ensurity
A Step Ahead!

Use Case - SI-MNC

Implementation of **FIDO2 Authentication** for cybersecurity wing at an IT company

CUSTOMER	:	A leading Multinational IT Company
DATE OF IMPLEMENTATION	:	July 2020
ENVIRONMENT	:	Across multiple geographical locations, uses Microsoft cloud environment for its' operations; and has deployed multiple Microsoft Windows systems that are connected to Azure AD.
PROBLEM STATEMENT	:	Enable FIDO2 based authentication to their enterprise applications and ensure all the employees integrate secure authentication through FIDO2 security keys for all enterprise applications. • Restrict employees from sharing their password and authenticators. • Eliminate PIN as an alternate to Bio authentication to avoid misuse • Enable employees to use any of the PC in the work area to access apps.

Solution Offered :

In response to these requirements, Ensurity has implemented its' ThinC-AUTH Biometric Security Keys with the following solutions:

- Customized the ThinC-AUTH Security Keys with provision to disable 'Fallback PIN' based authentication. This feature restricts the User to mandatory use of their registered biometrics. Even if anyone intentionally attempts with wrong fingerprint authentication, the device will NOT fall back to PIN

  This feature restricted all the users to authenticate only with their enrolled biometrics.

- Developed a customized Software Tool (Windows, macOS and Linux platforms) to enroll user fingerprints and a feature to disable the PIN based authentication. This process is one-time activity and these settings will be saved directly to the connected ThinC-AUTH device

- The users could login to their Windows systems without entering the password using ThinC-AUTH.

The IT company has been able to secure their systems and eliminate risks of credential sharing and attribute users access to systems.