

Secure Storage: A Necessary Evolution

White Paper by: Brendan Kinkade, VP Marketing, Nexsan Technologies

© 2007 Nexsan Technologies Inc.
All Rights Reserved.

Published by
Nexsan Technologies Inc.
21700 Oxnard Street, Suite 1850
Woodland Hills, CA 91367
USA
www.nexsan.com

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage and retrieval system, without prior permission in writing from Nexsan Technologies Inc.

The information presented in this white paper represents the views of Nexsan Technologies Inc. (Nexsan Technologies) The information was prepared and reviewed for accuracy. However, Nexsan Technologies cannot guarantee that there are no errors or omissions. Nexsan Technologies makes no warranties, express or implied in this document.

Many of the comments and examples are related to the laws of the U.S., the United Kingdom and Canada as of the date of publication. The laws, regulations and jurisprudence in the area of compliance storage are constantly changing. Readers should review the current laws of their country, with their legal council, before making any decisions.

Nexsan Technologies, and Assureon are trademarks of Nexsan Technologies Inc.

This paper describes areas of functionality that may not be available in all versions of Assureon, or on all OEM platforms.

Secure Storage: A Necessary Evolution

All large organizations have gone to great lengths to protect their information assets. All kinds of security systems, from network firewalls and VPNs to passwords and physical mechanisms have been implemented to prevent unauthorized access to networks and premises. Yet, even with all these security measures in place, highly publicized data breaches involving the leakage and theft of customer- and employee-sensitive information still occur. The resulting damage to corporate reputations and a climate of increased regulatory compliance, is forcing organizations to focus attention on protecting corporate digital assets even further.

When it comes to storage, businesses are only too well aware of the risks that hacking attacks, disgruntled employees, human error, loss or theft of hardware or backup media can pose. With these threats in mind, it is not possible for storage systems to continue to be simple repositories of data. Existing approaches using offline media such as tape or optical have proven to be unsuitable for the security and privacy requirements of today. What is needed is a new breed of secure storage system that safeguards corporate digital assets even when corporate security has been compromised; a secure storage system to help businesses meet compliance requirements and ensure good corporate governance.

Secure storage provides an integrated approach to managing, storing and protecting information over the course of its lifetime. Recent rulings have left companies with the "burden of proof" when it comes to defending themselves in a court of law. In this climate selecting and implementing a storage solution that is completely secure becomes a matter of the highest priority. Consideration must be given to how the full information lifecycle will be managed and how the storage process will take account of a multiplicity of demands from corporate data security policies to regulatory compliance constraints, from legal issues to protection against malicious or accidental loss, from retrieving information about unauthorized access attempts to disposal of data. Secure storage is essential if organizations are to comply with all the conflicting pressures on their business. In short, it totally changes the criteria for storage systems purchase.

Secure storage systems can only meet the goals of senior management, IT and corporate legal departments by combining secure encryption, storage management software, clustered servers and RAID protected hardware. This is the single and most powerful way to provide the multiple levels of protection need to minimize the risk of data security breaches at the point of storage and ensure ongoing good data management practices. Secure storage systems are also fault-tolerant and easily implemented within a SAN, NAS, or DAS storage infrastructure, with capacity and security features scalable to meet future growth.

Assureon® from Nexsan is the industry's most complete secure storage system. Assureon's secure storage architecture delivers a comprehensive array of intelligent features including constant monitoring of file integrity, Lifecycle Management, file authentication, missing file alerts, and support for remote replication, along with AES 256 file-level encryption.

The Assureon® secure archive ensures all copies of data in the system are protected in the event of loss or theft. How the encryption keys are managed is critical to whole data protection process. Encryption keys have to be kept safe – not just from outside attack, but from inadvertent tampering by insiders and from theft of the physical hardware where the keys reside. Assureon® provides a robust authentication layer, controlling whether or not a specific user is allowed to access the decrypted content.

Finally, Assureon® creates a complete, auditable data trail. Should a company's data policy ever be investigated, a file's proof of origin – who created it, when was it created and what application created it – and evidence of whether the data has been tampered is readily available. Many compliance regulations require organizations to be able to provide audit reports for historic data. The ability to provide extensive reports, throughout the data's lifecycle, is an important function of the Assureon® system. And at the end of a file's lifecycle, Assureon® users can ensure that all copies of the file have been irrevocably deleted in order to meet privacy regulations and corporate governance practices.

In summary, in a business climate where large organizations find themselves governed by regulatory compliance, data protection laws and intellectual property rights, the leakage of confidential data not only does damage to reputations but the financial repercussions can run into millions. Like it or not, this is the future we all face. Investment in secure storage systems is the only way to be confident that your company-confidential data will never be compromised.