Two-factor mainframe authentication

Achieve two-factor authentication for your entire IBM System z mainframe network or single business transactions with Defender Mainframe Edition (ME). This mainframe multi-factor authentication solution enables you to authenticate users through any of the most popular password tokens at three different levels: application selection, business transaction or network entry, enhancing your organization's security. Defender ME incorporates the most up-to-date cryptographic hardware technologies and includes support for several token types from various vendors

Features

- **Network security** – Validates your users before they enter the network by extending security defenses from the kernel of the individual mainframe systems to the network periphery.
- **Application/transaction protection** – Restricts your users to permitted applications only though user ID and passwords. You can also insist that users provide additional personal token information at the transaction level, the application level or both.
- **OATH-comliant** –Enables you to select a solution that fits your organization's needs with support for any OATH-compliant token (from any OATH-compliant hardware vendor).
- **RSA SecureID support** – Provides security and reliability, while reducing your overall investment with support for the latest RSA SecureID AES token with 9-digit serial numbers and fully integrated support for 128-bit AES tokens. Your users with AES tokens are not required to be authenticated by connecting to a RSA ACE®, Unix, or Windows Server.
- **Alerts** – Accelerates message warnings (including NewView alerts) to a central host or operator console.
- **MVS system support** – Provides support for Multiple Virtual Storage (MVS) systems with Defender's three levels:
    - Defender ME VSSE – Controls which LU-to-LU sessions will be allowed or denied by VTAM, including application-to-printer, peer-to-peer, terminal-to-application, and Network Job Entry (NJE) sessions.
    - Defender ME Secure – Restricts your users to permitted applications only, providing your organization with information protection and active network security. Also enables you to validate through a user ID.
    - Defender ME Authenticator – Provides you with all the features of Defender ME Secure, in addition to incorporating three-factor authentication: user ID, personal device-generated code and user-changeable password.
- **Transaction-level interface (TLI)** – Broadens security outside the VTAM network front end to your users' business transactions. Requests password validation and user ID from within the transaction to protect your organization's sensitive transactions.
- **Home-node processing** – Allows your users to specify the name of the machine on which they would like to be authenticated, which is especially beneficial if your users access their systems from both home and remote locations.