Vortex Terminal Security Solution

vortex™
Helping banks reach out

As the banking industry steps into challenges in the new normal, the self-service terminals, particularly ATMs being their strategic touchpoint between banks and customers will be the focus area again. As part of the effective utilization of the resources, we will witness steady growth in the deployment of self-service terminals and this can spur criminal attempts to extract the vulnerabilities in the ATM system. Self-service terminals that provide secure services to their customers are of the utmost importance to the banks.

For over a decade now, Vortex Engineering has been at the forefront of delivering unique and innovative security solutions to the banks. Ecoteller® range of ATMs with Swave® application runs on Linux OS. Apart from the inherent security offered by Linux OS, Vortex ATMs are equipped with Terminal Security Solution that provides comprehensive three-layer protection against different attack verticals.

LAYER 1 - HARDWARE

ENCRYPTED PIN PAD(EPP) - PCI certified EPP offer secure authentication of PIN

CARD READER - EMVCo certified card readers support chip cards

ANTI SKIMMING DEVICE - Vortex Anti-skimming device offers protection against card skimming and shimming

ALARM SENSOR - Alarm sensors for monitoring any kind of physical attacks on the ATM

SURVEILLANCE CAMERA - Portrait camera, cash slot camera and Digital Video Surveillance System which covers the entire event of transaction in the ATM room.

BIOS PROTECTION - Prevents unauthorized access to the system configuration

USB CONTROL - Prevents unauthorized access to the system via USB ports

LAYER 2 - OPERATING SYSTEM

HARD DISK ENCRYPTION - Full Hard Disk Encryption (HDE) prevents Data harvesting.

OS HARDENING - Hardened Operating System allows only the required functions and services in the machine rooting out common vulnerabilities

DISPENSER ENCRYPTION - Secure comminucation between the dispenser and the ATM software application prevents reverse engineering and replay of the dispenser commands

WHITELISTING - Whitelisting authorizes terminal application binaries and essential software components ensures complete protection against rogue applications taking control of the system

FIREWALL - A Robust firewall restricts hosts, networks, ports, and protocols of communication to protect sensitive transaction messages between the terminal and the host.

USER ACCESS CONTROL - Effective access control sets rights and roles for user profiles and provides strict password policies for accessing the terminal.

LAYER 3 – ATM APPLICATION

SWAVE® APPLICATION - Swave® terminal application runs on Linux operating system which is more reliable and secure. Swave® adheres to the international standards putforth by EMVCo and PCI Council.

HOST COMMUNICATION ENCYPRTION - Swave® terminal application enables TLS/SSL and VPN grade security for host message protocols.

SW UPDATES MANAGEMENT - Periodic upgrade mechanisms through authorized OTP sessions can be carried out onsite or through remote management sessions.

CONNECT WITH US TODAY FOR A SECURE BANKING TOMORROW

FOLLOW US ON

www.vortexindia.co.in