IBM Software
Thought Leadership White Paper

September 2013

Beyond passwords: Protect the mobile enterprise with smarter security solutions

Prevent fraud and improve the user experience with an adaptive approach to mobile access management

IBM

Introduction

Around the world, employees increasingly use their own mobile devices in the workplace, often accessing corporate applications after-hours and off-site. In fact, a recent survey found that 86 percent of organizations either allow or plan to allow the use of employee-owned devices for work functions. Within these bring-your-own-device (BYOD) programs, 42 percent allow employees to bring in any device—smartphones, tablets, laptops and other mobile devices—and access the network as long as they agree to certain policies. In reality, this can often mean employees are simply "trusted to do the right thing."[1]

Mobile security, and ensuring users do the right thing, is one of the highest priorities of today's CIOs. Although mobile employees can be more productive by working anytime and anywhere, they are now accessing corporate data and applications from outside the traditional network perimeter. This means traditional access and authentication controls are no longer sufficient. Meanwhile, cyber criminals are getting more sophisticated in their attack methods, just as organizations are adopting new types of mobile applications to be more open and connect with more customers.

This white paper will look at the challenges of providing secure access in this new mobile world, and will explore new security models, business policies and controls that can help protect your critical assets and data. It will explain how flexible authentication schemes, context-based access and behavioral analysis can help ensure that only authorized mobile users can access your valuable resources—onsite, in the cloud and beyond.

Mobile security in a multi-perimeter world

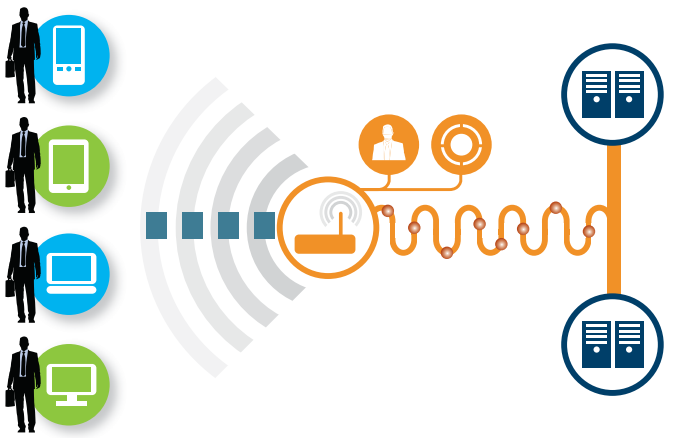
Thanks to the increasing popularity of BYOD programs, more and more users are connecting their personal mobile devices to corporate networks. At the same time, they are using cloud-based applications and services—such as Salesforce.com, Microsoft Office 365 and others—for their day-to-day tasks. Today's work gets done outside of the conventional network perimeter, resulting in a critical need for a new type of security. Organizations need mobile access policies and controls that are effective in this multi-perimeter world.

When mobile users access sensitive data, applications and infrastructure, their identity is the "key" that helps provide secure access. Many organizations still rely on a simple password as proof of identity. In fact, 80 percent of organizations with BYOD programs require only a password for mobile access to the corporate network.[1] But relying on passwords alone carries new risks for the mobile enterprise. What happens when a mobile device is lost or stolen? If a password is cached on the device, anyone can use it to access the password-protected assets.

To help prevent fraudulent access, mobile users need to be able to prove their identities within the context in which they are accessing corporate resources. This context may include the type of device they are using, the applications running on that device, their location or their patterns of activity. The latest security technologies can then use this context information to evaluate whether users are authorized for access.

For example, if a North American worker suddenly uses her mobile device from Africa, the software notes this unusual change in context and may require the user to provide additional proof of identity. User credentials are now accepted in many forms, such as one-time passwords (OTPs), facial recognition or other biometrics. IT organizations can also use context information to quickly identify anomalous behavior and mitigate security risks or regulatory compliance gaps.

IBM mobile security framework



Device management	Network, data and access security	Application-layer security
Secure endpoint devices and data	Achieve visibility and adaptive control	Develop and test applications

With an integrated portfolio of mobile security solutions, IBM helps organizations reduce security risks and improve compliance across the entire mobile environment.

IBM® Security access management solutions are designed to help organizations address the growing incidence of advanced security threats and risks associated with mobile, social and cloud access, while also helping clients comply with the latest security regulations. These solutions provide authentication, context-based access and behavioral analysis capabilities to enable mobile users to safely access online resources. Highly scalable and configurable, IBM Security solutions deliver both a fast time to value and a low total cost of ownership.

Adaptive mobile security in real-world environments

When it comes to the mobile world, change is a constant. Today's mobile users are using different types of devices and applications to access the corporate environment and exposing the organization to new security vulnerabilities on an almost daily basis. This can make it seem very difficult to protect your most critical resources from attack.

An effective access management solution can help prioritize your security measures, enabling you to provide a basic level of mobile security across all applications, and then add more advanced, policy-based protection on a case-by-case basis. The following use cases explain how IBM access management capabilities can be applied in the real world.

Use case 1: Reducing mobile security risks

Mobile users are using their devices from almost anywhere. However, what if employees try to access confidential information in a public place, such as an airport or coffee shop? Depending on your established security policies and the sensitivity of specific data, your organization may want to restrict mobile access to certain applications. This can help prevent legitimate users from doing unsafe things on their mobile devices.

IBM Security Access Manager for Mobile helps reduce mobile security risks by providing context-aware access control that can enforce established policies and guidelines. Using contextual data analytics to calculate risk, organizations can grant access based on a dynamic risk assessment of the confidence level of a transaction. When a user requests access to a protected resource, the IBM technology calculates the risk score and determines whether access is permitted, denied, or permitted after a condition is met (such as answering a specific question only known by the device owner). In some situations, depending on the risk score, the user may be denied access to certain IT resources because the security risk is deemed to be too high.

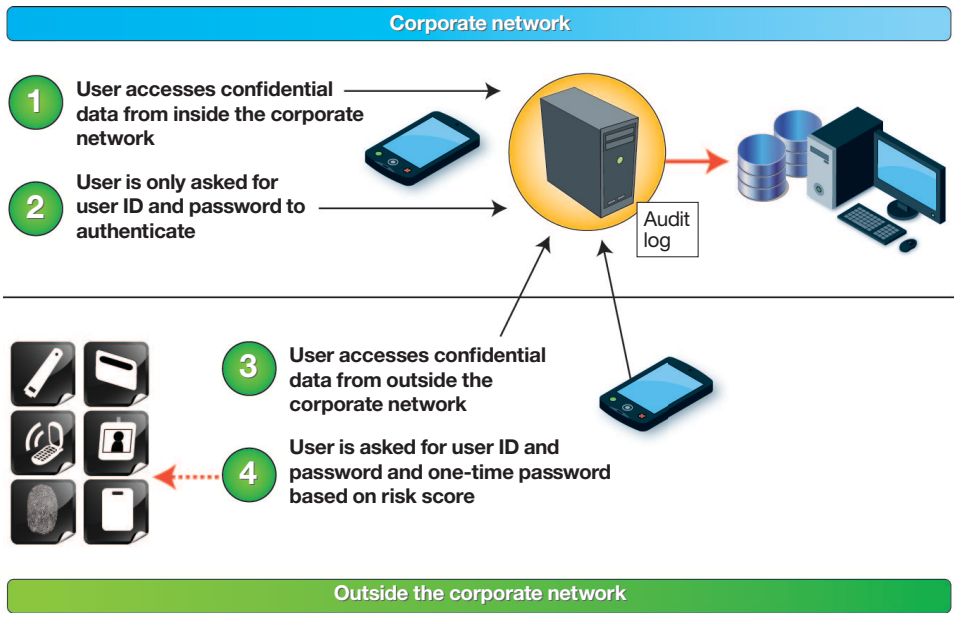
Use case 2: Preventing mobile fraud

As more personal devices are being used for work, a critical component of security is verifying the user's identity. For example, what happens when a device is lost or stolen or an employee's child gets hold of the device? If a tablet is lost at a coffee shop and has no PIN associated with it, any malicious user can simply open email, collect personal information and then act upon it. Or if someone steals a smartphone, and the login information is already stored in a banking application, the criminal is only a few clicks away from transferring thousands into his own account. An employee's child can also inadvertently wreak havoc in any number of ways.

By requiring more than one form of authentication, organizations can help ensure the right user is granted access to protected resources. In addition to traditional user authentication—for example, validating a name and password—organizations can also authenticate the device itself. Access to corporate resources is granted only when a device is being used in an acceptable, known context, such as during a specific time of day, from a specific location or using a specific type of browser. Organizations can also use session management to force an authentication challenge when the user has been inactive for a period of time.

Security Access Manager for Mobile enables organizations to easily deploy multi-factor authentication that requires users to prove their identities in more than way. For example, users can be sent OTPs via text or email, and then they can enter the OTP in addition to their regular login information to access the network. For added security, OTPs can also be provided by external devices, using hash-based message authentication code (HMAC) algorithms. In addition to standard challenge questions, the IBM solution also supports an emerging technique that connects to users' social networks and requires them to select friends from a collection of profile pictures for authentication.

For additional protection, Security Access Manager for Mobile also integrates with other third-party authentication solutions, such as RSA SecurID tokens.



IBM Security Access Manager for Mobile enables organizations to prevent unauthorized access to protected resources by requiring multiple forms of authentication.

Use case 3: Enabling identity-aware applications

Today's mobile applications typically require users to enter a name and password to prove their identity. For added security, some organizations also require credentials to be entered every time an application is launched or after a period of inactivity. But what happens when users have long names or complex passwords? Entering these credentials on a touchscreen can be difficult, leading to typing errors that can result in account lockouts. Some users may respond by creating weak passwords—thus, weakening security. Even worse, some applications may store the credentials locally to help improve the user experience, which introduces more vulnerabilities.

Security Access Manager for Mobile can help organizations make applications "identity-aware" by using OAuth standards-based technology. Users can obtain a one-time authorization code that enables their device to securely connect to applications, providing seamless, password-less access for users. User credentials are not stored on the device—only device tokens that are exchanged transparently each time the application is launched. An optional PIN can also be required during authentication for added security.

Use case 4: Leveraging mobile security intelligence

Traditional web-based access controls rely on user authentication and security policies to provide secure access to applications. In some cases, role-based authorization policies can help ensure more fine-grained control. Travelling users can be allowed access from multiple locations, while mobile access to SAP-based financial information, for example, can be restricted to anyone outside of the accounting department. What's the best way to prevent a US-based device from making hundreds of transactions from China? Or, to protect intranet access from a part-time employee?

Using Security Access Manager for Mobile, organizations can define context-based access policies at a transactional level and require additional authorization based on the type of device, environment, identity or behavior patterns. For example, when users want to make bank transfers above a configurable threshold, an OTP can be required for proving their identity. Or, expense reports may only be approved if they are submitted from a location within the US.

With a 360-degree view into all the elements of mobile user access, organizations can strengthen their security and compliance posture. Security Access Manager for Mobile integrates with IBM QRadar® Security Intelligence Platform to provide deep insights into how users access information hosted on-premises or in the cloud. Leveraging core capabilities within QRadar, organizations can identify anomalies and take proactive action to reduce risk. Plus, they can generate comprehensive reports to demonstrate a strong compliance posture.

IBM integrated solutions for investment protection

Easy to deploy and maintain, Security Access Manager for Mobile is available as either a standalone hardware appliance or a virtual appliance that fits easily within an existing virtualized environment, such as a VMware ESX hypervisor environment. It includes an intuitive graphical user interface for performance monitoring and analysis, configuration snapshot creation and restoration, and ongoing configuration management. The solution also provides a policy-authoring interface that enables IT personnel to easily create and implement context-based access and authentication policies. These capabilities help reduce the effort required for both the initial setup and ongoing management of mobile access—lowering the total cost of ownership for the long term.

In addition, Security Access Manager for Mobile integrates seamlessly with IBM Security Access Manager for Web for an end-to-end access management and application protection solution. Security Access Manager for Web provides a highly scalable reverse proxy that can be placed in front of web applications to centrally manage security threats. Plus, it offers single sign-on capabilities for web applications—so end users can authenticate once and then seamlessly access applications and services from outside the corporate network. Security Access Manager for Web also provides a web application firewall that can help protect applications from advanced web threats, such as SQL injection and cross-site scripting attacks.

Existing Security Access Manager for Web customers can link to the Security Access Manager for Mobile appliance with just a few clicks. The combination of both IBM solutions gives mobile enterprises an edge in securing user access and protecting applications from malicious traffic.

IBM Security Access Manager for Mobile	IBM Security Access Manager for Web
Mobile single sign-on and session management	Web single sign-on and session management
Context-based authorization with built-in OTPs, device fingerprinting, geo-location and IP reputation scores	Coarse-grained authentication
Mobile application access administration and self service	Highly scalable reverse proxy, web application protection (firewall)
IBM Worklight® integration for risk-based access enforcement	Policy enforcement for multi-factor authentication
IBM Security QRadar integration for security intelligence	QRadar integration for security intelligence
Available as a virtual appliance	Available as a virtual appliance

Conclusion

IBM Security access management solutions provide flexible authentication, policy management and access control services for today's increasingly complex mobile environments. Now you can more securely manage access to critical applications and data, while providing your users with fast, convenient access to the information they need. With user authentication and context-based access management for mobile devices, you can help prevent users from inadvertently exposing your sensitive IT assets to the latest security threats.

Instead of simply focusing on point solutions, IBM offers an entire portfolio of security products, thereby providing an integrated, holistic approach that can address the spectrum of information technology risk. IBM security solutions, such as Security Access Manager for Mobile, are designed to be easy to deploy and manage—delivering both a fast time to value and lower total cost of ownership over time. As a result, organizations can be confident that as more mobile devices are used for work, critical resources can be protected from attack.

For more information

To learn more about IBM Security Access Manager for Mobile, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security/

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
September 2013

[1] Michael Finneran, "2012 State of Mobile Security," *InformationWeek Reports*, May 2012. http://reports.informationweek.com/abstract/21/8792/

Please Recycle

WGW03036-USEN-00