Sensitive Information Management Solution

The Sensitive Information Management Solution is a secure platform for managing, sharing, and protecting critical information across the enterprise.

- Securely store, access and share confidential information
- Meet compliance and audit requirements
- Streamline management and control with a single enterprise platform
- Automate manual processes

CyberArk places your most important files into discrete safes that can be viewed via a tablet or a browser.

"CyberArk's Sensitive Information Management Solution is part of a holistic organizational change where efficiency and effectiveness are top priorities. Our operations team is now empowered to take on higher impact goals."

Louis Nel
CIO, MTN Group SA

The Challenge

In today's dynamic business environment that includes mobile, web and cloud-based interactions, users require convenient access to information wherever and whenever they need it. Therefore, the ability to share files internally and externally, as well as meet security and audit requirements, is a critical component of every business initiative. However, the sharing, distributing and accessing of information introduces significant risk of unauthorized access. Sensitive information in the hands of unintended users can be used to cause damage to the business, brand and reputation. As a result, IT and security teams are tasked with securing information while providing convenient, reliable access and reducing costs to ensure business efficiency.

Individuals sharing and accessing information

Employees, contractors and partners are spread across multiple locations and leverage convenience tools such as mobile and personal devices to maximize productivity. In order to work efficiently, employees are constantly sharing, distributing and accessing confidential information across geographic boundaries, using a wide range of devices and interacting with third parties such as customers, partners and contractors. Much of the information that is shared is sensitive business data, that can cause real damage if accessed by unauthorized users. As a result, it is the responsibility of IT to provide the tools users require to conveniently share and access information while also securing the information in transit and at rest. If IT does not provide the tools users need, users may opt for unauthorized tools, putting information outside of the control of IT.

Business processes collecting, distributing and accessing data

Streamlining business processes for efficiency requires automating systems to transport sensitive information. This can be a daunting task because it requires systems integration and process changes while still maintaining security standards. Therefore, organizations are often forced to make trade-offs between streamlined business processes and security, resulting in inefficient processes, unsatisfactory user experiences and new security risks.

Centralized management and control

The broad range of enterprise requirements for sharing information, including between users and in automated processes, often results in a patchwork of standalone solutions with varying levels of IT oversight. In today's environment of advanced and insider threats, all file sharing and access solutions must be managed and controlled by IT. As a result, the organizations must have a centralized solution that enables full visibility of all sensitive information sharing activity both from a security and business operations perspective.

The Solution

The CyberArk Sensitive Information Management Solution is a platform-based solution that addresses the needs of individuals storing, sharing and accessing information as well as business processes requiring sensitive information collection, distribution and access. Developed with a focus on security, the solution includes data encryption in transit and at rest, tamper proof auditing and granular access control, all built on a patented secure digital vault technology.

At the center, the CyberArk Digital Vault, a hardened server with multiple layers of security, creates an impenetrable electronic vault on the network. Within the vault, files are stored in discrete safes with segregation of duties between the content and operations to prevent file tampering or access by IT administrators maintaining the vault.

Organizations adopt the CyberArk Sensitive Information Management Solution to enable internal teams to store files securely in a central location, support the exchange information with external users, securely transfer files directly from e-mail clients, and share, distribute and collect files through automated processes. The wide range of use cases supported on a single platform maximizes the value of the investment while minimizing the IT resources required to manage the solution.

Benefits

Increase business collaboration, team productivity and project efficiency

CyberArk's Secure Data Room and Trusted Viewing are innovative technologies that deliver granular access controls, limiting the user's ability to read, write, share, download, forward or print documents. The technology tracks all activity, reducing the risk of unintentional changes and addressing the challenge of version control. As a result, users can confidently share information with internal and external users without putting information at risk.

Improve user convenience

An intuitive web interface, the Microsoft Outlook plug-in, and mobile application enable users to access confidential files from their native environment. Users are able to access confidential files anytime, anywhere, both online and offline, which improves user satisfaction and productivity. Adding to the convenience, business users can add third parties and control access to documents without involving IT.

Manage a single platform for multiple uses

Built in a unified platform, the solution supports web, mobile and e-mail interfaces for storing, sharing, distributing and collecting files securely. The solution can meet adjacent needs including server-to-server communication and encrypted e-mail seamlessly integrated into existing business applications. This single, robust and flexible infrastructure can expand as business needs change, delivering a lower total cost of ownership.

Meet compliance and audit requirements

Support for detailed audit capabilities with comprehensive audit trails and non-repudiation streamlines audit processes and reduces costs. Detailed logging includes all activity associated with information including version control and tamper-proof audit logs protect data from unauthorized personnel.

Features

Military-grade encryption in transit and at rest with transparent encryption key management minimizes IT resource requirements

Standard connectors enable seamless integration with every business application

APIs for easy deployment and integration with any target application or existing workflow

Integration with file scanning solutions to scan every file before it leaves the organization

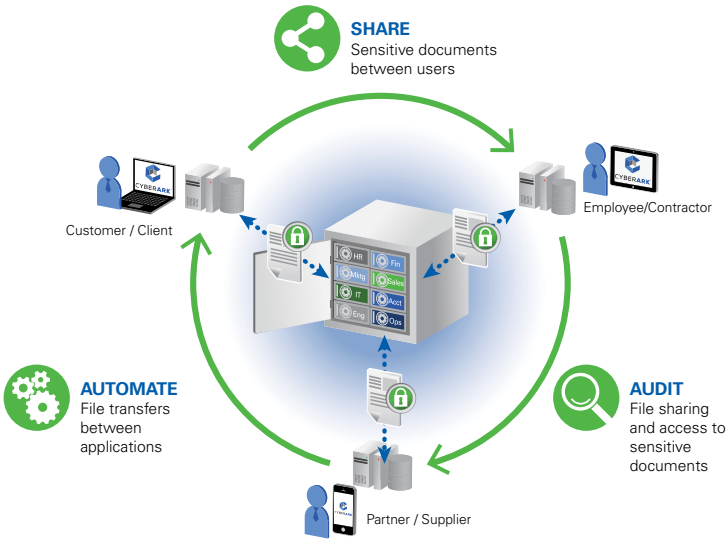
Flexible deployment on-premises or in the cloud

Business continuity including enterprise-level backup, high availability and disaster recovery

Scalability to support tens of thousands of file transactions and global accessibility

Strong authentication support including Radius, single-sign-on, LDAP and AD integration

Customized branding interfaces for customer facing solutions



Specifications

Security and Encryption Algorithms:

- A dedicated system for the Patented Digital Vaulting Technology™
- "Bastion" server-hardening
- Data-at-rest and communication encryption (AES-256, RSA-2048)
- HSM integration
- FIPS 140-2 validated cryptography
- Firewall protection
- Local disk level access protection
- File Integrity Checking
- Strong Password Policies, including Auto-Expiration
- Network Area for IP restrictions
- Allowed Interfaces – central control
- Built-in Automatic encryption key management

Access & Workflow Management:

- Trusted Viewing using patented Secure Data Room Technology
- Segregations of duties
- Safe Restrictions
- Automatic Version Control

Supported Platforms and interfaces:

- Windows desktops
- Browsers
- Outlook
- Tablets

APIs:

- Web Services/REST API
- .NET
- COM
- Command Line Interface

Protocols:

- SMB,HTTPS, FTP,SFTP, FTPS, SMTP

Authentication Methods:

- Username and Password
- RSA SecurID
- RADIUS
- PKI and smartcards
- LDAP and Windows-based Authentication

Logging, Monitoring and Reporting:

- SIEM integration
- Email notifications
- Encrypted and Temper-proof audit
- Extensive & Customizable Reporting

Redundancy:

- High Availability and Disaster Recovery Modules
- External Storage Support