MicroStrategy

WHITE PAPER

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

MicroStrategy Mobile App Platform

Table of contents

MicroStrategy

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

MicroStrategy Mobile App Platform

With ever-advancing mobile technology and the release of Apple's App Store in 2008, 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 MicroStrategy's exceptional security features including MicroStrategy-designed device protection code for Android, 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.

Since 2009, MicroStrategy has invested in creating the most secure, commercially available mobile app platform in the marketplace. MicroStrategy Mobile's security is state-of-the-art 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, remote data wipe, 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 http://www.apple.com/ipad/business/docs/iOS_Security_Oct12.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 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.

Introduced in 9.4.1 Update 1, MicroStrategy Mobile supports the enforcement of the Application Passcode for iOS. When configured, the Application Passcode 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

A user is required to establish a personal passcode, then enter the passcode upon opening the MicroStrategy app. If the passcode is not entered correctly within the threshold configured by the system administrator, the caches for the MicroStrategy app will be wiped from the device. Further, the system administrator has the capability of prompting the user to enter the passcode after the app has been in the background for a period of time. Because the Application Passcode encrypts the caches at a second level on top of the native encryption already included with the MicroStrategy authentication framework, the use of the passcode feature effectively double encrypts any MicroStrategy app and business data local to the device, providing unsurpassed native platform security.

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 a Device Protection Code (DPC) 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 DPC formatting options exist to establish the complexity of DPCs. 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 DPC is created when users access the app for the first time. Users input their DPC code and the MicroStrategy app checks whether the code meets the criteria set by the administrator. If the DPC fits the criteria, the DPC will be approved and when users are prompted to enter the app, they will input their DPC.

When users create a Device Protection Code (DPC), the MicroStrategy Android app generates an encryption key based on that DPC, 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 extensions to existing corporate VPNs to support a compatible environment with Apple and Android devices are readily available. 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 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 mututal 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.

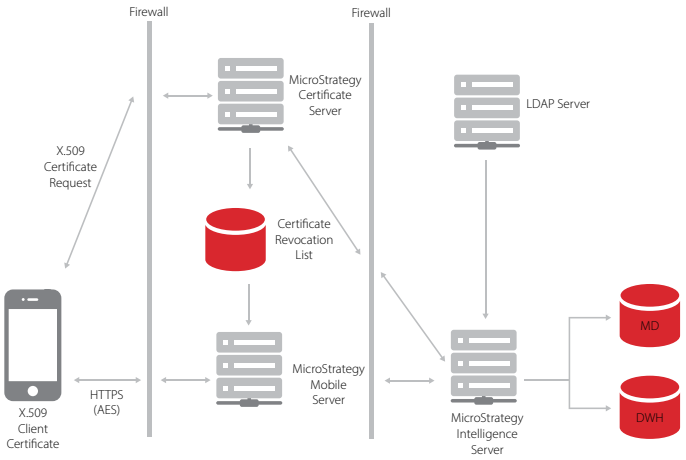
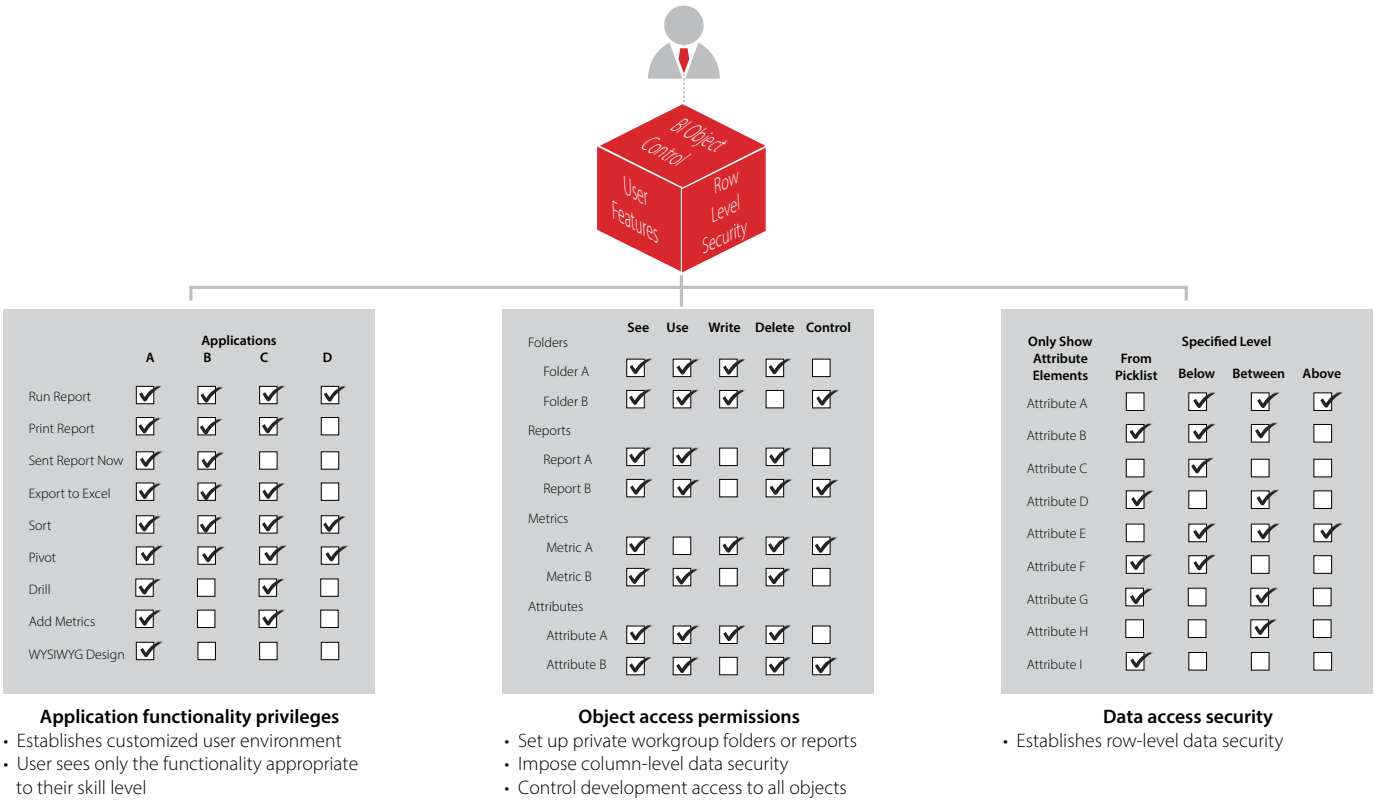


Figure 1

In the event that the device is lost or stolen, the MicroStrategy Certificate Server provides the means to place the certificate



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

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

Data access security
- Establishes row-level data security

Figure 2

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 on page 5 shows how MicroStrategy components interact to facilitate HTTPS communication with mutual authentication incorporating the certificate 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 above).

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.

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.

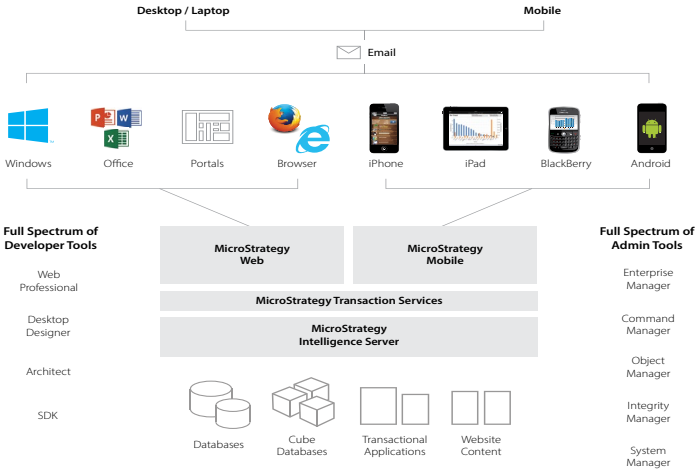


Figure 3

1. 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.

2. 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.

3. 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. MicroStrategy's Mobile and Web architecture allows administrators to configure which port is used for inter-server communication. Connections to other ports can be disallowed by the firewall, thus minimizing exposure.

4. 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.

5. 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.

6. 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.

7. 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.

Security partnerships

Good Technology

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

MicroStrategy Mobile Secured by Good (seen in Figure 4 above) 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 loss (i.e. users taking screenshots, copy paste), and administration will be eased through centralized, remote management and secure mobile app polices.

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,

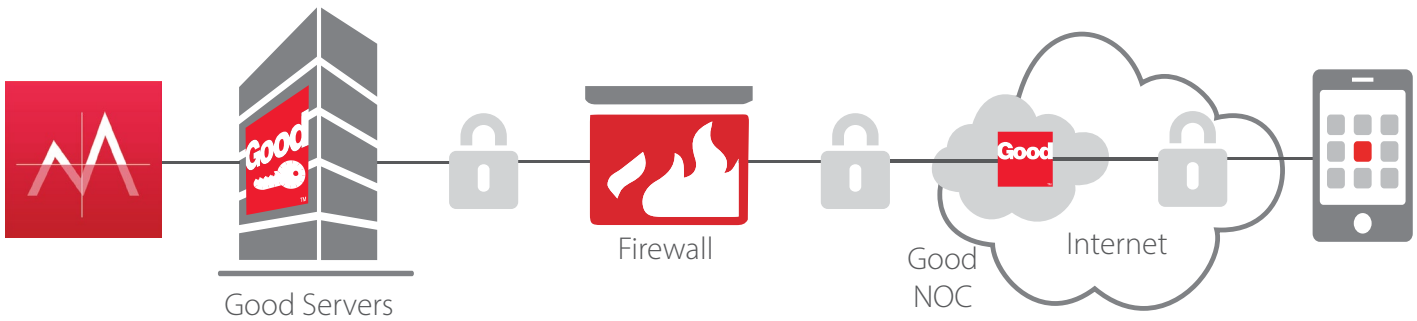


Figure 4

Oracle WebLogic, and SAP Enterprise Portal. MicroStrategy also integrates with any other third-party identity management system that supports Security Assertion Markup Language (SAML).

Mobile Device Management (MDM)

Many corporations decide to use a third-party mobile device management (MDM) solution to manage various aspects of workforce mobile devices. MDM solutions manage password protection and distribution and secure users. In addition, MDM solutions have the ability to influence updates, access, loopholes, password protocols per device, remote wipes and more. Two companies that provide MDM solutions are AirWatch and MobileIron.

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, wifi
- Restrictions enforcement: Manage access to browsing, app usage/installation, camera, 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, 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.