Armorlog

For the 21st Century

Protects users from credentials phishing attacks.
Each user gets a unique set of proprietary keyboards.
Each user has unique credentials.
Identify users uniquely without exposing user private information.
Simple convenient user-friendly interface.
User has confidence they are authenticating on an authorised site.
Maintain password complexity without inconvenience to users.
Multilevel routines prevent man in the middle phishing of credentials.
Lockout and time out combinations on separate levels.
Prevent user lockouts in brute force attacks.
No fall-back codes required.
No software for users to install.
No software for users to upgrade.
Device independent authentication.
Credentials cannot be key logged.
Keyboard resort & disabled screen feedback for surveillance protection.
(Feedback disable in development only available on chrome touch at present).
Lockout keys to immediately defeat unauthorised access (in development).
Notification keys to identify unauthorised attempts to access (in development).
Keyboard onetime encryption to prevent vector analysis attacks.

Protects against pass the hash attacks.
User access not lost by user device damage, loss, corruption or obsolescence.
User account not compromised by device malware attacks.
Credentials can be called in online routines without risk of phishing.
No complex second channel communications to be managed by network or users.
Prevent session hijacking by calling multilevel authentication.
Prevent account take over on sensitive transactions.
Increase levels of authentication to increase security
Reduce levels of authentication to simplify access (in development).
Choose password length.
Choose to allow or disallow duplicate or triplicate keys in credentials.
Virtual Environment Friendly.
Enable Random Subset Allocation For Decentralised User Access (Beta).
Prevent Password Reuse.
Prevent Password Duplication.
Prevent Delinquent Password Use

Reduce help desk costs.
Reduce fraud.
Increase user satisfaction.
Protect your brand from data breaches.
Be ready for quantum crypto cracking.

Multilevel Authentication.