Guidance

BYOD Guidance: Enterprise Considerations

Published

Contents

The threat model for end user devices (EUDs) assumes that devices are fully managed by the organisation that is using them, essentially meaning that the devices are an extension of their corporate network.

In the case of BYOD and unmanaged devices, this assumption does not hold true. Devices may be infected with malware, or could otherwise be more hostile towards the corporate network. This means care needs to be taken to protect internal services from attack from personally owned devices. This guidance highlights the steps that can be taken to reduce the risk of compromise in this way.

This guidance is supplementary to the Device Security Considerations, and is supported by the Architectural Approaches guidance which contains a collection of scenarios for deploying network components to provide services to unmanaged devices.

1. Network architecture

1.1 Key principles

Ideally, defensive network architectures should be used, which means:

- access from personally owned devices is brokered via a service mediation layer
- protective monitoring solutions are used to try and detect attacks from compromised devices

To prevent devices from accessing data they are not permitted to, network separation should be used within the organisation's networks. We recommend:

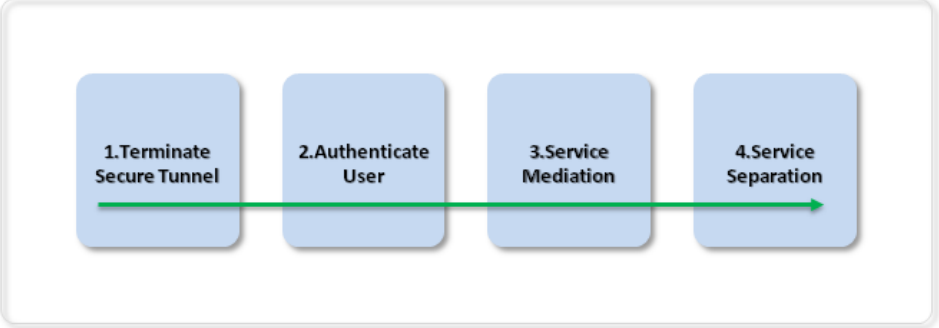
- where possible, technical controls should be used to prevent users from accessing data they are not permitted to access from personally owned devices
- services holding data not intended for consumption by personally owned devices should not be reachable from those devices

- where only a subset of data is required on the device, or read-only access is required, these policies should be enforced using the reverse proxy to filter requests
- user accounts in use by personally owned devices should be distinct from accounts used on corporately owned devices (including corporate desktops); passcodes must not be shared between accounts

1.2 Recommendations

The high level network architectures presented here build around a walled garden architecture. Worked examples of how to apply these architectures to particular services is given in the Architectural Approaches guidance.

Conceptually, any solution built to provide access to internal services from personally owned devices, should perform the four steps described below.

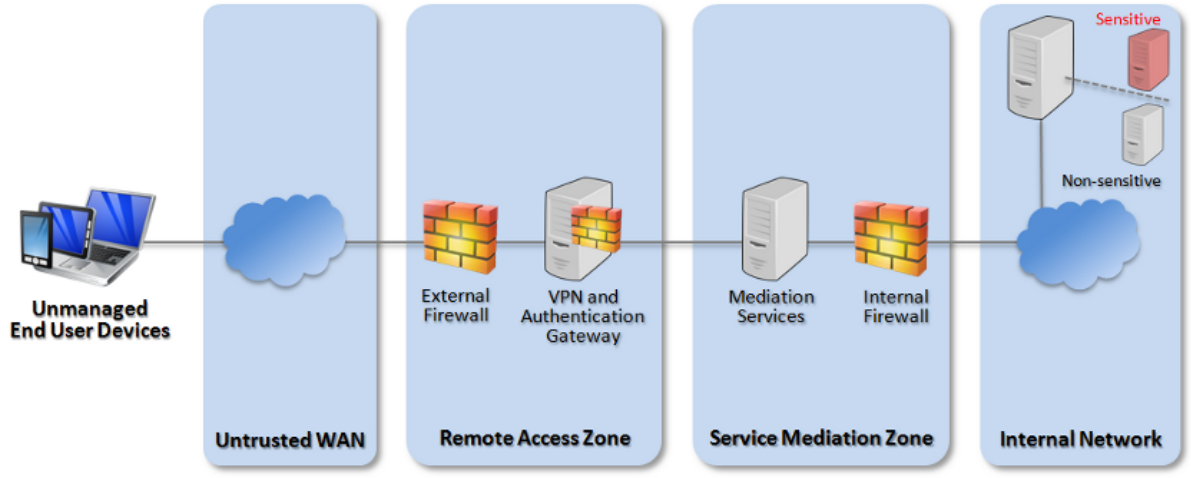


BYOD conceptual view

1. A secure tunnel provided by the device operating system or BYOD product terminates the encrypted session between the personally owned device and the corporate network boundary.
2. The user is authenticated to the corporate network, allowing the subsequent layers to provide access to only the data which that user is permitted to view on their device.
3. Access to internal services is brokered through a service mediation layer, such as a reverse proxy. These restrict access to only services permitted to be accessed from personally owned devices, and may in addition filter those requests. For example an application firewall may be able to limit the requests to be read-only, or for a particular subset of the data. Protective monitoring solutions can be added here to try to detect attempts to exploit services, or subvert technical controls.

4. Within the core network, services are logically separated to ensure that only specifically whitelisted services which do not contain sensitive data are exposed. The organisation needs to consider what internal applications will be made available to personally owned devices as this will not always be the same as for corporately owned devices.

An example of how to apply these principles using the walled garden architecture is shown below.



BYOD walled garden architecture

To use the services:

1. Remote users connect to the corporate network over a cryptographically secure tunnel.
2. The secure tunnel is terminated in a remote access zone at the edge of the corporate network.
3. Users are authenticated with their device passcode together with credentials held encrypted on their device when establishing the secure tunnel. This ensures user to device, device to service and user to service authentication steps have all occurred.
4. Each internal service exposed to remote users through this gateway needs to be subject to some mediation, the nature of which is dependent on the service.
5. Internal services are logically or physically separated when accessed by personally owned devices versus corporately owned devices. Either is acceptable, though physical separation further reduces the risks of data leaking from that service to the personally owned device.

2. Mobile device management (MDM)

MDM is a range of products and services used to monitor, manage and secure a range of mobile devices. It can also deploy applications and software updates to those devices. They usually comprise of an server and a client component.

The use of MDM does not imply that the device is trustworthy for the following reasons:

- The client on the mobile device is reporting values that imply a secure configuration, but these are not being implemented; this could be either because the device is incapable of performing them, or because malware is present and is subverting the response.
- The device has other management authorities which can override the settings being deployed such as a mobile operator, the handset manufacturer or the device owner.
- The MDM client on a device is not an integral part of the platform, and does not have the ability to enforce various settings.

These are particularly relevant in the case of personally owned devices, because the device may already contain malware when connected to the corporateand it is likely to have other management authorities in place.

An MDM solution can be run in-house, or purchased as a service. If purchased as a service then implicit trust is placed in the supplier. Organisations should consider the risk of the supplier having access to their information and networks that use of an MDM service would enable. For further information and guidance assessing the risks of using cloud service providers, see the Cloud Security Guidance.

As with all technical security controls, organisations should seek confidence that their MDM service has been implemented securely, is properly managed and maintained in accordance with internal policies.

Legal information

make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.