



WHITEPAPER

Sensitive Information Protection and SharePoint

Executive Summary

The adoption of SharePoint provides business users an improved platform to exchange information and collaborate more efficiently. Moving to a centralized platform such as SharePoint also allows IT teams to better backup, restore, and manage information. For SharePoint to continue to grow as a business platform it must be suitable for highly sensitive areas of the business such as the Executive staff and Human Resources. End users in these areas often have special requirements regarding the confidentiality of their information and will resist change, and resist using a collaboration platform such as SharePoint, until their security concerns are adequately addressed.

Transparent encryption for SharePoint can address security concerns relating to sensitive information being stored in SharePoint sites. Beyond addressing current security concerns, transparent encryption can also greatly expand the use cases for SharePoint, to include new areas such as HR, executive teams, and as a platform to store and process regulated information.

Problem Overview

To enable SharePoint for use for executive staff, boards of directors, and human resources departments, an organization must go beyond common SharePoint security mechanisms such as role-based access control and security for the network session. Specifically, the organization needs to ensure IT administrators cannot mistakenly or maliciously access sensitive content. An additional requirement is that the security control must not hamper the end users' productivity nor require additional training that distracts them from the value they bring to the company. In short, the security controls must be transparent and automated.

Security and compliance requirements include:

1. Strong authentication of end users and administrative staff
2. Access control to protect from unauthorized access and enforce business need to know
3. Protecting access to sensitive information through use of transparent content encryption
4. Activity auditing to track permitted and denied access requests
5. Separation of duties among IT administrators, the various tiers of SharePoint and storage administrators, and information security teams

Native SharePoint platform security controls provide well-documented options for user authentication. SharePoint's role-based access control is customizable to facilitate most any combination of permissions. Most organizations already have a trusted authentication mechanism in place and will prefer to use it.

The internal SharePoint team must then configure role-based access control to ensure only intended end-users have authorized access to the site or library. This task is straight forward as there are a small number of, for example, senior executives and the level of permission they need is rarely in doubt (full access and control).

Enabling audit trails for SharePoint user login activity, and for administrative changes to the groups that control access to data in SharePoint is also important. By completing these tasks, organizations can address requirement 1 above. However, these measures do not fully address requirements 2 and 4. Using SharePoint permissions to enforce business need to know is insufficient because, in most organizations, SharePoint administrators themselves control group membership and permissions. In the case of requirement 4, enabling audit logging for SharePoint sites is also typically a function that is controlled by SharePoint administrators. If the threat that is of concern is insiders and administrators, then it follows that separating duties in these areas is critical. For requirements 3 and 5 above, there are no effective security controls that are native to SharePoint that address these needs. Organizations wishing to deploy SharePoint to user communities including executive teams, HR, and Boards of Directors will need to look beyond the capabilities provided in SharePoint to fully address their security requirements.

CipherPoint Solution

The CipherPoint solution is specifically architected to maintain the confidentiality of information stored in SharePoint. The software provides transparent encryption of and optional access control to sensitive content to ensure that accounts with privileged IT rights cannot be used to maliciously or mistakenly view protected information. The native SharePoint authentication and access controls described above are still in effect and provide meaningful layers of defense. CipherPoint's solution complements SharePoint's existing capabilities and provides additional layers of security and separation of duties.

The Enterprise version of CipherPoint's solution includes a centralized management console, CipherPointKM. CipherPointKM allows for the configuration and management of the security and encryption of SharePoint content from outside the SharePoint farm. This architecture provides true separation of duties as the SharePoint administrators can manage the platform without being able to circumvent security, the security team can administer the

security controls without requiring access to SharePoint, and the authorized end-users are the only ones that can access their sensitive information. In addition, the CipherPoint technology inserts at the SharePoint web front end server, resulting in a user experience that is truly seamless. Transparent operation is critical for end user adoption of a SharePoint encryption solution.

Conclusion

The combination of CipherPoint's transparent encryption technology and key management capabilities with native SharePoint authentication and access controls fully addresses the requirements outlined above.

As SharePoint becomes more of a mission-critical business platform, organizations will require additional security controls to maintain the confidentiality of sensitive information stored in SharePoint sites.

Expanding the secure use of SharePoint to include senior executives, boards of directors, human resources staff, and other owners of sensitive content can be accomplished through the thoughtful deployment of appropriate security controls, including transparent encryption, access controls, strong authentication, audit trails, and separation of duties. As a SharePoint architect or administrator, CipherPoint's solutions and SharePoint's native security features allow you to provide a secure platform and enable collaboration within your organization. In doing so, you will provide a more efficient and secure way of doing business, increase SharePoint's visibility in your organization, and increase your value to your enterprise.

About CipherPoint Software, Inc.

CipherPoint Software is the first provider of transparent content encryption software for Microsoft SharePoint, and was founded by IT security industry veterans with deep experience in building security technology companies.