

IA

Primer

Content Security: Enabling Collaboration While Managing Risk

Content Security Redefined for the 21st Century

Introduction: Why the Content Security Game Changed

Securing digital content is not a new concept nor a new task for the enterprise. IT departments have been securing data since the first time-shared mainframe was deployed, perhaps earlier. Operating systems and databases have been providing read/write access control lists (ACLs) for decades. But much has changed since these early days of computing in terms of:

- networking capabilities (e.g. the reach of the internet and distributed wireless computing),
- business focus (e.g. the computer as a collaboration tool),
- online content (from data in rows and column to digitized images of contracts),
- modes of communication (e.g. the advent of e-mail and instant messaging)
- and the business applications associated with online content (e.g. online paid-for subscriptions).

Most organizations find that their ability to create and share content is out of sync with their ability to secure that content. Content security often lacks the flexibility and dynamic nature that content creation and management enjoy. A focus on and need to leverage and share content in order to maintain competitive standing requires more open approaches to access. Yet compliance, ethical and legal concerns mandate closer scrutiny and controls over access. Moreover, the proliferation of content and the potential for manipulation of content by non-authorized individuals, whether intentional or accidental, necessitates the need to authenticate and secure content.

Today, there is potentially great risk in assuming that content is, in any deep sense, secure simply because it is under the control of system level security, or even a traditional document or records management system. It is no longer reasonable to expect workers to be the watchful eye and only enforcement point in ensuring that information that should be private and/or protected remains in a secure state. The volume of content, the speed of creation and the reach of collaboration render this premise far too risky. Between accidental content exposure, purposeful content leakage and/or piracy, the problem of who is watching the watchers has become very real. Scalability, adaptability, awareness and enforceability of security policies are not reliable through a purely human effort, or a piecemeal technology deployment. Yet, as we have found in this study, that is often the case. In spite of threatened personal responsibility for inappropriate management of content, (e.g. SarBox), many organizations and their executives continue to rely on “good intention” and/or siloed technology solutions limited in

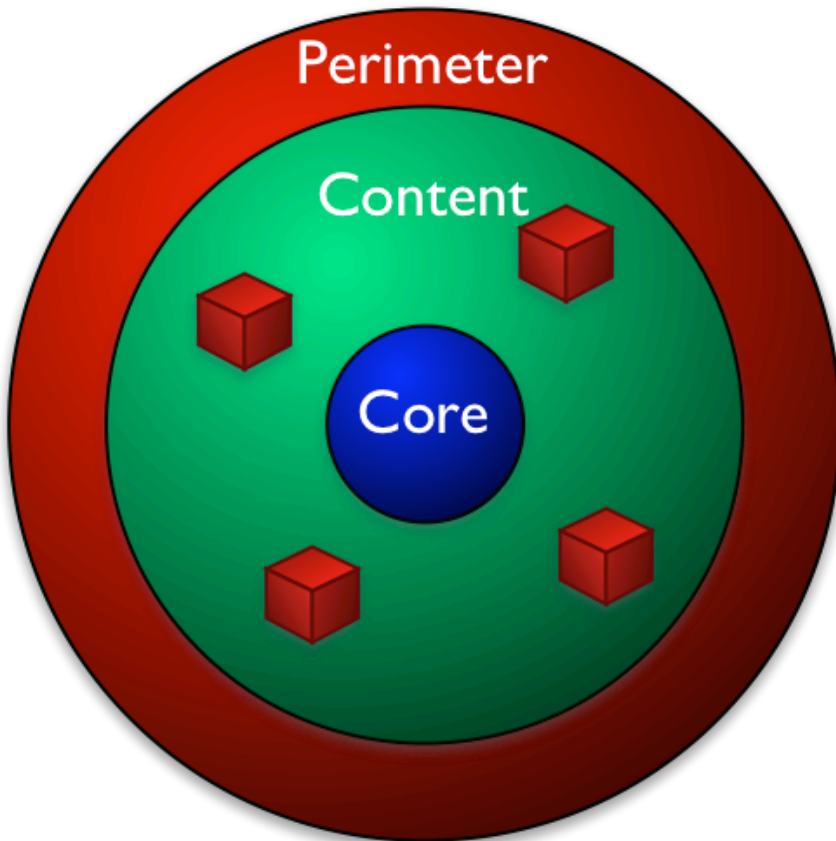
scope and capability that are several years behind the technology used for creation and sharing content. There is a family of technology point solutions specifically designed to address security in the 21st century, but, as this study found, understanding and deployment of these technologies is slow. Development of enterprise strategies to secure content in any meaningful way, leveraging the powers of available technology is nascent.

Enterprises must adapt approaches to securing content that differs from traditional approaches in two basic ways, the granularity of security and the authentication of security.

Focus on Changing Granularity

Traditional approaches to content security are focused at the perimeter of an organization and/or applications. This is the network-centric approach to content security that includes tools such as system login and firewalls. The focus is at a high level of granularity; network, server, desktops, and/or operating system level security. Content is holistically protected or secured from outsiders, and in some cases restricts insiders from accessing inappropriate outside resources. There is no contextual adaptability. The standard policy is one of “insiders are fully trusted, outsiders are completely distrusted.” This approach to content security is generic, providing lowest common denominator levels of protection to secure network applications and desktops, but not content specifically. Collaboration and knowledge sharing models under this approach require an all or nothing level of access to content, or the replication of content outside the system of control (e.g. a repository on a file server). The former is limiting, the latter represents abandoning any ability to control content and the issues associated with content replication.

Figure 1. The Network-centric Approach to Content Security



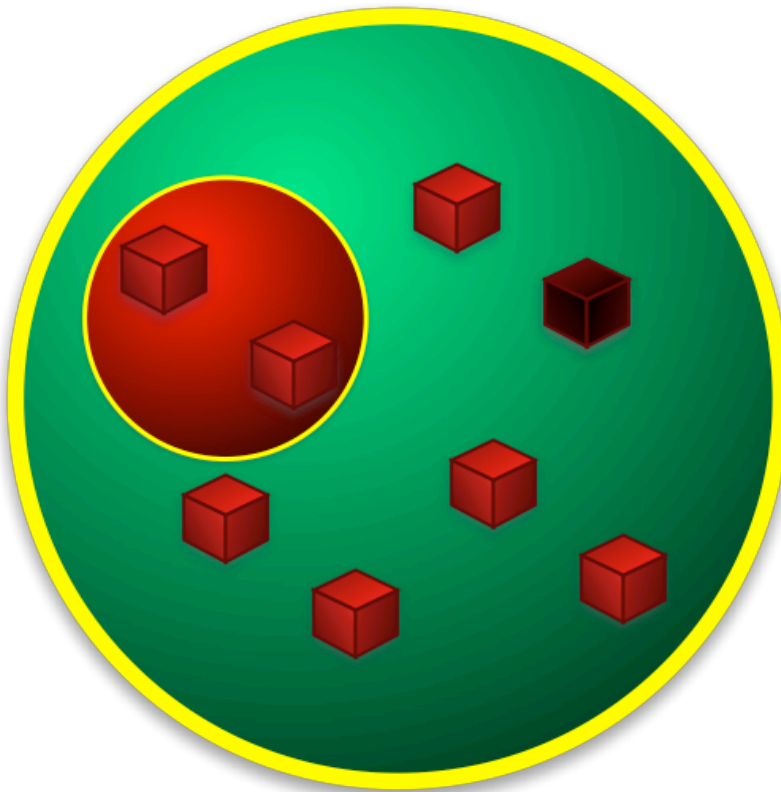
In this traditional approach to content security focus is at a high level of granularity. Content, represented by the red cubes, is protected holistically. A perimeter or firewall is created that allows for total access or no access. There is no monitoring of the individual content. Auditing occurs at the system level and there is no authentication of the content itself.

The Document-Centric Model

The application of certain content security technologies (e.g. records management and document management, which are discussed in more detail later in this report), push the level of granularity down to the individual file level. Using this approach, content, especially unstructured content is secured file-by-file, or in collections of files. The perimeter of control is constrained more tightly around a single file or group of files. Work areas, as sub-groups to an entire library can be established to enable shared access to a collection or single document. A limiting factor of this approach is that the security is enabled through the platform itself, (i.e the content or records management system). Using this ap-

proach to content security, it is possible for the content to be shared (e.g. e-mail attached) outside of the platform, and thus be manipulated once it is out of these systems. Users can check-out a file, modify it, share it (inappropriately), and not necessarily check the file back into the management system, or indicate what actions have been taken. Collaboration typically requires providing full access (read/write) to interested parties. Though an audit trail may be maintained, users are on their honor to “do the right thing” concerning editing and sharing. Authentication of time stamps and the audit logs may not provide meaningful evidence of content-centric issues.

Figure 2. The Document-centric Approach to Content Security



In the document-centric approach to content security focus is the individual file level, or a collection of files. Content, represented by the red cubes, can be individually protected. A perimeter or control can be created within the perimeter that allows for specific read/write/delete access to specific files (in this illustration the two cubes in the red circle contained in their own yellow ring are specifically protected, separate and distinctly from the rest of the content collection.) These files, however, are not protected from leaving this environment, and thus can “escape” the implied security.

Granularity – Targeting Sub-document Control

It should be appreciated that under the document-centric model, some platforms will provide control over sub-sets of a document (e.g. individual objects such as a single image or paragraphs of text.) In this way the level of control is at a lower level, and enables the repurposing of content in multiple delivery mechanisms (e.g. the usage of a single photograph in two separate documents and a web page), but the security and tracking of the image is maintained once – centrally. This level of granularity is particularly useful in a web-content management environment and/or in scenarios in which complex compound documents are created through links to a library of content “chunks”.

Additionally, granularity can be extended to metadata associated with each content object. This metadata can include properties such as author, title, summary, version number, an internal reference number, tracked changes and forwarding history. With this level of granularity, each tracked facet of the content, from the macro to the chunk level, and all metadata about the content is managed and secured providing a comprehensive content security system.

It should be noted that the granular levels of securing content are not necessarily hierarchical. That is to say, protection at a higher level of granularity may not negate the need specific protection at the lower level. Networks and platforms may be secured, even though specific chunks of content on those platforms or within those networks are also secured. A major component to any content security implementation is the strategy that takes a holistic approach to the business requirements and technology alternatives available, and weighs and leverages each.

The Content Security Lifecycle Model

One of the biggest challenges to securing online content stems from the fact that online content is not static. Online content can potentially be easily manipulated. Document properties, such as author, approval, and audit trail data are also subject to editing (legitimate and unauthorized). A comprehensive content security strategy must address this facet of online content, else render virtually all other attempts to security worthless.

The dynamic nature of online content is also associated with the ease with which content can be shared, duplicated and transported across systems and networks. Content/Data in motion as a term emerged in the ECM industry several years ago as a way to reference this very real property of online content. Yet most individuals still do not have a clear appreciation for what data in motion means and the complexity it poses to content security. Content security is, in many cases, embedded directly into content throughout its lifecycle - from creation, modification, distribution, archiving and destruction - regardless of format or transmission method. This is a policy-driven capability, distinct from the realm of Information Security. Where Information Security is primarily focused on securing infrastructure such as networks, servers, desktops, and operating systems, content security faces the challenge of development of policies and procedures policies across all content, at any level, in context.

Authentication

Authentication can be a pivotal and critical element to a content security system. Despite noble attempts to secure content, in all the manners discussed above, the content security system and its managed content can be rendered moot if there are no policies, procedures and mechanisms in place to manage and/or provide authentication of:

- user,
- author,
- approver
- and the content itself.

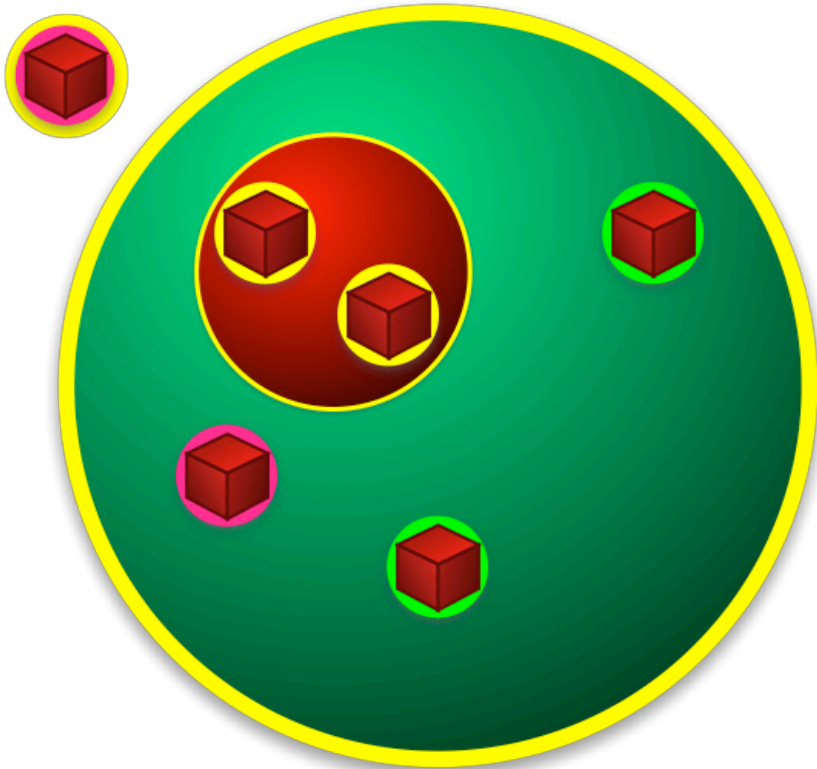
The value and criticality of authentication ranges from a need to ensure indisputable proof of authorship to indisputable proof of document validity. Users of online content need to be assured that content they are using is what it purports to be. In an age where “everyone can be an author”, controls may be necessary to ensure that content accessed online is legitimate, created by and/or approved by “appropriate or recognized” individuals, and in its latest approved revision. Mechanisms should provide reliability and/or an ability to reference and monitor the authentication of content and the data associated with that content. In issues of litigation and compliance, content can be deemed inadmissible if its authenticity cannot be proven beyond reasonable doubt.

The Object-centric Approach

A content security system needs to potentially address the fact that online content is often purposefully “content in motion”. Content is frequently shared, replicated, e-mailed and/or stored in multiple repositories. Content security models that rely on an underlying platform approach whose perimeter of control extends only as far as that platform, potentially fail an organization whose content extends beyond that platform. Content in motion (i.e. is in the process of being transported from one physical location to another), may undergo automated encryption. The object-centric approach to content security goes beyond encryption of “in motion” content, however, and incorporates approaches to managing the security of content “at rest” (after it reaches the end point of its “in motion” path.) The object-centric approach to content security deploys technology that extends the document-centric model, by embedding the security mechanisms within the content object itself. Content is transformed from an “ignorant” object that relies on outside mechanisms to assure its authenticity and security, to an “intelligent” object that manages its authenticity and security itself, in an omnipresent fashion, in context. This potentially enables wider distribution and ease of collaboration, without risk, because control and management of the content is not relinquished as a result of sharing. For example, press releases could be openly shared internally as a means of early education. Recipients however, would be automatically prohibited from attaching the press release to an e-mail message prior to the release date. The management of this policy would be embedded into the “intelligent” press release itself. Market reports could be provided to a paying customer, without permitting the customer to duplicate the report, print the report or e-mail attach the report.

The object-centric approach to content security represents the state-of-the-art in terms of flexibility, reach and type of business models it supports. It is again important to point out, however, that application of such security mechanisms does not necessarily negate the need for the other approaches to securing content. A state-of-the-art content security system is only accomplished through the application and integration of several point technologies, governed and orchestrated through a centrally developed, maintained and executed strategy and policy.

Figure 3. The Object-centric Approach to Content Security



In the object-centric approach to content security, focus is on the individual file level (similar to the Document-centric Approach, but the policies and mechanisms to secure the content are embedded within and thus move with the content itself). Thus the content becomes a self-regulating intelligent object that controls who and what can be done to the object, in context, at all times. The security associated with the content is omnipresent. Content, represented by the red cubes, are individually protected, and that perimeter of control (illustrated by the yellow circle) stays with the content, even when the content is “sent” outside the perimeter of the file, document or records management system. Unlike the situation in a document-centric security model, content can be protected from leaving this environment, and if permitted to “leave,” maintain its integrity and access permissions.

The Technology Components of Content Security

It must be continuously stressed that content security is more about a well defined and executed strategy model than it is about technology. It is nonetheless prudent to have a working knowledge of technology alternatives before embarking on a strategy. For too many organizations, the content security strategy is confined to “old approaches” or limited functionality due simply to an ignorance of technology alternatives and potential functionality. Indeed, there is predominately a dearth of knowledge regarding content security technology components in the market. Before organizations can embrace the state-of-the-art in content security they need to have an appreciation of what is possible.

The primary component technologies that comprise the state-of-the-industry for content security are described and positioned here. These technologies are:

- Records Management
- Document Management
- Web Content Management
- Workflow/BPM
- E-mail Management
- Enterprise Rights Management/Digital Rights Management
- Identity Management/User Authentication
- Policy-based Encryption
- Content Authentication
- Content Addressed Storage
- Trusted Time Stamps
- Data Loss/Leak Prevention
- Public Key Infrastructure (PKI)
- Digital Signatures and Hierarchical Storage Management

Records Management (Federated Records Management) systems manage declared business records against the records retention schedules of an organization. In this regard, records management addresses content security over a lifecycle, from declaration of the content as a record to the archival and possible destruction of that content. Records management systems address the “final resting place” or “life duration” of content, but do not address any other content security aspects. The perimeter of control of the records management system does not extend beyond the system itself. Content is not in any way managed until it is declared a “record” and thus “moved into” the control of the records management system. The integrity of the content and authenticity of the content prior to it being declared a record is not managed. Similarly, copies of content (records) existing outside the records management system are not managed in any manner.

Records management systems are relatively mature technology products. Records management is one of the more understood and utilized technology components of current content security strategies.

It is worth noting that a new approach to records management, known as federated records management or universal records management (URM) has emerged. In a federated records management system, the content (records) may be physically stored in multiple locations across the organization, including repositories that contain content not declared as records. The federated records management system can access the enterprise content stores and identify and manage records within them. Thus the records are managed in their “native” system or platform, in context. This somewhat extends the perimeter of control provided by the records management system and facilitates the integration of the records management system into an overall enterprise content management system.

Document Management systems are typically concerned with revision control (management and tracking of the current version of a content object and the ability to roll-back to prior versions), document lifecycle audit trails (tracking the history of authorship and modification via a date/time/author stamp), and rendition control (PDF versus MS Word copies of the same content – linking the two together). Document Management systems provide rudimentary content authentication functionality. Document Management systems typically provide simple security controls (i.e. read/write/delete) over files. Document Management is a core and fundamental capability for content security. But, typically the perimeter of control of the Document Management system does not extend beyond the system itself.

Web Content Management systems are similar to Document Management systems, but focus on web-based content. This includes management of the publishing process and maintenance of links between information chunks. Key features of a Web Content Management system include: creation and authoring process controls; authoring and presentation/display template design and management; content re-use management; and dynamic publishing capabilities. Web Content Management can be leveraged to ensure that content managed and deployed via the web remains in compliance with the policies established within the purview of the content security strategy.

E-mail Management systems are similar to Records Management systems, but are finely tuned to specifically handle e-mail messages, and in most cases their associated file attachments. These systems typically extract e-mails from the server and save them to a secure environment in the e-mail messages and their attachments are classified and maintained as business records. Typically the perimeter of control of the E-mail Management system does not extend beyond the system itself. An E-mail Management system can be integrated into a

broader records management system, in which case the perimeter of control is limited by the reach of the records management system.

Workflow/BPM (Business Process Management) technology is often deployed beyond the purview of content security. Workflow and BPM technology can be used to manage and automate virtually any business process. Their role in a content security system is to provide control of (and thus integrity) any and all processes used to move content through its lifecycle. This includes automation (i.e. enforcement) of the execution of critical steps and functions to securing the content. For example, a workflow enabled publishing process can ensure that a body of content is automatically declared a record when posted to a web site, or that a file cannot be released for the “general public” until a designated reviewer has “approved” its content. Workflow and BPM can be used to automatically and relentlessly apply policies key to policy-driven content security. Without automated processes enforce such policies, content security is vulnerable to human error, oversight and/or sabotage. Additionally, the Workflow system provides an audit trail on the processes, providing a further level of authentication and quality control over content across its lifecycle. This ability to provide business **process integrity**, especially in situations related to litigation, can be as critical as the securing of content itself. Workflow audit trails limit the ability of litigators to question the process used to manage content.

Identity Management/User Authentication, simply put, are systems and techniques used to ensure that users are who they purport to be. Authentication depends on one or more factors. At the low end, this could include administration of usernames and passwords. At the high end, this could include a retina or fingerprint scan. Authentication is typically a precursor to authorization – secure identification (authentication) of a user leads to an associated list of permissions (authorization) within content and processes.

At the higher end of functionality, Identity Management/User Authentication systems are used to ensure that access and audit controls feed from authoritative and current identity sources. Policies are connected to both higher-level groupings, and have fine-grained control down to each unique individual. While standard access control repositories such as Active Directory (AD) are typical end repositories of this information, they do not contain the “intelligence” to ensure that this information is verified and up-to-date. Regulatory compliance and general corporate governance standards state explicitly that access privileges need to be certified and audited. Individuals should have the appropriate level of access to content that they need to do their stated jobs, but no more than that. Typically permissions and identity are tracked at the roles & rights level. This eliminates the “rights creep” that can occur, if rights are tracked by individual, and an individual “moves” across jobs and functions within an organization, keeping past access rights even though they have changed roles and or project/department affiliation.

Enterprise Rights Management (aka Digital Rights Management) systems embed security policies within documents themselves (the object-based model). Under an Enterprise Rights Management system, the perimeter of control is tightly maintained around the content, even when the content is “in motion”, or is “at rest” in a repository that is outside the physical domain of the underlying or native platform. Enterprise Rights Management can control content usage to various levels (e.g. Read/write access, access based on the user’s current location, number of times or length of time a content can be viewed by a single user, whether cut/copy/paste of content is permitted, ability to forward or e-mail attach and online/offline access), both within and beyond organizational barriers.

Policy-based Encryption automatically encrypts content based on user-defined rules that are typically embedded into a user authentication and/or Enterprise Rights Management system. Using Policy-based Encryption, content may be physically “available”, but not “accessible” until conditions are met that ensure the “right person at the right time” is accessing the content. Policy-based encryption is predominately used on content in motion, or being transported from a protected system to another system.

Content Authentication refers to the orchestrated usage of many content security point technologies (e.g. trusted timestamps, content addressable storage, e-signatures, electronic watermarks and document management) used in aggregate. Content Authentication systems provide auditable assurance and reliance that the content is indeed what it represents itself to be (that it is “official”, is the latest version, has had no unauthorized modifications, etc.). Content Authentication rebbers electronic beyond refudiation.

Content Addressed Storage (CAS) technology focuses on content at rest, or endpoint data protection. It is used exclusively on content that is written once and never changed. Such targeted content might include invoices, financial statements, archived e-mails, medical X-rays or sealed records. CAS creates a digital fingerprint of the stored content. This fingerprint (also known as an ID or logical address) ensures that the content is the same exact piece of data that was saved. No duplicates are ever stored.

Trusted Timestamps work in concert with Records Management and/or Document Management systems to certify that content when submitted to the managing system, is the exactly the same when it is later recalled/retrieved. Trusted timestamps render online content beyond refutation and provide “proof” that content has not been modified, nor has any of its associated meta tags i(i.e., signatures/approvals or timestamps on such approvals). Trusted timestamps can be a critical component to content integrity and in some cases include services by an independent trusted third party to further separate the possibility of internal collusion.

Data Loss/Leak Prevention is intelligent filtering of content in motion, based on centrally administered policies, with as little human intervention as possible. Data loss/leak prevention systems “read” content that is targeted to be sent outside a defined perimeter (e.g. an internal system or an external firewall) and discern whether there is protected content or private data (such as social security numbers, credit card numbers, medical history) within the content. If such content is detected, the content is filtered, and kept from being shared. Advanced content filtering (e.g. semantic or linguistic content filtering) can detect protected or private content that is not directly contained in the content (e.g. rephrasing content to potentially bypass keyword filters.) Advanced systems can also process rules regarding the intended recipient of the content, (i.e. the content is only protected from certain people), for example, preventing buy-side and sell-side workers in a brokerage firm from sharing content that can be construed as internal collusion.

Public Key Infrastructure (PKI) uses a public and private key pair held by a trusted third party to transact business over the public Internet. PKI is typically used to verify digital signatures (see below.)

Digital Signatures refer to a spectrum of functionality. At the low end (where the functionality is also known as electronic signatures), this refers to the attachment of an image, electronic sound or symbol to content, providing association with a person to the content (e.g. as a reviewer or approver.) At the high end, digital signatures are created and verified by cryptography. Digital signatures employ an algorithm using two different but related “keys” (using PKI), one for creating a digital signature, and another key for verifying a digital signature or returning the content to its original form.

Hierarchical Storage Management (HSM) is a content storage system that typically transcends content security. HSM automatically moves online content between various storage mediums based on a variety of policy and efficiency reasons. HSM can be deployed as part of a content security system, typically in conjunction with a workflow-enabled process, to automatically move content to a specific type of storage medium at a particular point of its lifecycle (e.g. content when declared as a legal record is automatically moved to a WORM drive, and subjected to a trusted timestamp and or CAS system).

It is again stressed that content security is not embodied by any one of these technologies, but through orchestration, coordination and integration of these technologies in a complementary fashion. This requires the development of a content management strategy in which business needs are evaluated and specifically addressed through selection of appropriate content-security related technologies.

Developing a Content Security Strategy: Balancing Access and Risk

Organizations in the 21st century are met with an unprecedented ability to communicate. Content can be captured/created in multiple ways and published via multiple avenues. Content can be dynamically repurposed, tailored to individual consumers in specific business contexts. Online capabilities are changing the rate and flexibility of collaboration. But, such flexibility associated with content creation and collaboration bring with it heightened new challenge of security. As the desire and need to collaborate rise in organizations, so too do the demands to protect intellectual property and stay within compliance. Organizations must develop a content security model, based on well defined business needs, that exploits IT capabilities in order to enforce corporate culture and policy.

Traditional approaches to content security are founded in a directly adverse relationship between security and access. Traditional approaches view security as a black-and-white issue. A basic tenet of such approaches is that risk reduction comes at the price of increased security, which by definition limits accessibility. Higher degrees of security (lower risk) are only achieved through decreased sharing of content.

The modern perspective on content security introduces a vast gray area between the black-and-white, or polar approaches to securing content. Lower levels of granularity on the levels of security and tracking of content, along with embedded lifecycle policy-driven security, enable enterprises to provide secure access to content without jeopardizing content integrity and organizational exposure.

The creation of an enterprise content security model must be preceded with a careful analysis of organizational goals and objectives (business drivers), legal requirements, and an inventory of all user types and content sources. Additionally an assessment of technology platforms, integration issues and leverageable infrastructure should be taken into consideration.

It should be appreciated that the enterprise content security model is first and foremost driven by a business strategy. The role of technology is to support a content security strategy developed within the framework of corporate business goals and objectives. The decisions made within the business/policy context are far more critical, and often much more difficult to reach, than selecting technology components and alternatives. This cannot be stressed enough.

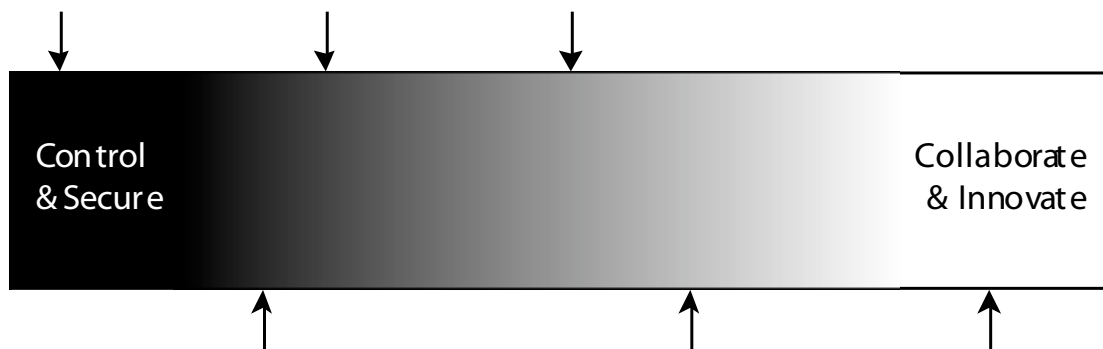
Although the strategy development process is wrought with decisions and alternatives, there are two basic tenets that can be focused on as foundational to the enterprise content security model. The first is weighing the balance between

control and collaboration. The second is determining the scope of lifecycle content security.

The ability to share and collaborate on content can be a major enabler to driving innovation and knowledge exchange in an organization. The ability to leverage collective intellectual property is an organizational asset, a point of differentiation and competitive advantage. Focused on such goals, organizations will be tempted to take very liberal views to content security, enabling rapid capture of content, dissemination of content and broad and deep approaches to sharing/ discovering that content. On the other hand, in many cases, intellectual property (e.g. patents, trade secrets, customer lists) are organizational assets that, if inappropriately shared can decrease in value, and, in the worst case, cause the demise of the organization. Inappropriate sharing of content can bring serious government-imposed and legal ramifications. Any prudent organization must manage its risk, as it relates to content.

Herein lies the ultimate challenge to the organization faced with forming an enterprise content security model. Business decisions must be made for each source of content, in each possible context, as to the potential and desired value in sharing the content versus the potential risk in exposing the content. Based on calculated and informed decisions, a system comprised of policies enforced through appropriate technologies, should be designed and constructed.

Figure 4. The Control/Security – Collaboration/Innovation Continuum



This figure represents a roll-up of the business needs of an organization, as they relate to a need to control and a need to collaborate. In this example, arrows have been inserted at various points of the continuum. These represent specific needs of the business, based on a full needs assessment. When viewed collectively, a full appreciation for the degree to which a strategy and system are needed to secure and control, the degree to which security is not an issue (open

content up to unfettered access), and the degree to which regulated and monitored access is required (the gray area), becomes evident. Based on this level of analysis, a technology strategy, to support the business strategy begins to emerge.

In this example, the organization has determined it has 6 specific policies or levels of security to provide. There is a slight leaning towards control & secure, as evidenced by the three arrows to the left of center. In these instances, there will be an emphasis placed on technologies such as e-mail management, trusted timestamps, CAS and records management. The two arrows located approximately in the middle of the continuum suggest that policies need to be created that support regulated and monitored access, indicating a need for technologies such as digital rights management, web content management and data loss prevention. The arrow at the far right of the continuum represents a need to make content available in a highly collaborative format. This may require technologies such as content and user authentication. The continuum is not the definition of the strategy per se, but a way to visually appreciate the range of needs that must be supported by the strategy. Heavy concentration of arrows (needs) at either end or squarely in the middle might suggest a compelling reason to initiate the content security deployment in that area, using the indicated/related technologies. This is, however, just a first pass. Underlying issues, such as a sponsor's preference or a compelling need in one particular situation may take precedent and dictate the focus of the content security initiative initially. (One might indicate these compelling needs via larger/more pronounced arrows on the continuum.) In either case, the continuum illustration helps to lay a foundation and appreciation for the full scope of enterprise need, and possible leverage points from specific technologies.

Content Lifecycle Security

As part of this exercise, the requirements for content security must be evaluated not only for each intersection of user type and content type, but throughout the lifecycle of the content.

Figure 5. The Stages of Content Lifecycle



An enterprise content security strategy must look at each content type throughout its lifecycle to determine if the needs for control and collaborate change over time.

The issue addressed in this exercise is the degree to which technology is applied at specific milestones of the content's life. Lifecycle management asks when should specific levels of security be applied, and does that need change over time. For example, content can be declared a record at any point of its lifecycle. Until that point, there is no record level control on the file. Is it necessary to provide the authentication and reliability of this content at each stage of its lifecycle (including earlier revisions), or simply on final approved formats? Should document and web content management functionality begin at the exact moment of creation (i.e. are only certain individuals permitted authors, editors, reviewers? Are templates provided to authors that control document structure and format?), or is this level of control only required at the point of delivery? As content is archived or preserved, do access rights (and means of access for that matter) change? When destruction occurs are security mechanisms required that automate and guarantee that all versions of the content are in deed destroyed – and by what method?

Policies and Enforceability

Based on the conclusions reached through a business needs and lifecycle needs assessment, a series of policies regarding content control can and should be developed. A major advantage of an enterprise content security model is the ability to define and manage content security policies centrally, and have them deployed locally, in context.

There is sometimes a tendency to view the flexibility and power of content security as a way to develop highly specialized security models for virtually every possible combination of content and user. In reality, the goal of good strategy design is to establish as few policies as possible, for as the complexity of a security model increases, so too does the propensity for the model to fail. Although the capability to execute an unlimited number of policies is possible, it needs to be appreciated that the policies themselves need to be managed. It is therefore advantageous to establish a manageable family of policies that can be

applied to groups of content under defined situations. Content and context should be grouped into categories of levels of control. Examine business applications (e.g. e-discovery, financial reporting, M&A activities, patent management, competitive intelligence, product management, R&D, board communications, etc.) and determine to what degree the levels of control for each can be shared or categorized. The resulting set can then be centrally administered and managed and applied locally in context.

The approach to enforcement, or application of these policies must then be addressed. A decision must be made as to whether policies are driven and enforced through workflow/BPM and/or manually at specific points throughout the content's lifecycle.

The Impact of Content Security

The formation of a strategy that looks at needs across all user types and content types, for the full lifecycle of content requires a formidable effort. But the effort provides great reward. The end result is not only a well thought out strategy, but a much clearer appreciation for how the investment in content security can be leveraged across the organization. Approaches taken to meet compliance issues, for example, can be leveraged to create new business opportunities, which in turn can capture and fuel additional innovation. On the other hand, if content security is addressed in a silo (e.g. a way to address compliance only) the impact of the solution and its ROI will also be siloed. The potential for redundant efforts increases and holes in content security between separate systems increases.

The orchestration of multiple point technologies, used in a coordinated effort, provides more than just security of content. Content security is a lifecycle approach to not only protecting content, but to maximizing the value derived from that content. It is most important to realize that the proposition being made here is not about security per se, at least not in the traditional sense. The focus is not just on control, but leverage, sharing and increased opportunity. As previously stated, traditional approaches to security are founded in an adverse relationship between security and access. The basic tenet of the perspective is that risk reduction comes at the price of increased security, which by definition limits accessibility. Higher degrees of security (lower risk) are only achieved through decreased sharing of content. The modern perspective on content security encompasses increased granularity on the levels of security and the ability to have security travel with the content. In this approach, as the levels of control increase, so too does the ability to share or collaborate in creative new, and secure ways. Understanding this new paradigm represents a new realm of opportunities for deriving value from content without compromising the organization or putting it at risk.