Websense® Data Security Suite and Cyber-Ark Inter-Business Vault®

The Power of Integration

Websense® Data Security Suite

Websense® Data Security Suite is a leading solution to prevent information leaks; be they caused accidentally from inside your organisation or as a result of a malicious attack from outside the company.

Websense Data Security Suite discovers where information is located in a network, monitors who is using the information and how they are using it.

It protects valuable corporate assets, secures business processes and minimises the risk associated with conducting business in a connected world.

Highly regulated industries will also benefit from improved compliance with data management regimes. Websense has the only data loss prevention (DLP) solution that includes a robust data analysis engine that integrates with directory services and web intelligence solutions to provide in-depth reporting of users, groups and destinations. It includes intelligent protocol inspection to detect protocol communications regardless of port and automatically categorises incidents by type, regulation and severity to provide valuable insight into regulatory compliance and corporate governance incidents. Powerful forensics and distributed analysis technology allows sharing of remediation tasks across large, decentralised organisations for better efficiency, while core policy decisions are administered centrally.

Monitor
Websense Data Security Suite provides complete real-time monitoring of your information wherever it resides or method of transmission; even actions such as printing are included in the monitoring process. Websense Data Security Suite passively monitors most business communications—both external and internal—including a wide range of protocols such as email, network printing, FTP, HTTP and HTTPS and instant messaging (IM).

Administrators can identify what data is being used, where it is being transmitted and by whom from a centralised management and reporting console.

Discover
Websense Data Security Suite discovers information located throughout the network.

Armed with the knowledge of where data is, organisations can identify broken business processes, create efficient workflows and establish policies to protect confidential information.

Protect
Websense Data Security Suite can protect information while in use or in motion with pre-defined, automated policy-based enforcement controls. User and content-based policies can be defined to automatically block, encrypt, quarantine, notify and remediate potential security breaches.

How Websense Data Security Suite works
Websense Data Security Suite enables organisations to secure privileged and confidential data with a unique appreciation of information content, context and destination by:

- Discovering the location of sensitive data inside the network
- Monitoring the data as it travels around and beyond the organisation
- Protecting the data with policy-based controls that reflect business processes

The Websense difference - Deep Content Control™
Websense Data Security Suite goes beyond simple keyword and pattern matching solutions; it provides Deep Content Control™ to discover, monitor and protect confidential information.

Deep Content Control combines the ThreatSeeker™ and PreciseID™ technologies to enable organisations to discover where confidential information is on the network and secure "what goes where, to whom and how."

The PreciseID fingerprinting technology generates an "information fingerprint", a mathematical representation of a group of characters, words, sentences or data fields within a document, message or database and precisely identifies the designated sensitive data together with its extended metadata. Websense Data Security Suite fingerprints information from most databases and analyses hundreds of megabytes each minute. Its sophisticated algorithms can, for example, distinguish if a social security number belongs to a customer or an employee, allowing organisations to implement data protection policies that are relevant to specific business processes. Our fingerprinting technology also covers a broad range of unstructured data, including financial data, software source code, business plans and product designs.

Websense Data Security Suite can categorise content by type, risk and applicable regulation. These capabilities enable IT departments to enforce security policies, in line with business requirements.

Summary
Protecting customer and other confidential information from malicious and accidental leaks is a top business and IT security challenge facing organisations today. Websense Data Security Suite is a leading leak prevention solution that prevents data loss (both external and internal), improves business processes and manages compliance and risk management policies.

Cyber-Ark Inter-Business Vault®

The Challenge
Information leaks in all forms are occurring with increasing frequency today within some of the largest and most important organisations and enterprises. These breaches, whether inadvertent or as part of a coordinated attack, release highly sensitive information into the larger market where it could be used to damage the originating organisation's business, competitiveness and reputation and also significantly impacts the privacy and confidence of customers, partners and vendors.

One of the main challenges in securing sensitive information, whose leakage could have significant impact on the organisation, is to be able to prevent from powerful users such as IT Administrators to access the sensitive documents, making sure that data access would be allowed to data owners only.

In addition, organisations continue to grapple with requirements posed by SOX, PCI and the Basel II regulations which protect access to, and the modification of, highly sensitive documents and files. Considering the breadth and reach of these substantive government and industry regulations, the increasing frequency and granularity of compliance driven IT audits, and the wide media and public attention being paid to data breaches due to California Bill CA 1386, securing this highly sensitive information both while at rest and while in motion is top of mind with technology personnel today and an important imperative that organisations must deploy, monitor and enforce.

Cyber-Ark's Inter-Business Vault (IBV), addresses these business concerns and regulatory mandates by providing a centralised secure repository and sharing platform for an organisation's most highly sensitive information.

Based on a patented and ICSA validated Digital Vault™ technology, the IBV creates a multiple-layered information security infrastructure that is easy to use, simple to adopt and efficient to administer, all while providing the security, flexibility and detailed tracking capabilities missing from today's plethora of one-dimensional encryption only based solutions.

Whether it's securely storing, sharing and tracking the internal use of customer credit card information, protecting sensitive HR and legal information, or creating a secure workspace for the sharing of critical documents, vital financial information or confidential business planning documents between different business groups, the Inter-Business Vault is the information security platform of choice of top enterprise class organisations.

The Solution

For years, Inter-Business Vault (IBV) has delivered a solid array of benefits to organisations needing to secure their most highly sensitive information, including:

- **Segregation of duties - Data access to data owners only.** Cyber-Ark's Digital Vault Technology includes built-in segregation of duties for data access. As data is always encrypted at rest, IBV makes sure that only authorised users can access the data, prevents exposure of data to administrators and IT personnel, and maintains strict audit logs for all data access. This approach guarantees that the data owners are the only people who can actually access and see the data, and share it with their colleagues as they see fit.

- **Eliminating the need to manage encryption keys** - Sharing or exchanging sensitive information over the internet requires encryption keys management, often based on a PKI infrastructure or PGP. Managing encryption keys, certificates and revocation lists is a complex and costly task. Moreover, it makes it difficult to recover from a disaster, or to recover files when users who encrypted them have left the organisation. Cyber-Ark's unique and patented Digital Vault technology eliminates the need for key management for the encrypted data and assures smooth recovery that is independent of the key management system.

- **Compliance with Regulatory Mandates.** With ICSA validated security and complete, fine-grained logging and tracking of all document accesses, modifications and transfers, the IBV is proven to meet and exceed the demands of most challenging government and industry regulations.

- **Powerful and Proven End-to-End Secure Platform.** Designed with multiple layers of security built in, IBV provides an industry validated and customer proven secure infrastructure that protects highly sensitive information throughout the information pipeline, from creation through to distribution.

- **Increased Productivity and Easy Adoption.** With the easy to use robust client, or the powerful web-based interface, the IBV makes adoption of enterprise grade information security intuitive for the end-user, easy to expand and efficient to manage and administer.

- **Assured Business Continuity.** With the Digital Vault technology at its core and full High-Availability and Disaster Recovery modules, IBV provides the assurance that your most highly sensitive information will always be secure, safe and available in any circumstances.

- **Cost-Effective Secure Infrastructure.** Rather than install, manage and integrate a multitude of information security point solutions around your most highly sensitive information, the IBV provides a single, secure, robust and flexible infrastructure platform.

Additional Capabilities

- **Full Audit and Control of all Access.** Via our fine-grained authentication and access control capabilities, IBV ensures that only authorised users see and access the information that is specific to their requirements. If they do not have rights to a document, the Vault does not even allow the user to know that the document exists within the system. This allows you to ensure complete separation of duties between different roles and users that may require access to this information, while also protecting the data from access by a system administrator, IT staff or any unauthorised user.

- **Flexible Integration with Target Applications and Workflows.** With a web interface, a full range of API's and our proprietary Distribution and Collection Agent technology, the IBV solution is designed from the ground up for easy yet powerful integration with any target application or workflow within your organisation. Whether it's securing a financial transaction file needed by an existing workflow, or creating a centralised space that automatically tracks all accesses, modifications and transfers of a customer's credit card information between users and applications, IBV's interfaces and API's are designed for easy integration and deployment with your existing workflows and processes.

- **Enterprise Class and Enterprise Ready Architecture.** Built to meet the strictest security, audit and control requirements posed by government and industry regulations, Cyber-Ark's Vault is the product of choice for many Fortune 500 organisations in the financial, healthcare, insurance and manufacturing industries. Cyber-Ark's IBV is a robust and scalable solution that will fit your current needs, as well as your growth needs in volume of files, users and implementations. The IBV features built in support for all of the industry's leading authentication technologies, Radius compatibility, full LDAP and AD integration, robust, proven High Availability and Disaster Recovery capabilities, as well as support for leading backup, remote control and identity management solutions.

Websense® Data Security Suite and Cyber-Ark Inter-Business Vault® - The Power of Integration

The joint solution provides the following benefits for managing sensitive data throughout its lifecycle:

- **Sensitive Data Discovery** – Websense Data Security Suite can scan Desktops, Laptops, File Shares, SharePoint sites and more data sources and discover whether sensitive content which should be kept only in Cyber-Ark's IBV was also saved on unsecured locations. Websense DSS can also use remediation and remove the secure data from those locations leaving "random notes" instead.

- **Highly Secure Sensitive Data Repository** – Protecting identified content in Cyber-Ark's IBV, using a patented Digital Vault™ technology, which includes data encryption at rest, strict access controls, tamper-proof audit logs, segregation of duties to prevent system managers from accessing the information, strong authentication and other layers of security.

- **Data Leak Prevention for Data in Motion and Data in Use** - Websense Data Security Suite will monitor or block all communication (e.g. email, printers, etc) which contains documents or even partial content of sensitive content originated from IBV. Websense DSS can also control users actions on Laptops and Desktops preventing them from saving data originated at the IBV into USB devices or attaching/pasting this content to un-authorised applications.

- **Conduct secure communications with business partners, customers and other 3rd parties** – IBV provides a secure Managed File Transfer solution which enables businesses to exchange sensitive information such as financial transactions, medical information, PCI data and other sensitive content with 3rd parties. While Websense DSS ensures that forbidden content cannot leave the organisation, IBV provides a secure platform to allow sensitive content exchange with designated and authorised partners; Websense DSS can enforce that by ensuring that no other distribution mechanism is used. Together, they provide a complete solution to prevent data leakage, yet allowing secure business data exchange.

Who	What	Where	How
Human Resources	Source Code	Benefits Provider	File Transfer
Customer Service	Business Plans	Internet Auction	Web
Marketing	Employee Information	Business Partner	Instant Messaging
Finance	M&A Plans	Blog	Peer-to-Peer
Accounting	Patient Information	Customer	Email
Sales	Financial Statements	Spyware Site	Network Printing
Legal	Customer Records	North Korea	

Corporate Headquarters

Cyber-Ark Software, Inc..
57 Wells Avenue, Suite 20A,
Newton, MA 02459
tel 1-888-808-9005
fax (617) 965-1644
www.cyber-ark.com
Sales Info: sales@cyber-ark.com

Websense UK Ltd.
420 Thames Valley Park,
Reading, Berkshire,
RG6 1PU, UK
tel 0118 938 8600
fax 0118 938 86981
www.websense.co.uk

Cyber-Ark®
Managing Highly-Sensitive Information

websense®
ESSENTIAL INFORMATION PROTECTION™