Guidance

BYOD Guidance: Device Security Considerations

Published

Contents

The End User Devices (EUD) Security Framework describes 12 areas of security controls for end user devices. The same framework can also be applied to Bring Your Own Device (BYOD) products.

In these security considerations, each of the 12 areas has been considered in the context of deploying BYOD. It should be read alongside the EUD Security Framework . In general, as an organisation relinquishes its management of an EUD, the technical risks to the device and the data on it increase. This increase in risk is usually due to an increase in the likelihood of an opportunity presenting itself to an attacker. If sensible precautions are taken, the impact of compromise of an unmanaged device will be similar to the impact that the same compromise would have on a managed device.

1. Assured data-in-transit protection

Whilst a correctly configured, corporately owned and managed EUD will rely on a secured VPN connection to protect data-in-transit, a personally owned device cannot necessarily rely on such a connection. Consequently the security of data-in-transit will need to be provided by the BYOD product.

The connection from remote devices to your organisation will likely be via untrusted networks such as 3G/4G and/or Wi-Fi. This means that the confidentiality of data transiting those networks needs to be protected, but also the integrity and authenticity of that data to prevent attacks being made on the data and corporate network.

To prevent against this type of attack, data should always be encrypted in transit between the mobile device and your corporate endpoint, and should subsequently be checked at the corporate boundary for potential attacks from the device onto your corporate network. These attacks could be from a man-in-the-middle (MITM) or malicious code running on the personally owned device.

If you want to implement data-in-transit protection you should consider using one of the following mechanisms:

- an IPsec VPN established between software on the device and a gateway within the organisation
- an SSL/TLS VPN established between software on the device and a gateway within the organisation
- an HTTPS (TLS) session between the BYOD product and the application gateway within the organisation

Risk owners should be aware of the difference in risk that is inherent in these options. For more information refer to the Architectural Approaches guidance. In addition, the product guidance for BYOD indicates what options are provided by that platform to meet these requirements. Decisions can then be made on which product(s) are most suitable to your particular business needs and security requirements.

2. Assured data-at-rest protection

Data stored on an EUD needs to be protected against online and offline attacks when in its ‘rest’ state. For most EUDs, this will be ‘powered on but locked’. Data may also be stored at rest in cloud services, either as part of another third party application on the device, or as part of a device backup service provided by the device vendor.

In a BYOD scenario where work and private data may coexist on the same device, protection of data-at-rest has the following additional complexities.

2.1 Corporate and user data separation

The device now handles two types of data, one owned and managed in accordance with corporate policies and procedures, and one owned and managed by the end user. How is separation maintained and managed on the device? If the user picks a weak passcode for their own data, how does this affect the security of the corporate data?

2.2 Unintended application activity

Some applications installed by the user for individual use have the potential to automatically share data held on or accessed by the device. Social networking applications may share contacts or calendar information. Cloud storage applications may share files as part of a synchronisation process.

2.3 Cloud storage and local backup

Many devices now feature automatic backup services, either to a cloud service or local backup solution. This poses another challenge for the control of corporate data on personally owned devices, as data which formerly existed in a single place may now exist in several locations. An attacker who obtains encrypted data may be able to perform an offline brute-force attack on it to recover the original data.

Some devices configure automatic backups to cloud storage when the device is first set up, and the user does not have to think about it again until they want to restore their data. The methods that different cloud services use to protect user data vary enormously; some cloud services may encrypt all of their users' data so it is inaccessible to the service provider and also, therefore, attackers. Others may store it in a more accessible way in order to provide additional services such as searching. However, this also enables some third parties to access that data.

If data is copied to a cloud service, the organisation will have even less control over it compared to being stored on the user's device. If the cloud storage account is shared with others, then other people may have access to your corporate data.

Cloud services have variable levels of security and can provide attackers with alternative ways to access your data. For more information on the secure use of cloud services, refer to our Cloud Security Principles.

2.4 You are still responsible

The published advice on BYOD from the Information Commissioner's Office states that an organisation must take appropriate measures to protect personal information, regardless of where it is stored. Should any such data leak from a personally owned device then you will be held responsible.

2.5 Reputational damage and legal non-compliance

In the event of a Subject Access Request or Freedom of Information Request there is a danger that data backed up by your users may no longer be under the control of the organisation and may come to light at a later date. This places the organisation at risk of reputational damage and legal or regulatory non-compliance.

3. Authentication

The EUD Security Framework describes three types of authentication that are important to consider:

- user to device: the user is only granted access to the device after successfully authenticating to it
- device to service: only devices which can authenticate to the enterprise are granted access
- user to service: the user is only able to access corporate network services after successfully authenticating to the service, via their device

When developing an approach to BYOD, you need to consider these three stages of authentication. In some cases, 'device' in this context may actually only be a subset of the device, or an application running on the device. If a user only requires a weak passcode, or no passcode, to access the device, but then accesses data through a container application or bootable media, then that product needs to authenticate the user with appropriately strong authentication before permitting access to data.

3.1 User to device

For user to device, the user is only granted access to the device and its data after successfully authenticating to the device. There may be a second level of authentication required to access a container application on the device. When developing a BYOD approach, organisations should consider what requirements to set for both

the device passcode and application passcode if applicable. In some cases the container application may share data with the host platform (for example contacts or lock-screen notifications), so organisations should consider both steps of the authentication process.

3.2 Device to service

Device to service authentication can present some challenges in a BYOD context, as users may want to use a variety of devices to access corporate network services. However, the organisation may wish to limit access to only those devices which have been approved. To strike a balance, consider the use of certificates or other authentication methods which explicitly identify devices that have been allowed to connect to the organisation. This prevents users from connecting any device to the infrastructure using their existing credentials.

3.3 User to service

For user to service, the user is only able to access enterprise services after successfully authenticating to the service, via their device. The authentication can be at the corporate boundary as part of VPN access, or additionally for each application enabled for the BYOD community.

4. Secure boot

In the context of BYOD, achieving secure boot requires support from the underlying platform. The devices used should be up to date and patched in order to mitigate vulnerabilities. Organisations may require users to adopt certain behaviours, which include regularly patching their device, and/or configuring certain features.

It is unlikely that a BYOD product will be able to alter these settings automatically, but it may be able to read the settings to be verified and monitored for compliance remotely via mobile device management (MDM). For example, an application may be able to check what Wi-Fi network is being used or if a device passcode is set, but it will probably be unable to change the Wi-Fi settings, or device passcode itself.

Some products may attempt to detect jailbreaking or rooting. Administrators should enable jailbreak detection and configure it to wipe application data if possible, but must understand that it can be defeated by malware.

5. Platform integrity and application sandboxing

Any security features which are offered by a BYOD product will fundamentally depend on the integrity of the underlying device, and its ability to enforce separation between the BYOD product and any other code running on the system.

Organisations should use a number of procedural and technical controls to ensure only ‘clean’ devices with strong device integrity features are used, such as:

- Take measures to ensure devices are free from malware when initially provisioned, for example by restoring to factory defaults prior to allowing access to enterprise resources. Assume that a percentage of devices will be infected with malware. The malware may not be targeting the organisation itself, but the organisation’s data may end up being compromised as a result.
- Use products which try to detect jailbreaking. Devices which are rooted or jailbroken may be more easily

subverted by malware than unmodified devices. This may either be because the jailbreak itself is malicious, or by a subsequent attack on the device which now has fewer security features enabled. However, jailbreak checks rely on the integrity of the underlying platform which may be compromised by the jailbreak software itself, so some caution should be taken when using these tools.
- Consider carefully which devices users are allowed:
  - What devices and versions of operating systems are you going to support? What security features do they need to have?
  - How will you keep your solution up to date? Remember users will update their devices as new versions of the operating system are released, or as their network contract ends. You cannot plan your support on a traditional corporate upgrade cycle.
  - If a user's device has been modified, how will you inform them, and what support are you willing to provide? If they can no longer use their personally owned device, is there an alternative means of access to enable them to continue to work?

6. Application whitelisting

For EUDs, application whitelisting is about:

- allowing only approved applications to access corporate data
- limiting attacks against the security boundaries around the enterprise data

In a BYOD scenario, application whitelisting is equally important:

- applications running 'inside' the BYOD product, if supported, will be permitted access to the enterprise data stored and processed by that product
- applications running 'outside' the BYOD product may be able to attack the product, or leak data from shared resources (for example contacts)

It is important to consider limiting which applications can coexist with sensitive data. Unless the organisation is going to take total management control, there will be limits to how effective this approach can be. If the user retains overall management control you have no way to restrict what they can install or uninstall in terms of applications and settings.

While some environments have an inbuilt whitelisting capability, this is usually tied to the manufacturer's application store. To support an organisation-specific whitelist, an MDM solution or an enterprise application store will probably need to be considered.

The risks associated with third party applications to an organisation considering BYOD can be broken down as:

- unless an organisation has total management control of the device, the user can bypass any whitelists
- if your MDM or similar capability does not include jailbreak detection there is an ongoing risk that users will be able to install local apps with no control (though note that jailbreak detection can be bypassed)
- if your application whitelisting controls are too strict there is a risk of frustrating your staff by restricting how they can use their device
- the impact on your support organisation needs to be considered; as users upgrade their devices, expect services to be disrupted and to have to update the corporate infrastructure and software versions in the whitelist

As part of your approach to personally owned devices or BYOD you need to consider:

- the use of an MDM system to control what is loaded on to the device and to supplement any inbuilt controls
- introducing an enterprise app store to allow your organisation to review third party applications before they are installed on the device alongside having the ability to deploy apps created in-house

7. Malicious code detection and prevention

As with secure boot, and several other recommendations, this recommendation relies on the security of underlying platform. Having a host platform (hardware, and usually software) which is robust to attack from malicious code is imperative in maintaining the security of the data stored on it, both inside and outside any BYOD product. Even the best BYOD products cannot be secure when running on a compromised platform.

As such, organisations may wish to consider which devices they permit their users to use in a BYOD scenario. Up to date, well maintained and patched devices are clearly preferable to devices which do not regularly get updated. Most BYOD products will allow organisations to limit connections to only approved devices, and this option should be used where possible. Further guidance explaining how various platforms defend against malicious code can be found in the End User Devices Guidance.

8. Security policy enforcement

When deploying corporately owned EUDs, organisations typically have full control over those devices and can enforce technical security controls on the device to minimise their exposure to risk. Where a BYOD approach is used, the organisation will have much less control (or no control at all) of those devices.

An organisation will therefore need to use a balance of technical and procedural controls to achieve the security posture necessary for their business. This can be supported by robust event collection and incident response procedures.

When deploying a BYOD model, organisations should:

- ensure user education programmes are in place, and users' responsibilities are clear
- generate acceptable-use policies and security operating procedures for users' devices
- put processes in place for auditing users' behaviour (ie trust and verify)

The End User Devices Guidance can be used as an example of policies to apply in BYOD scenarios, but many will need to be enforced procedurally instead of technically in a BYOD approach.

9. External interface protection

On EUDs, there is a large variation in what can be accessed by an attacker with physical access. This varies from very little that can be obtained without the attacker knowing the device passcode, up to full device memory access on some other devices. In the latter scenario, an attacker would be able to access all the data being stored and processed on the device.

If the user were to synchronise their device with another system (for example their home PC), then some data could be backed up to that location, or malware on that system could begin to attack the EUD. This is essentially how most jailbreaks work, so care should be taken when connecting devices to untrusted

computers.

An MDM solution may offer controls for a particular hardware and software configuration, but the device owner will normally have the option to override this at the local level. Interfaces to consider include USB, Wi-Fi, Ethernet, Bluetooth, FireWire and NFC (Near Field Communication).

10. Device update policy

When devices are owned and managed by a third party, that third party is typically responsible for applying security patches and updates once made available by the manufacturer and/or carriers. These updates may be critical to the security of the whole system, but the organisation will be unable to guarantee that these patches/updates are applied promptly, if at all. This leaves a device vulnerable to compromise.

In some cases, the host platform may no longer be supported by the vendor, potentially leaving the device vulnerable to attack. Organisations may wish to limit connections from host platforms which have not been updated recently.

From a business perspective, users may update faster than the organisation can tolerate. If internal applications and services are only tested against a certain subset of BYOD versions, and the user advances past those versions, then applications may break. Organisations should anticipate some increased support costs from this.

11. Event collection for enterprise analysis

In EUDs, event collection by an organisation allows them to monitor logs for attacks, security breaches, and suspicious user behaviour. In a BYOD scenario, some of the logs may not be available to the enterprise, so some malicious activity could be undetected.

Some events collected only from a container may still affect employee privacy, for example, location data, roaming connectivity and Wi-Fi details. The organisation should consider whether these details need to be collected for business purposes. If so, they cannot necessarily be distinguished from private location data.

The organisation should develop ‘user scenarios of security concern’ that their events data collection should be geared towards detecting. These may include:

- unauthorised access or download of corporate information to the device
- unauthorised saving of corporate data to non-corporate containers
- jailbreaking
- inappropriate use of corporate email or web browsing
- use of corporate functions and data by unauthorised personnel

MDM and events data collection should enable the detection of these scenarios.

12. Incident response

When allowing employees to work remotely, it is important to be able to respond to security incidents and understand their impact. In a BYOD scenario, this can prove to be especially challenging as the examples

below illustrate.

12.1 Limited access to devices for incident response

When dealing with a security notification, for example a published vulnerability in a platform being exploited in the wild, it is imperative to be able to know which device hardware and software versions are on an organisation's corporate network. This allows the organisation to assess the potential damage that the vulnerability may cause, and take remedial action appropriate to their scenario. In a network where there are a wide variety of devices at different versions and patch levels, this can be especially challenging.

12.2 Incident reporting

When configured for BYOD, it may not be obvious to the user that they need to report a missing personally owned device to their employer. Clear procedures detailing the reporting of lost, stolen or otherwise compromised devices should be given to users so that a remote wipe command can be sent either to the BYOD product or to the entire device to remove any corporate data.

12.3 Inability to fully wipe a lost device

Some solutions for BYOD may only allow the corporate section of the device, or a specific application, to be remotely erased. This means that if some enterprise data has been inadvertently written to another area of the device, then this data will not be deleted when the organisation wipes the corporate data. This would give an attacker the opportunity to recover corporate data should they subsequently steal (or otherwise compromise) a user's device.

12.4 Renew device

For personally owned devices, renewal and change is under user control. Whilst this is not strictly an incident, a process must be established with the users if exposure to corporate data is to be prevented. This could involve similar processes to those used for incident management.

Legal information