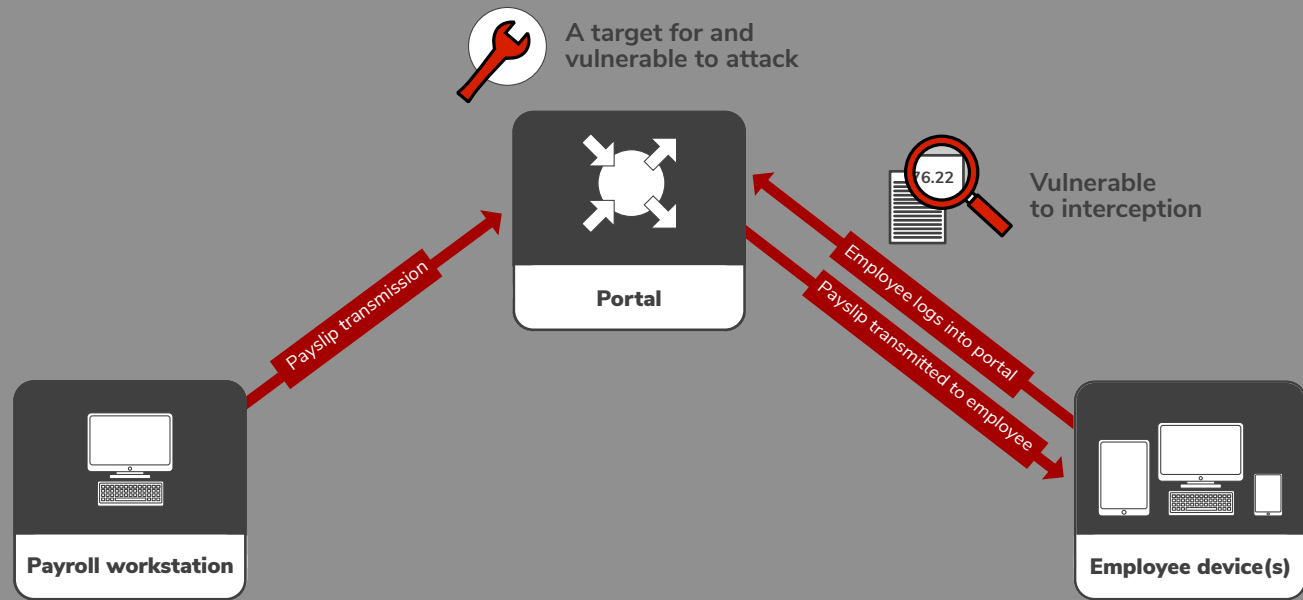
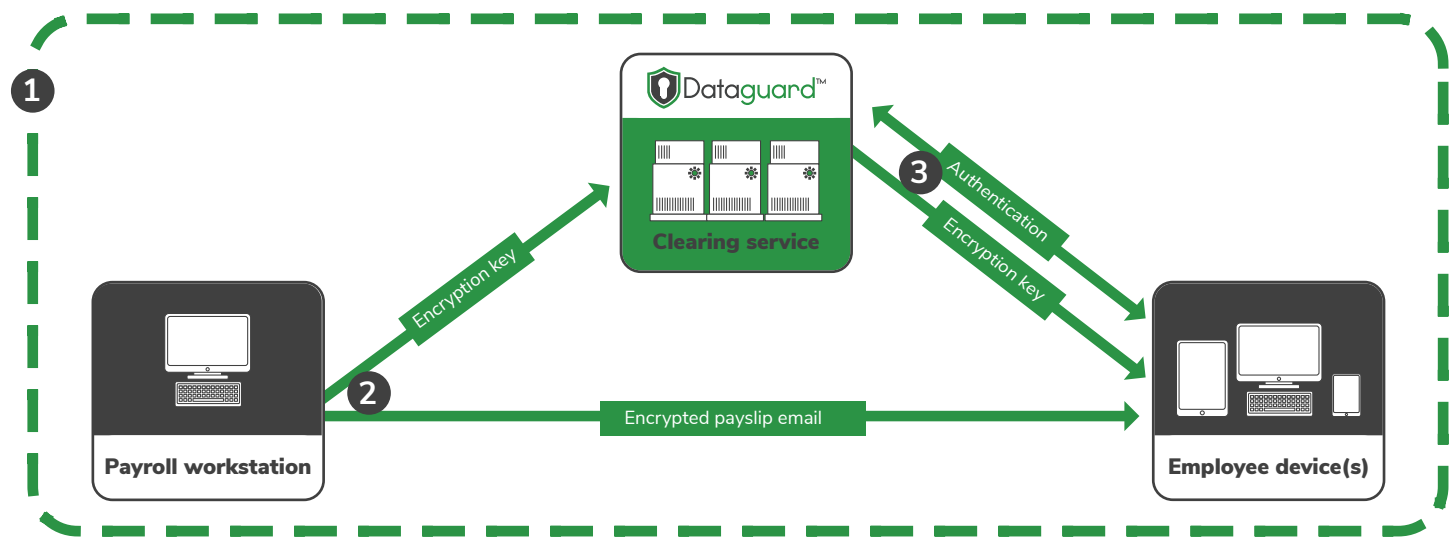


- ⚠️ Portals are potential targets for attack. Worst case scenario is if portal itself stores payslips in unencrypted form.
- ⚠️ Employer owned portals require maintenance and security. The responsibility for backup and security applies as it would for any employer controlled data.
- ⚠️ Transmission of payslip between users and portal vulnerable to interception.
- ⚠️ Infrequency of log-in by employees mean passwords liable be forgotten causing user difficulty and upstream admin workloads to reset passwords.
- ⚠️ Access to portal is removed upon employee leaving organisation, meaning no further access to payslips.



- ✅ ⚡ Fast to adopt
- ✅ £ No expensive consumables
- ✅ ⚙️ Low administration commitments
- ✅ ♻️ Very low environmental impact and carbon footprint



- 1 Fully encrypted AES 256 capability established between payroll, employee and Dataguard
- 2 Encrypted payslip sent by email to recipient, encryption key sent to Dataguard clearing service
- 3 Recipient authenticated, encryption key passed on, message decrypted and read