STEALTH
SOFTWARE

STEALTH Content Store

how to deal with the explosive growth of unstructured data in SharePoint in a secure and transparent manner….

1. Introduction

Traditionally, ECM platforms were enterprise business applications with a high level of out-of-the-box features and functionality. These applications were expensive to procure and costly to implement.

Customization was required in order to provide customers with specific functionality and implementations often took many months to years, rarely delivering to original expectations.

The Enterprise Content Market (ECM) has changed substantially with the arrival of ECM "platforms" such as SharePoint. Gartner predicts that, "By 2015, SharePoint will be, for enterprise business applications, what iPad and iPod are for consumer applications."[1] At the end of 2013, SharePoint had an installed base of 311 million users, expected to grow to 609 million users by the end of 2017.[2]

SharePoint has become the platform of choice for thousands of enterprise business applications. As a result, SharePoint functionality has exploded. Whether a bank is looking for an application for unified reporting[3] after a M&A spree, or a hospital for an electronic intensive care (EICU) application[4] - they have been integrated in SharePoint.

> *SharePoint will be for enterprise business applications, what iPad and iPod are for consumer applications"*
>
> *- Mark Gilbert Gartner*

SharePoint has become mission-critical for many organizations. The applications that have been integrated hold highly sensitive information and must be available 24/7.

SharePoint has also been leveraged to reduce time to market and time to revenue for large enterprises.

SharePoint's popularity has, however, resulted in substantially elevated requirements for security, scalability, performance and risk mitigation. To further enhance the usability of SharePoint customers are looking to reduce the cost, complexity and management overhead of existing SharePoint deployments. Data confidentiality, integrity, and availability are all major concerns that directly relate to the protection of sensitive customer data and/or intellectual property of an organization, and its continuous availability.

SharePoint (cloud) service providers, another group of SharePoint users, also have to address these concerns in a seamless manner.

STEALTH Software has developed a solution that can meet current and future SharePoint requirements regarding all the above mentioned scenarios. It provides a secure way of handling the explosive growth of SharePoint data in a unique manner. The software can write transparently and securely to any external (storage) platform of choice; on premise, cloud or hybrid. The solution can also write concurrently (encrypted) to multiple external storage platform and there is no need for complex, costly and insecure middle layers between SharePoint and the external storage platform. Cost reductions compared with a traditional SharePoint environment save up to 30%.

2. Customer Requirements

Interviews with both enterprise and government customers resulted in a number of clearly defined requirements from three distinct teams involved in running and supporting an organization's SharePoint environment:

- The SharePoint Application teams, who are the point of contact between the users
- The Operational/Infrastructure department who are responsible for managing and administering overall IT operations
- The Information Security teams, tasked with risk mitigation, protecting intellectual capital, and policy/regulatory compliance.

The SharePoint Application teams require massive scalability – 10's to 100's of Terabytes, in addition to high performance, to meet current and future customer demand and drive user productivity.

> *"SharePoint versioning could be impacted by stubs as SharePoint might think about the stub as being an additional version of the document"*
>
> *- Michael Mueller*
> *Chief architect Large Financial Institution*
> *Microsoft Germany*

Time to market, for example, was a critical factor for Pharma vendor Pfizer. The company increased top-line revenues for their drug Lipitor by $146M, using SharePoint to reduce approval and introduction time of Lipitor by 2 weeks. SharePoint is installed in four Pfizer data centers to support 11 Pfizer divisions and 122 departments.[5]

The Bechtel Group leveraged SharePoint to dramatically improve project management. Bechtel's ROI on ProjectWise – a project management application integrated with SharePoint - was approximately 19x after 18 months. The time to ROI was 4x faster than the industry benchmark of 12 months.[6]

Part of SharePoint's flexibility can be found in its customizability as a web-based application platform. The SharePoint Application teams are often confronted with so-called "web parts" and "stubs" needed to run the current SharePoint environments. Web parts and stubs are "hooks" in SharePoint used by middle layers such as data repositories, gateways, appliances, archiving layers, media/web servers and agents to apply data policies to the SharePoint data. Web parts and/or stubs however, make managing a SharePoint environment substantially more difficult and can potentially affect the usability of SharePoint. They also add to the workload when migrating data from one SharePoint release to the other.

The Operational and Infrastructure teams are confronted with, on one hand, reduced budgets, and on the other hand, increasing Service Level Agreements (SLA). In many cases, SharePoint is introduced on a departmental level to work around documents, however, with the evolution of SharePoint and the growth of (business critical) files stored in SharePoint, the SLA's changed from 9-5 weekly into 24/7. Management overhead is a major concern; handling 1 TB of data in a traditional SharePoint architecture equates to handling 5-8 TB in day-to-day operations.[1] At the same time, customers tell STEALTH Software that a substantial cost reduction is required to ensure that the internal risk/reward requirements are met to make changes to the SharePoint environment. Business cases have to be presented based on objective and hard Total Cost of Ownership (TCO) and Return on Investment (ROI) numbers.

As SharePoint now holds mission critical data, full content failover and business continuity have become increasingly important but have also become more cumbersome and expensive in traditional SharePoint environments. Organizations are losing important skill sets due to the financial crisis, or through normal attrition of key personnel, making it far more difficult to operate and maintain the existing environments.

Every day, the Information Security teams are confronted with persistent threats aimed at stealing sensitive customer and/or user information or extracting highly valued intellectual capital from their organization. Security requirements are becoming paramount as an increasing number of organizations are contemplating moving their information to the cloud or hybrid architectures, with an on premise and off premise component.

The layer between the on premise SharePoint application layer and the external (cloud) storage platform has been identified as one of the areas most vulnerable to attack. Appliances, gateways and media/web servers with agents are being used to address data protection, but by doing so they add a high degree of cost, complexity and management overhead to the environments, and even with that complexity they do not provide complete protection.

Another group of solutions provide cloud security to protect the mission critical data after it has been stored in an off-premise or cloud environment. These solutions do not address requirements for security between the application layer and the cloud. Organizations need to address these so-called “man in the middle” attacks on their data that occur between the SharePoint application layer and the external storage platform and/or the hardware appliance and gateways. Data needs to be encrypted while it is still in the secure, on premise SharePoint environment. It is critical that the encryption takes place before the data leaves SharePoint to be stored via a network connection on the external (cloud) storage platform even if the communication is through a secure protocol such as SSL. Compliance requirements demand that the encryption keys are generated and stored on premise within the safe boundaries of the organization.

Article 29 on Data Protection released by the European Commission makes Cloud Service Providers responsible and liable for the content they store on their cloud platforms, unless they can show that data has been encrypted at the application layer and is stored encrypted on the cloud storage environment.

3. STEALTH Software

STEALTH Software started developing its software-only solution with a number of key basic principles in mind:

- **Software-only solution**: no requirements for middle layers, data repositories, gateways, appliances, web/media servers, agents or tiered storage
- Aimed at a substantial **cost reduction**, compared with traditional SharePoint environments; at a minimum of 30-50%
- In-line, **file level encryption** at the application layer with an AES 256 key (or alternative cryptographic when desired) without adding any third party products, gateways or appliances
- Substantially **reduced complexity and management overhead** for all stakeholders
- A **TCO/ROI tool** to help stakeholders build the necessary business cases
- A **Web Console** to provide visibility of the SharePoint environment from a data management point of view with the possibility of integrating with existing charge-back models for shared IT services
- **Increased Performance** for the users

> *"Leverage Partner Ecosystem to fill Gaps -EBS/RBS: STEALTH Software"*
>
> *Mark Gilbert*
> *Gartner*

- The STEALTH Software philosophy is to simplify and improve SharePoint infrastructures by using native SharePoint capabilities and by offloading complex data management tasks to external (cloud) storage platforms. Instead of storing complete files (structured and unstructured data) in a SQL server database, Stealth Content Store patented solution separates "structured" and "unstructured" data at the SharePoint application layer – only the "structured" data (Metadata and Content ID) is stored in the SQL database while the "unstructured" (binary large objects (BLOBs)) data is stored on less expensive storage platforms, including object-based storage. In doing so, the STEALTH Software delivers more performance, scalability, and reliability and allows organizations to scale SharePoint farms to petabytes. To achieve this STEALTH Software has a built-in data consistency mechanism and no additional hardware or software is required.

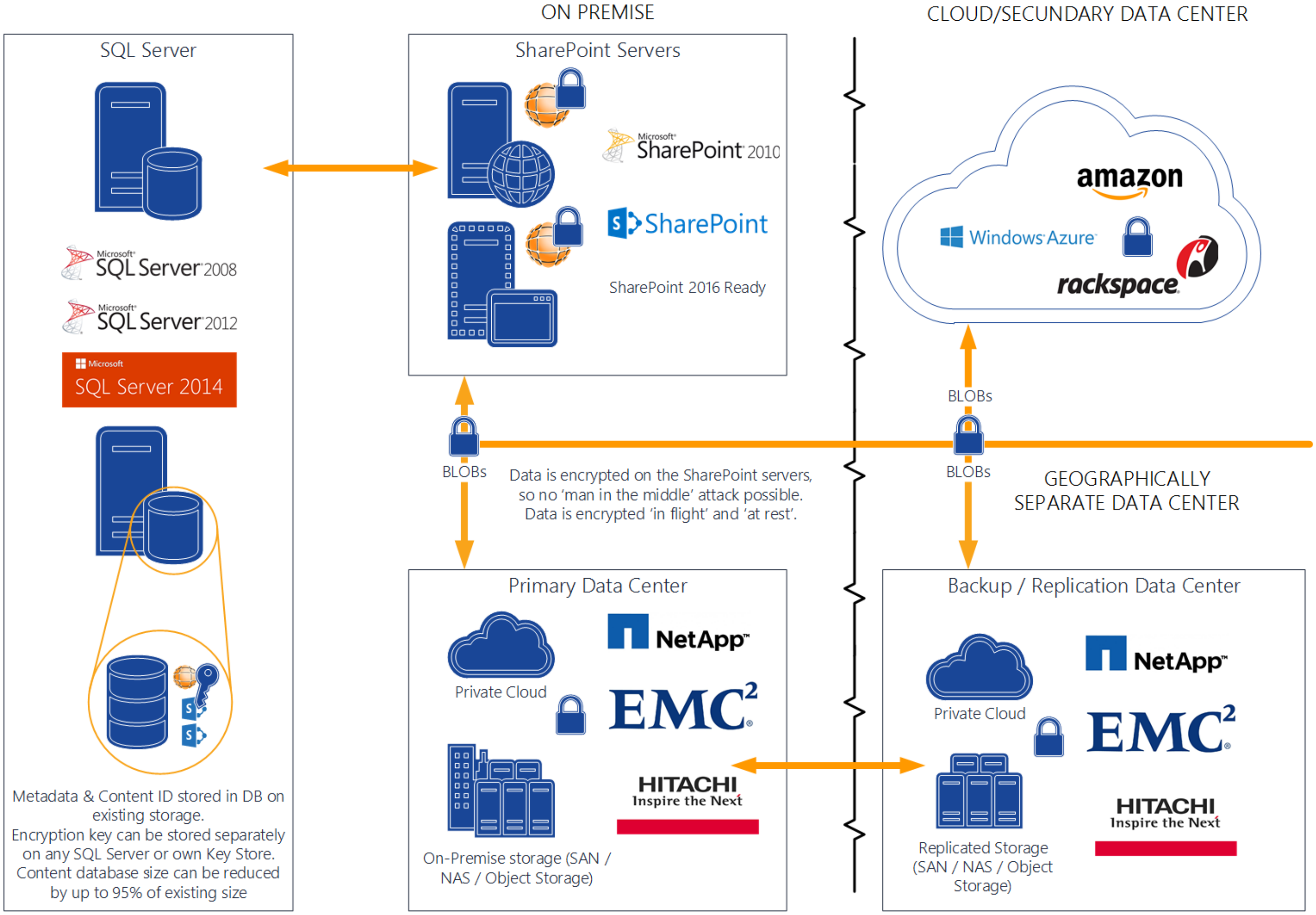
> *"Use BLOB API's to Optimize Repository Scalability: STEALTH Software"*
>
> ***Mark Gilbert***
> ***Gartner***

SharePoint end-users will not notice any difference when using the STEALTH Software solution as the offering is fully transparent and non-intrusive to the SharePoint user. There is no need for middle layers of any kind such as data repository, gateways, appliances, web or media servers, agents or archiving layers that are often used in traditional SharePoint environments to provide scalability and a certain level of data management. This has a marked effect on potential future migration processes as well as deploying industry specific applications in SharePoint. STEALTH Software works closely with the key vertical industry application developers to help facilitate the deployment of those applications in a streamlined and enterprise ready SharePoint environment. A SharePoint farm supported by the STEALTH storage solution will be easily capable of supporting a user base of hundreds of thousands of users or hundreds of millions of documents. It can also seamlessly facilitate the migration of large file share environments, My Documents and Public Folders.

Security

Stealth Content Store encrypts (optionally) the data at the SharePoint application layer with an AES-256 key at an individual file level so that the data is protected “in flight” and “at rest”. When a user uploads data, it is encrypted immediately, in memory, on the SharePoint server. This encrypted data is then stored on the storage device of choice and the encryption key is stored either on the SharePoint server, in a separate database or in an existing key store. At this point the encryption key is required to get access to the data - accessible only via the SharePoint server, and the data needs to be obtained from the external storage platform. Further, a second vector is stored in the data access token used by SharePoint to request the data. This requires 3 separate pieces of data to be re-combined to allow access: data from storage, the encryption key and the secondary vector. By utilizing this separation and immediate in memory encryption, the STEALTH Software offering prevents internal and external bad actors from accessing data either at rest or in transit. The only point of access is the SharePoint front end. Concurrent and encrypted off-loading of unstructured data to both on and off-premise platforms is also possible. Below is a high level overview of the mechanism employed.

Picture - 1

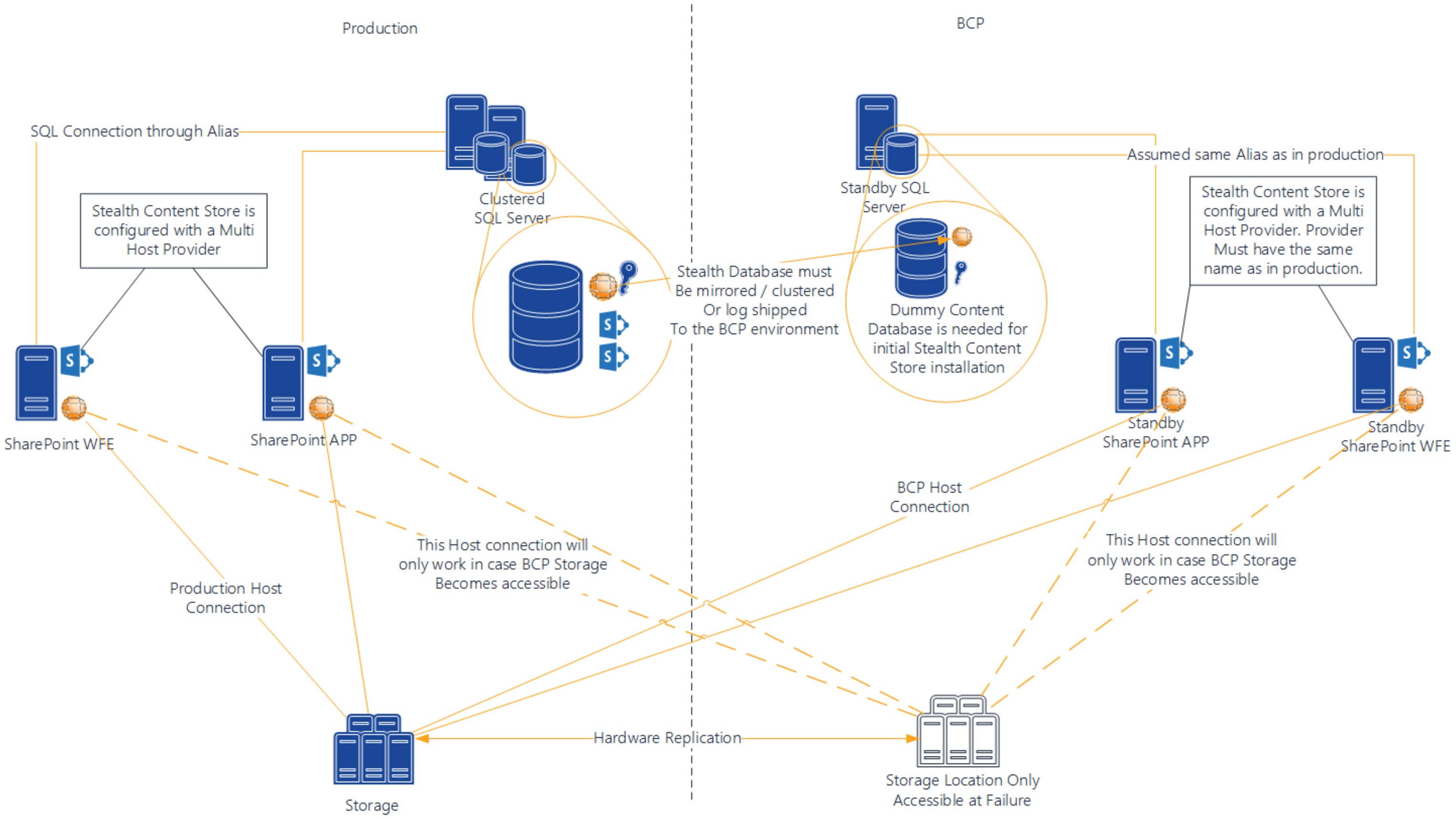

ON PREMISE
CLOUD/SECUNDARY DATA CENTER
SQL Server
Microsoft SQL Server 2008
Microsoft SQL Server 2012
Microsoft SQL Server 2014
Metadata & Content ID stored in DB on existing storage.
Encryption key can be stored separately on any SQL Server or own Key Store.
Content database size can be reduced by up to 95% of existing size
SharePoint Servers
Microsoft SharePoint 2010
SharePoint
SharePoint 2016 Ready
amazon
Windows Azure
rackspace
BLOBs
BLOBs
BLOBs
Data is encrypted on the SharePoint servers, so no ‘man in the middle’ attack possible.
Data is encrypted ‘in flight’ and ‘at rest’.
GEOGRAPHICALLY SEPARATE DATA CENTER
Primary Data Center
Private Cloud
NetApp
EMC2
HITACHI Inspire the Next
On-Premise storage (SAN / NAS / Object Storage)
Backup / Replication Data Center
Private Cloud
NetApp
EMC2
HITACHI Inspire the Next
Replicated Storage (SAN / NAS / Object Storage)

Business Continuity

Typically, SharePoint Farms start off small; for example, on a departmental level to support a project or project collaboration, and because of its ease of deployment, the use of SharePoint expands rapidly to other departments, often without the proper oversight or governance. Before long users and teams are storing business critical information in SharePoint. As a result, Service Level Agreements with regard to availability and content failover, become substantially stronger.

STEALTH Software provides SharePoint Content Failover to support business continuity and availability of the file content to end users. Stealth has developed a Multi-Host Provider and Concurrent Provider for various business continuity scenarios. Picture 2 shows the mechanism for the Multi-Host Provider. No third party products have to be added to the environment when using the Multi-Host Provider.

Picture – 2


Production
BCP
SQL Connection through Alias
Clustered SQL Server
Standby SQL Server
Assumed same Alias as in production
Stealth Content Store is configured with a Multi Host Provider
Stealth Content Store is configured with a Multi Host Provider. Provider Must have the same name as in production.
Stealth Database must Be mirrored / clustered Or log shipped To the BCP environment
Dummy Content Database is needed for initial Stealth Content Store installation
SharePoint WFE
SharePoint APP
Standby SharePoint APP
Standby SharePoint WFE
BCP Host Connection
This Host connection will only work in case BCP Storage Becomes accessible
This Host connection will only work in case BCP Storage Becomes accessible
Production Host Connection
Hardware Replication
Storage
Storage Location Only Accessible at Failure

STEALTH Software delivers an additional use case to support business continuity in SharePoint by leveraging technologies such as cloud storage.

Summary

STEALTH Software provides a seamless, integrated solution to any SharePoint implementation. The solution extends the value and performance of Microsoft SharePoint with optimal security that is designed to leverage performance and availability benefits of the enterprise's storage and server resources.

Benefits include:

1. **Application Layer - SharePoint users and SharePoint Administrators**

   - Unlimited Scalability – from 100's of Gigabytes to 100's of Terabytes.
   - Improved Performance - multiple lines from an external platform to SharePoint user instead of one connection via the SQL server - depends on storage platform used; up to 30% improvement.
   - No web parts and stubs - positive impact for migration, SharePoint management and application deployment.

2. **Infrastructure layer - SQL and Infrastructure Administrators**

   - No unstructured content data in SQL databases.
   - No data repositories, archiving layers, tiered storage or appliances needed to run, manage and scale the SharePoint environment.
   - No agents, no web/media servers.
   - No more traditional back up/recovery for the unstructured content.

3. **Security - Compliance, Risk & Information Security Officers**

   - Encryption (AES 256 key) before the data leaves SharePoint and is stored on any external platform on or off (cloud) platforms – preventing "man in the middle" attacks.
   - Encryption key is generated on premise in the SharePoint environment and stored on premise.
   - Physical separation between data access, data management and the data stored on the external platform.
   - The so-called Content ID is also kept on premise in the SQL database.
   - Transparent and non-intrusive to all SharePoint security capabilities e.g. SSL, permissions etc.
   - No additional third party products required.

4. **Business Continuity - Infrastructure Administrators**

   - Built-in Content failover for SharePoint environment based on capabilities of SharePoint STEALTH Software and the external storage platform.
   - Ability to write concurrently (encrypted) to various platforms – either on or off premise or a combination of both. This addresses any outage or disaster recovery requirements for e.g. cloud service providers or private cloud environments.

> *"Big SharePoint Means Global Architecture: Consider hybrid architectures if needed using tools like STEALTH Software"*
>
> *- Mark Gilbert*
> ***Gartner***

[1] Mark Gilbert, Lead SharePoint Analyst, Gartner: Portal, Content and Collaboration Summit. Los Angeles, March 2011 and London, September 2011.

[2] Microsoft SharePoint Market Analysis, 2010-2014, Radicati Group, March 2010.

[3] Tagetik (www.tagetik.com).

[4] Philips Medical eICU application.

[5] Pfizer: http://www.pointsharepoint.com/2009/04/case-study-pfizer-content-managment.html.

[6] Chuck Faunce, SMART Business Advisory and Consulting, LLC, May 2007.

© STEALTH SOFTWARE

STEALTH SOFTWARE is a registered trademark and logo of STEALTH Software. All other trademarks, service marks and company logo and names mentioned in this document or web sites are property of their respective owners.

Notice: This document is for informational purposes only, and does not set forth any warranty, expressed or implied, concerning any equipment, software or service offered or to be offered by STEALTH Software. This document describes some capabilities that are conditioned on a maintenance contract with STEALTH Software being in effect and that may be configuration dependent. Contact STEALTH Software at info@stealth-soft.com for further information on features and products.