ensurity

True Passwordless Is Distributed

xsense
Extra Identity Sense

True Passwordless is Distributed

"By 2022, 60% of large & global enterprises and 90% of midsize enterprises will implement passwordless methods" - Gartner

- ✓ **Passwordless solutions solve deficiencies of existing identity & access methods.**
- ✓ **But to be really effective, passwordless solutions need to use distributed methods.**
- ✓ **Pain points of recovery, reset & auth transportation need to be better addressed.**
- ✓ **Passwordless solutions must also address bot & app authentication.**
- ✓ **Existing solutions do not offer sufficient security against replay, spoofing & key theft attacks.**
- ✓ **SaaS Passwordless solutions are only as secure as the last mile – OAuth tokens!**

XSense solves several pain points around identity by leveraging distributed security concepts & the patented NLSS[1] technique to achieve secure & sustained passwordless world

xsense
Extra Identity Sense

[1] NLSS: Non-Linear Secret Sharing Image Cryptography (US Patent)

Mutual Authentication

Identity solutions typically ensure Users are genuine.
But how does the User ensure he is connected to the genuine Server?

- ✓ **Lack of mutual authentication results in spoofing & JS attacks.**
- ✓ **Existing solutions do not address the gap.**

- ✓ **Mutual authentication is integral to the XSense solution.**
- ✓ **Backed by the patented cryptographic technique[1].**

xsense
Extra Identity Sense

[1] NLSS: Non-Linear Secret Sharing Image Cryptography (US Patent)

Anti-Replay

ensurity

Session replay attacks pose significant risks to identity & access.

- ✓ **Most identity solutions do not offer protection against replay attacks.**
- ✓ **Some competing solutions offer anti-replay protection but require additional layers of crypto management.**

- ✓ **Anti-replay protection is integral to XSense's patent pending challenge-response method[1].**
- ✓ **Verification coordinates change every authentication attempt, needing new C/R[1].**

xsense
Extra Identity Sense

[1] Challenge-response based on NLSS image cryptography

Secret Rotation

ensurity

Password rotation is a big pain point for the enterprises; Costs money & wastes invaluable management resources.

- ✓ **Key management overload increases proportionately with rotation frequency in existing passwordless solutions**

- ✓ **XSense offers infinite, seamless secret rotation, without needing external setup**
- ✓ **Users/Enterprises can rotate keys any number of times**

xsense
Extra Identity Sense

Secret Recovery/Re-Set

Secret recovery Another big pain point for enterprises & users.

- ✓ **Users being able to reset credentials with minimal overloads & costs is a key target for enterprises.**
- ✓ **Recovery options should not only convenient & but should be highly secure due to lack of second defense.**
- ✓ **Some existing solutions offer recovery.**
- ✓ **Trusted/Federated recovery – recovery using federated devices within the trusted network.**

- ✓ **XSense offers multiple modes of highly secure, yet decentralized recovery**
- ✓ **User can simply use any one of the four recovery codes generated from patented [1,2,5] NLSS schema to automatically recover the account without even needing email.**
- ✓ **Auth transportation from additional registered devices through codes or QR. Without the secret share from either of the devices, recovery can't be completed.**
- ✓ **Trusted/Federated recovery – recovery using federated devices within the trusted network.**

Federated Logins

ensurity

Passwordless security can be enhanced by federation.

- ✓ **Periodically, say once a month or a week, require a second device to approve.**

- ✓ **Federated devices share secret shares with the original user device. Multi-party computation to complete access.**
- ✓ **Xsense's technique minimizes user any inconvenience that comes with federated logins, while enhancing security.**

xsense
Extra Identity Sense

ensurity

Temporary Auth Transportation

Temporary access to other users a key unsolved requirement.

- ✓ **Users often share passwords or OTPs for temporary access.**
- ✓ **Users need to reset passwords after sharing with others; OTPs give one-time access, but not dynamic or timebound.**

- ✓ **XSense dynamic, timebound access codes that can easily be transported to other devices for secure, temporary access.**
- ✓ **User can block temporary access any time without Server approval at any time due to the patented Essential Share concept.**

xsense
Extra Identity Sense

Bot/App Authentication

ensurity

Proliferation of automation & distributed apps increases the need for passwordless credential management.

- ✓ **Existing PAM / app authentication solutions are centralized, expensive & lack second line of defense.**
- ✓ **Current access token management is clunky & requires too many gateway hops.**
- ✓ **Existing SSO / Session tokens have no defense against token loss.**

- ✓ **XSense passwordless technology offers strong defense against loss of access tokens.**
- ✓ **Token management is distributed, rapid & cheaper, doing away with the need to refresh “refresh” tokens.**
- ✓ **XSense extends passwordless to bots / apps as a strong alternative to existing PAM solutions.**

xsense
Extra Identity Sense

Thank you

info@ensurity.com
www.ensurity.com