

Monitoring authorized users for security, compliance and risk management

TODAY'S REGULATORY ENVIRONMENT

Data privacy has catapulted to the top of every CIO's list as a major IT initiative that must be addressed in the short term for security, compliance and overall risk management. Many laws, regulations, industry standards and even internal audit requirements are driving companies to find a solution that addresses their specific needs for monitoring access to their systems applications and sensitive data by authorized users.

Many laws governing data protection and security exist today and the list continues to grow:

DATA PROTECTION AND SECURITY – U.S.

- Sarbanes-Oxley Act (SOX)
- Graham-Leach-Bliley Act (GLBA)
- Health Information Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Federal Information Security Management Act (FISMA)
- Payment Card Industry Data Security Standard (PCIDSS)
- Data breach notification laws (e.g., CA SB1386)
- Federal Trade Commission "Red Flag Rules" and "Risk of Harm" standard

DATA PROTECTION AND SECURITY – INTERNATIONAL

- Canada - Personal Information Protection and Electronic Documents Act
- Argentina - Personal Data Protection Act
- Chile - Personal Data Protection Law
- Europe - European Union Data Protection Directive

- United Kingdom - Data Protection Act
- Japan - Act on the Protection of Personal Information
- Korea - Promotion of Utilization of Information and Communications Network and Data Protection Act
- Taiwan - Computer-Processed Personal Data Protection Law
- China - Provincial consumer protection regulations
- India - Information Technology Amendment Act
- Australia - Privacy Act

The common theme is the importance—and in most cases, an absolute requirement—for a company to have internal controls and documented procedures in place for the protection of sensitive information, including personally identifiable information (PII) and personal health information (PHI). Many organizations are also establishing similar internal requirements for the protection of data considered critical to the business, such as customer lists and other intellectual property.

PROTECT YOUR COMPANY FROM "INSIDE JOBS"

As evidenced by the onslaught of media attention to privacy breaches, there should be no question about the need to secure and monitor access to sensitive data.

And when a breach does occur, an increasing number of laws require notification of customers who may have been impacted. This notification process can be very costly, not to mention the potentially severe impact on the business resulting from the breach itself. According to a Ponemon Institute study, 20 percent of consumers have terminated a business relationship when a data privacy breach occurred; an additional 40 percent would consider doing so.

Chances are, you have taken steps to do so by installing a host of anti-intrusion technologies that keep unauthorized parties—both internal and external—from accessing your critical data.

But is a focus on the risk of exposure from unauthorized users, whether internal or external, really enough? What about exposure to breaches or misuse of sensitive data by authorized internal users? Study after study reveals that the biggest security threat organizations face is internal.

Industry analysts such as Gartner and Forrester indicate an overwhelming majority of security incidents incurring actual losses are inside jobs. These findings are mirrored in another report, issued by the Ponemon Institute in 2008: An estimated 40 percent of data security breaches are caused by non-malicious employee error; 30 percent by malicious employee activity.

COMPUWARE'S APPROACH TO APPLICATION AUDITING

Compuware's unique solution for Application Auditing takes IT security one step further than traditional approaches. Today, IT relies on system logs that only identify what was accessed, by whom and when it occurred. No detail is provided to actually show what the end-user was doing or more importantly what data they were viewing. Our solution acts like a surveillance camera for your application by recording authorized internal activity between users and the application. Not only does this deter inappropriate activities, but it also provides a detailed audit trail if a breach of your systems, applications or data were to occur.

Compuware's Application Auditing solution:

- requires no changes to your existing applications, due to its non-intrusive design
- monitors end-user activities in test and production on both the mainframe and distributed platforms
- provides proactive alerts when suspicious activity is detected
- serves as a deterrent to inappropriate activities
- contains—and lessens the impact of—a breach if one occurs
- lowers the cost of regulatory compliance
- reduces risk and liability associated with production security and data privacy
- improves rapid response for auditing infractions and application problems
- includes a documented set of “Best Practices” and project methodology for a successful implementation.

Founded in 1973, Compuware provides software, experts and best practices to ensure applications work well and deliver business value. Compuware solutions **optimize application performance across the Enterprise and the Internet** for leading businesses around the world, including 46 of the top 50 Fortune 500 companies and 12 of the top 20 most-visited U.S. web sites. Learn more at compuware.com.

Compuware Corporation Corporate Headquarters
One Campus Martius
Detroit, MI 48226-5099

All Compuware products and services listed within are trademarks or registered trademarks of Compuware Corporation. Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems Inc. in the United States and other countries. All other company or product names are trademarks of their respective owners.

Using our mainframe technology, your company can efficiently record all users of any mainframe application using a traditional green screen (3270) interface. In addition, you can record all users and applications accessing mainframe services and data from the distributed platforms that use TCP/IP or WebSphere MQ for communication with the mainframe. For distributed HTTP/S applications, use our new integration with Compuware Vantage to document the transaction input activity of all users from that platform. If a breach were to occur, a resulting audit trail of this user activity would help pinpoint who may have been involved and what customers were affected—limiting notification costs.

PART OF A RISK MANAGEMENT SOLUTION

Application Auditing is one component of Compuware's Data Privacy solution for risk management in both test and production environments. Providing transparent application surveillance and audit data, in addition to automated processes and technology for the subsetting and disguise of sensitive production data used in test, Compuware solutions help you to reduce the overall risk to critical data and allow you to test and deploy your applications with confidence.

CONCLUSION

The risk associated with negligent or malicious acts by authorized users of sensitive applications and data is a very real one. In order to effectively address this threat, organizations must implement appropriate controls designed not only to deter these activities, but also to provide a detailed audit trail. This audit information is valuable not only in minimizing the cost of responding to a breach, but also as effective forensic evidence for use in legal action. Compuware's Application Auditing solution gives you the precise data needed.

To learn more about Application Auditing, visit:
www.compuware.com/dataprivacy

