

Securing Legacy Systems

Legacy Systems

Securing Legacy Systems

Legacy Systems

- There is a clear general process for evolving legacy systems and clear evolution options can be considered.
- We will consider some examples of legacy systems, in terms of those connected to the Internet and not connected to the Internet.
- We will also consider a bump-in-the-wire (BITW) solution for addressing some of the concerns with legacy systems.

Process

Securing Legacy Systems

- Create an **inventory** of the legacy systems that exist within the enterprise.
- Prioritise and **identify high-risk legacy systems** to the enterprise.
- **Assess** identified legacy system to determine the actual level risk.
- **Define** and develop plans to evolve high-risk legacy systems.

Options for Evolution

Evolving Legacy System

- Enterprises may opt to handle any concerns with legacy systems by developing **policies**.
- Legacy system can be **harden** against attackers by reducing vulnerabilities or wrapping some components.
- **Enhancing** the legacy system by developing and integrating new hardware and software.
- **Replace** legacy system with alternative system to serve the needs of the enterprise.

Systems

Systems

Securing Legacy Systems

All
Legacy
Systems

Internal
Legacy
Systems

External
Legacy
Systems

All Legacy Systems

Systems

- Determine what categories of data you have stored on these legacy systems. Update your inventory accordingly.
- Decommission systems that are within the environment, but are no longer being utilised by the organisation.
- Determine owner or individual responsible for the legacy system (e.g. server, application etc).



All
Legacy
Systems

Internal Legacy Systems

Systems

- Update the software on the legacy system (e.g. operating system) and begin hardening the operating system, remove unnecessary components (e.g. unused applications).
- Develop policies as treatment to mitigate against the threats presented by the legacy system.
- Determine access to the legacy system (e.g. application, processes, people etc) and reconsider if access is necessary.
- Ensure the legacy system and data are properly duplicated to ensure optimal disaster recovery.

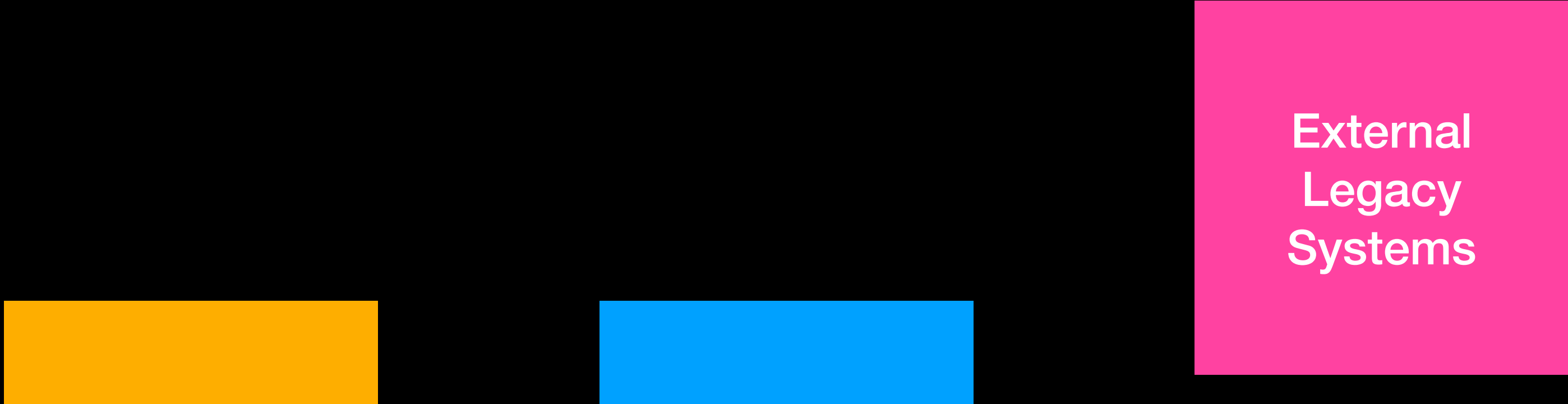


Internal
Legacy
Systems

External Legacy Systems

Systems

- Decommission or replace legacy system server. Otherwise adopt aggressive strategy to minimise the impact of the legacy system.
- Determine the data assets the legacy system utilises or the data assets that reside on the legacy system. Reduce or remove access for legacy system to data and remove any valuable or sensitive data from the legacy system.
- Continually consider the weaknesses in the legacy system and respond accordingly. Minimise access of the legacy system to internal components.



External
Legacy
Systems

Systems

Systems

All
Legacy
Systems

Internal
Legacy
Systems

External
Legacy
Systems

Bump-in-the-wire

Bump-in-the-wire

Securing Legacy Systems

- Not always possible to harden systems or update them with new software or standards, in such situations it may be possible to add a **bump-in-the-wire**.
- Bump-in-the-wire can be considered broadly as an appliance, an element that can be added to the network to provide authentication, integrity or confidentiality.
- Legacy system could output unencrypted data, that is then intercepted and encrypted before being dispatched to another system which potentially has another bump-in-the-wire to unencrypted the data.
- Bump-in-the-wire is effective to some extent, but also has limitations - does not work if the legacy system access point is compromised.

Securing Legacy Systems

Legacy Systems