GATEKEEPER

COMBAT BRUTE-FORCE ATTACKS

Prevent brute force attacks with a proximity 2FA solution. All it takes is one weak link in the chain. One person to mess up on one account.

Make passwords complex!

You can make 120-character long passwords that takes centuries to crack and let the user login without typing the password.

Require physical presence.

Proximity-based authentication means cyber criminals have to be right in front of the PC to even try to login.

2FA without extra work.

Traditional 2 factor-authentication has proven to be a powerful defense against brute force attacks, but takes more work. Proximity 2FA turbo-charges login speeds.

Deter poor password hygiene.

Monitor password strengths. Securely share passwords. Prevent users from writing passwords down and other bad habits.

Prevents password fatigue.

Humans are the weak link in cybersecurity. With password management automated, users are less likely to use weak passwords.

Smaller cyberattack vector.

Smaller attack windows greatly increase the chances of successfully avoiding brute-force attacks.

Access is limited to right in front of PC.

www.gkaccess.com