bigtincan™

Security and Governance for Content Distributed on Mobile Devices

Introduction

These days, business productivity depends largely on the ability to securely access and interact with a wide range of information over mobile devices, such as tablets and smartphones. From sales executives to field technicians, the demand for accessing corporate content securely on mobile devices is growing exponentially.

In the past, implementing security measures to protect corporate content has involved VPNs, intranets, firewalls and passwords. However, the increasing uptake of mobile devices in corporate settings means security measures must be implemented over a plethora of networks and devices.

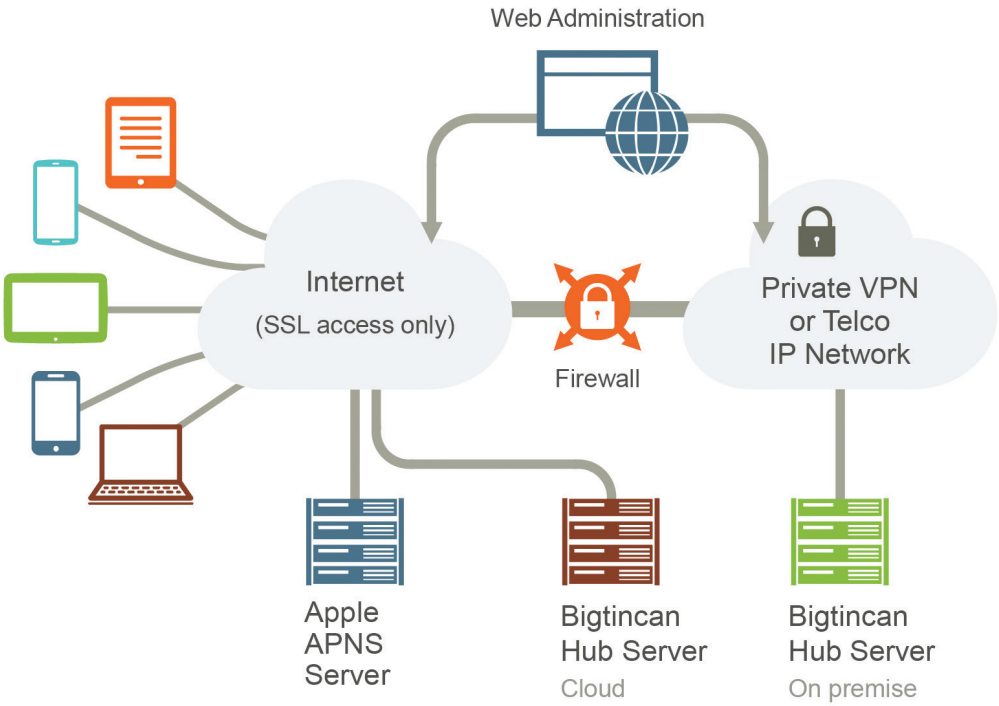
bigtincan has created a powerful solution with bigtincan hub™. An application for mobile devices, it allows for the distribution, management and governance of a range of content, including documents and rich media content, with enterprise-grade security.

bigtincan hub Architecture

The bigtincan hub system uses a flexible content store. Content is added dynamically to a server, referenced from a database and then pushed to mobile devices using a set of secure programming interfaces (APIs).

bigtincan hub clients (web, mobile and desktop) leverage our secure interfaces to query, retrieve and audit the content that has been specifically assigned to the device/user combination. bigtincan hub securely encrypts content at rest as well as in transit with Advanced Encryption Standard (AES) and FIPS+ encryption capabilities.

Figure 1 – How it Works



bigtincan™

Key Security Advantages of bigtincan hub

- Secure protocol use: The system is based on Secure Sockets Layer (SSL) communications, encrypting the link that end-user devices use to get access to the server.
- File obfuscation: Files are not stored using their original file names. All files uploaded to the server are obfuscated.
- Internal content store: The content store server can be hosted in a secure bigtincan cloud facility or internally, behind the corporate firewall and other secure private network access restrictions. With the creation of an internal content store, the enterprise can control access to data for its employees and approved external parties. All content stored on the server is encrypted and access is controlled through user authentication.

> "85% of employees use phone/tablet applications and web-based services for both purposes which is putting corporate information security under serious threat."
>
> **Forrester's Forrsights Workforce Employee Survey, Q4 2012**

- Ability to remote wipe: The bigtincan hub server can initiate a remote wipe of content from devices automatically over the air. This allows the organization to immediately remove content, including both read and unread, from the device in real time. This system works even if the user has the bigtincan hub application open and is engaged in the content to be deleted. This process also allows for live-editing content, with new content replacing existing content on the device.
- Selected content cache of file attachments: bigtincan hub offers the option of providing device-side content cache for file attachments. Organizations that choose to disable content cache will force a reload of file content each time the user accesses it, ensuring that no secure content is on a lost or stolen device.
- Two-factor authentication: bigtincan uses a unique device identifier to identify the specific device that a user is using to access the content store. It is possible to whitelist devices that are usable on the system and tie them to a user account to select which content is delivered to each device. This gives the ability for the end system to deliver specific content to a unique device.
- Jailbreak detection: bigtincan hub incorporates technology to work with Apple iOS-delivered encryption to detect 'jailbroken' iOS devices, and 'rooted' devices on Android. This secure structure controls highly sensitive content and ensures that the organization does not expose secure content to devices that have been compromised.
- Network access control: The system allows network access to be controlled to a specific set of IP addresses, ensuring that only approved users are able to access the server and engage with content.
- Content expiry: Content can be automatically removed from a device by setting an expiry date for specified content. The content will be removed automatically from all the devices with no user intervention.

bigtincan™

- Location-based content controls: Content can be tied to a location determined either by a GPS co-ordinate (Lat/Long) and radius, or by micro-location systems like iBeacons, allowing users to only get access to the content when they are in a particular area.
- Device whitelisting: bigtincan hub can allow the administrator to white list a set of devices and map those devices to a particular user, thus enabling them to control which users can access the content from which devices. This ensures that access rights are preserved.

Cloud or On-Premise

bigtincan hub is deployed as either a cloud-based solution or as an on-premise solution for organizations

Documents are stored securely and managed by bigtincan hub in the cloud. bigtincan hub employs a controlled architecture with firewall access and other industry standard security measures or counter-measures.

On-Premise

When deployed as an on-premise server, such as in a demilitarized zone (DMZ), behind a firewall or with access through a private APN, security levels can be controlled by the user organization. This includes restricting access to the server for publishing and retrieving content.

Device-Side Security Benefits

Using bigtincan hub with secure mobile devices enables increased security:

- Apple® iOS devices: bigtincan hub creates secure file access for each application on the device. Based on Apple documentation, without explicit user instruction is it not possible to obtain access to content in one application from another application. Secure content sent to bigtincan hub cannot be viewed by other apps without user instruction, although this ability can be removed.
- bigtincan hub includes the ability to specify an 'encrypted channel' for iOS devices where the application uses the hardware accelerated encryption chip on iOS to encrypt content inside the bigtincan hub secure container, without the need for any external 'wrapping' or other device hardware control systems.
- Android devices: Devices that provide hardware encryption (i.e., most Samsung devices) can be remotely controlled to ensure encryption is enabled before content is loaded to the device.
- Mobile platform enterprise distribution tools: These are a range of tools that include the ability to perform remote wipe of a device, restrict the device's access to certain apps, and other advanced enterprise management tools. These tools are part of a standard enterprise deployment of mobile devices and add to the security of sensitive documents.
- Content level controls: bigtincan hub supports content level controls based on user roles to govern how users can access, edit, and share content inside bigtincan hub. These controls are set on the server and can be remotely reset, allowing the administrator to control how users access content on a globally distributed set of mobile devices.

Contextual Security

Location-based content controls prevent users from accessing or taking content to places that they shouldn't. Based on device ID, access to content by devices that are not controlled by the organization can be restricted. Content restriction can also be based on network connectivity by requiring a password to authenticate which requires a mobile user to be on-line.

Server Side Security

bigtincan hub has integrated security on the server side for both cloud-hosted and on-premise private server implementations. All content on the server is encrypted, and access is restricted and controlled using managed user/password access. This includes automatic restriction of IP addresses based on failed logins.

> "By 2016, 20% of enterprise BYOD programs will fail due to enterprise deployment of mobile device management features that are too restrictive."
>
> **Gartner – Bring Your Own Device: Mobile Trends & Securing The Transition, February 2014**

Installing an on-premise private server behind a corporate firewall offers enterprise customers complete control of their content. The addition of a private APN (delivered by a carrier) allows the transmission of content that never touches the public Internet.

Private Content

For users that require additional security measures on particular groups of files, bigtincan hub allows individual content to be set to 'private.' When the content and files are added, the recipient device sees only a lock icon. To unlock the content, the user must enter a separate password known only by the user of the app.

bigtincan hub removes private content after the user moves away from the story. When the user moves back and unlocks private content again, it's downloaded again, ensuring that the content is delivered securely, and then wiped after use.

Control of Data Loss Prevention

With the increasing use of mobile devices to review, annotate and comment on secure documents, it is increasingly important to be able to control how they are used and to be able to control file sharing. bigtincan hub includes the ability to turn sharing on or off on a piece of content level basis. With sharing turned off, all content inside that content bundle is delivered to the device in the same way, but the ability to share the documents is turned off.

bigtincan™

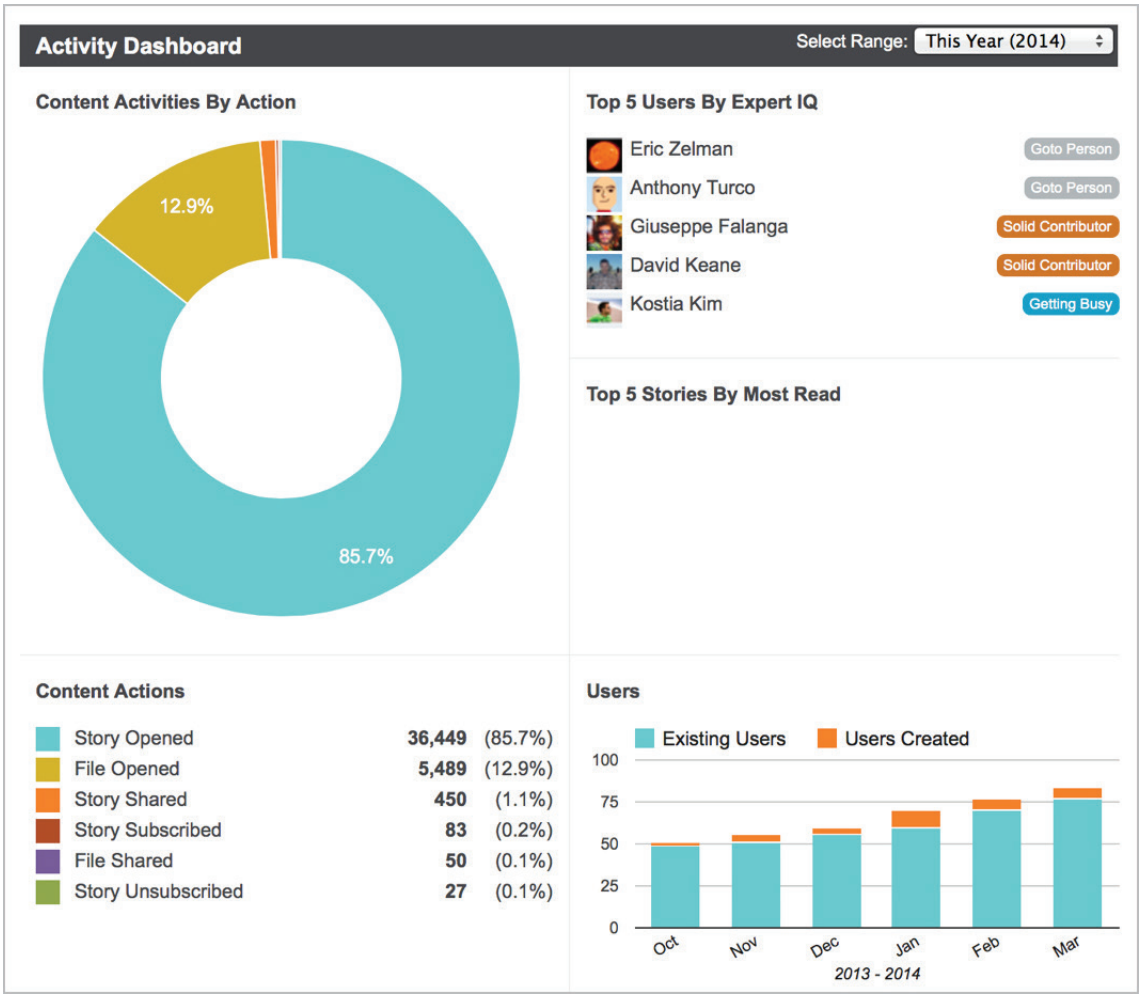
This extends the ability to use the 'Open In,' print or email functions that are common in iOS apps, and application 'intents' in Android. This control ensures that no content inside bigtincan hub is backed up to iTunes® either through a physical connection or an WiFi connection.

Documents delivered through bigtincan hub can be controlled and managed in a way that allows the IT department to ensure that they are maintained there.

Content Usage Auditing and Reporting

bigtincan hub provides a powerful real-time usage auditing & reporting system. bigtincan Content IQ allows an account administrator to view how end users have used content on their devices. This extends to identifying each time a user opens a story or a document, how long it was opened, and with whom the content was shared.

This information can be viewed in the Admin Web UI or is exportable as a csv file for analysis in other reporting tools.



Custom Configurations for Authentication

The bigtincan hub system allows for custom security configurations that extend to linking authentication to Active Directory or LDAP through to integrated VPN and other security access classifications. Users that implement single sign-on technology like SAML can use their standard SAML based service to authenticate users.

bigtincan Delivers On the Security Enterprise Customers Need

bigtincan hub delivers on the security enterprise customers need with the document encryption, secure internal server options and private story capabilities required to allow the most secure content to be published to mobile devices. Security and content control are key to the bigtincan hub platform and are part of our plan to enable mobile content on the widest range of mobile devices.

bigtincan™