



Intelligent Protection:

Your Enterprise
and
Document Security for Data in Motion

Copyright 2007 Vincera, Inc. All rights reserved.

About Vincera, Inc.

Vincera, Inc. is the document security company whose Vincera Intelligent Protection™ (VIP) software securely protects and converts more than 300 types of digital assets into PDF documents, and then enables their clients to monitor and measure the distribution of these protected data in motion, including intellectual property and other sensitive data. Vincera's clients can then manage that distributed data based on their company's associated security policies. VIP enables business to proceed at its necessary rapid pace while permitting enterprises to apply the appropriate security level and to decide how they use the resulting information. Only Vincera combines three vital document security software services- document threading, behavioral monitoring, and access management.

Vincera's clients include enterprises in diverse industries that use Internet-based technology to e-distribute documents with sensitive data in motion such as intellectual property, proprietary information, personally identifiable information, and/or personal health information. Vincera's clients share a need to guard this sensitive data in motion and to track how their own customers, employees and partners are using their licensed products, enterprise documents or other intellectual property. For more information, please visit:

www.Vincera.com

Intelligent Protection Forward

A complete enterprise data security solution requires five pillars of intelligent protection:

- **Confidentiality** – data is only accessible by those authorized to view or use it.
- **Use Control** – data is only usable in approved contexts.
- **Integrity** – data cannot be changed or manipulated without authorization.
- **Availability** – data must be readily accessible to those with proper authorization to view or use it.
- **Accountability** – data availability is traceable back to a source such as a user or machine.

Electronic data exists in two states: either data is *at rest* or *in motion*.

Data at rest is typically stored in databases waiting to be used. Once data at rest is needed for a business use, it becomes portable, i.e. it becomes *data in motion*. A common example of data at rest becoming data in motion includes typical reporting scenarios where databases are queried for certain data, which is then packaged in a portable format for distribution to one or more recipients.

Aside from genesis as data at rest, data can, and often is, created in a highly portable state. Examples of data created in a portable state include everything from business emails to Word documents.

And, after data in motion reaches the end of its cycle of use and distribution, it often continues to exist stored on hard drives, in archives, knowledge bases or other data repositories, available to be used and distributed again.

Data at rest is fundamentally different from data in motion as, once portable, data becomes much more difficult to protect, monitor, measure and manage with respect to its authorized use and distribution.

Today, great effort and expense has produced viable technologies, such as firewalls, that support the five pillars of intelligent protection for data at rest.

A large gap, though, exists for applying those same pillars to data once it goes into motion. Currently, intelligent protection of data breaks down at the point data goes into motion, especially once it is distributed outside the managed enterprise network.

One instance of brand damage due to a security breach can destroy a company; who takes the blame?

Enterprises today, because of the security gap that exists for data in motion, are completely in the dark as to where their sensitive data in motion travels outside the network and who might have access to it.

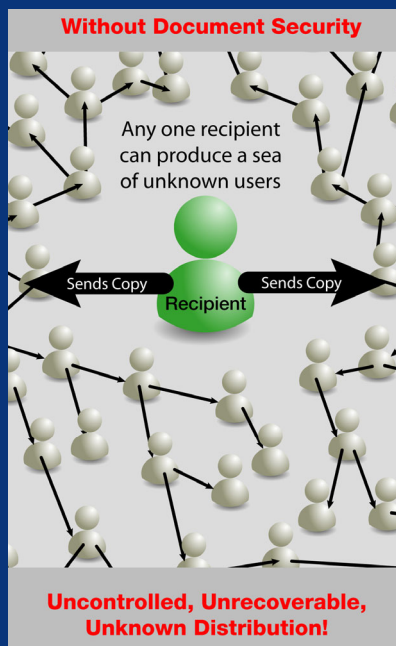


Figure 1 – Unbounded Distribution

Unbounded Distribution

The Extent That You Do Less, You Incur Risk

Currently, the vast majority of enterprises do not use technology that can apply the five pillars of intelligent protection for data in motion. Instead, distribution of portable data is unbounded, relying on documents that are easily breached and transferred outside of acceptable distribution networks without any information about the unauthorized distribution reported back to the enterprise.

Enterprises today, because of the security gap that exists for data in motion, are completely in the dark as to where their sensitive data in motion travels outside the network and who might have access to it.

This is dangerous for the enterprise. Without the technological means to protect and manage the electronic distribution of sensitive information, all sensitive data from personally identifiable information to product plans to executive communications can be distributed outside a corporate firewall and become subject to the whims and agendas of recipients. For instance, sensitive product planning documents sent or accessed electronically can easily be redistributed, unfettered, in an unauthorized manner well beyond the expected distribution. Motivations for such actions can range from simple, honest mistakes by naïve employees to premeditated attacks on the enterprise by disgruntled employees, partners or fraudsters.

Any one document recipient (i.e. a receiver of data in motion) can produce a sea of unknown recipients, both inside and outside the enterprise network and that of its authorized partners (figure 1).

With unbounded distribution, document recipients have the ability to create vast unknown and unmonitored document threads. A document thread, the chain of custody for data once it goes into motion, can extend sensitive data without restriction to unauthorized recipients such as the press, competitors and fraudsters.

Unbounded distribution leaves the enterprise with no means to ensure confidentiality, use control, integrity, availability or accountability over its data in motion.

This means that when data security breaches occur, they only become known to the enterprise when it is far too late - after the damage has been done. And, without technology that supports the pillar of accountability, the enterprise is hard-pressed to hold anyone but itself responsible, resulting in unacceptable levels of compliance, competitive ability, risk and liability.

Bringing Distribution Back Within Bounds *Extending DLP, DRM and BI*

To avoid legal woes and corporate loss, enterprises must control access to systems and documents containing sensitive data, i.e. employment data, business information, intellectual property, etc. Fortunately, just as technology has created the capability to widely distribute sensitive data, so it has enabled the protection of that same data. Today, technology exists that applies the pillars of intelligent protection to data in motion.

Specifically, enterprises must identify and apply a solution that will perform **four key functions**: to protect, monitor, measure, and manage the distribution of sensitive or potentially sensitive data in motion, otherwise known as the document thread.

Such solutions incorporate or extend technological elements of data loss prevention (DLP), digital rights management (DRM) and business intelligence (BI) solutions. These component elements converge to form a targeted, efficient security solution, based on document thread technology (*figure 2*) for data in motion, without the high management and implementation overhead required by the three separate regimes in their entirety. Document thread technology is a nimble platform from which to apply intelligent protection for data in motion that does not impede business.

Most enterprises have explored and many have implemented standalone DLP, DRM and/or BI solutions that focus on in-network data in motion security. Once data in motion, though, is released into the “wild” these solutions do not extend outside of the known managed network.

Effective intelligent protection technologies are designed to integrate with and extend any existing DLP, DRM and BI enterprise solution to solidify in-network data security as well as fill the security and knowledge gap that exists when data in motion travels out-of-network, i.e. beyond the enterprise and its partners.

With intelligent protection applied to data in motion, the previously unknown, unseen and undetectable document thread becomes entirely visible and measurable to the enterprise. Document distribution can be reported as it happens and document threads can be managed based on acceptable, defined limits and ranges of distribution behavior.

Intelligent protection travels with every instance of the document to actively control its real-time distribution to authorized recipients and report distribution behavior back to the enterprise. Along with distribution behavior, intelligent protection offers the enterprise the power to disable or life-limit a document thread (i.e. to turn off all access to every instance of a document) before a breach occurs.

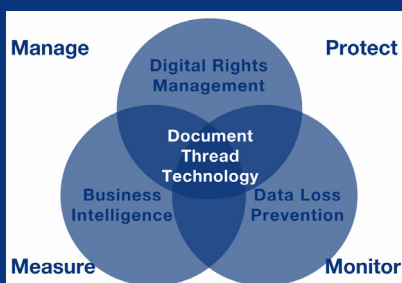


Figure 2 – Extending elements of DLP, DRM and BI to form document thread technology to Protect, Monitor, Measure and Manage data in motion

Sizing Up the Data before it goes into Motion *Document Protection and Security Policies*

The first step in securing data in motion is to understand its sensitivity and associated security needs.

Intelligent protection solutions can efficiently leverage existing enterprise data classification systems (such as content filters, document management systems, or roles-based scenarios) to determine the appropriate security policy needed for every document prior to distribution.

Once the sensitivity of the data in motion is known, the second step is to apply an appropriate security policy that balances the necessary security with business friendly distribution – i.e. the need to not inhibit legitimate, business-critical distribution of data.

Intelligent protection security policies establish a configurable (by the enterprise) set of rules that can be automatically assigned to all enterprise data in motion contained within enterprise documents. Such rules include whether or not recipient authentication is required; whether or not offline access is allowed; whether or not document expiration timings are set and enforced; and whether or not certain document usage functions (such as print, copy-and-paste and save as) are allowed for the protected documents.

Based on the sensitivity classification of data contained within a portable document, intelligent protection then encrypts and applies the appropriate security policy to each document. The most sensitive data automatically has the most rigorous security policy assigned to it whereas the least sensitive data may only require a security policy that applies distribution tracking for business intelligence purposes.

Now that the data in motion is protected, it can be distributed to its intended recipient, thus beginning a protected document thread. The intelligent protection security policy always travels with the data in motion as it may be redistributed to other recipients beyond the initial recipient, continuously enforcing the usage and distribution rules for that data as the document thread grows.

In this way, the pillars of confidentiality, use control, integrity and availability are actively supported for every instance of data in motion, wherever it may exist – inside or outside of a known network.

And, because intelligent protection digitally watermarks the data in motion with an original recipient identifier, all distribution within that document thread is traceable back to an original source; supporting the pillar of accountability.

Applying Protection is only the Beginning *Monitoring Distribution*

The technological ability to monitor the distribution and usage of data in motion adds to the value of intelligent protection. Instead of simply knowing that data in motion is safe in the “wild”, monitoring provides continuous feedback and actionable knowledge regarding the document thread.

As data in motion takes the form of a document thread that may span recipients inside and outside of the managed enterprise network, monitoring that distribution makes that document thread visible to the enterprise.

Monitoring provides the enterprise with specific information about where the data in motion, a.k.a. document, is distributed:

- machines (i.e. desktops and laptops) are fingerprinted for unique identification
- IP addresses are recorded
- individual recipients, in instances where security policies require user authentication to access the data, can be identified through authentication credentials

Additionally, monitoring provides detail about how often the data in motion is accessed (i.e. how often it is viewed). And, when the security policy allows offline access to data in motion (i.e. when an internet connection is not present such as during air travel), intelligent protection still monitors usage and reports it when an Internet connection becomes available.

If all this monitoring sounds cumbersome, it need not be. Intelligent protection with business friendly distribution has a minimal impact on current business process and IT environments, end-users, and partners.

Intelligent protection uses information provided through monitoring to provide distribution audit trails that squarely support the fifth pillar of accountability and eForensics. This key function of intelligent protection greatly reduces risk to the enterprise by knowing where data in motion exists at any point in time, past or present.

Making the Most of Monitoring *Measuring Distribution and Usage*

As the monitoring function of intelligent protection reports back details of the document thread, these details are measured and reported to the enterprise. The consolidation and presentation of monitoring data makes the information actionable.

Intelligent protection provides roles-based reporting whereby individuals within the enterprise are presented with reports containing information pertinent to their role within the enterprise.

For example, executives are presented with executive summary reports regarding compliance and enterprise-wide distribution of data in motion; department heads are presented with reports concerning data in motion that is distributed through their team; and infosec professionals are presented with detected security concerns for data in motion.

Additionally, intelligent protection allows for limits to be defined for data in motion distribution and use. These limits are commonly referred to as thresholds. As monitoring data is measured, it is continuously compared to any existing threshold limits defined by the enterprise.

When limits are reached, automated email alerts can be generated that notify appropriate personnel. For instance, if a particular instance of data in motion is not expected to be distributed to more than three distinct machines (i.e. desktops and laptops), an email can be sent to infosec personnel alerting them to the fact that the machine threshold has been reached and further document thread management may be warranted. The alert email contains current information regarding the data in motion's document thread along with quick links to document thread management options.

Alerts can be generated based on any metric monitored through intelligent protection.

Furthermore, measuring document thread activity enables continuous process improvement by providing the enterprise with granular intelligence regarding data distribution and behavior, which, in turn, is used to define and refine data in motion discovery, classification, security policy associations and distribution limits.

Taking Action when Needed *Managing the Document Thread*

Intelligent protection provides the technological means to manage the document thread at any point in time.

Based on the constant measurement and reporting of data in motion as it travels and is used in the “wild”, it may become necessary for the data to be rendered inaccessible.

This need may be well understood prior to the initial distribution of the data in motion and fulfilled through the planned expiration of the document thread. For instance, a particular piece of data in motion may be created with a known useful life of six months, beyond which the data should no longer be accessible. In such cases, intelligent protection provides the means, at the time of protection, to life-limit data in motion. Once the data in motion reaches the end of its predetermined usefulness, intelligent protection automatically and irrevocably disables access to every instance of the data in motion associated with the particular document thread.

In other cases, measurement of behavior within a document thread may reach predetermined limits of acceptable usage and distribution behavior. Here, intelligent protection provides the technological means for automatic or manual disablement of the document thread based the usage and or distribution of data in motion reaching a predetermined threshold. For instance, if a sensitive electronic communication that is only intended for distribution within the enterprise network is accessed from a non-network IP address, the distribution exception generates an email alert and, if necessary, the document thread can be disabled automatically, or manually by infosec personnel.

Management of the document thread can also be valuable to the enterprise outside of time-based and threshold-based contingencies. For instance, when an employee leaves the enterprise and becomes an ex-employee, sensitive document threads associated with this person can be selectively disabled by infosec personnel with a click of a button. With intelligent protection for data in motion, enterprises have more control than ever over data held by former employees and partners.

And, when necessary, intelligent protection also provides the ability to re-enable a document thread should circumstances arise that require such an action.

Available Today: Intelligent Protection *Conclusion*

Securing data in motion, and hence your own enterprise business, has never been easier.

Vincera Intelligent Protection™ (VIP) software from Vincera, Inc. delivers behavioral intelligence, data loss prevention, and business friendly rights management in one software solution for all your business-ready documents and digital assets. With automated conversion of over 300 types of digital assets to Adobe's PDF (Portable Document Format) your data in motion is fingerprinted to detect tampering, digitally watermarked as a unique document thread, encrypted for protection and associated to a security policy to ensure secure distribution and access. With every desktop fingerprinted and document behavior monitored, VIP Alerts and Management Reports meet compliance, forensic and audit requirements for managing your digital assets and sensitive information throughout the distribution lifecycle.

In addition to VIP's stand-alone value:

VIP leverages your investment in content filtering and data loss/leakage prevention (DLP) by creating an additional decision path for the DLP appliance. Currently, DLP is limited to a relative binary decision to quarantine the content or allow the content to be distributed. And worse, many DLP solutions make that decision based on querying the sender for what they want to happen. With the rise and awareness, regarding internal content leakage, a better solution is needed. VIP associates the classification of content from a DLP solution and then assigns the related VIP security policy to the content. This means that security is applied to content consistently and automatically, similar to how data at rest is accessed, without involving the human-factor which is the greatest risk to data in motion security today.

VIP operates stand-alone or in conjunction to Digital Rights Management and Data Loss Prevention solutions. In conjunction, VIP extends DRM to business units that will not deploy restrictive access solutions and yet they need encryption and security for a significant proportion of their data as well as the distribution knowledge of where that content is being accessed and how that content is behaving. In conjunction, VIP extends DLP to out-of-network desktops and content recipients to identify, discover, and report that your content is now on their desktop!

Contact Vincera today at: 512-443-8749 ext 121 or
VIP-sales@vincera.com