Bloombase
Least Invasive Security

Achieving IT Governance with Bloombase Least Invasive Security Solution

WHITE PAPER

"With the sole exception of the war on terrorism, no issue dominates current thought more than the corporate and accountancy ethical scandals which have rocked our country"

Enforcing Corporate Management Ethics and Data Privacy throughout the Enterprise

Sarbanes-Oxley (SOX) Act, passed in year 2002, has huge impact on how enterprises are managed. The Act requires enterprises to change their business processes to adapt to assurance of finance data at high integrity. The act was enacted in response to numerous accounting fraud caused by enterprise top-management that arose public attention worldwide.

"With the sole exception of the war on terrorism, no issue dominates current thought more than the corporate and accountancy ethical scandals which have rocked our country"

Sarbanes-Oxley Requirements

Section 103

"an evaluation of whether such internal control structure and procedures... include maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the issuer... [and] provide reasonable assurance that transactions are recorded as necessary."

Section 302

"the signing officers have disclosed... all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls; and any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls."

Section 404

"each annual report... contain an internal control report, which shall... contain an assessment... of the effectiveness of the internal control structure and procedures of the issuer for financial reporting."

The Security Challenge

Sarbanes-Oxley and other associated privacy legislations are laid and established to mandate enterprises to protect interests of investors and consumers through effective IT and corporate governance. To ensure data integrity, traditional solutions suggest the use of audit trail and logging which are exhaustive and cannot prevent intended alteration acts. Audit trail is often considered resource expensive and relatively unsafe as contents of audit logs can as well be tampered and hacked leaving no traces in unauthorized offence.

To protect data from unwanted disclosure, one might suggest access control and block unauthorized users from reading the sensitive data. However, to administrators and operators who have superuser privileges, they have full access to any system resources even if the resources are not owned by them. Access control to these privileged users means nothing.

Existing security measures cannot protect data from alteration. Statistics showed private enterprises raise their investment by 30% yearly on data security. However, the number of data security incidents grows at the same rate if not exceeding [CERT, IDC, RBCCM 2002].

PricewaterhouseCoopers reported that 50-80% of data attacks are from company insiders. CSI/FBI investigation in year 2002 showed insider attack has caused the industry monetary loss of more than USD 50 million.

Command-based encryption utilities only work with offline archives instead of processing real -time data on-the-fly. They require much operation by administrators and at the end, it is still unsafe. Volume protection is considered transparent, however, it is limited to direct attached storage and is not scalable for enterprise use.

Bloombase Solution

Bloombase created Spitfire security platform to address compliance requirements suggested by Sarbanes-Oxley to maximize IT governance in corporations. Spitfire security appliances protect encryption and digital signing keys inside hardware security module (HSM) from disclosure and duplication. Spitfire appliances encrypt data with NIST certified AES, 3DES and DES cryptographic algorithms and create digital signatures to assure data integrity by international standards including Public Key Infrastructure (PKI), X.509 digital certificates and W3C XML digital signature.

Data Integrity

Spitfire XML EAI appliance signs financial documents and archives with digital certificates. Digital signature provides evidence to possible alteration of data being signed. Spitfire XML EAI signs plain data, data files, XMLs, emails and Adobe PDF files. Spitfire XML EAI appliance can detect data changes by examining signature value and message digests previously generated against signer's digital certificate. Corporations have assurance over financial data archives and gaurantee data integrity by use of Spitfire EAI appliance.

Data Confidentiality and Change Resistance

Spitfire StoreSafe protects storage data by strong encryption. Encrypted data appears as garbage and meaningless information to unauthorized users. Intruders will have to pay tremendous efforts to undo the encryption process which is considered technically impossible. Seeing confidential data appeared as corrupted information, trespassers and casual crackers immediately lose their interest and turn away for other plain data to hack with. Disappointment and frustration are the best weapons for hackers as they seek for fun and they do not like spending time on difficult tasks.

Application Transparency

Spitfire appliances are network based hardware which can easily fit in any enterprise systems and do not invade existing computing infrastructure. Spitfire operates as a network blackbox transferring data between components of a system. Spitfire detects network packets for plain data and encrypt them before sending to data's original destination. As encrypted data pass through Spitfire, Spitfire Cryptographic Engine (SCE) immediately decrypts data and delivers plain data to the next hub. Spitfire gaurantees zero-downtime deployment and works transparently under the covers without applications or users' intervention.

No Single Point of Failure

Mission critical systems require extra high level of service availability. To cope with the ever increasing storage and challenging service requirement of customers, Spitfire appliances have prepared for mission critical use as well. Spitfire appliances are high availability (HA) ready. Corporations can multiplex Spitfire boxes to run in a cluster. Failure of any single Spitfire appliance will not affect service of the entire cluster. Spitfire appliances are built with concern on failover and non-stop - redundant cooling fans, redundant and hot-swappable power-suppy and multiple network and storage interfaces.

Effective Compliance

To address Sarbanes-Oxley and other numerous IT governance compliance requirements, enterprises should act immediately to secure their financial data and various information archives. Bloombase Spitfire Security Platform provides a cost-effective, scalable and secure solution to protect these invaluable corporate assets from unwanted alteration.

Bloombase
Least Invasive Security

Bloombase Technologies - Least Invasive Security **email** info@bloombase.com **web** bloombase.com