BLACKBERRY

White Paper

Ensuring Document Security Across Any Device with the WatchDox Platform

Table of Content

"Almost all the enterprises in the world today are dealing with mobility in one form or another. There is a need for a very good integrated solution."

Introduction

The confidentiality and integrity of our customers' documents is of the utmost importance. The objective of this white paper is to describe how WatchDox assists organizations in ensuring that sensitive documents can be shared and accessed securely from any device.

WatchDox is a document-centric security platform that allows enterprise users to easily and effectively access, share and control all their important documents across the extended enterprise on any tablet, smartphone, or PC – even those outside the corporate firewall.

The WatchDox solution can be deployed in multiple ways, as a cloud-based solution, as a dedicated private cloud, or as an on-premise virtual appliance.

The WatchDox service is currently used by thousands of organizations worldwide in various industries including financial services, pharmaceutical and biotechnology, legal, energy, healthcare, manufacturing, insurance, real estate, technology and government agencies.

Our Philosophy

The need today for businesses to share documents internally and externally and to report information to regulators, investors, patients, partners, and customers is greater than ever. Businesses also need to enable new mobile devices - that are changing the way people work - without sacrificing security of the information being shared. Enterprises can no longer rely solely on the protection of a network perimeter technology - and controlling access to documents on bring-your-own-device (BYOD) or third-party devices is impossible with such solutions.

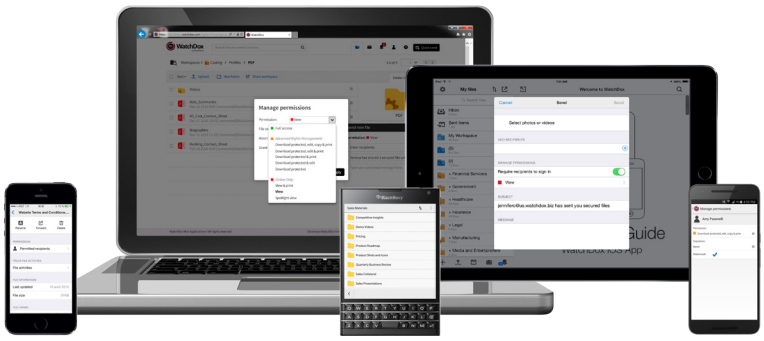
The WatchDox document-centric approach is the ideal way to secure organizations' most sensitive documents in today's mobile and collaborative world.

WatchDox embeds protection into the documents themselves so it can protect, control, and track them wherever they go, regardless of their physical or virtual location, or on what sort of device they are accessed.

At WatchDox we believe that putting in place extreme and complex security measures typically hinders productivity and does not allow sharing across organizational boundaries and devices. WatchDox is designed to carefully balance both user productivity and security requirements, first making sure the solution is truly intuitive and usable anywhere and on any device, while applying powerful security, control, and tracking measures.

Key Features

- **Control** – Allows restriction on who can view, print, edit, or forward documents.
- **Tracking** – Provides visibility into who views, downloads, forwards, edits, updates or prints your organization's documents, where and when, and maintains a full audit trail for compliance purposes.
- **Remote document wipe** – WatchDox administrators can wipe access to documents at any time – even after they have been downloaded.
- **File Sync** – Provides real time updates of all documents accessed through the various WatchDox end user interfaces.
- **Quick Send** – Securely share documents through Outlook or through a web based GUI.
- **Device optimized access** – Allows documents to be rendered in high fidelity and with platform-neutral controls thereby allowing access of documents on PCs, mobile devices (such as iPad, iPhone, Android, BlackBerry), or through a web browser.
- **Workspace** – A site can be created to allow for document collaboration.
- **Connectors** – Integrates via APIs with enterprise systems, such as Exchange, SharePoint, Windows File Shares and proprietary applications.



Document Control and Tracking

Document Control

Using the WatchDox solution, document owners or WatchDox system administrators can maintain control over their documents at all times – even after they have been sent and downloaded to a recipient's PC, smartphone, or tablet. Document control allows applying granular permissions to documents, enabling or restricting recipients from:

- Viewing a document
- Downloading a document
- Copying a document
- Printing a document
- Forwarding a document

Additionally, controls can:

- Set document expiration time
- Add individualized watermarks to a document
- Invoke advanced anti screen-capture measures (the patent-pending WatchDox "Spotlight" feature)
- Auto-update the document to enforce the most up-to-date content

Document permissions are entirely dynamic, and may be changed by the document owner or system administrator at any time. Most importantly, a document may be remotely destroyed after it has been sent or downloaded to a PC or mobile device. This allows the control of the document to adapt to changing business relationships or workflow needs. To enable the latter, WatchDox also provides an intuitive workflow for recipients to ask document owners for additional permissions and for document owners to approve or deny these requests.

Document Tracking

Document owners and WatchDox system administrators have access to the full log of activities associated with a document. WatchDox provides visibility into who, when, where and what actions occurred for each document – even if the document has been downloaded to a business partner's PC or a consultant's smartphone. The granular visibility enables enterprises to demonstrate compliance with regulations like PCI, HIPAA, and others that require tracking access to sensitive data types. This full audit trail can be accessed or downloaded by the administrator or collected by a log management solution or security information and event management (SIEM) product.

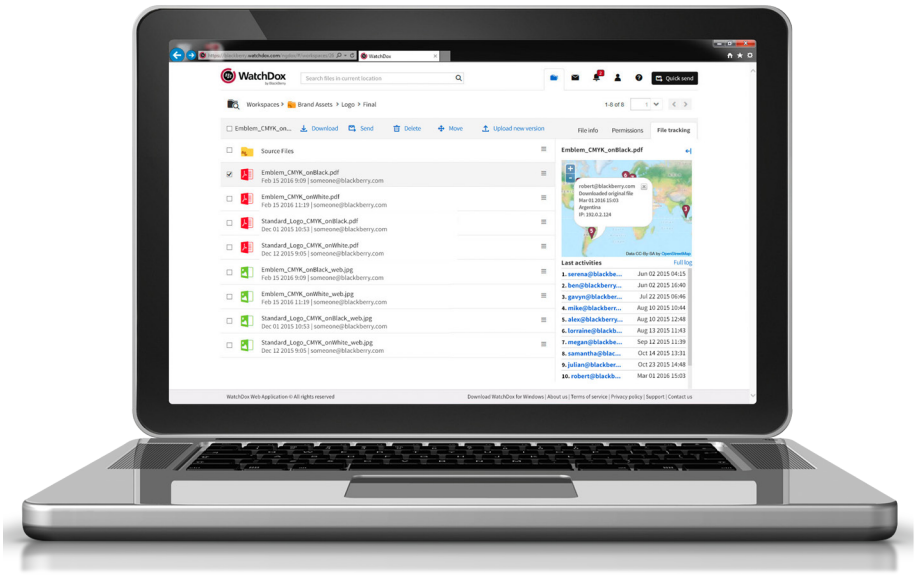


Figure: WatchDox workspace interface with tracking map

High Level System Workflow

Documents protected by WatchDox are secured at all times – at rest, in motion, and in-use. The WatchDox system works as follows:

1. Documents are uploaded to the WatchDox servers over an encrypted SSL connection. These documents may be uploaded via the WatchDox web interface, synchronized from a local folder, or potentially drawn from various enterprise systems, such as Outlook or SharePoint.

2. When a user requests to view a document, he or she is prompted to authenticate (if not already authenticated). Authentication may involve a username and password, email answer-back to verify the user's identity, or may be integrated with enterprise multi-factor or single-sign-on (SSO) systems (See 'User Authentication' section for additional information.) Once the WatchDox server has validated the authentication credentials, the user is authorized to view the document

3. The requested document is then converted into one of several different formats, so it is optimized for high fidelity rendering on the device that is requesting it: an online web browser, PC, iPhone/iPad, BlackBerry, etc. (See 'Device-optimized rendering' for more information.) These documents are then encrypted using industry standard 256-bit Advanced Encryption Standard (AES) encryption with WatchDox viewers and native apps and 128-bit AES as required by MS Office WDRM.

4. When an authorized user accesses a document via a web browser, the file is presented using WatchDox's secure online viewer.

An encrypted version of the original document can also be downloaded onto a mobile device, or to a PC. On a PC environment, documents may be viewed (or edited) natively within Microsoft Office or Adobe PDF.

5. A lightweight plug-in reinforces all permissions on the offline document. All communication is performed over encrypted HTTPS connections.

6. The WatchDox servers log the user identity, device, and IP address of each download of the document.

Device-Optimized Rendering

WatchDox has developed unique technology that allows the rendering of Microsoft Office®, Adobe PDF and most image file formats (GIF, JPEG, TIFF, PNG, EPS, PSD) with 100% fidelity on any device, while maintaining full protection and control. This addresses serious fidelity issues employees, partners and clients face every day when attempting to access documents from tablets and smartphones and often find them unintelligible. To achieve that, the WatchDox servers preprocess the documents uploaded to them, and employ various techniques to convert these documents into device-optimized versions. These versions are optimized for viewing inside a browser, on iOS, BlackBerry, and Android devices, and for viewing and editing them within Microsoft Office and Adobe PDF Reader or Acrobat.

User Authentication

User authentication is one of many ways to enforce security when using WatchDox. To address ever-growing regulation and to fit into any sort of authentication scheme, WatchDox is architected to flexibly support the variety of enterprise-level methods for authenticating users.

Integration Into Enterprise Authentication Schemes

WatchDox can integrate with whatever scheme is used by your organization: password-based, multi-factor authentication, or single-sign-on (SSO). These can be integrated with WatchDox using Active Directory, or the SAML or OAuth 2.0 protocol. As part of the system's security mechanisms, every authentication event is monitored and logged.

Out-of-the-box Authentication

Additionally, WatchDox offers out-of-the-box authentication schemes: username/password or one-time email authentication procedure that associates a user's email identity with the user's device (or multiple devices). The latter process is similar to accepted practices used by some of the top banking and credit card sites. These processes allow companies to easily and securely share documents with external parties without setting up cumbersome identity federation.

During the authentication process, the user may choose whether he or she is using a public machine (like an internet kiosk at an airport), in which case authentication would be limited to a single session. Alternatively, if the machine is designated to be private, authentication is persistent. Various measures that are part of the WatchDox unique IP are taken to ensure the security of the authentication email.

Document Security 'at-rest'

All documents stored on the WatchDox server (either in the cloud service or on-premise appliance) are kept in encrypted form using individual, strong, randomly generated 256-bit AES encryption keys. These keys are part of a key-chain hierarchy, which includes a top-level 256-bit AES master key. Decrypting a document requires access to all elements of the key-chain.

WatchDox also supports the use of an optional Hardware Security Module (HSM) to store the top-level master key and compute the document-specific keys.

All content, including meta-data, is encrypted and stored in a secure volume. This volume is accessible only via secure WatchDox API calls. Firewalls, monitoring, and other security tools are used to inspect the content residing on the server and to mask it from the outside.

Online Content Security

The WatchDox secure online viewer allows high fidelity online viewing of secure documents without requiring the recipient to install any software or plug-ins. The secure online viewer uses various methods for protecting the content of documents presented in it:

- The document is streamed over SSL
- Documents are encrypted using AES 256-bit and RSA-2048 encryption.
- The viewer's browser does not cache the document locally.
- Code is obfuscated using various techniques, making its protection logic very difficult to analyze
- Various protection measures are taken to prevent viewers from copying the document's text or images.
- Watermarks unique to the recipient can be added to the document.
- The administrator can customize a watermark's position, text, structure, and color.
- The operating system's print screen function is hampered (for more advanced protection users can always use the WatchDox Spotlight feature, which is demonstrated at www.blackberry.com/watchdoxspotlight).

- The document owner or administrator can deny print permissions, but the recipient can always request print permission. The browser's print function is always disabled (a print job will result in blank pages).
- The owner can set an expiration date or revoke the document at any time.
- The owner can track the viewer's actions (such as opening and printing the document). Log attributes include the time and date of the action, the user's IP address and geographical location (based on IP geo-location technology), and the viewing machine's ID.
- The document owner can modify all user rights easily at all times.

Downloadable Content Security

Document owners or WatchDox system administrators can choose to allow documents to be downloaded for secure offline viewing and editing on mobile devices or within Microsoft Word, Excel, and PowerPoint or within Adobe PDF Reader/Acrobat[1]. on Windows desktop and OSX computers. Using the plug-in capability, recipients of WatchDox documents can:

- Access their documents offline as well as online
- View the document using the document's native application (for example a .docx file will open within Microsoft Word, as it normally does)
- Edit the documents natively within Microsoft Office (if permitted by the owner)

All the above is accomplished while preserving the WatchDox controls set by the document's owner and maintaining persistent tracking capabilities. Documents are downloaded in encrypted format and can only be opened if the user has been granted the correct permissions. Permissions are enforced on Microsoft Office files leveraging the embedded WDRM capabilitites. The WatchDox plugin for Adobe .pdf viewers uses proprietary technology to enforce DRM permissions.

Tracking and Control

Even though WatchDox allows the recipient to take the document offline, the WatchDox advanced tracking and control capabilities are maintained in the following manner:

- Operations performed on a WatchDox protected document (such as viewing, printing, or editing the document) are sent to the WatchDox server and the document owner gets a full audit trail of these activities. If the recipient is offline while performing these operations, the plug-in enforces a caching policy and notifies the server of all operations once the computer goes online again.
- Before each operation is performed, the plug-in checks with the WatchDox server and verifies if the operation is permitted according to the latest policy.

If the recipient is trying to access the document when offline, a policy cache is valid for a limited period of time (72 hours by default, but configurable by the administrator). The expiration timer is reset each time a synchronization event occurs. Once this period of time has expired, the recipient must go online in order to open the document. This process verifies that the recipient's access policies are still up to date (e.g., that the owner has not revoked this user's access or changed the user's permissions)

Plug-in Security

Multiple measures have been added to the plug-in that ensure its integrity. A partial list of these measures includes:

- The plug-in code is digitally signed and verification is performed before the plug-in loads.
- Document encryption and decryption, as well as key management are done in a secure, external process.
- All communication, both outbound (to the WatchDox server) and inbound (between the plug-in and the external process) is encrypted over SSL.

Note: Download and sync of files to mobile devices is decribed in the Mobile Document Security Section on page 10.

[1]Office 2003, 2007 and 2010, 2013 supported (32-bits), Adobe PDF Reader and Acrobat 8.0+

- Encryption keys are securely stored encrypted on the computer and cannot be accessed by any party, including the user working on the computer.
- When disconnected from the Internet, if the plug-in is unable to "call home" to check on permissions, a configurable "grace period" is given to allow users to access documents on the go.

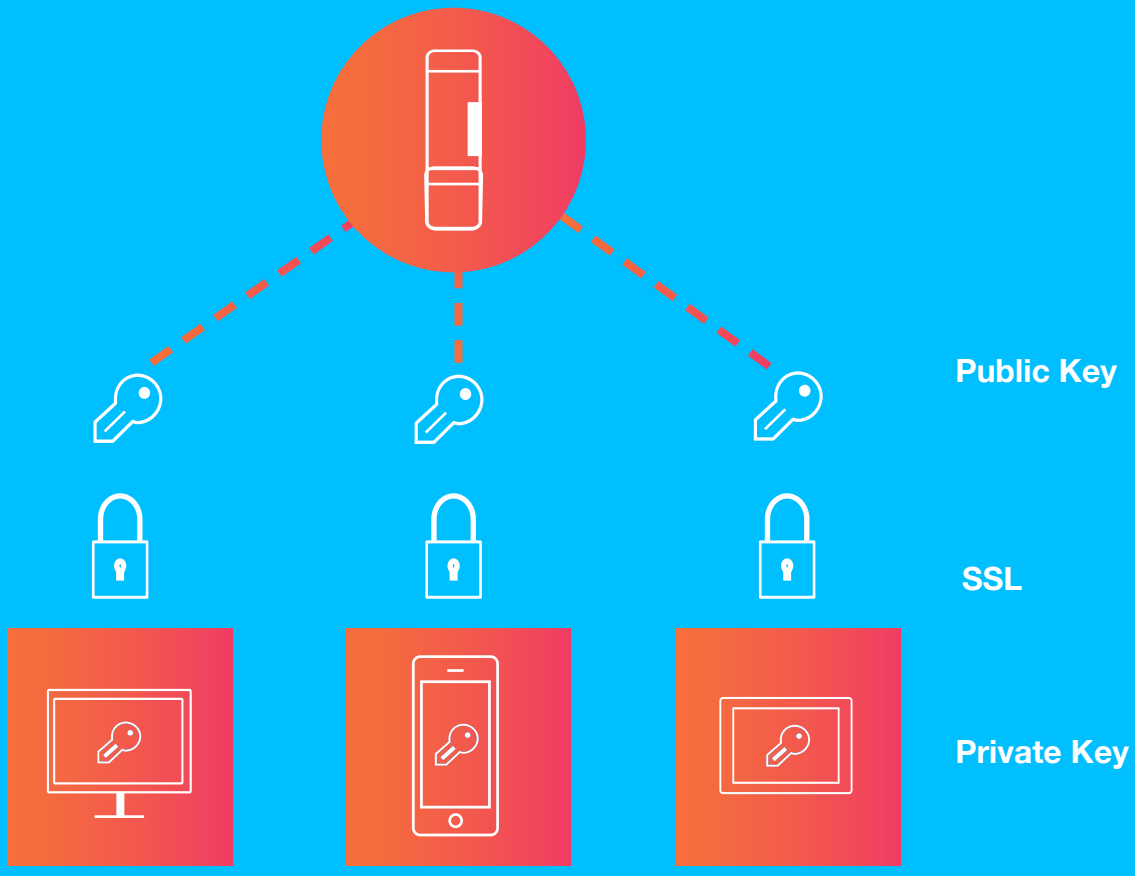
Encryption and Key Management

Each document stored on the WatchDox server is encrypted using its own encryption key and industry-standard 256-bit AES cipher. The document keys are stored in a secure keystore. To further augment the security model of the key management, the keystore can also make use of a hardware security module (HSM).

Once a device is authenticated, it is associated with a user/email address. A unique 2048-bit private-public keypair is generated for this user and communicated to the device over SSL. (Note that when used with Microsoft WDRM, WatchDox uses 1024-bit encryption in accordance with the WDRM standard.)

The asymmetric keys are then used to securely transfer individual documents' encryption keys from the server to the plug-in that can then decrypt documents and display them on the device. The retrieved keys are securely stored on the device and cannot be accessed by any party, including the user working on the computer.

Diagram 2: WatchDox Key Management



Mobile Document Security

The WatchDox Mobile App

The WatchDox app for iOS, Android and BlackBerry 10 devices goes to great length to keep your organization's documents secure. Unlike mobile device management and control solutions, the WatchDox security is document-centric, and can therefore work seamlessly on employees' personal devices or on partners', customers', or third-party devices.

The WatchDox app provides many security features, including:

- 256-bit AES encryption at rest (for documents synchronized to the device or cached)
- Optional user passcode required for access to the WatchDox documents (centrally provisioned)
- Document watermarks
- Document expiration
- Disabling of iTunes and iCloud sync and backup
- Secure key storage
- Document tracking and remote document kill
- Jailbreak detection
- Anti-clock tampering measures

Please refer to the "Downloadable Content Security" section for more information about key management. More detailed information about iOS security features is provided in the "WatchDox iOS Security White Paper" which is available upon request.

Appendix: WatchDox Cloud Security

The following sections are relevant for customers using the WatchDox Cloud (or SaaS) solution, hosted on the Amazon Web Services (AWS) EC2 cloud. The Cloud service can be deployed as a shared cloud or as a private cloud. The same server software is offered for the WatchDox on-premise solution for maximum flexibility and ease of migration between the deployment options.

Cloud Compliance

WatchDox has completed a SOC 2 certification of its internal processes. Additional documentation available under NDA.

WatchDox is able to support the HIPAA and HITECH regulations, as well as sign HIPAA Business Associate Agreements (BAAs) with customers.

WatchDox by BlackBerry encrypts files while they're in use, at rest or in transit using FIPS 140-2 validated cryptographic library and 256-bit AES encryption."

WatchDox has obtained a Safe Harbor certification, controlling and restricting the transfer of data between US data centers and European data centers.

Security Processes and Controls

Secure Design Principles

Multi-tier Architecture

The WatchDox system is a multi-tier application with strict separation between the web application serving the users, the database holding the system meta-data, and a secure file system holding the encrypted documents.

Input Validation

The web application architecture stops web-based attacks (such as spoofing or reengineering of the URL and code injection), always redirecting the malicious user to the main application page.

Compartmentalized architecture

Using a compartmentalized software architecture, WatchDox web applications are protected against outside intrusion.

Physical and Environmental Secuirty

WatchDox utilizes the Amazon Web Services (AWS) cloud for its public cloud infrastructure. Please see 'Hosting and physical security' section below for additional details.

Network and Remote Access Security

Secure network architecture

Firewalls monitor and control communications at the external boundary of the network and at key internal boundaries within the network.

Role Based Access

WatchDox web applications employ a Role Based Access Control security methodology. The security layer of the software restricts the user according to security permissions, with no ability to move across unauthorized boundaries.

Two-Factor Authentication

Administrative access to production systems requires strong two-factor authentication.

Data Privacy

Data Encryption

WatchDox uses the FIPS 140-2 compliant 256-bit AES encryption, which is a modern and very strong cryptography system used by businesses and governments to protect sensitive information.

All key data fields that contain data from user input, registration, content, and policies are encrypted at-rest. The storing of the documents and meta-data in encrypted form ensures that even if intruders obtain the actual physical disks on which they reside, they will not be able to read or modify them.

Communication Security

All user data transmissions over the Internet to and from the WatchDox servers are sent using HTTPS (Secure HTTP connections), and are encrypted via SSL/TLS (Secure Sockets Layer/Transport Layer Security) employing strong keys (128-256 bit, depending on the browser capabilities).

Secure Storage

Once documents are uploaded to the WatchDox servers, they are immediately encrypted and stored on a secure volume, accessible only to the WatchDox application server. Direct access to this volume from outside is impossible, as this volume is not accessible to the Internet in any way other than through the mediation of the WatchDox application servers. The application servers moderate the access of users to content based on their assigned permissions within the policy set by the content authors.

Secure Key Management

Each document is stored encrypted using its own unique cryptographic key. Thus, gaining access to one key does not invalidate the security of the rest of the documents in the system.

Secure API Access

The application server does not expose any files (documents, executables, or configuration). The only way to access files on the system is by providing the server with a valid security token tied to both the verified user and to the user's physical machine, and transmitted in encrypted form (using HTTPS) to prevent interception.

Data De-identification

Encrypted documents are stored in a manner that prevents association between the document itself and meta-data information such as the document's owner, its recipients, or its original file name.

Incident Response

24/7 Monitoring

The hardware and software performance in the data center is monitored 24/7 using software monitoring and alerting technology with messaging to pagers and mobile phones of our operations personnel in the event of software or hardware problems.

Incident Response

BlackBerry Product Security begins with our front-line responders. BlackBerry's Security Incident Response Team (BBSIRT) is the industry's gold standard in security incident response, ensuring that public and private reports of vulnerabilities are rapidly received, triaged, analyzed, and mitigated in order to protect your organization. An essential part of the daily work of BBSIRT includes collaborating with customers, partners, vendors, governments, academics, and the security research community, with a triage team monitoring the threat landscape 365 days a year from several top private and industry sources. This ongoing

resource engagement helps BlackBerry deliver a unique level of security that customers depend on, by building collaborative relationships across the industry, responding rapidly to emerging incidents, and providing the guidance and tools customers need to protect their systems and devices.

Business Continuity Management

Policies and Procedures

WatchDox has put in place policies defining the mission-critical personnel, procedures, and notifications schedules. Periodic exercises are carried out to test backup and DR readiness.

Fault Tolerant Design

The WatchDox system is designed to utilize multiple, geographically distinct, isolated regions, or availability zones. In the event that an entire geographical region is down, WatchDox can transition to a secondary region.

Backup and Disaster Recovery Procedures

Hourly snapshots of user data are performed, as well as periodic full system backup. WatchDox regularly tests such procedures. Data is stored on highly redundant AWS storage, whereby each file resides on at least three geographically distinct data centers at any given point in time.

Uptime, Backup and DR Objectives

- **Uptime** – The WatchDox service utilizes Amazon's highly redundant and scalable cloud infrastructure, with an uptime goal of 99.9%.
- **Recovery Point Objective (RPO)** – Backup state frequency up to 1 hour of user data.
- **Recovery Time Objective (RTO)** – Recovery time objective is 3 hours after a critical system malfunction is detected. Up to 1 hour assigned for attempting to fix existing conditions without resorting to full disaster recovery procedure. 2 additional hours for full disaster recovery.
- **Backup Retention** – Backup default data retention period is 14 days.

Risk Management

The Security Research Group (SRG) within BlackBerry Product Security provides groundbreaking insights into both the hardware and software security we're developing and the malware and hacking tools constantly coming to light in the field. A global team of ethical hackers are mandated to ensure and extend the security of BlackBerry products and remove security specific barriers to success related to product security. SRG identifies security issues in the BlackBerry product portfolio and works closely with development teams to get issues resolved. They also actively conduct research into advanced security threats to BlackBerry products and recommend defensive technologies.

WatchDox Access

WatchDox maintains administrative and technical controls to ensure customer data is always protected from unauthorized access by third parties as well as from WatchDox personnel, and that it can meet strict regulatory compliance. These include:

Privacy Procedures

WatchDox employees are trained to keep information on a need-to-know basis, sign applicable privacy and non-disclosure agreements, and apply standard industry practices for safeguarding any customer and proprietary information. Under no circumstances are WatchDox employees allowed to access user data.

Data Encryption

As described above, all customer data is encrypted and not accessible by WatchDox personnel.

Employee Screening

All WatchDox employees with access to production systems undergo criminal and background checks (as permitted by applicable law) commensurate with employee's position and level of access. Only a small number of pre-screened WatchDox employees are allowed to access the production systems, for the purpose of maintaining it and providing customer support. These employees have no access to user data and have clear procedures for handling any confidential information.

Segregation of Duties

WatchDox maintains segregation of duties between system level administrators and operational support teams. Production systems are isolated from development and testing systems.

Account Review and Audit

User access is assigned according to an approved process, with review and re-certification performed every 90 days.

Credentials Policy

Passwords must meet minimum length and complexity criteria. Users are required to regularly change their passwords.

Hosting and Physical Security

WatchDox utilizes Amazon Web Services (AWS) as its hosting facility provider. Amazon Web Services (AWS) delivers a highly scalable cloud computing platform with high availability and dependability, and the flexibility to enable customers to build a wide range of applications. In order to provide end-to-end security and end-to-end privacy, AWS builds services in accordance with security best practices, provides appropriate security features in those services, and documents how to use those features. WatchDox has used those features and best practices to architect an appropriately secure application environment. Enabling WatchDox to ensure the confidentiality, integrity, and availability of its customers' data is of the utmost importance to AWS, as is maintaining trust and confidence. At a high level, Amazon has taken the following approach to secure the AWS infrastructure:

- **Certifications and Accreditations** – AWS has successfully completed SSAE-16 and SOC 2 type II audits, and will continue to obtain the appropriate security certifications and accreditations to demonstrate the security of our infrastructure and services. Additional information on the audits is available under NDA.
- **Physical Security** - Amazon has many years of experience in designing, constructing, and operating large-scale data centers. AWS infrastructureis is housed in Amazon-controlled data centers throughout the world. Only those within Amazon who have a legitimate business need to have such information know the actual location of these data centers, and the data centers themselves are secured with a variety of physical barriers to prevent unauthorized access.
- **Secure Services** - Each of the services within the AWS cloud is architected to be secure and contains a number of capabilities that restrict unauthorized access or usage without sacrificing the flexibility that customers demand. For more information about the security capabilities of each service in the AWS cloud, consult the Amazon Web Services: Overview of Security Processes whitepaper..
- **Data Privacy** - AWS enables WatchDox to encrypt its customers' data within the AWS cloud and publishes backup and redundancy procedures for services so that users can gain greater understanding of how their data flows throughout AWS. For more information on the data privacy and backup procedures for each service in the AWS cloud, consult the Amazon Web Services: Overview of Security Processes whitepaper.

Aditional Information About AWS Security

The AWS Security Center provides links to technical information, tools, and prescriptive guidance designed to help companies build and manage secure applications in the AWS cloud. As a WatchDox user, you are welcome to review these resources.

About WatchDox

WatchDox by BlackBerry makes files secure and users productive. Our products enable enterprises to secure their files wherever they are against widespread threats, and to facilitate collaboration while protecting files wherever they go. Available as SaaS, a virtual appliance or a hybrid, WatchDox provides a single pane of glass to work with personal and enterprise content, uniquely combining consumer-style app interfaces with security to suit any enterprise use case. Over 150 of the Fortune 1000, including the largest civilian federal agencies, 6 of the top 12 private equity firms and most of the 6 major Hollywood studios, depend on WatchDox. For more information, visit www.blackberry.com/watchdox.