GOV.UK

Guidance

BYOD Guidance: Architectural Approaches

Published

Contents

This guidance contains examples of common BYOD scenarios that an organisation may face when using personally owned devices to access enterprise services and data, and highlights risks associated with each scenario. Organisations may wish to consider which of the examples best matches their business, cost, and security requirements (and also consider other architectures) before committing to any particular one.

1. Service separation

One of the fundamental ways of reducing the risk of compromise of sensitive business data is to not expose it to threats. This can be achieved by separating sensitive business data within your corporate services, and not allowing personally owned devices access to it.

However, reorganising your corporate data to facilitate this approach can require substantial and costly changes to your corporate infrastructure and business processes. Whilst there are challenges applying this approach for existing infrastructure, it is worth considering when designing new services and data repositories that you may want to expose to personally owned devices.

The benefits of service separation include:

- preventing exposure of sensitive business data to personally owned devices
- reducing the restrictions and configuration needed on personally owned devices
- reducing the amount of data loss

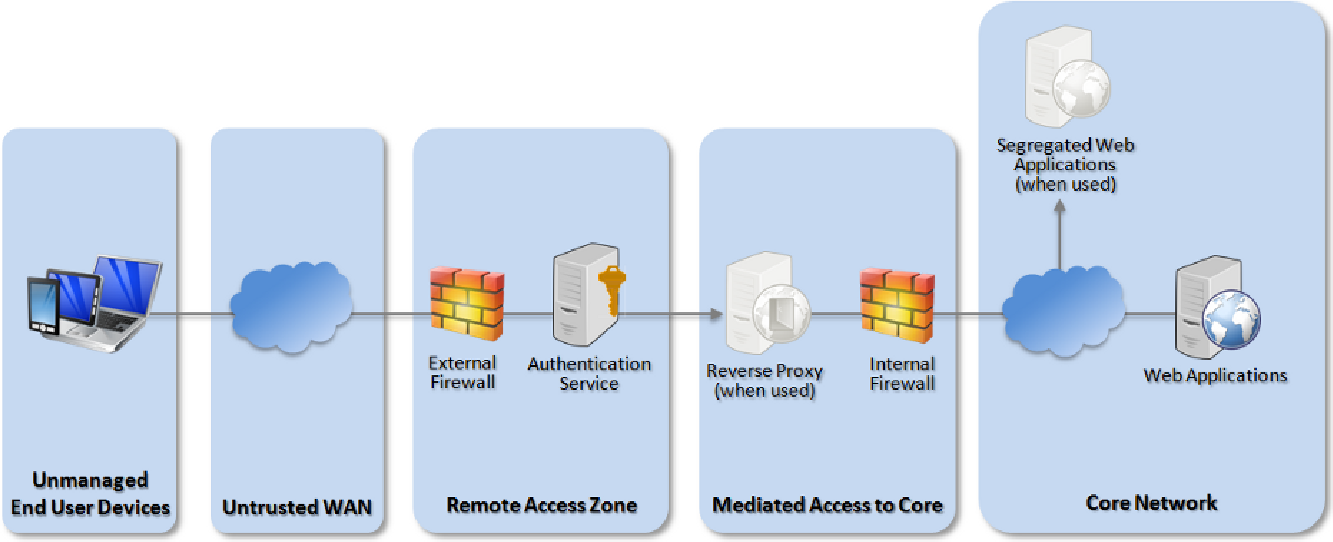
1.1 Network zones

One method of providing such separation would be to split services into separate network zones based on their desired exposure to personally owned devices. Exposed applications would be made accessible via URLs and IP addresses that are not shared with any services containing data not for consumption on personally owned devices. This would allow the internal firewall and network-level controls to be more effective.

The following scenarios provide ways of helping to manage the risk of compromise of your sensitive business data. There is no reason why they cannot be used in conjunction with the above service separation approach.

2. Scenario 1: Exposing internal web applications

Assuming a user is authenticated and connects over a secure tunnel to the remote access zone, the user will browse to the URL of an exposed web application.



Network architecture for personally owned devices to access intranet web services

2.1 Key risks

The key risks to consider with this scenario are:

- if a single web browser instance can access both intranet and internet websites, then a malicious website may be able to attack and/or access data from poorly protected internal sites
- the cache (temporarily stored offline data) of a native web browser may not be protected; other applications or physical attackers may be able to retrieve sensitive data from the cache
- access to internal web services from personally owned devices may allow malware stored on the device to be imported into the network

2.2 Endpoint options

Native web browser

All mobile platforms will feature a native web browser which can be used to browse internet websites. This native web browser can also connect (for example by a VPN) into the corporate network to access internal web services. However, this directly exposes the corporate internal web services to attacks from malicious internet websites using the browser as a conduit.

This can result in exposure of the whole corporate infrastructure and connected partners relying solely on the existing internal corporate security mechanisms for protection.

The risks posed by this option can be mitigated by use of a reverse proxy and service separation at both the application and network level.

BYOD product web browser

This option proposes using two separate web browsers on the personally owned device, the native web browser for the user’s private internet access and a browser within a BYOD product exclusively for accessing internal corporate web services.

The result is a significant reduction in the risk of malicious websites using the browser as a conduit for attack. Attacks such as cross-site request forgery and cross-site scripting are mitigated.

Due to the separation of functionality within the personally owned device that this option provides, attacks which compromise the native web browser will not leak contents of potentially sensitive internal corporate web applications.

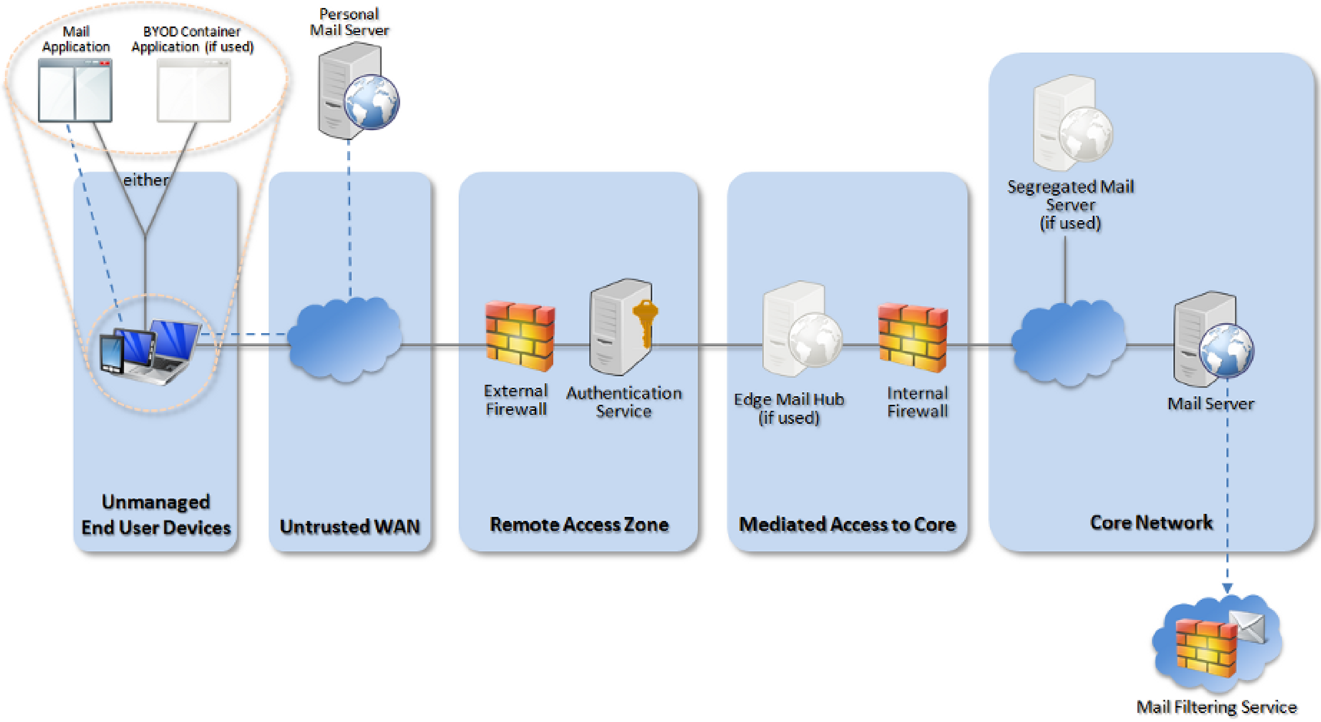
2.3 Infrastructure options

The reverse proxy adds a layer of separation between the personally owned device and internal web services. This prevents the user’s browser on the personally owned device from directly interacting with the internal web application. Instead they connect via the reverse proxy, which interacts with the internal web application on the user’s behalf.

This provides a second layer of authentication to services. When combined with application-specific protective monitoring solutions, this can be an effective way of reducing the risk of attacks on corporate infrastructure from compromised devices and malicious internet websites.

3. Scenario 2: Exposing email, calendar and contacts

Note that if users are accessing corporate email through webmail, refer to scenario 1.



Network architecture for personally owned devices to access email

3.1 Key risks

The key risk to consider with this scenario is that devices which can send and receive email from two accounts may be able to bridge those accounts, thereby:

- allowing corporate data to be sent via personal accounts, bypassing any outgoing email filtering or logging in place
- allowing malicious code to transit from the personal account to the corporate one, exposing other internal corporate users and external corporate partners to malware
- inadvertently allowing devices to synchronise inappropriate data from personally owned devices onto corporate systems, potentially exposing the organisation to legal issues
- allowing the exposure of sensitive corporate email, calendar and contact data to other personal applications, cloud-based storage and backup facilities.

3.2 Endpoint options

Shared native applications

By using one application on a personally owned device to access both personal and corporate data, the risk of data transiting from the corporate account to the personal account is high, unless managed appropriately using technical controls within that application to enforce the separation of those accounts.

Disadvantages of this approach include:

- it may be difficult to recover from a device loss or compromise without removing private data
- personal backup services may back up both business and private data
- business and private contact data may be merged
- data sharing applications may have access to business data
- there is a greater risk of malicious email entering the business environment
- enrolling the device onto MDM may be required in order to manage the native applications

On some platforms, MDM can be used to configure a single email application to control a corporate account whilst allowing a personal account to be configured separately by the user.

If suitable management features exist (eg through MDM), then this separation can be enforced, preventing business emails from being copied into the personal account and vice versa. If such features do not exist, then this will need to be procedurally managed through user security procedures which prohibit forwarding emails between accounts.

Business data is accessed through a separate email/calendar client

In this case, a separate email and calendar client is used for accessing the corporate account. This reduces the risk of the user accidentally transferring data between accounts or sending data from the wrong account. The separation of the personal and corporate accounts into different applications could be procedurally enforced. However this will not mitigate the risk from a malicious user, or a malicious application on the personally owned device.

The disadvantages of this approach are similar to the previous option, but with the added benefits that:

- users are less likely to accidentally transfer data between corporate and personal accounts
- MDM is not required

Business data is accessed exclusively through a BYOD product

This option also uses separate email, calendar and contact applications on the personally owned device exclusively for accessing internal corporate services, but also suggests embedding them within a BYOD product.

The result is applications on the device (including the personal email application) are unable to access the corporate data on the personally owned device. The corporate data is only accessible when the user launches the BYOD product, and this product handles the secure connection to the enterprise and limits data transfer between it and the underlying unmanaged platform.

Due to the separation of functionality within the personally owned device that this option provides, attacks which compromise the native email and calendar applications will not leak contents of potentially-sensitive internal corporate email and calendar applications.

Disadvantages of this approach include:

- it’s necessary to license a BYOD product to perform this function
- the enterprise network will likely require configuration changes to set up the BYOD product

3.3 Infrastructure options

Service mediation

When exposing internal email systems to personally owned devices, there should be a service mediation zone which:

- authenticates credentials to provide access to authorised users
- filters email access to accounts authorised to use personally owned devices
- collects audit and monitoring data for successful and unsuccessful requests

The wider email solution should check for malicious email content and ensure that there is no internal routing of email between mailboxes; all email should be routed as external email would be via an email filtering service.

An edge email hub can be used in the service mediation layer to expose emails to personally owned devices in a controlled manner. Accounts which are permitted to be accessed in this way are provided access to an edge hub, which can access the core network's email service and replicate content out to the devices.

This approach reduces the risk of inappropriate accounts being accessed from devices which aren't approved to store and process that data.

Email labelling

Labelling can also help manage which emails are appropriate to be exposed to personally owned devices. Email routing and synchronisation decisions can made based on the label applied to the email. When used correctly, labelling can reduce the risk of accidental data leaks.

Legal information

CESG: This guidance is issued by CESG, the UK's National Technical Authority on Information Assurance. One of the roles of CESG is to provide advice to UK government entities and organisations providing services to UK government. The guidance found here is provided and intended for use by this audience. It is provided 'as-is' as an example of how specific requirements could be met. It should be used to help inform risk management decisions on the use of the products described, but it should not be used for procurement decisions; it is not intended to be exhaustive, it does not act as an endorsement of any particular product or technology, and it is not tailored to individual needs. It is not a replacement for independent, specialist advice. Users should ensure that they take appropriate technical and legal advice in using this and other guidance published by CESG. This guidance is provided without any warranty of any kind, whether express or implied. It is provided without any representation as to the accuracy, completeness, integrity, content, quality, or fitness for purpose of all or any part of it. CESG cannot, then, accept any liability whatsoever for any loss or damage suffered or any costs incurred by any person as a result of, or arising from, either the disclosure of this guidance to you, or your subsequent use of it. This guidance is UK Crown Copyright. All Rights Reserved.

CPNI: Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.