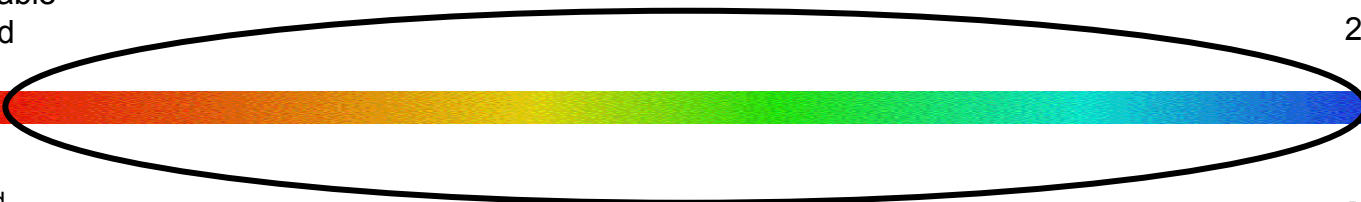


Building a "Grid" to cross and cover the authentication spectrum

Static/Reusable Password

2FA / Multi-factor



- Weak and vulnerable against the most prevalent and easily executed attacks

- Attempts to make them "limited time passwords" i.e. expire every 30,60,90 days add no real strength to the threat matrix, but add a real Total Cost of Ownership (TCO) burden to users and organizations

- Passwords are the most pervasive form of authentication for the majority of users

- Increased strength from One Time Password generation and "having something"

- Physicality and the very nature of the "something you have" unfortunately create real limitations

- Heavy Burden on Total Cost of Ownership (TCO)

- Limited deployment – due to budget constraints and/or mandated/suggested deployment - e.g. SOX, to only users deemed absolutely necessary to have greater security

- No secure, un-intrusive "plan B" for lost, stolen or broken devices



It is this large part of the authentication spectrum that Grid Data Security's unique approach and methodology addresses. Grid delivers proven, effective security through One Time Passwords or PINs, while allowing IT security a viable *alternative* for greater information access control .

- Utilizes a user's *existing* password and organization's database store
- Absolute ZERO footprint and device-less in nature
- Lower TCO and lightweight aspects, allow for complete user coverage
- Bolsters and works in conjunction with other factors and security measures
- Grid's OTP system eliminates or mitigates the following attacks:

- | | |
|-----------------------|--------------------------------------|
| * Key loggers | * Replay attacks |
| * Shoulder surfing | * Stored browser passwords |
| * Brute force attacks | * Dictionary attacks |
| * Phishing | * Password sniffing and interception |

Building a “Grid” to cross and cover the authentication spectrum

Static/Reusable
Password

2FA / Multi-factor



	Zero Client Foot-print	Device-less	Static PIN or Password	TCO Costs	Re-play	Key-loggers	Shoulder-surfing	Stored Browser Password	Universal Access Security	Self – Service
Grid's Approach	Yes	Yes	No	Low	No	No	No	No	Yes	Yes
Static Password	Yes	Yes	Yes	Low	Yes	Yes	Yes	Yes	Yes	Yes
Mutual Authentication	No	Yes	Yes	Low	No	Yes	Yes	Yes	No	Yes
Soft Token	No	Yes	Yes/No	Moderate	Yes	No	No	No	No	No
Out-of-Band	Yes	No	No	Moderate	No	No	No	No	Yes	Yes
Digital Certificates	No	Yes	Yes	High	No	No	No	No	No	No
Time based Hard Token	Yes	No	Yes/No	High	Yes	No	No	No	Yes	No
Smart Card	No	No	Yes	Very High	No	No	No	No	No	No
Biometrics	No	No	Yes	Very High	Yes	No	No	No	No	No