, or transmit payment card data on any of the following systems and devices?
- Database or application servers
- Workstations
- Firewalls
- Routers

If the answer to either of the preceding questions is yes, then the organization needs to be compliant with the PCI DSS regulations. One key poin t to understand is that these regulations apply equally to organizations of any size, whether they have one employee or one million employees.

Key requirements of the PCI DSS

The PCI DSS version 2.0 took effect on Jan 1, 2011, bringing more clarity to the existing set of requirements and introducing new ones. The PCI DSS is composed of six best-practice areas and 12 high-level requirements for securing protected data that include strong access controls, user activity monitoring, change tracking, and record retention.

Key requirements of the PCI DSS 2.0 are outlined below.

Establish reliable & meaningful audit trails

Today, almost all elements of organizational IT infrastructure—including operating systems, network devices, firewalls, databases, and applications—have some kind of auditing built in. However, native audit trails inherit the following issues that are difficult to manage:

- **Unmanageable volume of generated events** —In a typical IT environment, the various systems log gigabytes of event data daily and provide no native log consolidation tools. Therefore, organizations risk losing event data when logs roll over. Since no one can tell beforehand what log data will be needed when bad things happen, it's critical to ensure that all audit data is captured and saved in a reliable manner.
- **Cryptic descriptions of events**—Most native audit logs were added as an afterthought once the main functions of the system or application they belong to were developed. That's why a disconnect exists between what the system or application puts in its logs and what administrators would like to see in the logs to understand what specific users actually did in the system or application.

> ...companies and their auditors are required to retain more records than before, including all documents and data that relate to an audit.

Without appropriate tools, administrators are hard-pressed to distinguish the most important events from a myriad of others. Moreover, they must then try to obtain all the information they need from the cryptic descriptions recorded in the logs.

To enable administrators to use native logs effectively, a solution must address both of these issues as well as cover the gaps in what the native logs record.

The PCI DSS regulations require organizations to collect audit data located anywhere on the network and store it for an average of at least two years.

Preserve audit data in long-term storage

The PCI DSS regulations require organizations to collect audit data located anywhere on the network and store it for an average of at least two years. Organizations often underestimate their log storage needs and run into significant issues when they run out of the storage they allocated upfront.

Track user access to protected data

The PCI DSS requires organizations to prove "who did what" for each user action involving any protected data. The organization must capture the entire context of each user action, including all of the following:

- The "before" and "after" values for each change event—Simply recording that a given user made a change to a particular IT resource is not enough; each change event contains the "before" and "after" state of that resource. For example, each time a critical Active Directory object is changed, the corresponding event must contain the value of the object attribute before and after it was altered.
- The origin of the event—Sometimes, when several people share the same administrative account to do their jobs, it's impossible to trace an action back to a particular individual without knowing which computer the action was performed from. In those cases, it's essential to track the origin of the event down to the particular workstation the user was logged into when taking the action.

Monitor file integrity

The organization must monitor the integrity of all critical files and folders whose modification can compromise system security. This process must meet the following requirements:

- Staff in charge of system security must be notified of all changes to critical system files. Every time a critical system module or data file is changed, the appropriate personnel should get a notification that kicks off a change review process.
- As part of the change review process, administrators must have tools to distinguish legitimate changes from accidental and unwanted ones that can impair normal business operations.
- If a file change under investigation is deemed inappropriate and in violation of the established security policy, the organization must be able to roll the change back before it adversely affects the business.

Establish & enforce separation of duties

Organizations must implement the principle of separation of duties to separate auditors from administrators whose actions are being audited. In particular:

- Organizations have to make sure that audit trails are tamper-proof and protected from unauthorized modification. Attempts to clear up the log may be a sign of covering tracks after a successful attack to the compromised system. That's why it's important to ensure integrity and authenticity of the logs in the first place.
- A thorough delegation model must be available to grant different levels of log data access to different people within the organization. For example, the help-desk personnel might need access to only the parts of the audit trail showing account lockout events while internal auditors will most likely need access to all log data to conduct periodic log reviews.

Review audit data regularly

The PCI DSS standards require organizations to carefully review the activity of both regular and administrative users and evaluate that activity against established security policies. Different types of activity require review at different frequencies:

- Administrative activity—Daily
- Access to critical system files and

folders—Daily

- Failed access attempts—Weekly
- Successful resource access—Monthly

According to the Verizon 2012 Data Breach Investigation Report, 96 percent of victims subject to PCI DSS had not achieved compliance because they had either not conducted regular assessments or had never assessed and validated their controls.

Compliance benefits

Compliance with any of the four compliance regulations discussed above has broad benefits:

- **Avoiding fines and loss of business**—The costs of noncompliance often exceed the costs associated with maintaining compliance over time. If organizations fail to comply, not only will they face stiff fines and penalties, but partners and customers may take their business elsewhere, where they can be assured that their interests are protected.
- **Increased security and operational efficiency**—Compliance initiatives often increase security and operational efficiency across the organization. When IT staff starts implementing security best practices described in compliance regulations, they often expose security holes and inefficiencies in internal processes that the organization was unaware of.
- **Visibility into day-to-day IT operations**—Looking into what resources IT staff can access and what actions they are permitted to perform is often eye-opening. Organizations often find that employees have access to sensitive data they shouldn't see or that multiple administrators use the same account and password. Knowledge is power, and this knowledge will empower organizations to improve the security of their data and IT systems.

Internal security policies

We have discussed several external regulations that are driving corporations to perform audits and prove compliance. Organizations may also put into place internal controls, typically through their IT, human resources, legal, security, or compliance departments. Many companies put auditing and security policies in place to maintain control over their infrastructures. Some companies capture daily events, such as successful logons and logoffs, so they can understand who is on their networks at any given time. Another example of an internal security policy is the requirement to track the activity of privileged users who have been granted the rights to set up new user accounts or remove users from the enterprise. The rights granted to these users can easily be abused, leaving the organization exposed to an internal security threat.

Summary

Maintaining compliance with external regulations or internal policies means, at a minimum, keeping track of all electronic documents (data files, email, images) that are covered by those regulations and tracking access to those files. Upon request, organizations need to prove, through reporting, that they have established appropriate control over access to resources. With the right auditing solution, organizations can capture, collect, store, and report on events related to security-sensitive user activity (such as account creation, group membership changes, and permission changes) and also notify the responsible personnel of events that might indicate an intrusion.

Best practices for managing compliance

Now let's turn our attention to best practices for implementing a compliance solution. These best practices can be grouped into three key steps:

1. **Planning**—Determine how the regulation affects the organization. What functionality is needed from a solution, and which parts of the infrastructure are involved?
2. **Selecting**—Review vendors and solutions that best meet the requirements.
3. **Deploying**—Consider issues that may occur when rolling out the compliance solution.

Planning

To successfully implement an IT compliance solution, organizations

Organizations have to make sure that audit trails are tamper-proof and protected from unauthorized modification. Attempts to clear up the log may be a sign of covering tracks after a successful attack to the compromised system.

must plan carefully and pay special attention to both technical and business needs. They must also be keenly aware of how external regulations and internal policies affect the organization and IT in general. Here are the recommended steps for planning the deployment of a compliance solution:

With the right auditing solution, organizations can capture, collect, store, and report on events related to security-sensitive user activity... and also notify the responsible personnel of events that might indicate an intrusion.

Step 1: Define the critical reasons for implementing a compliance solution
When defining the reasons to implement a compliance solution, pay special attention to the business and best practice reasons discussed in the Regulations and Corporate Governance section of this paper. Understanding auditing requirements and how they affect an organization early in the process will help them conduct a stress-free audit when the time comes. Also consider the recipient of the auditing information; is it someone like the CISO or will it be an auditor?

Step 2: Determine what functionality is required from a solution Based on a list of reasons defined in the previous step, identify what type of information needs to be collected and reported on. For example, HIPAA requires organizations to archive logon attempts. For this type of task, many organizations need to collect and store events from their servers' security logs.

Once this information has been identified, choose the functionality required from a solution:

- **Caching** enables organizations to provide reasonable assurance that no logs have been lost or tampered with.
- **Archiving** enables organizations to prove compliance with legislative regulations and prepare for forensic investigations.
- **Analysis and reporting** allows organizations to track user activity.
- **Baselining** enables organizations to measure a specific system and compare it against all other servers in the organization for standardization and compliance.
- **Real-time monitoring** provides alerts on events critical to business continuity. In addition, many products can prevent certain actions that might be detrimental—such as domain renames—even when attempted by properly provisioned users who would normally have the right to take the action.
- **Provisioning** automates the process of assigning rights to users and groups based on variables set in their profiles.

It is also useful to rank requirements by importance. For example, is the ability to select a compatible font as important as the ability to schedule a report?

Step 3: Choose which components of the environment are critical for compliance
Based on the reasons for implementing a compliance solution, organizations can single out the resources necessary for the corresponding processes. For example, if a government regulation requires organizations to track user access to protected data, then those organizations need to monitor only computers that contain protected data as well as track who has access to them at any point in time and how their rights change. In other instances, organizations may need to collect information from all servers or even from individual users' workstations.

Performing a technical assessment will help the organization determine which parts of the environment need to be monitored. This knowledge will help in estimating the required scalability of the solution. For example, a regulation might require the collection of the following information about computers on the network:

- Computer roles, such as domain controller, member server, and workstation
- Platforms and operating system versions installed
- Resources, such as file shares, directory objects, and printers, for which access will be reviewed

Step 4: Estimate the volume of information
Ascertaining the space required to store events and various configuration data is very important since the reporting and

archiving functions of the compliance solution usually store a large amount of data. Estimation can be a time-consuming and laborious task, which is best handled by automation.

Determining the number of resources, the type of information to be retained, and the retention period helps establish the performance requirements of the compliance solution.

Evaluation criteria for selecting a solution

Once the requirements have been defined, it is time to choose the solution to implement. We recommend that organizations perform a technical evaluation, preferably in a lab environment that closely mimics the production environment. The evaluation process includes determining specific technical criteria and prioritizing them. The most important criteria for evaluation relate to the main functions a solution should perform—that is, assess, audit/alert, and remediate. The importance of each criterion depends on the type of solution required.

Our recommendation is to evaluate each solution against the criteria presented below and choose the one with the highest scores in the areas most important to the particular organization. Regardless of the type of solution required, it is important to evaluate each function (assess, audit/alert, and remediate). We recommend that organizations consider the following for each function:

	Automation	Analysis & reporting	Storage
Assess	Collection of data as it relates to configuration information for the server environment should be automated.	Detailed reporting should be provided in categories, such as permissions, policy settings, and hard-ware/software information.	Information should be stored in a secure, streamlined storage area to enable the organization to track changes over time.
Audit/alert	The capture, aggregation, and storing of events involving user access to sensitive information resources should be automated. Alerting should be available through a choice of technologies, such as email or SNMP, and easily integrated into existing processes and tools.	Detailed reporting and alerting is required to provide both periodic review of user activity and security.	Because audit logs can grow quickly, compression is a key to long-term storage.
Remediate	Provisioning should be automated to ensure that all users are assigned the correct permissions based upon their roles in the organization.	Detailed reporting should be available to ensure that all users are assigned permissions in accordance with established security policy and business needs.	Information should be stored in a secure, streamlined storage area to enable the organization to track changes over time.

Configuration management

The solution must be able to take a complete snapshot of a system and compare it against a known or recommended state of another system.

It's also important to consider events that track configuration changes to the compliance solution itself to know if users are changing the auditing system.

Scalability

Scalability is the product's ability to maintain its efficiency when the environment grows in size or volume. Consider several features when determining the solution's scalability:

- **Traffic compression**—The ability to compress traffic across the network and on file storage systems
- **Filters on data sources**—The ability to specify what data to collect at a granular level
- **Compare**—The ability to compare the collected data against a defined list of requirements
- **Distributed collection**—The ability to load-balance the data collection process among several collector servers, which may be spread out geographically
- **Incremental updates**—The ability to update a configuration data store with only the changes that occurred since the last data collection

Security

Consider whether the solution provides the following security features:

- **Traffic encryption**—Encryption of traffic between agents and servers
- **Agent/server authentication**—

> The most important criteria for evaluation relate to the main functions a solution should perform—that is, assess, audit/alert, and remediate.

Delivery of alerts to responsible persons should be fast and reliable and include a number of notification methods. In addition to the notifications, a series of linked response actions should be available.

Authentication between agents and servers

- **Optional agent-less collection**—The ability to optionally collect data without agents is required in environments where the use of agents is prohibited on important servers for security reasons
- **Caching of local data**—The ability to cache audit logs as they are being created in a separate, secure location to prevent anyone from tampering with and losing audit log data
- **Guaranteed message delivery**—The ability to withstand network or server outages and maintain a list of events that occurred during the outage. Local agent-based alerting for critical events can also be useful.

Performance

Two important criteria for evaluating performance are the number of events the agent collects per second and the maximum number of agents a single instance can support. Also, the solution must scale horizontally through the addition of management servers and distributing agents.

Alerting / correlation

Delivery of alerts to responsible persons should be fast and reliable and include a number of notification methods. In addition to the notifications, a series of linked response actions should be available.

- **Notification methods**—The product should be able to send alerts via Web, email, and smartphone, as well as SNMP for organizations that have deployed broad monitoring solutions, such as HP OpenView.
- **Response actions**—The product should provide the flexibility to link other processes to the event when certain criteria are met. For example, if a policy change occurs, the application should be able to launch another application in response.
- **Correlation**—The product should allow organizations to gather events from different systems and group them into an alert or report to inform the administrator of suspicious activity.

Storage

Consider whether the solution offers the following features:

Two data storage types—A complete product must have two data storage types: a file repository structure for archiving and database support for analysis and reporting.

- **Backup technology**—The ability to easily back up collected event data is mandatory since some regulations require long-term storage of event data.
- **Granular restore**—The ability to restore selected granular portions of event data is a must.
- **Consolidation technology**—For widely distributed networks or networks with slow links, the product must be able to automatically consolidate event data from multiple data stores on a scheduled basis.
- **Retention management**—The ability to delete unnecessary granular portions of event data from the data storage is required.

Data collection management

Data collection management refers to the resources required to deploy and manage the entire data collection process. Below are criteria by which to evaluate this effort:

- **Configuration flexibility**—It should be easy to specify computers, define event filters, and schedule settings.

Agent deployment—In order to accelerate the deployment process, a product should be able to install agents remotely. Note that a manual installation process may also be necessary when remote access to the target computer is blocked (e.g., by a firewall). Also consider other ways of automating the deployment process, such as using Group Policy.

Agent management and troubleshooting

The product should provide for centralized, low-cost agent management through important features, such as remote activation and deactivation of agents; automatic delivery of upgrades to agents; deployment of custom utilities on monitored computers for use by agents; and monitoring of agent functioning.

Automated provisioning

The solution should enable the organization to set rules for provisioning and de-provisioning all user accounts and associated permissions based on certain variables in the account.

Change control

The solution should enable the administrator to require a chain of approvals by email before an actual change takes place in the infrastructure.

Adjust auditing

The solution needs to be able to separate the "wheat from the chaff." The organization must be able to exclude events from alerting and reporting that are considered "white noise" or normal operations.

Reporting

The solution should include the following reporting capabilities:

- **Predefined expert knowledge**—The solution should either contain reports to meet auditing requirements or should permit editing of the reports that come with the product to meet the requirements.
- **Data analysis and representation features**—The product should offer well-formatted reports, advanced filtering, drilldown features, charts, and forensic analysis capabilities. Some reports will need to be text-based while auditors may want more visually appealing reports.
- **Report distribution system**—The solution should enable organizations to export reports to commonly-used formats and distribute them as needed, for example, through email or by publication to a Web portal. Automation of the report creation and distribution is also important.
- **Single view**—The solution should take all information from different sources and provide a single view into the organization's compliance initiatives.

Deploying a solution

Once the appropriate solution has been selected, the final step is deployment. Two key issues that should be considered before starting the deployment process are:

- Performance
- Audit and event log retention settings

Once organizations are armed with a comprehensive technical view of the environment, they need to determine the number of management servers and their locations on the network to effectively distribute the load. Take into consideration the following issues that may affect the performance of the solution.

Collector servers

For servers dedicated to collecting the data:

- **Performance rate**—The performance rate is defined as the number of events processed per second, the number of changes per day within Active Directory, or the number of objects being managed. This measurement will help with the estimation of how many monitored computers one collector server can handle. However, for best results, always test the solution in a lab environment as similar to production as possible.
- **Traffic load**—Ensure that the link between the collector server and the monitored computers is sufficient. Otherwise, network bottlenecks may impede data collection or changes being pushed to the environment. In regard to audit log management, we recommend agent-based solutions with compression and alerting as well as the ability to schedule collection during non-business hours.

This information will enable organizations to deploy one collector server per N computers and run the collections every X hours (or minutes), where N and X depend on the organization's unique characteristics and needs, including the following:

- Growth rate of the logs
- Collection performance rates
- Periodicity of reporting
- Impact on traffic

Storage servers

For servers dedicated to storing event data, be sure to distinguish between storage servers designed for archiving purposes and those for analysis and reporting purposes. Archiving storage servers should minimize space

> The solution needs to be able to separate the "wheat from the chaff." The organization must be able to exclude events from alerting and reporting that are considered "white noise" or normal operations.

Confirm that the systems will register only events needed to satisfy the requirements outlined earlier and no more so as to limit the amount of storage the solution requires.

consumption whereas reporting and analysis storage servers should be optimized for fast analysis of data.

- **For archiving**, consider using a long-term storage system rather than a database system. A database system requires several times more space and therefore has a higher total cost of ownership than specialized file-based repositories or native file formats (.EVT, for example) due to the cost associated with purchasing and maintaining more disks and the cost of underlying database management software.

For analysis and reporting, a database is preferred since the ability to analyze, correlate, and report is paramount. However, keep the database reasonably small for fast report compilation by:

- Storing data for a defined short period of time (two to four weeks)
- Maintaining separate reporting databases for different parts of the environment.

Forensic analysis of security incidents and suspicious user activities usually involves digesting large amounts of historical data that cannot fit in a relational database. In such cases, consider alternative audit log data storage and querying technologies. File-based data repositories featuring sophisticated data compression and indexing techniques, as well as powerful interactive querying capabilities are becoming a de-facto standard for dealing with vast amounts of audit log data.

Storage consolidation

To minimize traffic and performance issues, consolidate storage. Using this technique, which is illustrated below, each collector server has its own local storage, where frequently collected logs reside. Collections may occur every one to two hours to prevent the logs from being overwritten. Then, periodically (every night or even less often), these local storages are consolidated into a single global archive, satisfying the need to archive data or to perform ongoing analysis and reporting

Audit and event log retention settings

Another important step in the deployment is to verify that the audit settings for the selected part of the environment are appropriate. In other words, confirm that the systems will register only events needed to satisfy the requirements outlined earlier and no more so as to limit the amount of storage the solution requires.

If audit logs of a particular system, application, or device do not provide a satisfactory level of detail for critical types of user access or system changes, consider solutions that offer proprietary methods to capture needed audit information, not dependent on the native logs.

Conclusion

Whether to comply with federal regulations like HIPAA, SOX, or GLBA, or to meet internal security policies, managing the infrastructure effectively can eliminate stress.

Maintaining IT governance and compliance has become a standard operating procedure for many organizations. The key to successfully deploying a solution lies in:

- **Defining requirements**—Determine the business need and how that translates into necessary IT controls and requirements. Assess risks, assign values to them, and then identify gaps in the current security environment.
- **Selecting a solution**—Be sure the selected solution has sufficient functionality to assess, alert, and remediate in line with the organization's specific compliance and business requirements.
- **Deploying the solution efficiently**—Take into account performance factors for the solution and the environment.

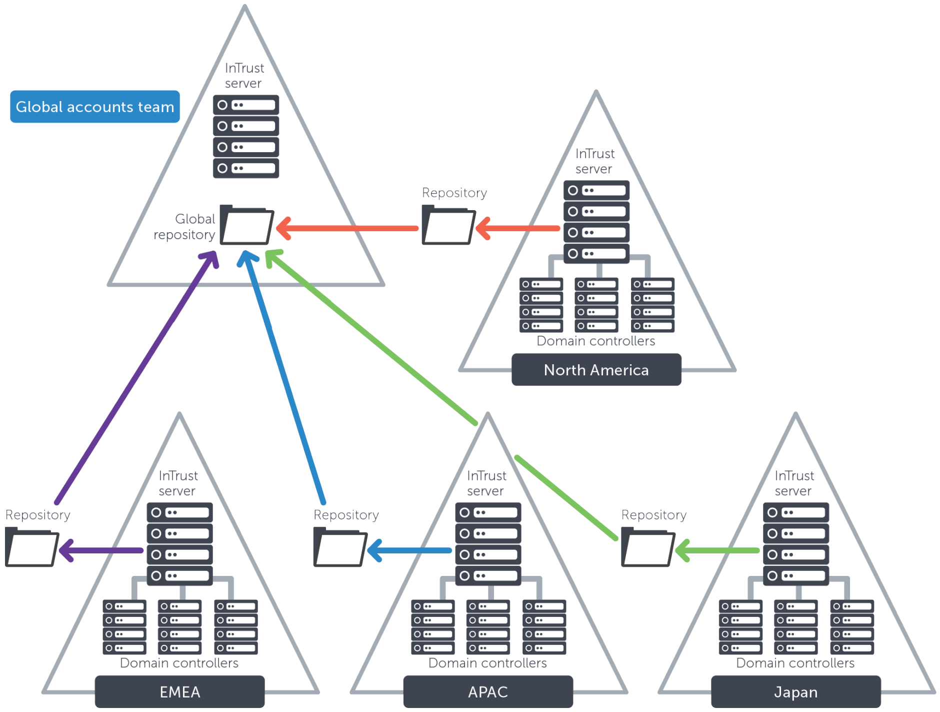

Figure 1. Storage consolidation allows widely distributed networks to regularly collect data locally and consolidate it into a central database.

Whether to comply with federal regulations like HIPAA, SOX, or GLBA, or to meet internal security policies, managing the infrastructure effectively can eliminate stress.

For More Information

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

About Dell

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.dell.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dell.com
Refer to our Web site for regional and international office information.