WHITE PAPER

Secure mobile computing and business intelligence on Apple and Android mobile devices.

Overview of the security features and capabilities in MicroStrategy Mobile.

MicroStrategy®

Copyright Information

Trademark Information

MicroStrategy, MicroStrategy 6, MicroStrategy 7, MicroStrategy 7i, MicroStrategy 7i Evaluation Edition, MicroStrategy 7i Olap Services, MicroStrategy 8, MicroStrategy 9, MicroStrategy Distribution Services, MicroStrategy MultiSource Option, MicroStrategy Command Manager, MicroStrategy Enterprise Manager, MicroStrategy Object Manager, MicroStrategy Reporting Suite, MicroStrategy Power User, MicroStrategy Analyst, MicroStrategy Consumer, MicroStrategy Email Delivery, MicroStrategy BI Author, MicroStrategy BI Modeler, MicroStrategy Evaluation Edition, MicroStrategy Administrator, MicroStrategy Agent, MicroStrategy Architect, MicroStrategy BI Developer Kit, MicroStrategy Broadcast Server, MicroStrategy Broadcaster, MicroStrategy Broadcaster Server, MicroStrategy Business Intelligence Platform, MicroStrategy Consulting, MicroStrategy CRM Applications, MicroStrategy Customer Analyzer, MicroStrategy Desktop, MicroStrategy Desktop Analyst, MicroStrategy Desktop Designer, MicroStrategy eCRM 7, MicroStrategy Education, MicroStrategy eTrainer, MicroStrategy Executive, MicroStrategy Infocenter, MicroStrategy Intelligence Server, MicroStrategy Intelligence Server Universal Edition, MicroStrategy MDX Adapter, MicroStrategy Narrowcast Server, MicroStrategy Objects, MicroStrategy OLAP Provider, MicroStrategy SDK, MicroStrategy Support, MicroStrategy Telecaster, MicroStrategy Transactor, MicroStrategy Web, MicroStrategy Web Business Analyzer, MicroStrategy World, Application Development and Sophisticated Analysis, Best In Business Intelligence, Centralized Application Management, Information Like Water, Intelligence Through Every Phone, Intelligence To Every Decision Maker, Intelligent E-Business, Personalized Intelligence Portal, Query Tone, Rapid Application Development, MicroStrategy Intelligent Cubes, The Foundation For Intelligent E-Business, The Integrated Business Intelligence Platform Built For The Enterprise, The Platform For Intelligent E-Business, The Scalable Business Intelligence Platform Built For The Internet, Office Intelligence, MicroStrategy Office, MicroStrategy Report Services, MicroStrategy Web MMT, MicroStrategy Web Services, Pixel Perfect, Pixel-Perfect, MicroStrategy Mobile, MicroStrategy Integrity Manager and MicroStrategy Data Mining Services are all registered trademarks or trademarks of MicroStrategy Incorporated.

All other company and product names may be trademarks of the respective companies with which they are associated. Specifications subject to change without notice. MicroStrategy is not responsible for errors or omissions. MicroStrategy makes no warranties or commitments concerning the availability of future products or versions that may be planned or under development.

Patent Information

This product is patented. One or more of the following patents may apply to the product sold herein: U.S. Patent Nos. 6,154,766, 6,173,310, 6,260,050, 6,263,051, 6,269,393, 6,279,033, 6,567,796, 6,587,547, 6,606,596, 6,658,093, 6,658,432, 6,662,195, 6,671,715, 6,691,100, 6,694,316, 6,697,808, 6,704,723, 6,741,980, 6,765,997, 6,768,788, 6,772,137, 6,788,768, 6,798,867, 6,801,910, 6,820,073, 6,829,334, 6,836,537, 6,850,603, 6,859,798, 6,873,693, 6,885,734, 6,940,953, 6,964,012, 6,977,992, 6,996,568, 6,996,569, 7,003,512, 7,010,518, 7,016,480, 7,020,251, 7,039,165, 7,082,422, 7,113,993, 7,127,403, 7,174,349, 7,181,417, 7,194,457, 7,197,461, 7,228,303, 7,260,577, 7,266,181, 7,272,212, 7,302,639, 7,324,942, 7,330,847, 7,340,040, 7,356,758, 7,356,840, 7,415,438, 7,428,302, 7,430,562, 7,440,898, 7,486,780, 7,509,671, 7,516,181, 7,559,048, 7,574,376, 7,617,201, 7,725,811, 7,801,967, 7,836,178, 7,861,161, 7,861,253, 7,881,443, 7,925,616, 7,945,584, 7,970,782, 8,005,870, 8,051,168, 8,051,369, 8,094,788, 8,130,918 and 8,296,287. Other patent applications are pending.

TABLE OF CONTENTS

Overview 1

Mobile device security 1

Apple iOS device security 1

iOS configuration 2

Android OS device security 2

Data protection and encryption 2

Apple data protection and encryption 2

Touch ID™ integration 2

MicroStrategy Mobile secured with Usher 3

Android data protection and encryption 3

MicroStrategy mobile app security 3

Data transmission 3

Authentication 4

Secure application authentication 4

Confidential project mode 4

HTTPS with mutual authentication 4

Authorization 6

Analytics platform security 7

Secure communications across firewalls 7

No database connection from the MicroStrategy mobile server 7

Single port control for data access 7

No external Remote Procedure Calls (RPC) or Remote Method Invocation (RMI) calls 7

Transmission security 7

Protection of stored user credentials 8

Intensive testing 8

Third-party enhancements 8

Single sign-on (SSO) form-based authentication 8

Enterprise Mobility Management 8

MicroStrategy Mobile secured by Good 9

MicroStrategy Mobile secured by MobileIron 9

MicroStrategy Mobile secured by Airwatch 9

MicroStrategy Mobile secured by AppConfig 11

Corporate policies for operational security 11

Operational security 11

Conclusion: MicroStrategy, a secure mobile computing and mobile BI solution 11

With ever-advancing mobile technology, mobile device security has become a vital topic that every major corporation must consider and understand. Gone are the days of performing a keyword search in a browser for business information. Today, corporations leverage mobile apps to distribute relevant, critical data to their workforce, partners, and customers. Due to the nature of mobile devices, apps present new security challenges that hardware and software must address.

This paper will give an overview of mobile security risks, explain the capabilities of the MicroStrategy Mobile App on Apple and Android mobile devices, and explain security partnerships and third-party features leveraged by MicroStrategy Mobile. The combination of exceptional security features by MicroStrategy including MicroStrategy-designed app-level protection code for Android, Touch ID™ integration for iOS, secured access with Usher by MicroStrategy, several layers of authentication control, the MicroStrategy Certificate Server, and other important technologies provide enterprises with a flexible security architecture strong enough to protect business information.

Overview

The use of mobile devices in the corporate environment is on the rise. As more employees interact with corporate data anywhere and at anytime, attackers have increased opportunities to compromise the data. When organizations allow employees to bring their own devices, corporations have even less control over the places employees bring and use corporate data. The risks that corporations should be most aware of include mobile device loss and theft, malicious attacks from outside networks, and dangerous exposure of servers to the internet.

MicroStrategy has invested in creating the most secure, commercially available mobile app platform in the marketplace. MicroStrategy Mobile features state-of-the-art security and in almost all cases requires no further integration with third-party solutions to deliver enterprise-class security. For almost all mobile app security requirements, customers have everything they need within the MicroStrategy platform: encryption of data in transit and at rest, remote access revocation, support for certificate server, single sign-on, credential management, and user-level security controls across data and objects.

This paper discusses the range of security capabilities offered by MicroStrategy Mobile, including mobile device security, data protection and encryption, mobile app security, Business Intelligence (BI) platform security, security partnerships, and third-party features.

Mobile device security

When discussing the security of mobile computing and BI apps, it is essential to consider the security of the mobile device itself. Apple and Android platforms enable administrators to establish strong policies for device access. All devices have password formats that can be configured and enforced over-the-air and—for Apple devices—via the iPhone Configuration Utility. These passcode format options meet passcode complexity requirements that fit any company policy.

Passcode and password options can be managed by a third-party mobile device management (MDM) solution such as AirWatch or MobileIron.

Apple iOS device security

Apple mobile devices support passcode protection that prevents unauthorized users from accessing data stored on the device. An extensive set of formatting options exists to establish the complexity of passcodes. Some of these options include:

- Timeout periods
- Password strength and if it is required or not
- Maximum number of failed attempts before all data on the device is erased
- Password history
- Auto-lock device
- How often the password must be changed

iOS configuration

Apple provides its own device configuration and is managed via the iPhone Configuration Utility. The iPhone Configuration Utility allows an administrator to set up certain resources that the mobile users can access including—among other things—setting complexity requirements for passcodes, granting access to corporate email and accessing VPN.

You can learn more about Apple security by reading the iOS Security Guide at https://www.apple.com/privacy/docs/iOS_Security_Guide_Oct_2014.pdf

Android OS device security

Android devices support password protection that prevents unauthorized users from accessing data stored on the device. Android provides an extensive set of formatting options to establish password complexity. Some of these options include:

- Minimum password length
- Maximum number of failed attempts
- Lockout duration

It is important to note that although Apple and Android offer security features and passcode complexity, these features are only enabled and secured if organizations create and enforce corporate policies on devices as most security features can be disabled by the user.

Data protection and encryption

Apple data protection and encryption

Mobile devices include a variety of security features designed to protect data stored on the device itself, which enhance the security of a mobile computing or BI implementation. MicroStrategy Mobile takes full advantage of the security features available within iOS.

iPhone 3GS, iPhone 4s, 5, 5c, 5s, 6, 6+, and iPad offer hardware-based encryption. A MicroStrategy application running under iOS encrypts data to the file system using AES 256-bit encryption. Encryption is always enabled and cannot be disabled by users.

MicroStrategy Mobile supports app-level passcode (9.4.1 Update 1) and Touch ID™ (9.4.1 Update 5) access for iOS. When configured, the app passcode or Touch ID™ (depending on the device and operating system) is required before a user can access information on the MicroStrategy Mobile app. The user must define a passcode based upon configurable requirements such as:

- At least one numeric character
- At least one special character
- At least one capital letter
- Minimum password length
- Maximum number of failed logon attempts
- Lockout duration

The system administrator also has the capability of prompting the user to enter the passcode after the app has been in the background for a period of time. The app passcode software encrypts application data on top of the native hardware encryption (this happens as long as users have an iOS system passcode set), and it effectively double encrypts any MicroStrategy app and business data local to the device, providing unsurpassed native platform security. It also enforces the passcode requirement for hardware encryption.

Touch ID™ integration

In 9.4.1 update 5, MicroStrategy Mobile became the first platform to integrate with Touch ID™, the fingerprint identity sensor created by Apple. If users have an iPhone 5, 5s, 5c, 6 or 6+, iPad Air 2 or iPad Mini and iOS 8, they have the option to access MicroStrategy Mobile apps and documents via Touch ID™. Touch ID™ allows users to use fingerprint verification to access MicroStrategy Mobile apps and/or certain documents and reports within the app.

Developers can configure Touch ID™ at the app or document level. At the app level, when users launch a MicroStrategy Mobile app, and successfully validate their identity using a fingerprint, the application will load. At the document level, system administrators can require authorization for certain document and reports. Content that is marked as secured will have additional restrictions, and users will be prompted to verify a fingerprint before getting access to certain documents and reports. When configuring, developers are able to require Touch ID™ only or either Touch ID™ or device passcode verification before users can access apps, documents and/or reports. These features are available in both online and offline mode.

MicroStrategy Mobile secured with Usher

Since 2012, MicroStrategy has invested in developing an enterprise-grade mobile identity platform, MicroStrategy Usher. Usher delivers a simple, seamless, and secure user experience that protects systems across the enterprise. Usher allows enterprises and users to:

- Replace traditional forms of enterprise identity such as IDs, passwords, and tokens with mobile identity badges securely delivered on a smartphone
- Provide identity verification over the phone or in person
- Give a 360-degree view of networks by reporting on user activity, location monitoring, and alerts

Integration with Usher allows users to access information at the application and/or document level without the need for a password. Instead, users receive badges that will allow them to access their MicroStrategy apps. Once Usher is downloaded from the Apple and/or Google Play app store and is installed onto a device, users receive a badge unique to their enterprise. Usher badges can then be used to access certain projects or documents, or to access physical entryways using digital keys. Further, with Usher badges, administrators can gain a 360-degree view of their network to understand what documents, apps, and physical locations are being accessed, by whom and at what time. As an added security measure, administrators can geo-fence and time-fence access of specific badges.

Android protection and encryption

Not all Android mobile devices offer hardware encryption. To protect data stored on MicroStrategy apps on Android devices, MicroStrategy gives organizations the opportunity to create an App-level Protection Code that a user must input before accessing information on the app. This feature is specific to MicroStrategy Mobile software and ensures that data stored on a MicroStrategy Mobile app is protected at all times regardless of the device being used.

An extensive set of App-level Protection Code formatting options exist to establish the complexity of the code. These options include:

- Fixed number of characters from a minimum of four to a maximum of eight
- At least one numeric character
- At least one special character in the ASCii range of 33 to 126
- At least one uppercase alpha character

The App-level Protection Code is created when users access the app for the first time. Users input their code and the MicroStrategy app checks whether the code meets the criteria set by the administrator. If the code fits the criteria, the code will be approved and when users are prompted to enter the app, they will input their code.

When users create an App-level Protection Code, the MicroStrategy Android app generates an encryption key based on that code, which is then encrypted and stored in the MicroStrategy app secure keystore. Further, MicroStrategy Mobile for Android can employ software encryption to secure caches using a 256-bit AES encryption method.

MicroStrategy Mobile app security

MicroStrategy Mobile effectively takes advantage of Apple and Android operating system features to secure the actual MicroStrategy Mobile app running on the mobile device.

Data transmission

Secure data transfer between MicroStrategy Mobile apps and the MicroStrategy Mobile server involves secure internet transfer connections and secure communication channels.

In addition to HTTP, MicroStrategy Mobile apps support HTTPS (Hypertext Transfer Protocol Secure). HTTPS is a combination of the HTTP protocol with the SSL (Secure Socket Layer)/TLS (Transport Layer Security) protocol. It provides encryption and secure identification of the server. Essentially, HTTPS provides a secure channel over an unsecured network. If corporations want to ensure data security by establishing a secure and encrypted connection between MicroStrategy Mobile apps and the MicroStrategy Mobile server, the MicroStrategy Mobile server should be configured to receive requests only over the HTTPS protocol.

Secure communication channels are important when it comes to data transfer. Data can be transferred by placing the MicroStrategy Mobile server behind a firewall and using a VPN (Virtual Private Network) connection to retrieve data using MicroStrategy Mobile apps, regardless of the transfer protocol or wireless network to which they are connected. The VPN connection creates a secure communication channel between the MicroStrategy Mobile app and the MicroStrategy Mobile server. A VPN set up between the mobile device and the MicroStrategy platform will provide the strongest security available for communications with iPad and iPhone devices. VPN provides secure authentication using standard X.509 digital certificates to ensure that the devices can legitimately access the server, and also encrypts data communications.

iPhone, iPad, and Android devices integrate with a number of VPN technologies and protocols, including IPsec (Internet Protocol Security), L2TP (Layer 2 Tunneling Protocol), PPTP (Point-to-Point Tunneling Protocol), and SSH (Secure Shell).

The implementation and setup of VPN is straightforward regardless of the corporate environment, and there are readily available extensions to existing corporate VPNs to support a compatible environment with Apple and Android devices. Setup can be automated, managed by an MDM, or secured by a reverse proxy.

Authentication

MicroStrategy Mobile follows the "defense in depth " approach, which calls for several layers of security throughout an IT system. MicroStrategy provides several layers of authentication and password control.

These authentication methods include secure application authentication, confidential project mode, and mutual authentication. These layers of authentication assure the confidentiality of data on MicroStrategy Mobile apps at all times.

Secure application authentication

When opening a MicroStrategy Mobile app, the app performs credential validation. MicroStrategy offers various authentication methods—in addition to third-party single sign-on, which is discussed in a later section. These authentication methods include:

- Standard: Intelligence Server is the authentication authority. This is the default authentication mode.
- Database warehouse: The data warehouse database is the authentication authority.
- LDAP (lightweight directory access protocol): An LDAP server is the authentication authority.
- Windows NT authentication: Windows is the authentication authority.
- Integrated authentication: A domain controller using Kerberos authentication is the authentication authority.

Confidential project mode

In the MicroStrategy Mobile configuration, organizations can designate session expiration time limits for the mobile app and configure project-level authentication. These settings work when the mobile device is either online or offline, ensuring both live and cached data are secured.

By default, MicroStrategy Mobile for iPhone and iPad do not require users to reconfirm their credentials when re-entering the app. From the Mobile configuration page, you can change this behavior and set a session expiration time limit. You can choose unit intervals of days, hours, or minutes. When the app has been running in the background, or the device has been locked for the allotted period of time, MicroStrategy will attempt to re-authenticate the user. At least one project must be treated as confidential for password expiration to take effect.

HTTPS with mutual authentication

MicroStrategy 9.2.1m (and on) supports HTTPS mutual authentication, also known as two-way authentication. Mutual authentication is facilitated by the addition of a new server component called the MicroStrategy Certificate Server. The Certificate Server has the sole purpose of ensuring added security by providing mobile devices with specific certificates that are later used in authentication.

In order to gain access to the MicroStrategy Mobile Server, the user must first enroll the device with the MicroStrategy Certificate Server. This entails presenting the user's credentials to the Certificate Server and, upon validation, the Certificate Server will issue an X.509 certificate that is then sent to the device and stored. (Note: this certificate is only associated with the MicroStrategy app.)

All communications with the MicroStrategy Certificate Server are conducted via an encrypted link using the HTTPS protocol. MicroStrategy customers can select the validation process for authenticating user credentials in accordance with their internal security guidelines and procedures. The Certificate Server provides an API to allow it to interface with various third-party authentication components.

The Certificate Server can be supported on the same application server as the MicroStrategy Mobile Server; however, if desired for operational purposes, it may also be hosted on a different application server and/or machine. The MicroStrategy Mobile Server is configured in the system to require client side certificates. In keeping with best practices, we also recommend that the Mobile Server be restricted to the use of the AES cipher suite. To accomplish this, make the appropriate setup changes on the application servers hosting the Mobile Server.

Once the user attempts to access the Mobile Server from the device, the device must present its X.509 certificate to the Mobile Server. The Mobile Server then validates the certificate by checking the subject name of the certificate, which should correspond to the device, and validates that it was signed by a recognized certificate authority. Similarly, the Mobile Server presents its X.509 certificate to the device and the device performs the identical process to authenticate the server.

In the event that the device is lost or stolen, the MicroStrategy Certificate Server provides the means to place the certificate associated with the device on the Certificate Revocation List. The Certificate Revocation List is always checked during the validation process after the certificate is received from the device by the server. If the certificate has been revoked, then communications will not be permitted, and the user will be denied access to the system.

Once the device has been authenticated by the server and the server has been authenticated by the device, communications proceed with the Mobile Server using AES encryption. One advantage of using mutual authentication is that certificates can be issued to devices that are not associated with the enterprise (e.g. to customer devices). This is in contrast to devices operating in a VPN where enterprises would be reluctant to issue access through their corporate VPN to third parties; as such, access often entails the ability to gain entry to servers and resources not associated with the MicroStrategy Mobile system.

Figure 1 shows how MicroStrategy components interact to facilitate HTTPS communication with mutual authentication incorporating the certificate server.

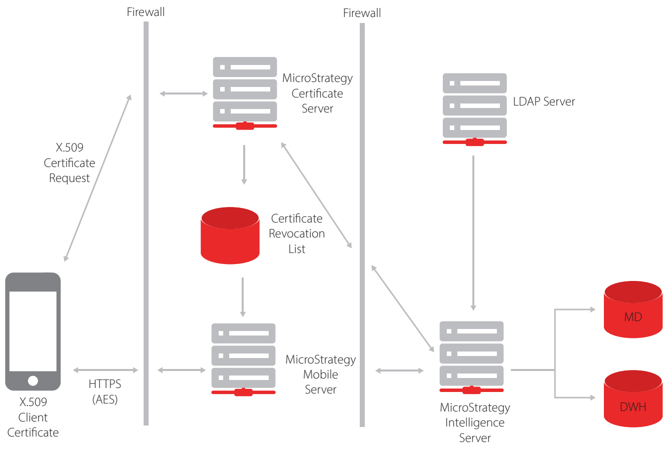

Firewall
Firewall
MicroStrategy Certificate Server
LDAP Server
X.509 Certificate Request
Certificate Revocation List
MD
DWH
MicroStrategy Mobile Server
HTTPS (AES)
X.509 Client Certificate
MicroStrategy Intelligence Server

Figure 1

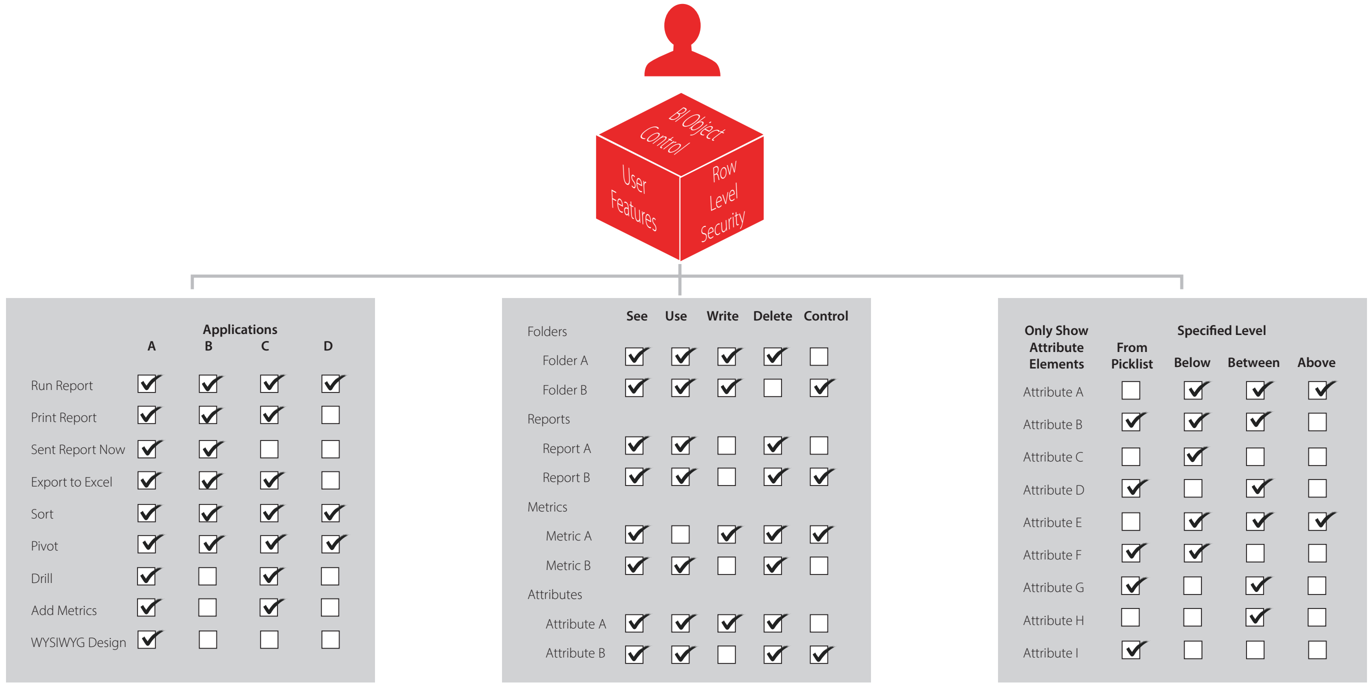
Further, MicroStrategy supports Client Certificate Authentication. When any of the mobile clients try to connect to a MicroStrategy Mobile Server, the Mobile Server can be configured to first request that the client issue a digital certificate. The mobile client creates a private-public key pair and sends the public key to a trusted Certificate Authority (trusted by the MicroStrategy Mobile Server). The Certificate Authority issues a digital certificate that contains the public key, which is then sent to the MicroStrategy Mobile Server by the client. Since the digital certificate is issued by a Certificate Authority that the Mobile Server trusts, the client is authenticated by the Server.

Authorization

Authorization refers to the three-dimensional process by which the app determines app functionality privileges, object access permissions, and data access security (as seen in Figure 2 below).

MicroStrategy Mobile utilizes the same sophisticated user authorization management framework available in the MicroStrategy Analytics Platform. This framework uses security filters to distinguish between users based on each individual's knowledge, business needs, and security level, allowing for more secure and organized data access. Each user's access to app functionality, reports, and data within those reports is managed dynamically based on their profile and privileges. As a result, data security is maximized while every user benefits from a personalized app experience, tailored for their particular organizational role.

For example, one report is used by the CEO to view sales data for all products. A regional manager may view the same report but may only be able to view data related to the multiple production lines in his jurisdiction, while a national production manager may only have access to the data about the product line he/she manages. Thus, a single report with specific authorizations can satisfy the reporting needs of all these individuals.



	Applications			
	A	B	C	D
Run Report	☑	☑	☑	☑
Print Report	☑	☑	☑	□
Sent Report Now	☑	☑	□	□
Export to Excel	☑	☑	☑	□
Sort	☑	☑	☑	☑
Pivot	☑	☑	☑	☑
Drill	☑	□	☑	□
Add Metrics	☑	□	☑	□
WYSIWYG Design	☑	□	□	□

Application functionality privileges

- Establishes customized user environment
- User sees only the functionality appropriate to their skill level

	See	Use	Write	Delete	Control
Folders					
Folder A	☑	☑	☑	☑	□
Folder B	☑	☑	☑	□	☑
Reports					
Report A	☑	☑	□	☑	□
Report B	☑	☑	□	☑	☑
Metrics					
Metric A	☑	□	☑	☑	☑
Metric B	☑	☑	□	☑	□
Attributes					
Attribute A	☑	☑	☑	☑	□
Attribute B	☑	☑	□	☑	☑

Object access permissions

- Set up private workgroup folders or reports
- Impose column-level data security
- Control development access to all objects

Only Show Attribute Elements	From Picklist	Specified Level Below	Between	Above
Attribute A	□	☑	☑	☑
Attribute B	☑	☑	☑	□
Attribute C	□	☑	□	□
Attribute D	☑	□	☑	□
Attribute E	□	☑	☑	☑
Attribute F	☑	☑	□	□
Attribute G	☑	□	☑	□
Attribute H	□	□	☑	□
Attribute I	☑	□	□	□

Data access security

- Establishes row-level data security

Figure 2

Analytics platform security

MicroStrategy Mobile is based on a secure, multi-tier architecture that makes up the MicroStrategy Analytics Platform. Within this architecture (as seen in Figure 3), seven characteristics ensure the integrity of the data in the mobile computing/BI system, making MicroStrategy one of the most secure platforms for both BI/Analytics and Mobile.

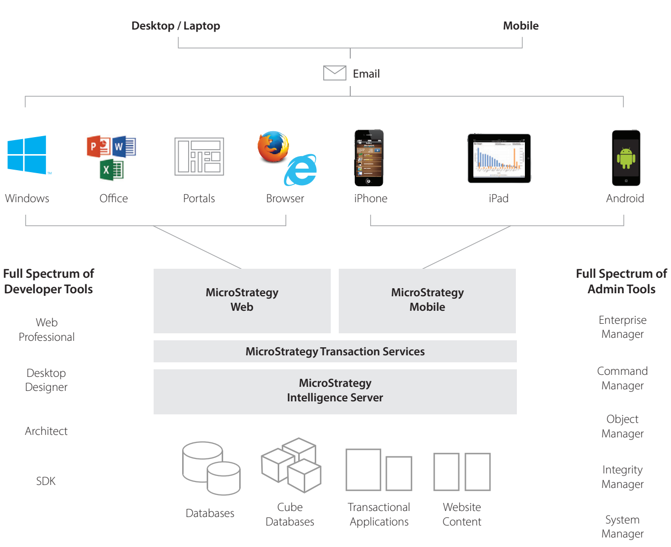


Figure 3

Secure communications across firewalls

Customers typically install the MicroStrategy platform on more than one server to distribute the workload. Secure communication across these servers is often governed by layers of firewalls constructed into Demilitarized Zones (DMZ). Using multiple firewalls, two distinct DMZs are created with one DMZ protecting the Mobile and Web servers and the second DMZ securing the infrastructure of the data sources and MicroStrategy Intelligence Server.

No database connection from the MicroStrategy Mobile Server

An effective DMZ is characterized not only by the presence of firewalls but also an architectural component that accesses the database, which resides behind a firewall. The MicroStrategy Intelligence Server is the core of MicroStrategy's Analytics Platform, and is the only component that accesses the database. It resides between two firewalls in the same way that the MicroStrategy Mobile Server resides between two firewalls. Only in this configuration is a hacker who gains access to the MicroStrategy Mobile Server prevented from accessing the database.

Single port control for data access

Firewalls protect corporate information assets by limiting which application has access rights to certain computer network ports. To take full advantage of this protection, the Web-based application must allow for granular port access control. The MicroStrategy Mobile and Web architectures allow administrators to configure which port is used for inter-server communication. Connections to other ports can be disallowed by the firewall, thus minimizing exposure.

No external Remote Procedure Calls (RPC) or Remote Method Invocation (RMI) calls

RPC and RMI calls are hazardous because they allow hackers to access and control remote and distributed computer processes. These calls often allow anonymous access through separate, open ports in the firewall. MicroStrategy Mobile uses only XML to communicate with the Intelligence Server, eliminating the need for RPC or RMI calls completely.

Transmission security

The MicroStrategy Analytics Platform provides an option to encrypt communications between its server components (i.e. between the MicroStrategy Intelligence Server and MicroStrategy Mobile Server, using an AES 128-bit algorithm). As AES is in the class of block code ciphers (i.e. the same input plaintext will result in the same cipher text), MicroStrategy has employed the algorithm in cipher block chaining mode (CBC), where previously transmitted cipher text is combined with the input plaintext in successive cipher blocks, which randomizes the input. This is particularly important for BI applications since the transmitted information tends to be primarily numeric. If CBC mode were not used, the likelihood that the cipher stream could be broken by a motivated attacker would be considerably higher.

Protection of stored user credentials

MicroStrategy follows industry standard security practices for the protection of sensitive user credential information that is stored in the MicroStrategy metadata repository. Rather than storing the actual user password, a secure hash of the password is stored. Because the hash is a one-way secure operation, even if this data were compromised, the information would not be useful as there is no known way to derive the original password from the hashed value in order to gain access to the system.

Intensive testing

No industry standard has yet been established for mobile security, but MicroStrategy has worked to create the most secure product commercially available. MicroStrategy uses third-party vendors for security and vulnerability testing. Testing includes automated tools, static analysis of code, and internal penetration testing.

Third-party enhancements

Customers can integrate the MicroStrategy platform with a variety of third-party add-ons. These include single-sign-on, mobile device management, and operational security.

Single Sign-On (SSO) form-based authentication

MicroStrategy Mobile provides a seamless integration with third-party single sign-on (SSO) tools including Tivoli, SiteMinder, Oblix, Okta and others. Enterprise network users can access MicroStrategy content and functionality on the basis of a single authentication, performed when they initially connect. This allows users to avoid redundant logins.

In addition, MicroStrategy has built-in SSO support for four portal server applications: Microsoft SharePoint, IBM WebSphere, Oracle WebLogic, and SAP Enterprise Portal. MicroStrategy also integrates with any other third-party identity management system that supports Security Assertion Markup Language (SAML).

Enterprise Mobility Management

MicroStrategy Mobile features state-of-the-art security that, in most cases, requires no further integration with third-party solutions to deliver enterprise-class security. In terms of mobile app security, customers have everything they need within the MicroStrategy platform: encryption of data in transit and at rest, remote access revocation, support for certificate servers, credential management, user-level security controls across data and objects, and more.

However, many organizations decide to use a third-party enterprise mobility management (EMM) solution to govern various aspects of workforce mobile devices, applications, and services—including updates, access settings, device restrictions, password protocols, and more.

Currently, EMM vendors offer two methods for incorporating their libraries into mobile apps: app wrapping or native SDK integration. MicroStrategy customers can pursue both of these options, but SDK integration is the recommended route.

MicroStrategy offers native SDK integration with three EMM providers: MobileIron, Good, and AirWatch. These builds are available to our mobile customers for free on the MicroStrategy download site. MicroStrategy Mobile also supports EMM capabilities via implementation of the AppConfig guidelines.

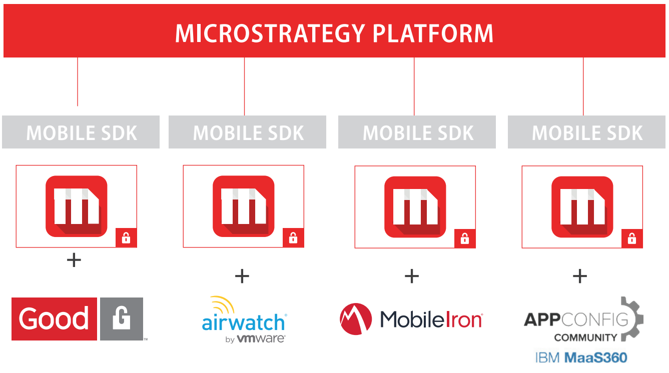


Figure 4

MicroStrategy Mobile secured by Good

MicroStrategy Mobile in iOS platform has partnered with Good Technology, a market leader in secure mobile solutions.

MicroStrategy Mobile secured by Good (seen in Figure 4) is an option for deploying MicroStrategy Mobile powered apps. This is the best option for customers who have Good licenses or Good as a security requirement. Good's network replaces traditional connectivity solutions including VPN, DMZ, Proxy/reverse and a plethora of network devices that compete in the mobile connectivity for enterprise marketplace.

MicroStrategy Mobile secured by Good offers proprietary AES 192-bit equivalent encryption over-the-air and at rest, which meets a majority of data protection standards including HIPPA and PCI. It provides an outsourcing of DMZ network functionality, and the Good Technology network solution has its own 443 port—this can be thought of as its own tunnel—which any number of apps can use. Further, users can move data between applications with AppKinetics.

By using this deployment, users will see a reduction in data leaking (i.e. users taking screenshots, copy/paste), and administration will be eased through centralized, remote management and secure mobile app polices.

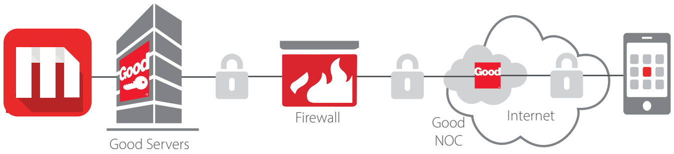


Figure 5

MicroStrategy Mobile secured by Mobile Iron

MicroStrategy has partnered with MobileIron to add an extra layer of security to MicroStrategy Mobile applications running on iOS devices.

By implementing the security policies and configurations provided by MobileIron, administrators can apply enhanced protections to mobile devices in use across the enterprise. These settings help organizations add additional security around apps that handle sensitive data.

There are three kinds of security policies available on MobileIron to help administrators prevent data leakage.

Copy and Paste: This policy is used to either allow or disallow users from copying and pasting content to and from an app managed by MobileIron.

Print: Using this policy, administrators can set whether users are allowed to print content from an app managed by MobileIron. When you disallow this privilege, no data can be printed from the app.

Open in: This policy is used to determine where users can open files in specific apps managed by the MobileIron VSP. The administrator can choose to allow users to open files in all apps, apps that are managed by MobileIron, or apps in a white list.

MicroStrategy Mobile Secured by AirWatch

MicroStrategy also offers native integration with the AirWatch platform to add an extra layer of security to MicroStrategy Mobile applications running on iOS and Android.

With AirWatch's mobile application management (MAM) capabilities, administrators can distribute, secure, and track mobile applications directly from the AirWatch Admin console, which can be integrated into your mobile environment.

The AirWatch platform allows you to add an additional level of security by setting restrictions within the security profile. For example, you can enable Data Loss Prevention to protect sensitive data in applications. This setting controls copying and pasting, printing, taking pictures and screen captures, using Bluetooth, and other actions that involve the transmission of data.

Features:

		EMM		
Feature	**Description**	**Good Dynamics**	**MobileIron**	**AirWatch**
Provisioning and authentication	Adds an additional EMM-specific authentication, e.g. PIN with configurable security settings. This is in addition to the authentication required by the MicroStrategy application.	Yes	Yes	Yes
Data leakage Prevention	Controls to govern whether data can be transmitted, shared, or copied outside of the application ecosystem.	Yes	Yes	Yes
Application ecosystem	Allows data to be transmitted to other applications in the EMM ecosystem (i.e. other applications that are integrated with the EMM SDK) in a secure manner.	Yes	Yes	Yes (open in other managed apps)
Tunneling	Use a secure channel or gateway provided by the EMM platform to transmit data from client to server.	Yes	Yes	Yes
Data Encryption	Ensure that all persisted data are automatically encrypted on the device.	Yes	Yes	Yes

Secure MicroStrategy Mobile application by AppConfig – Compliant EMM providers

MicroStrategy Mobile for iOS devices further supports EMM capabilities by incorporating guidelines set by the AppConfig Community. (http://www.appconfigforenterprise.org/). AppConfig delivers the first standard approach to configuring and securing apps in the enterprise. This initiative defines a collection of best practices that enterprise application developers can use to interpret app configurations and security policies from EMM systems. These guidelines also ensure that EMM systems configure and secure mobile applications by leveraging app security and configuration frameworks available in the OS.

Following the AppConfig standard allows MicroStrategy Mobile apps to make use of the features provided by iOS, like sending configurations from console to the app via NSUserDefault, per-app VPN, certificate-based authentication, and much more, to control the behavior of the app.

Benefits:

- Provides EMM vendor neutral solution and helps to build enterprise-ready apps faster.
- Helps enterprises to use existing VPN solutions and leverage existing EMM investments.
- Provides EMM providers with larger ecosystem of business apps and easy management workflows.

Capabilities:

- **App configuration**
  Configure information such as Intelligence Server connectivity, project information, home screen setting, and general app settings to eliminate the need to educate end users about first-time setup.
- **Security policies and access control**
  Restrict apps to run only on approved devices and enforce security policies such as required encryption and data loss prevention at the app level.
- **App Tunnel**
  Selectively enable approved apps to use an app tunnel to connect to backend and corporate networks.

Corporate policies for operational security

Operational security

Secure devices, apps, and network connections can be easily compromised if corporations don't set operational security measures and educate employees. Operational security includes the procedures and discipline that an enterprise gives to security within its system. Corporations need to establish a security policy that addresses the following:

- Enrolling devices: device activation, user authentication, certificate enrollment
- Configuration profiles: restricting device features, wifi settings, VPN settings, email server settings
- Policy enforcement: device passwords and management
- Asset management: device information, network information, compliance, and security information
- Accounts and services integration: email, calendar, contacts, VPN, and wifi
- Restrictions enforcement: Manage access to browsing, app usage/installation, camera, and screen capture
- Theft and loss prevention: standard policies for users to handle their device
- Loss device procedures: policies for actions taken when the device is lost or stolen, how to notify, remote lock, remote wipe, and local wipe

Conclusion: MicroStrategy, a secure mobile computing and mobile BI solution

MicroStrategy Mobile is built to meet the security requirements of any organization and integrates seamlessly with the proven security features of the iPhone, iPad and Android. Robust features for device security, data security, authentication, and authorization combine to provide a layered and effective approach to protect sensitive data in mobile business apps.