VELOX

WHITE PAPER

ScanPlus ATM Terminal Security Solution

2021// VSPL

VELOX®
Develops Opportunities For Enterprises...

PREFACE

Today bank's IT departments and ATM service providers face tremendous pressure to ensure that their ATMs comply with many different security concerns, policies, operating procedures, corporate IT standards, and regulations.

Velox has introduced ScanPlus ATM Terminal Security to ensure the greatest degree of visibility and control over secured ATM operations and helps to enforce regulatory compliance put forward by RBI. ScanPlus ATM Terminal Security is bundled with Application White Listing, Full Hard Drive Encryption, USB Enable/Disable, Bios Password & LAN Monitoring.

This White Paper will explore the need for the ScanPlus ATM Terminal Security product and its various modules that facilitate monitoring and prevent the increasing Cyber Crime & also Safeguard the Assets.

INTRODUCTION

Cybercrimes in the area of ATM system is a major incidence such as:

- The Citibank rip-off of US $ 10 million was fraudulently transferred out of the bank and into a bank account in Switzerland
- List of data breaches and cyber-attacks in October 2017 – 55 million records leaked
- 27,482Cases of Cybercrimes Reported in 2017, One Attackin India Every 10 Minutes

Several preventive measures had also been taken to curb the increasing number of cybercrimes. The introduction of the IT Act 2000 was enacted to boost the growth of computers and the Internet; to provide legal recognition to electronic records and e-transactions, and to prevent computer-based crimes. The problem in most cases remains unreported due to lack of awareness. Law enforcement agencies are not well equipped and oriented about cybercrime yet there is an immense need for such a unique solution to seize these cybercrimes and put an end to the era of Cyber Crimes resulting in Safeguarding for the Assets.

ScanPlus ATM is a unique solution offered by Velox Solutions keeping in view the depth of the involvement of the computer facility in exploring new avenues of crime and its inference, ScanPlus ATM Terminal powerful security & monitoring tool that aids to curb cybercrime and maintain a serene environment to defined domains.ScanPlus ATM Terminal security showcases the power of technology and the true utilization of cyber security for restoring peace in the banking industry.

All About ScanPlus ATM Terminal Security:-

Sub Modules :

ØWhite listing Application
ØBlack Listing Application
ØSandboxing
ØOS & Hardening Management
ØFull Hard Drive Encryption
ØBIOS Password
ØUSB Protection
ØOS & Access PrivilegeManagement
ØPatch Management
ØLAN Monitoring

There are the following mode of Installation mention below:

- Standalone Installation
- Centralized Installation

1. White Listing:

Application whitelisting is the practice of specifying an index of approved software applications that are permitted to be present and active on a computer system. The goal of the white listing is to protect computers and networks from potentially harmful applications. Applications blocks unauthorized executables on ATM Systems as a part of security measures.

2. Black Listing:

- Applications and their hash (SHA-256)
- Applications filtered due to applications learned as Whitelisted
- Applications restricted due to marked as blacklisted
- Reports available in PDF, CSV, and Excel formats

3. Sandboxing:

- Logs the activity of the running application to create sandbox database.
- In active sandbox mode application are only permitted to access the files and registry learned in learning mode.
- Applications restricted to access the protected files and registry keys.
- Application are configured for READ or WRITE operation access of the files and the registry

4. Full Hard Drive Encryption:

Full-disk encryption (FDE) is encryption at the hardware level. FDE works by automatically converting data on a hard drive into a form that cannot be understood by anyone who doesn't have the key to "undo" the conversion. Without the proper authentication key, even if the hard drive is removed and placed in another machine,the data remainsinaccessible. FDE can be installed on a computing device at the time of manufacturing or it can be added later on by installing a special softwaredriver.

The advantageof FDE is that it requires no special attention on the part of the end user after he initially unlocks the computer. As data is written, it is automatically encrypted. When it is read, it is automatically decrypted. Because everything on the hard drive is encrypted, including the operating system, a disadvantage of FDE is that the encrypting/decrypting process can slow down data access times, particularly when virtual memory is being heavily accessed.

5. BIOS Password

BIOS Password is authentication information that is required to log into ATM BIOS setting. BIOS is shortfor Basic InputOutput System. It is much more than the name suggests. One might think that BIOS controls input and output system. But the BIOS does much more, and it is not possible for any operating system to continuewithout a proper BIOS in place

6. USB Protection:

In USB protection, device with only allowed Device-ID is allowed to access in ATM system. In USB disable,all external USB devices are blocked to be accessible from ATM system.

7. LAN Monitoring:

ATM machine which are connected through LAN or branch attach MPLS network can be monitored for it disconnection in local area Network.

LAN Monitoring immediately alerts the central Dashboard about any system disconnection.
IP based device such as Bio-metric, Camera, ACs etc. can be monitored for it disconnection or failure from centralized location.Alerts will be shown on dashboard whenever device is down

8. OS & Access PrivilegeManagement:

·ScanPlus ATM Terminal has the ability to manage entire Windows Operating Services and Policies from central location.
User can create WindowsUser and WindowsGroup and manage following services of the user centrally
Windows Services LevelManagement
Local User & Group Creation,Deletion, Modification Policy
Dynamic password with reset facility
User right assignment
Firewall protection

9. Patch Management

- ScanPlus Patch management uses multicasting for content distribution across the ATMs
- ScanPlus allows users to control bandwidth consumption by dividing the content into packets of user-defined size
- In a failure of transmission ScanPlusresends the only required data
- Parameterized reports of all the send and received files

Conclusion:

Protection of critical information infrastructure is of prime importance to national security, economy, public health, and safety and as such, it has become imperative to declare such infrastructure as 'protected' in order to restrict its access. ScanPlusATM would help to superimpose several gray areas that exist within the law and would help in enforcing the prevalent IT Act in an entirely different form. Cybercrimes have increased in vast numbers ScanPlus ATM is an appropriate solution to it.

By means of this document, we would bring safety to the assets / resources allocated. This safety & safeguard activity is carried in conjunction on parameters defined. Real time measures with support of alert are being mapped to action taking team. various reports with defined analysis arebeing shared with stakeholders. Health of the assets / resources being monitored on regular interval of time. This solution is an aid to investigation & vigilance team to drill down on specific activity. Product is flexible in incorporating new cyber law with any additional measures. We enable to block the assets outside the resources allocated; free access to outside devices such as external hard drive, pen drive is prohibited.

In today's information age every enterprise need solutions which can help them accelerate their work process in a secure way and at the same time following all the standards and regulations. We specialize in providing solutions in almost all verticals of IT. Starting from providing solutions Network administration and management and also provides solutions for data security and storage.

Velox has continuously been working as a leading Products and Services company, catering innovative security products in Information Technology in INDIA.