Select the right security information and event management solution

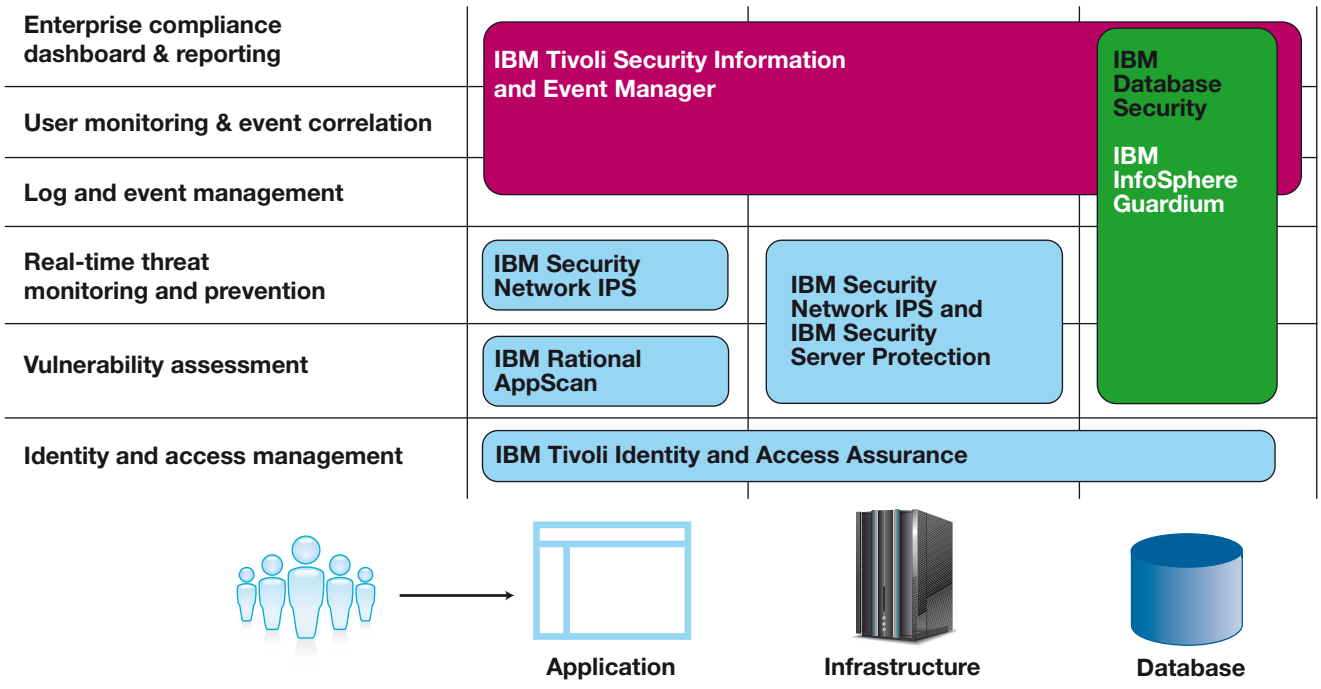
Enhance security and facilitate compliance with IBM security information and event management solutions

IBM

Security information and event management (SIEM) is a fundamental control of security frameworks. IBM offers a complete SIEM solution that provides for integration with identity and access management (IAM), database access monitoring (DAM), vulnerability assessment, compliance management, log management and threat monitoring and prevention. Your SIEM vendor must provide this same breadth of coverage in order to provide security and facilitate compliance across the enterprise.

SIEM solutions allow enterprises to cope with the proliferation of security events and alerts that IT systems generate daily. These solutions automatically separate the small but critical number of potential breaches from the vast majority of nonthreatening noise from routine events. SIEM solutions also help ensure that security information and events are properly monitored, recorded and reported for regulatory compliance. By centralizing relevant events, then analyzing and reporting on the consolidated data, the right SIEM solution can help:

- Increase visibility into user activities and noncompliance.
- Manage compliance initiatives effectively and efficiently.
- Automate repetitive time-consuming and expertise-intensive activities.
- Improve responsiveness to requests for audit information.
- Reduce the costs associated with audits and failed audits.



IBM solutions provide comprehensive security capabilities across applications, databases, and infrastructure.

Organizations often begin by deploying a log management solution to collect, record and store voluminous, diverse data. Then they will expand to a full SIEM solution that translates raw log data into meaningful information. A solution such as IBM Tivoli® Security Information and Event Manager makes it possible to detect security threats quickly and easily, and even prioritize threats based on business relevance. This solution enables you to easily know and prove exactly who did what, when, where, where from, where to and on what, reducing audit costs and consequences.

The accompanying diagram shows how SIEM can be integrated with other components—particularly DAM—to protect sensitive data against internal and external threats. DAM complements SIEM by providing deep analysis of database traffic and extensive profiling of database queries. DAM, with its focus on real-time analysis of transactions, does not need to rely on log collection as SIEM does. This allows DAM solutions to monitor DBA and other privileged-user activity more effectively than SIEM alone. SIEM, with its broader enterprise scope, collects logs from devices, databases (through DAM integration), systems and applications. Results from both can then be correlated to provide an unparalleled picture of events across the IT infrastructure.

Getting started with SIEM

This buyer's guide outlines features and capabilities that comprise an effective SIEM solution, including:

1. Centralized log management
2. Insider threat analysis and privileged user monitoring
3. Reporting for audit and compliance
4. Event source support
5. Productivity, flexibility and integration

This guide discusses the benefits of each capability and provides check lists to help you evaluate whether or not a particular vendor's solutions address each of these areas effectively. You will also find check lists to help you evaluate improving productivity and time to value, as well as tips to help you select a provider that can support the full breadth of your security requirements.

1. Centralized log management

One of the most critical components of SIEM is the ability to reliably and verifiably collect original log data while ensuring provable non repudiation of the data. The typical large enterprise generates gigabytes of log data every day from critical applications, databases and platforms, all of which must be captured and retained for extended time periods. Few organizations possess the necessary time and man power to manually collect this information, nor would it be strategic to do so when these resources could and should be allocated to higher-value activities.

Centralized, automated log management can significantly reduce the time and effort needed to efficiently collect, organize, archive, investigate and retrieve logs for forensic and historical analysis. A superior SIEM solution allows you to reliably collect log data from dispersed sources across the enterprise in a continuous, sustainable manner. Just as important, it provides fast, easy-to-use search capabilities that allow you to retrieve the data without having to resort to cumbersome, homegrown tools or highly technical query languages. So whether you need evidentiary proof or information for historical analysis, the right SIEM solution can ensure you will have the answers you need quickly.

2. Insider threat analysis and privileged user monitoring

While external security threats typically receive the majority of the attention, internal security incidents can pose an equal—if not greater—threat. Privileged users are the main source of insider threat. These users often have unrestricted access to critical intellectual property and proprietary confidential information that resides in databases, applications and mainframe systems—access that is largely unmonitored. Insider threats can cause irreparable loss of information and a great deal of harm to your enterprise, whether intentional or accidental.

Centralized log management

Look for a solution that:	IBM	Other Vendor
Provides a reliable and verifiable log management process.	✓	
Includes a log management dashboard to view the overall status of the log management process.	✓	
Provides administrators with a log collect history report that enables them to view the history of the collection process, determine if it is running well, and perform a level of diagnosis using the report.	✓	
Enables auditors and security officers to effectively monitor and audit the actual collection of log data to ensure that no data is lost.	✓	
Provides auditors with a log continuity report (in both graphic and table format) to enable them to see which devices and applications are being monitored, determine if a continuous set of collected logs exist for those devices, and indicate issues that need to be addressed.	✓	
Includes a log investigation tool with a Google-like search facility to search the collected raw log data for specific events or data.	✓	
Includes a log retrieval tool that enables the user to search for and retrieve specific log files from the log archive.	✓	
Provides proactive alerting on collect failures so that any potential loss of audit data can be minimized or mitigated.	✓	
Provides 18 out of the box reports that work directly on the collected logs for rapid time to first report.	✓	
Provides scheduled reporting on a user-defined schedule.	✓	
Enables reports to be exported in common formats such as PDF and CSV for interfacing with other applications and workflows.	✓	
Leverages advanced reporting tools (BIRT) to create new custom reports according to your specific requirements.	✓	
Organizes the logs collected using an indexing schema for easier identification and storage.	✓	
Stores logs in a compressed format to reduce storage requirements.	✓	

Continual oversight is needed, along with maximum visibility of user activity and ready access to information that enables you to monitor who does what, when, where, where from, where to, and on what systems. An effective SIEM solution not only collects and preserves raw log data for evidentiary purposes but also translates and normalizes it into meaningful information that enables you to monitor user access and policy compliance.

Your SIEM solution should display this normalized information through an enterprise audit dashboard and dynamic reports that allow you to view logged activity in comparison with user profiles or drill down to detailed, easily understood reports. Through a comprehensive dashboard, organizations should be able to instantly view their compliance status, allowing them to pinpoint areas of concern and potential violations that require immediate investigation and remediation. If someone is doing something that is out of compliance with policy, the solutions should quickly generate an alert in a form that can be easily understood and actioned as needed.

Furthermore, you should have a quick way to demonstrate to auditors that your organization:

- Logs and reviews systems administrator and systems operator activities on a regular basis.
- Analyzes and investigates security incidents and suspicious activity, plus takes remedial actions.
- Logs access to sensitive data, including root/administrator and database administrator (DBA) access.
- Continually maintains and reviews application, database, operating system and device logs.

Finally, you should be able to monitor for the following activities and alert your security administrators in near real time:

- Alert me when someone attempts to access a business application and fails many times but succeeds on the last time.
- Alert me when an administrator creates several users, elevates those users' permissions, uses those users to run privileged transactions, then deletes those users.

Insider threat analysis and privileged user monitoring

Look for a solution that:	IBM	Other Vendor
Includes events from all your major IT infrastructure components allowing a complete and overall picture to be formed.	✓	
Identifies anyone exercising technical authority without authorization.	✓	
Identifies system changes made outside of the approval process or change control process.	✓	
Identifies accidental destruction of high-value data.	✓	
Identifies malicious or deliberate acts of sabotage.	✓	
Includes a strong normalization process so all events look the same and are transformed into a common and consistent format so they can be easily understood by non-subject-matter experts.	✓	
Supports compliance- and regulation-specific module definitions that include: – A set of classifications for each of the W dimensions (who, did what, when, where, where from, where to, and on what) so that policy rules can be written at a higher level than individual events (for example, referring to the group of users who administer the domains as "Domain Admins" rather than having to list every administrator individually). – A set of audit policy rules that describe acceptable behavior. – Attention rules that define activity that you want to be notified of, even if it's not a policy exception.	✓	
Includes privileged user monitoring and auditing to monitor, report and investigate the behavior and actions of privileged users on databases, applications, servers and mainframes to ensure that acceptable-use policies are followed and that effective controls are in place.	✓	
Supports exception severity calculations based on the priority of the assets involved in an exception, allowing more critical systems to create higher severity events in reports.	✓	
Supports insider threat analytics to respond to your most important insider threat concerns, such as: "Alert me if someone tries and fails to login to my key finance server n times in a row and succeeds on the final attempt in a five-minute period." Or "Alert me if an administrator creates several new users, elevates the privileges of those users, masquerades as those users to run privileged transactions, and finally deletes those users in a 24-hour period."	✓	

3. Reporting for audit and compliance

The ability to quickly produce easily understood, detailed reports is a vital concern for most organizations. The right SIEM solution provides superior reporting features that make it easy to analyze thousands of security events to detect potential threats and policy violations, as well as alleviate the compliance burden. These features should include standard and customizable report templates, and an advanced report definition wizard that enables you to create customized reports from scratch. In addition, the wizard should allow you to create best-practice, industry-standard audits and compliance-oriented reports to help you get started quickly. These reports should help you manage operational security issues as well as provide support for internal and external auditors.

Compliance management modules are a key part of an effective SIEM solution. These modules provide reports for a specific regulation or best practice and present the information in a format that is customized to the vocabulary of the typical user of the report to more effectively convey the information, making it much easier to understand. Compliance management modules enable both technical and business users to very quickly understand your compliance posture as it relates to user activity. However, out-of-the-box reports provide only the basics of monitoring systems and are focused on demonstrating the specific data points required for compliance with individual regulations and standards. When your requirements extend beyond these out-of-the-box reporting capabilities, you need an advanced report definition wizard that can easily customize existing reports or build reports from scratch.

Compliance management modules should provide:

- A classification template allowing you to group users and information assets into specific compliance or best practice groups.
- A set of policy template rules for the relevant controls for the regulation or best practice.
- A set of reports to monitor the controls as defined in the policy. Reports should be specific to the control (or multiple controls) and demonstrate the monitoring of that control to the auditor.

You will also want to keep in mind the importance of automated report distribution capabilities that provide fast integration into verification processes or other business workflows, as well as the ability to export reports to other formats or send them to business owners for review, verification and action.

Reporting for audit and compliance

Look for a solution that:	IBM	Other Vendor
Enables you to easily sort and browse a multitude of events and analyze them from different vectors.	✓	
Provides reports in plain language that can be understood by auditors or other nontechnical personnel.	✓	
Includes the user's real name as known by the directory or security system to make the report more readable.	✓	
Provides compliance management modules with reporting capabilities specific to your compliance needs, covering major regulations and best practices including International Organization for Standardization (ISO 27001), Sarbanes-Oxley (SOX), Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Basel II, Federal Information Security Management Act (FISMA), Control Objectives for Information and related Technology (COBIT), North American Electric Reliability Corporation – Critical Infrastructure Protection (NERC-CIP) and others.	✓	

Reporting for audit and compliance

Look for a solution that:	IBM	Other Vendor
Includes more than 50 parameterized best-practice audit reports (equivalent to many hundreds or even thousands of individual reports) out of the box.	✓	
Uses a patent-pending strong normalization model.	✓	
Includes a flexible custom report writer that is optimized to the normalization model, allowing you to create your own compliance and audit reports without needing to understand or write SQL.	✓	
Includes a report distribution system to distribute compliance and audit reports to business owners and stakeholders for review, approval, comment and action.	✓	
Provides compliance-specific classification templates.	✓	
Provides a compliance-specific policy template that represents the controls within a regulation.	✓	
Provides compliance-specific reports that allow you to monitor compliance posture against specific controls.	✓	
Provides compliance reports that are designed, created and based on standards (versus renaming operational reports).	✓	
Provides a compliance dashboard that shows the current compliance posture in the vocabulary of the regulations or policies in place for easy understanding.	✓	
Provides trending information at the dashboard level to help indicate the trend for compliance posture and ensure goals are being achieved.	✓	
Provides drill-down from the high-level compliance dashboard through to the underlying detail events for further investigation.	✓	
Provides reporting at the raw log level using a simple query mechanism for forensic-type investigations.	✓	
Includes a full-featured reporting engine with scheduled reporting.	✓	
Automates the distribution of reports to business owners for their inspection and approval as part of the overall compliance and business process.	✓	
Includes a custom report designer that requires no special skills (such as knowledge of scripting or SQL) to create reports quickly.	✓	
Facilitates communication of threat levels and security activities through out-of-the-box standard and customizable report templates, driven from an automated report scheduler.	✓	
Provides a wide variety of report output formats, including HTML, PDF, CSV and XLS exporting of all graphs and charts.	✓	
Includes default templates for regulation-specific compliance reports.	✓	

4. Event source support

Monitoring thousands of network and security devices, hosts, applications and other sources of events throughout your enterprise can represent a potentially enormous task for your IT staff and can take a substantial amount of manual effort. That's why it's critical to have a single view of security events from diverse devices across the enterprise infrastructure, so you can know exactly who did what, when, where, where from, where to and on what. It's also important that the SIEM solution you choose should be able to support a wide variety of devices—both out of the box and through a toolkit or guide that allows you to add support for unique devices.

Event source support

Look for a solution that:	IBM	Other Vendor
Supports more than 300 event source types out of the box, each at different version levels and running on different platforms.	✓	
Supports the whole enterprise infrastructure including IBM z/OS® on mainframes; IBM iSeries® application servers, and applications running on application servers such as IBM WebSphere®.	✓	
Supports each event source through its specific log or set of logs (ASCII or databases), through the appropriate protocols, like Syslog, SNMP, XML, SDEE, OPSEC or other proprietary interface, as well as collection of the native audit logs from applications, databases, servers and mainframes.	✓	
Includes a toolkit to enable you to easily add support for additional, unique event sources.	✓	
Has the capability to automatically recognize an existing data stream and configure the collection according to the device type.	✓	
Provides support for end points primarily through agentless support, and only uses agent support on special cases, thus minimizing the deployment and event source support burden.	✓	
Provides vendor services to add support for unique customer event sources.	✓	
Provides support for an expanding list of specific event sources and devices.	✓	

5. Productivity, flexibility and integration

As you're evaluating different SIEM solutions, it's important to select one that offers rapid time to value. A cost-effective solution includes a number of key features designed to help improve productivity, flexibility and integration within your infrastructure.

Improving productivity

Look for a solution that:	IBM	Other Vendor
Can be deployed using a phased approach.	✓	
Offers automatic configuration capabilities for real-time event sources.	✓	
Provides immediate coverage for policy exceptions through robust policy-based correlation and default or customizable event classification.	✓	
Demonstrates immediate value with extensive out-of-the-box reports.	✓	
Integrates with identity and access management solutions to address the user lifecycle in your organization.	✓	
Automates manual processes, from log collection and analysis to compliance reporting.	✓	
Is mature, robust and proven in the marketplace as evidenced with numerous worldwide customer installations.	✓	
Is backed by its own experienced worldwide services teams, as well as a strong business partner community available to ensure that your project does not suffer through vendor staff that are learning while implementing your solution.	✓	
Has education and training courses available to enable your staff to become productive more quickly.	✓	
Supports a flexible deployment model with an agentless-centric architecture for noninvasive deployment, or agents where required.	✓	
Provides clear and straightforward vendor pricing and licensing.	✓	

Selecting the right security provider

The provider you choose should be able to support the full breadth of your security requirements. Ideally, you will also want a provider that can support you throughout the process of implementing your solution. Before you select a provider, make sure to ask these questions:

Does your vendor's security vision align with yours?

Find a vendor that takes security as seriously as you do and understands how the absence of a solid security infrastructure can impact your organization.

Is your vendor focused on true enterprise security needs?

With a vendor who is focused too narrowly on a point solution that addresses only a particular environment, you can run into the "islands of security" problem. Choose a vendor who can address the big picture, including:

- Identity and access management.
- Mainframe security.
- Application security.
- Information and data security.
- Threat protection.
- Managed services.
- Service management.

Is your vendor's SIEM solution integrated with database monitoring, identity and access management and network and IT management solutions?
Look for a vendor who can extend the value of your SIEM solution with strong integration with these and other key areas.

Does your vendor provide managed services for SIEM?
Look for vendors who provide a complete picture with managed services solutions. Managed services reduce the time and complexity and thus help in lowering the total cost of ownership and providing better ROI.

Does your vendor support your business goals through their technology?
Look for vendors whose solutions align with your business objectives. Do their solutions promote efficiencies, reduce business service deployment time, reduce costs, and speed time to market?

What type of global presence does your vendor have?
If your organization has international offices, you should look for a vendor with a global presence and proven international business experience. Make sure the vendor can support your offices abroad with their own local resources.

Is the solution supported by a mature support organization with the expertise and bandwidth that can be relied on when you need them?
Find a vendor that has a proven support organization to help you maximize the value of your software investment.

Are the vendor's solutions consistently rated highly by the analyst community?
Look for solutions that are recognized through independent analysis and examination across multiple dimensions by leading analysts.

How sure are you of your vendor's stability and staying power in today's tough economy?
A big issue in today's economy is vendor stability and viability. You should consider a vendor who has a long history in the industry, a solid, forward-looking strategy and the resources to overcome adverse economic times.

Can your vendor deliver products that are strategically designed and technically superior?
When comparing various security solutions, look for technical superiority—well-designed functionality, an intelligent architectural design and broad support for industry standards.

Closed-loop integration with user information

When you evaluate SIEM solutions to meet your goals, you will find that IBM offers not only a best-of-breed solution, but also exceptional breadth and integration across its security solutions. IBM offers an SIEM solution built to provide visibility into your organization's security posture, help control the cost of demonstrating compliance, and help reduce the complexity of managing a heterogeneous IT infrastructure.

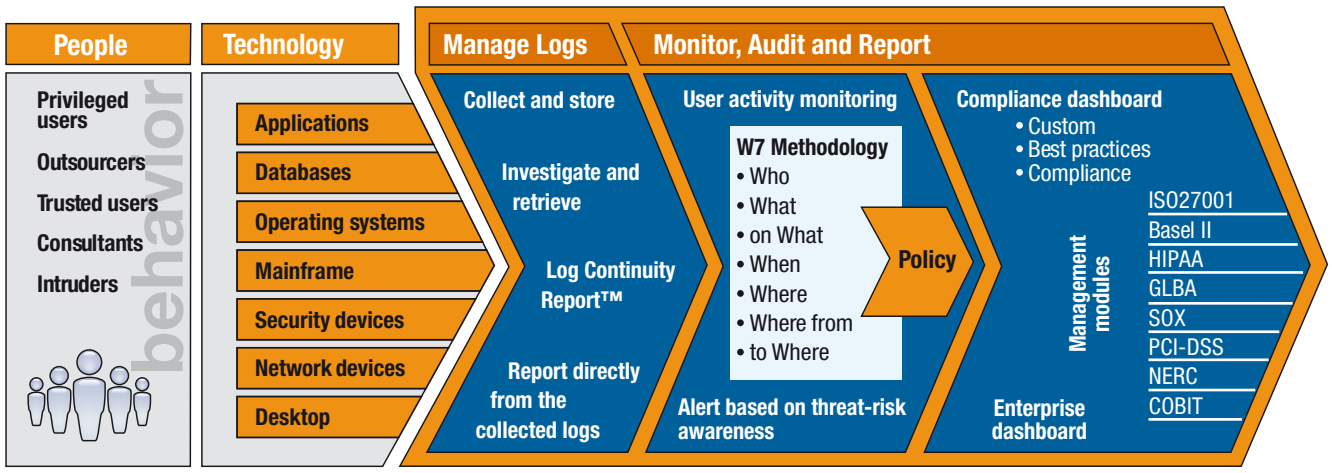
It integrates seamlessly with other IBM Tivoli® software solutions such as IBM Tivoli Identity Manager, IBM Tivoli Access Manager, IBM Guardium, IBM ISS and IBM Tivoli zSecure suite, and with other IT processes to help you achieve an end-to-end view of your security and compliance measures. IBM Tivoli software offers comprehensive security across identities, data and information, applications, processes, and infrastructure. Automated compliance management capabilities are integrated with each offering, closing the security best-practice loop of implementing controls, managing controls, and monitoring those controls for process improvement and for audit and compliance initiatives.

The Tivoli portfolio of security offerings includes the following:

- **IBM Tivoli Security Information and Event Manager**, which delivers a foundation from which to address your SIEM requirements. It centralizes log collection and event correlation across the enterprise, and leverages an advanced near real-time analytics engine, compliance management dashboard and reporting engine to link security events and user behavior to corporate policies. It includes numerous compliance management modules that jump start the compliance management process, such as for PCI DSS, ISO 27001, Basel II, HIPAA, GLBA, SOX, FISMA, NERC-CIP and COBIT.

- **IBM Tivoli Identity and Access Assurance**, which can help organizations ensure that the right users have access to the right information in a timely manner, providing comprehensive identity management, access management, and user compliance auditing capabilities. The solution centralizes and automates the management of users, then closes the identity and access loop, providing industry-leading capabilities not only for assigning and enforcing user access rights, but also for monitoring user activity and for detecting and correcting situations that are out of compliance with security policy.
- **IBM Tivoli Data and Application Security**, which helps organizations protect data and applications by providing auditable access controls, enabling fine-grained control of user privileges, and centralizing management of data encryption keys. This industry-leading solution provides end-to-end protection of sensitive data both in enterprise storage systems and within critical applications, helping organizations support regulatory compliance initiatives and improving data and application reliability.
- **IBM Tivoli Security Management for z/OS**, which enhances the flagship security of the IBM z/OS platform by providing integrated, automated and simplified mainframe security capabilities. This comprehensive solution brings together key functionality from the IBM System z® security software portfolio to help organizations automate audit analysis and compliance reporting, enforce compliance policies, achieve new levels of operational efficiency, and reduce both costs and risk. The solution closes the identity and access management loop by monitoring mainframe user activity and detecting and correcting situations that are out of compliance with security policy.

IBM Tivoli Security Information and Event Manager



Tivoli Security Information and Event Manager provides a comprehensive foundation for addressing your SIEM requirements.

Address your security information and event management needs with IBM

IBM can help provide the infrastructure necessary to support today's security requirements. By monitoring privileged users and facilitating audit and compliance initiatives, IBM Tivoli Security Information and Event Manager can become a business enabler, helping you:

- Minimize the complexity of responding to multiple internal and external controls and regulations.
- Optimize productivity and costs by capturing, creating and automating best practices for repeatable tasks.
- Free IT staff to focus on higher-value activities.
- Provide the agility needed to stay ahead of new business opportunities by removing the barriers to innovation.
- Drive the integrity and confidentiality of business processes.
- Manage the complexity of heterogeneous technologies and infrastructures.

For more information

To learn more about how Tivoli security solutions can help your organization facilitate compliance, protect intellectual property and privacy, and optimize security operations, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli/solutions/security

IBM Corporation Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
September 2010

TIO14001-USEN-02