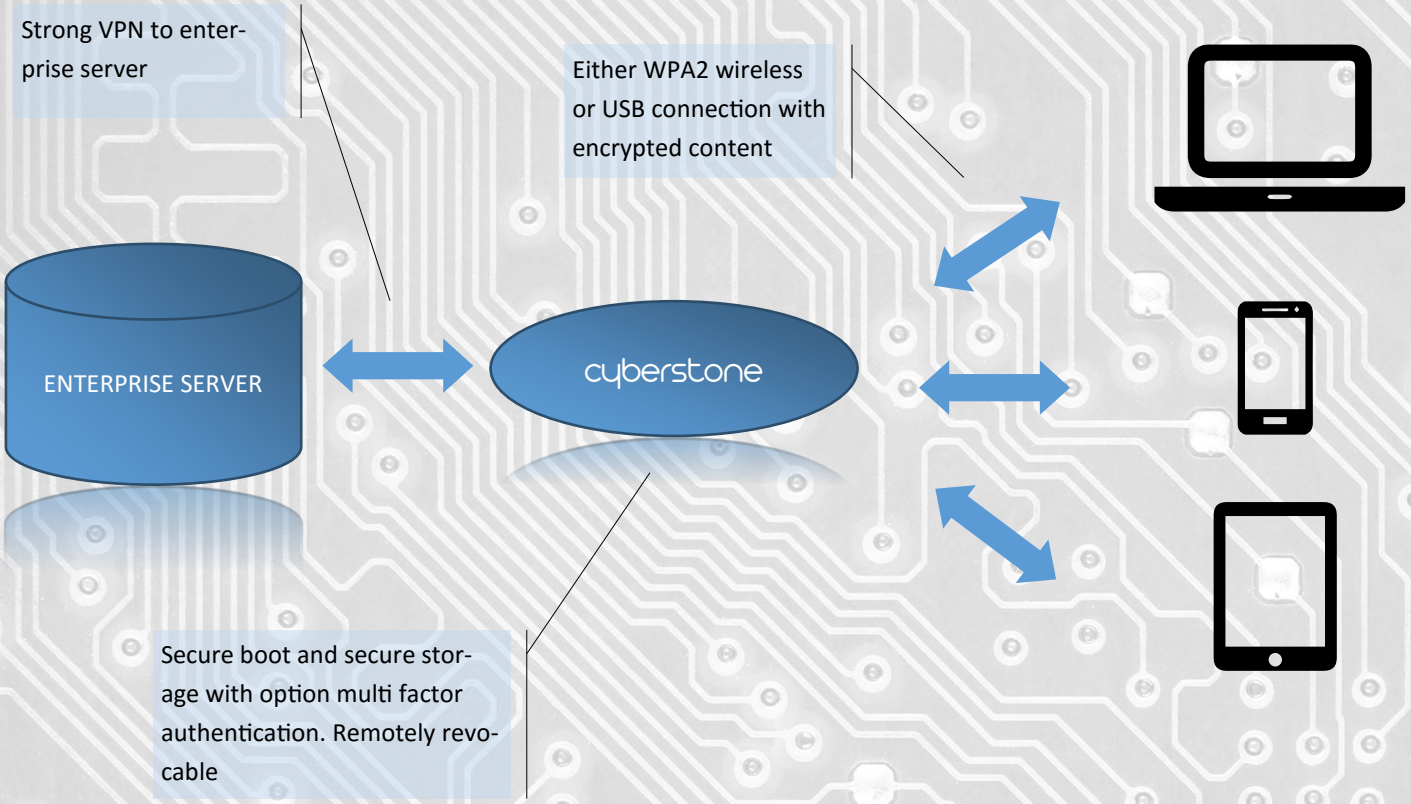
SECURE BYOD

How do you secure corporate data when on your employees own purchased devices? This is the fundamental paradox of BYOD – securing a device which you don't own. CyberStone introduces the concept of a "Secure Intermediary Device" that holds data securely meaning the BYOD device stays clean

FEATURES

- Easy to setup, no installation
- VPN to Enterprise
- Encrypted data at rest
- Remote lock and wipe
- Access secure data when disconnected
- Use public WIFI safely
- Multi factor authentication
- Share/Access data between your devices
- Protect against hackers
- No data left on 3d party devices

HOW DOES IT WORK



HOW DOES IT WORK

The Challenge

Employees are increasingly using their own devices to access sensitive corporate data and applications. Irrespective of whether a formal BYOD policy is in place users will "always find a way".

The Corporation by definition has no control of the employees devices, so how can the data and applications be properly secured.

Connectivity is also an issue: people naturally use the cheapest method to get online. Public WIFI is notoriously easy to compromise.

Conversely consumers are getting increasingly sensitive to snooping. They want to know who can see what. Employers have a right to see what the employee does if its directly related to their job. But if this requires installing highly privileged applications on their own device that essentially give the employer the ability to see everything that's going on, this is not going to be sustainable.

These are the challenges CyberStone addresses; how to protect corporate data on consumer owned devices, without compromising employer privacy.

Technology

CyberStone is a revolutionary new concept. Introducing an Intermediary device, fully owned and controlled by the corporate; it addressed the fundamental conundrum behind BYOD.

CyberStone can be used by many employee devices at once: Tablet, PC and Laptop. It also therefore helps sharing between these devices. The connection between CyberStone and the BYOD device is either over secure wireless WPA2 connection, or a VPN setup over a USB connection. Both data and applications can be served from CyberStone over HTTPS web connections, ensuring security and no device side caching.

Sensitive data and secure applications are securely held on the CyberStone device meaning employees can continue to work event when offline. Data is held in secure storage and secure boot capability gives confidence the device cannot be compromised.

CyberStone connects to the Enterprise of over a highly secure VPN underpinned by a strong PKI implementation