

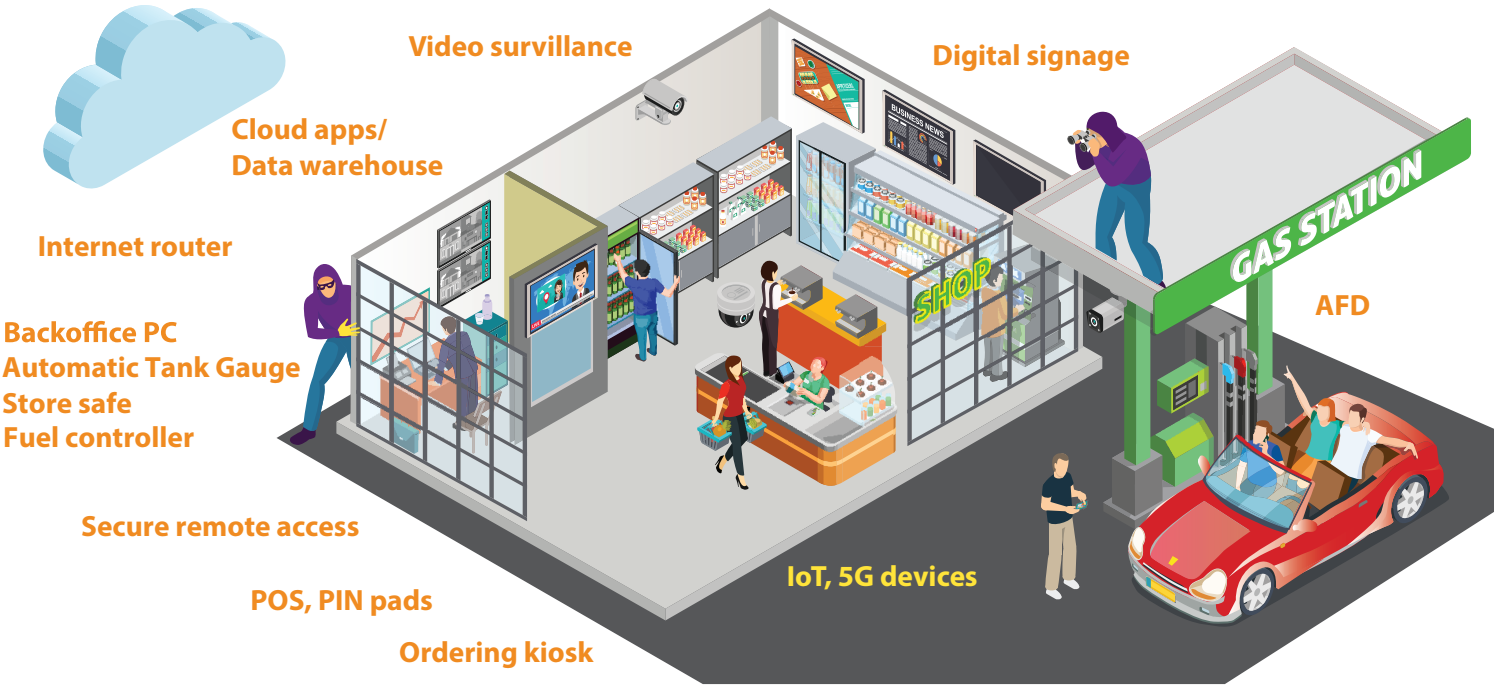
## COMPANY DATA SECURITY AND USER PASSWORDS

### What's The Problem?



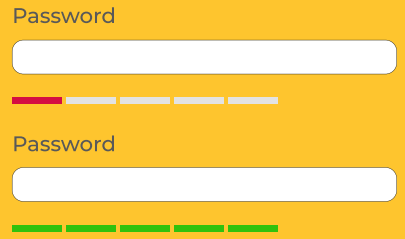
- WEAK PASSWORDS** — 81% of data breaches due to poor passwords<sup>1</sup>
- PASSWORD REUSE** — Breach at home becomes breach at work
- TOO MANY PASSWORDS, TOO MANY USERS** — front line, manager, third party

### Where are C-Store Passwords? EVERYWHERE... From ATGs to IoT



### Common C-Store Password Problems


- Techs use a **default admin password**
- Front-line workers need **manager's password** when manager is not available
- SaaS, Cloud apps**





 Passwords need to be easy for users to remember, but hard for computers to guess. In practice, they are typically the opposite...


### What Should We Do?


Recommendations range from simple to complex, low cost to expensive


 Take inventory of passwords used in your c-store, and who should have them *(but do not write down the passwords!)*


 Not all passwords are the same! Which ones provide access to sensitive systems?


 Set up a password vault to support strong passwords.

 In addition to securely storing passwords, most vaults also help you create unique, complex passwords

 Change all your passwords, generating strong passwords and saving them into your vault; change passwords on a regular basis.

 All remote access is highly recommended to require "Two-Factor" or "Multifactor Authentication"

 Contact your vendors (MNSP, Oil Brands, POS Vendors, etc.) to discuss other security best practices

 **PASSWORD VAULTS:**  
Conexxus users have reported success using password managers such as 1Password, Dashlane, Keeper Security, LastPass, NordPass, Password Boss, and Securdien.<sup>2</sup>

### Where Can I Learn More?

To find more data security resources for your team and organization, visit the Conexxus Resources Library at [Conexxus.org/Data-Security](https://conexxus.org/Data-Security)  
Or visit the PCI Security Standards Council website: [pcisecuritystandards.org](https://pcisecuritystandards.org)

<sup>1</sup> www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Strong-Passwords.pdf  
<sup>2</sup> This list is provided as a convenient resource only. Conexxus has no relationship with these vendors and shall not be held responsible from damages resulting from improper use or vulnerabilities that may exist within these third-party tools. Due diligence should be performed for any software installed on sensitive systems