

# Securing and protecting enterprise data on mobile devices

Use cases in mobile security



Securing and protecting enterprise data, especially in a mobile world, is a complex problem that can be easily solved. Organizations can enable greater use of mobile devices while keeping mission-critical data, applications and systems secure and protected.

## The elements of mobile security

### Endpoint security

All aspects of security that protect information on a physical device

### Information protection

All aspects of security that protect data that is on or leaving an enterprise device; includes end-to-end encryption, accidental data leakage and data controls

### Identity protection

All aspects of security that protect a user's identity; includes control measures such as conditional access and multifactor authentication

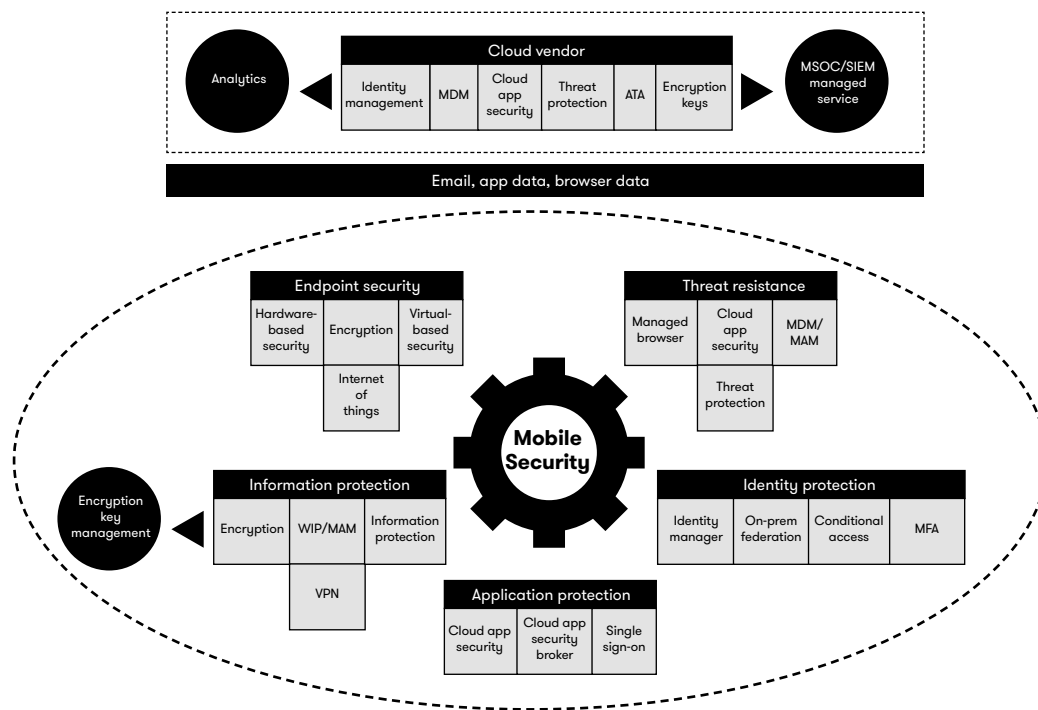
### Application protection

All aspects of security that help protect users and devices from rogue applications

### Threat protection

All aspects of security involved in alerting users to potential risks on their devices; can protect users by blocking access to corporate resources when a risk is identified

Here's a case study to suggest new ways your organization can implement mobile security and protection. It follows a fictional user through various scenarios and examines how organizations can address identity protection, information protection, application protection and threat resistance (**Figure 1**).



**Figure 1.** Components of mobile security

## Meet Bobby

Bobby has just started a new job, and his company has given him an iPhone, a Windows 10 laptop (with Office 365 for email) and an Android tablet. After being assigned a corporate username, Bobby has also set his password and enrolled his devices as part of the company's onboarding process.

As part of his enrollment, Bobby enters a security passcode for each device. These passcodes, set by his company, help secure the devices by ensuring that unauthorized users cannot gain access to either his devices or corporate data. To further protect Bobby's device data, his company enforces native encryption by pushing down mobile device management (MDM) security policies.

### How mobile device management works

“Data at rest” protection is achieved by pushing policies through the MDM provider. For Apple devices, encryption is enabled by default on iOS when a personal identification number (PIN) is set. Android devices, due to the large range of products, all with different security policies, need to be reviewed before approval. To achieve enterprise-grade protection with Windows 10, encryption should be enabled using BitLocker and Trusted Platform Module (TPM) configured in alignment with the BitLocker configuration settings.

When creating a device PIN, for greater security, consider using eight-digit codes that include both letters and numbers. Fingerprint and facial-recognition authentication are now becoming standard for enterprise authentication. They can also be part of a multifactor authentication program, following conditional access rules set by your mobile services provider.

Even with all this protection, sophisticated threats may still get in. To protect against this, install threat-protection software with a monitored service on all devices. If and when an attack is detected, this software will allow you to identify, alert and automatically lock down corporate devices.

### Use case: Identity protection

During enrollment, Bobby sets up email on his devices and is asked to download his assigned applications. Once these are installed, Bobby launches his email application and signs in with his corporate credentials. Instantly, Bobby has access to all the corporate resources he requires.

To ensure that only Bobby can use his devices to gain access to enterprise data, Bobby’s company uses an identity manager. His company can set up conditional access rules to further help protect its data. Access rules can help define the company’s perimeter, allowing access only to devices on a corporate network, or allowing only specific types of devices to connect. What’s more, if Bobby’s company detects suspicious activity on his account, it can revoke access at any time. The company can also integrate on-premises federation tools using Security Assertion Markup Language or SAML (an XML framework for authentication), or certificate-based logins for enterprise-level access to its on-premises applications.

A few weeks after joining the company, Bobby is asked to travel overseas for training. During his trip, Bobby loses a bag that contains his Windows 10 laptop. He reports the loss to IT, which immediately sends a wipe command to Bobby’s device, removing corporate data.

Bobby then uses his iPhone to check email. After entering his username and password, Bobby is prompted for a second authentication code rather than being logged right in. That’s because Bobby’s company has set multifactor authentication for uncommon login situations, which includes Bobby’s signing in from a different country.

A code is sent to Bobby’s phone and, after entering it, Bobby is up and running with very little hassle.

### How identity protection works

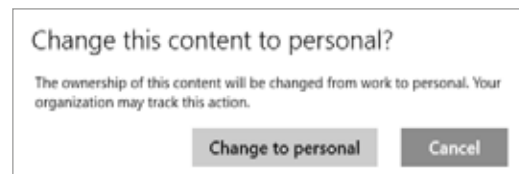
Identity management helps your organization provide application provisioning, self-service catalog, conditional access controls and single sign-on (SSO) for software as a service (SaaS), web, cloud and native mobile applications. It provides all users a single identity for their resources, with controls to allow the organization to monitor and revoke access as required. One important security feature consists of temporary admin accounts with expiration dates. This lets the company terminate an employee's device access after they leave the company.

To further protect corporate data, multifactor authentication and conditional access should be set up for all users. This involves a careful balancing act. On the one hand, you need to protect your data. But on the other, you don't want to hinder users.

Most companies will still use on-premises federation to integrate with Lightweight Directory Access Protocol (LDAP) for authentication. When considering authentication methods, examine whether to use emerging technologies, such as Microsoft's Azure Active Directory Pass-through Authentication, which can be configured to let users sign in to both on-premises and cloud-based applications with the same passwords.

### Use case: Information protection

Next, Bobby wants to ask his manager for a clarification regarding a possible new contract. He copies text from the contract, but before he can email it to his manager, Bobby gets distracted and steps away from his desk. On his return, he checks his personal Twitter account and, by mistake, tries to paste content into his feed, forgetting that he had previously copied a section of the contract. Now Bobby is presented with this message:



Realizing his mistake, Bobby clicks "Cancel" and returns to his application.

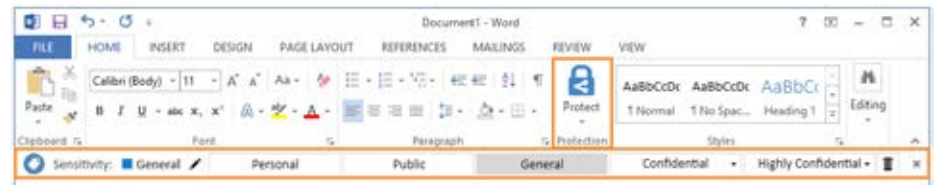
### How mobile application management works

Mobile application management (MAM) and Windows information policies set by your administrator can help prevent accidental data leakage by employees. To do this, your administrator will first need to identify which applications are trusted for work and which are for personal use only. The administrator will then set and enforce policies to prevent any accidental interaction between the two.

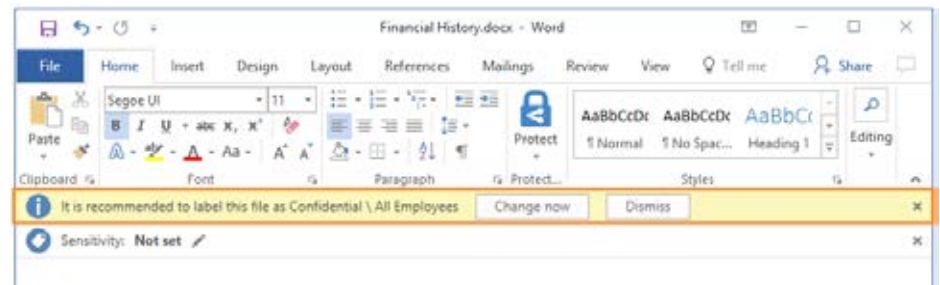
MAM access control policies can also protect against accidental data leakage. They do this by segregating corporate and personal resources, and enforcing rules that prohibit interaction between them.

MAM policies can also be effective for "bring your own device" (BYOD) implementations, segregating corporate and personal data on users' personal devices. For example, Google Android allows this.

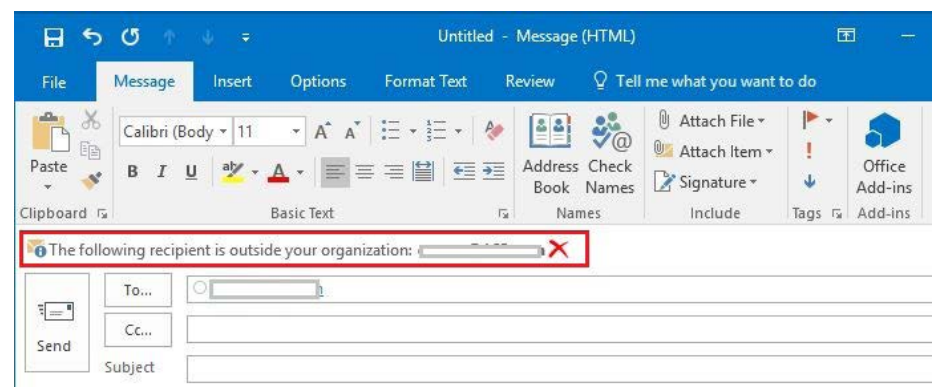
Next, Bobby pastes the contract content into an email. During Bobby's training, he learned how he can protect his company by classifying his email and applying data protection (encryption) if necessary. Bobby looks at his options and classifies the document as "General":



As the email contains sensitive information, it triggers a policy that prompts Bobby to change the label to "Confidential," which he does.



Next, Bobby enters his manager's email address, but mistypes it. His email app automatically detects the personal email account of a friend with similar name. Because the message has already been marked "Confidential," Bobby is presented with a new message:



Bobby corrects his typing error and this time sends the confidential email to the correct email address.

Since Bobby's organization had configured policies to help users classify and protect sensitive information, if one of these prompts had been ignored, the transaction would have been logged in Azure, where administrators could have reviewed the record and, if necessary, taken action.

### How classification and encryption work

Information protection helps classify, label and protect documents and emails. Built-in functionality helps protect company data by guiding the user to correctly classify and protect sensitive information. The protection remains a part of the content, regardless of where it lives during its life cycle. This provides greater control over corporate data by enabling administrators to track where data resides, govern who can access the content, and even revoke data if they believe it's being accessed by an unauthorized user.

Protecting your information at the file level is a real enabler for companies. Not only can they comply with regulations concerning data control, but they can also safely collaborate with external partners and users. For example, companies can send encrypted email from Mobile Outlook to third-party mail providers such as Gmail, safe in the knowledge that the user will be able to view the content easily, but control stays with the sender. The user can download the content to their local storage or to a USB drive, but the file still maintains its encryption and information protection access controls, allowing the sender to revoke the file at any time, regardless of where it lives.

### Use case: Application protection

A few months later, Bobby has taken on new responsibilities and requires access to a broader range of applications. When Bobby logs into his device now, he sees many more apps than he did before. And because his company has configured SSO, Bobby can launch these applications and get instant access to the content.

Bobby can also copy and paste among his corporate applications, increasing his productivity. A safety feature prevents him from mistakenly copying to noncorporate applications.

### How application protection works

Cloud Application Security (CAS) and Windows Defender Application Control (WDAC) can be used to whitelist web and device applications, respectively.

CAS allows for real-time analysis of applications, giving administrators the power to act before harm can be done, and can detect nonsanctioned use of SaaS applications. It can also monitor and control data in the cloud, providing visibility and enforcing data-loss protection policies. Finally, CAS can detect anomalous uses and security incidents, use behavioral analytics and advanced investigation tools to mitigate risk, and set policies and alerts to achieve maximum control over cloud-oriented traffic.

WDAC can prevent users from installing unapproved apps. MAM/Windows Information Protection (WIP) policies help further protect apps and associated data.

### Use case: Threat resistance

One evening Bobby brings his corporate devices home, and his young daughter asks whether she can watch YouTube on the Windows 10 laptop. Bobby unlocks the device, launches the browser and goes to YouTube. Later, when Bobby comes back to check on his daughter's progress, he sees a message saying that she does not have

permission to download a certain application. Bobby's child had clicked on a link to download an application, but was unable to do so because of application control policies configured by Bobby's company.

In the meantime, Bobby hands his child his iPhone to watch the video while he looks at what the child has done. Later, when Bobby picks up his Apple device, he sees a threat protection alert notifying him that an application on his device is not safe, and that he needs to remove the app before he can regain access to his corporate data.

Threat protection can detect a bad app and immediately prohibit all traffic (blackholing) from the rogue app, simultaneously notifying the mobile endpoint security console administrator.

On another evening, Bobby's home network is down, so he visits an internet café. He sees that two connections are listed: "Café Wi-Fi" and "Café de Wi-Fi." One is legitimate, but the other is a malicious signal set up by a hacker with the intent of capturing user credentials, keystrokes, data transfers and other sensitive data — all without the user's knowledge.

Bobby receives an alert from his threat protection service notifying him of the unsafe network and recommending that he disconnect from the service. This happens before any of Bobby's user information can be compromised.

Still later, Bobby receives what appears to be an email message from PayPal. But when he clicks on an embedded link in the message, it tries to connect him to a rogue service. Threat protection alerts Bobby, blocks his access to the site and alerts the network administrator of the threat.

### **How threat resistance works**

To stay safe, users need secure identities and measures that protect their devices from being compromised. This is especially important as attacks grow more sophisticated, with hackers using applications, web browsers, WiFi networks and more to illegally gain access to device data.

MAM/WIP policies can protect from user error; information protection can protect data at its source; and identity management can protect identities. But without the additional security of threat protection, all these efforts can be in vain.

Windows Defender is a native antivirus option built into Windows 10. Allowing it to send data to the Microsoft cloud further enhances security. It empowers Microsoft to view potential threats on your organization's devices and to compare them against a database of known threat signatures.

On iOS and Android devices, organizations should use mobile endpoint threat-protection software. This will protect against risks based on apps, networks and devices. A user whose device supports threat protection will be alerted of any malicious compromise. While threat protection doesn't replace an encryption service, it does help to ensure the integrity of those related services.

Other tools — such as managed browsers, Windows Defender application control and intrusion detection — can help lock down devices and block access to nonapproved resources.

## **How DXC can help**

DXC Technology offers a wide range of mature offerings to help your organization secure its mobile devices, vital data and mission-critical systems. DXC's Workplace and Mobility professionals worldwide offer vendor-agnostic advice, integration services, and around-the-clock management and monitoring.

Your organization can turn to DXC's mobility security for help with threat protection, information protection, multifactor authentication, identity management, device encryption, VPNs, cloud access security and much more.

Learn how DXC can help you secure your mobile devices and data today at [www.dxc.technology/workplace\\_and\\_mobility](http://www.dxc.technology/workplace_and_mobility).

## **About DXC**

A market leader in advanced digital workplace services, DXC provides enterprises with a more consumer-like, digital workplace experience to attract, delight, engage and retain employees. Together, DXC and our network of strategic and solution partners enable new ways of working, communicating and collaborating to increase productivity and drive profitability. Our solutions support millions of desktops and mobile devices for ~1,100 customers in 67 countries.

**Learn more at  
[www.dxc.technology/  
workplace\\_and\\_mobility](http://www.dxc.technology/workplace_and_mobility)**

### **About DXC Technology**

DXC Technology (DXC: NYSE) is the world's leading independent, end-to-end IT services company, serving nearly 6,000 private and public-sector clients from a diverse array of industries across 70 countries. The company's technology independence, global talent and extensive partner network deliver transformative digital offerings and solutions that help clients harness the power of innovation to thrive on change. DXC Technology is recognized among the best corporate citizens globally. For more information, visit [www.dxc.technology](http://www.dxc.technology).