

cyttek GROUP



CATALOG OF
PRODUCTS AND SERVICES

2023

WWW.CYTTEK.COM

XFS

A N A L Y T I C S

XFSA: THE MARKET SOLUTION FOR REAL-TIME ATMs ANALYSIS

Our solution is based on analyzing different ATM layers such as operating system, Journal and Service Provision, to provide 360° visibility and answer any questions you may have on how to improve the operation of your ATM network.

XFS ANALYTICS

To benefit companies and financial institutions, so that they can automate the resolution of any case or question they may have about their operation in real time.

XFS IS A WEB BASED INTERFACE SOLUTION, PROTECTED WITH PASSWORD AND SSL BASED ACCESS.

This means all banking cases and logs are fully safeguarded under the best industry standards.



Eliminate the need for highly specialized and dedicated full-time staff to identify and analyze ATMs network problems.



Control the hardware and cash replenishment supplier in their routine transactions.



Save time and resources in analyzing all types of ATM network issues in the ATM network, regardless of the hardware and software brand.



Carry out impartial and truthful analyzes of the information collected in real time.



Information collection and processing fully insured.

CHARACTERISTICS

- Detection of cash replenishment errors.
- Analyze cash shortage cases in real time from multiple ATMs simultaneously.
- Results and data extraction via CVS or Web.
- Information storage in a secure and reliable environment.
- Access and role control for all information analysis processes.
- Interactive interface with ATM/PoS location management.
- Roles and permissions management for information access.
- Information analysis through CEN XFS visibility even when the event does is not included in the journal.

- Multiple banks management.
- Multi-currency capabilities.
- Real-time ATM error detection and cash shortage detection.
- Secure and user-friendly Web.
- Extraction of logs from virtual journal, XFS software (Agilis, APTRA, Dybasty, KAL) among other sources.
- Window and third party software (such as McAfee/GMV Checker/Symatec) log retrieval
- Extraction of hardware events such as skimming
- Ability to create all kinds of reports and graphs without limitation.

REQUIREMENTS



Operating System
Windows XP, 7 y 10



Hardware
All models of NCR, Diebold-Nixdorf (diebold and Wincor Nixdorf), OKI, GRC, WRG, Nautilus, among others.



Software XFS
Kal, Agilis, APTRA, Procash/probase, MP2, Dynasty, Proflex, Phoenix XFS and many others.

DETECTED ATTACKS

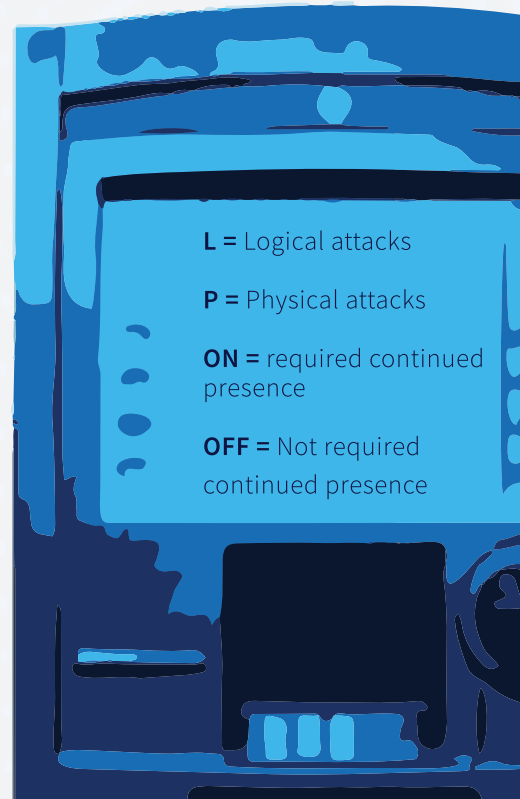
LOGICAL ATTACKS

- (L-OFF) Malware
- (L-OFF) Unauthorized management applications and services
- (L-ON/OFF) PAC=MITM
- (L-OFF) Black box
- (L-ON) Malicious dispense orders
- (L-ON) Malware distribution
- (L-ON) Active Man-in-the-middle (A-MITM)
- (L-ON) Passive Man-in-the-middle (P-MITM)
- (L-OFF) Host spoofing

PHYSICAL ATTACKS

- (P-OFF) Ram raid
- (P-OFF) Smash and grab
- (P/L-ON) Card trapping
- (P/L-ON) Skimming
- (P/L-ON) Shimming
- (P-ON) TRF I / II
- (P-ON) Cash trapping I / I

Some physical attacks are we detect by connecting to perimeter solutions.



Gen3XFS

Global Automated teller machine

- Designed for the digital transformation of the ATM channel.
- Multi-manufacturer, multi-entity, multi-currency, and multi-language.
- It is a scalable solution where each functional module is independent of the rest.
- Facilitates collaboration via mobile, telephone banking, and branch channels.
- Includes access and transaction security.
- Provides early warning services and failover automation.
- Allows the customization of the online and dynamic presentation.
- Technology and HW supplier independent.
- Forward-looking and innovative: Biometrics, facial recognition, accessibility, XFS4IoT, etc.

TECHNOLOGIES



PLATFORMS



1. TOOLKIT

Self-service toolkit for development and testing.

2. KERNEL EMV/

Janux Kernel modules with self-contained functionality for EMV transaction integration, one for contactless cards and one for chip cards..

3. SELF-SERVICE APPLICATION

State-of-the-art Self-Service application with new design and user experience standards. It is a hybrid solution capable of handling both large and small customers.

4. SOFTWARE PLATFORM

The infrastructure framework (API Services) ensures a flexible multivendor Self-Service application that is modular and innovative.

5. CORE SERVER

Standard Self-Service services, including remote key loading ("RKL"), single point of entry, and connection to different environments and protocols like ISO, NDC, and others.



Gen3XFS application is based on simplicity and security in mind to be able to provide any financial institutions the flexibility to develop their own flows of applications, and they own personal self-service experience with accessible technologies that developers with no previous experience in CEN XFS software development can implement the application, this application is open to change and adapt to any financial institution.

WE SUPPORT
Any ATM that supports CEN XFS standards

CORE SECURITY

With ATX, financial institutions and ATM networks can change the way they operate and manage their security and operation in the face of ATM failure.

Through ATX it is possible to reduce time and operating costs in the ATM network, as well as ATM recovery, by remotely facilitating ATM installations and improving their turnaround times.

We are the first solution in the market by which any ATM network will be able to reduce its operating costs and increase its availability to 99.99% by preventing ATM downtime and unavailability remotely in the event of any software problem.

-
-  Multi-Vendor Remote BIOS Password Change Remote.
 -  ATM Images Remote Backup and Recovery.
 -  Fault-proof Operating System Remote Journal Extraction.
 -  ATM Images Remote Installation.
 -  No vault opening visits required to repair the ATM
 -  Remote Desktop via KVM Technology (intel AMT vPRO).
 -  KVM session recording during the entire ATM operation in Windows or BIOS.
 -  Protection against endoscope attacks and Blackbox.
 -  Intel AMT PRO technology control.
 -  ATM hardware and firmware data extraction.
 -  Rules and Protection actions Programming.
 -  Alerts and protection against physical attacks (firmware change, disk replacement, USB insertion among other low-level detections).
 -  Connection of physical sensors and response to sensor events



THE ATX SOLUTION COMPRISES SEVERAL COMPONENTS, MAKING IT A MODULAR SOLUTION:



ATX Hardware (encrypted vault)



ATX Software



Firmware

TECHNOLOGY USED:

- Windows Server
- Redhat
- Django
- Python
- C+
- Net.
- IIS
- HTTPS
- Intel AMT vPRO
- HTML5
- REST API
- POSTGRESQL

REMOTE BIOS MANAGEMENT

Our solution supports the management of bios passwords in a multivendor way, so there is no need to have multiple management solutions for different ATMs and different ATM firmware models. NCR, Diebold Nixdorf and Hyosung ATMs can be operated from a single solution.

Remote ATM Installation Times: We support reinstallation processes with the disk or image already in production, encrypted or not. Our times for a completely remote reinstallation range between 20 minutes to 3hours, thus saving additional costs of physical installation visits, waiting times, reprogramming staff visits to the field, and additional support fees. with ATX under a single license you simply can reinstall completely remotely, more efficiently and faster, the same ATM as often as needed.

Information:

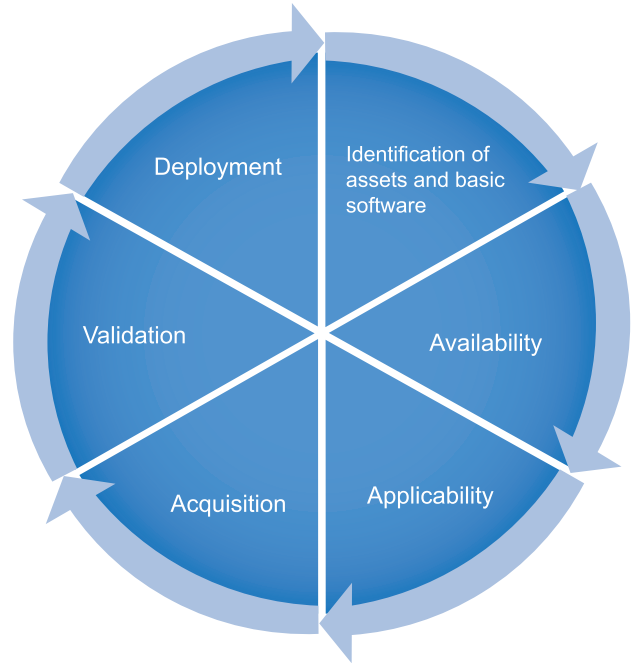
Since 1970, ATM software issues have been solved on-site. ATX has created an innovative technology that allows to solve all the problems that arise in the software layer by installing remotely all the necessary information from the base image and leaving the ATM ready to operate in production without the need for human intervention or on-site technicians. We can help you increase the security and reduce the operating costs of your ATM network in an easy and secure way. Just ask for an expert consultation.

Monthly ATM network risk mitigation monitoring service

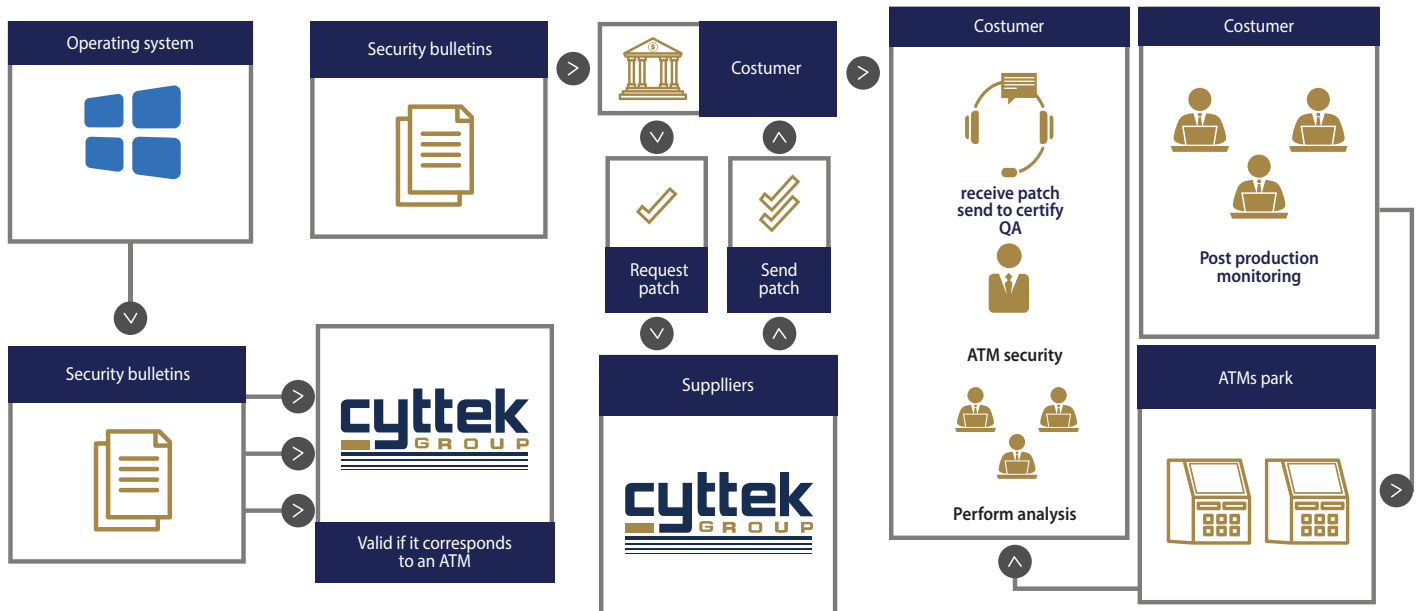
allows evaluating or implementing an incremental security analysis in the form of “penetration testing” for carrying out assessments based on the already evaluated ATM multivendor hardware and image.

This process includes the phases as described here. Within the validation phase, our team of consultants will agree upon an evaluation schedule where, according to the product, an offensive security technical evaluation will be performed to implement or evaluate necessary security corrections.

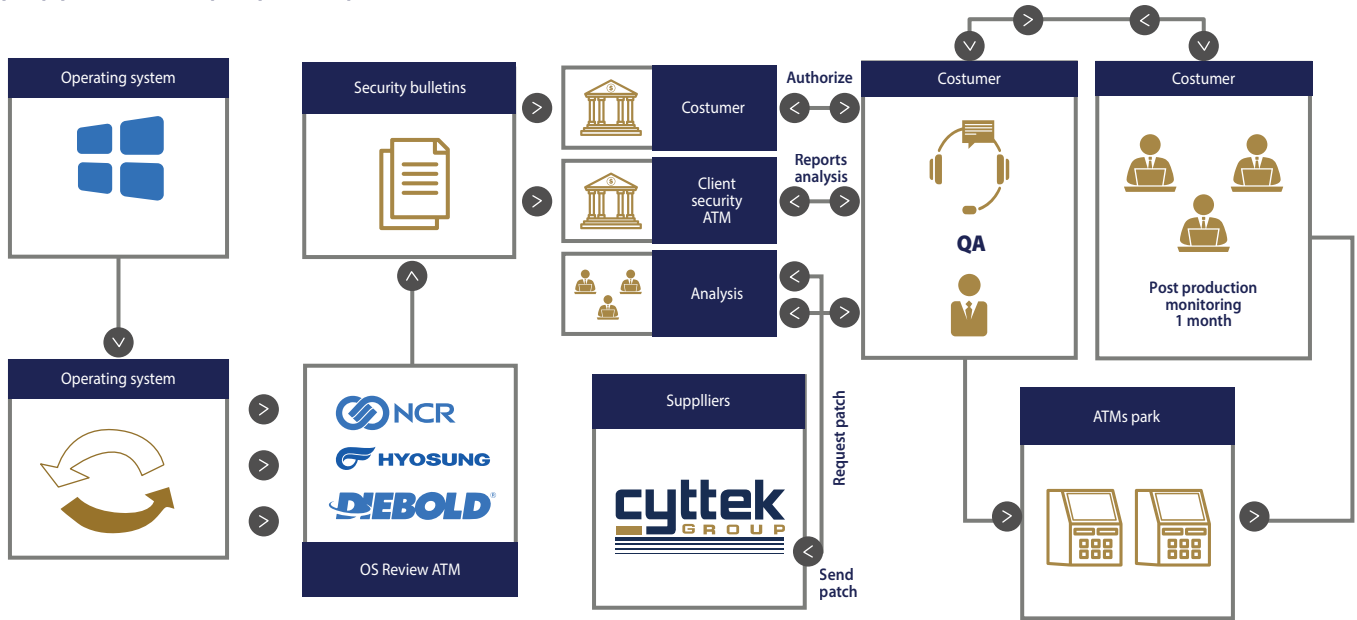
Currently, there is no formal instance where a review and installation of Hotfix Windows is performed to keep the ATMs updated and secured. It depends largely on the manufacturer’s vision and the type of service purchased from the supplier. More often than not, the manufacturer simply does not make the best security decisions. Our service is focused 100% on the security and stability of the ATM network.



WINDOWS PATCH FLOW



SECURITY PATCH SERVICE



Our team will be responsible for the technical assessment of each new product, patch, or solution to incrementally evaluate it based on image security already evaluated, and deliver a security, functionality and operation analysis of the new product, service, or manufacturer's patch. This will be measured incrementally over what is already available in the image or current network manually, using with the experience of our consultants who will accompany the process month after month.

Ask about our arch and security management service, we will take care of eliminating a real risk and will work hand in hand with you on a monthly basis.

PROFESSIONAL SERVICES ATM

“360° Risk Assessment”

To the entire ATM infrastructure

“Advanced Software Development”

Development of customized solutions for customers.

“Tuning and patch management”

of ATM applications.

“Advice and support in security solutions” such as sensors, anti-skimming, anti-shimming, electronic locks, among others.

“Solution Design” custom monitoring and security for ATMs for any XFS Software.

“Server auditing” of transactions and protocols; NDC, DDC, ANDC.

“Solution development” for all brands of custom ATM hardware.

PROFESSIONAL SERVICES PoS

“360° Risk Assessment”

to the entire PoS infrastructure

“Ethical Hacking” to all brands of Hardware and software developments for PoS equipment.

“Advice and support” in the process of acquiring point-of-payment solutions in accordance with the regulations.

“Customized Solution Development” for PoS

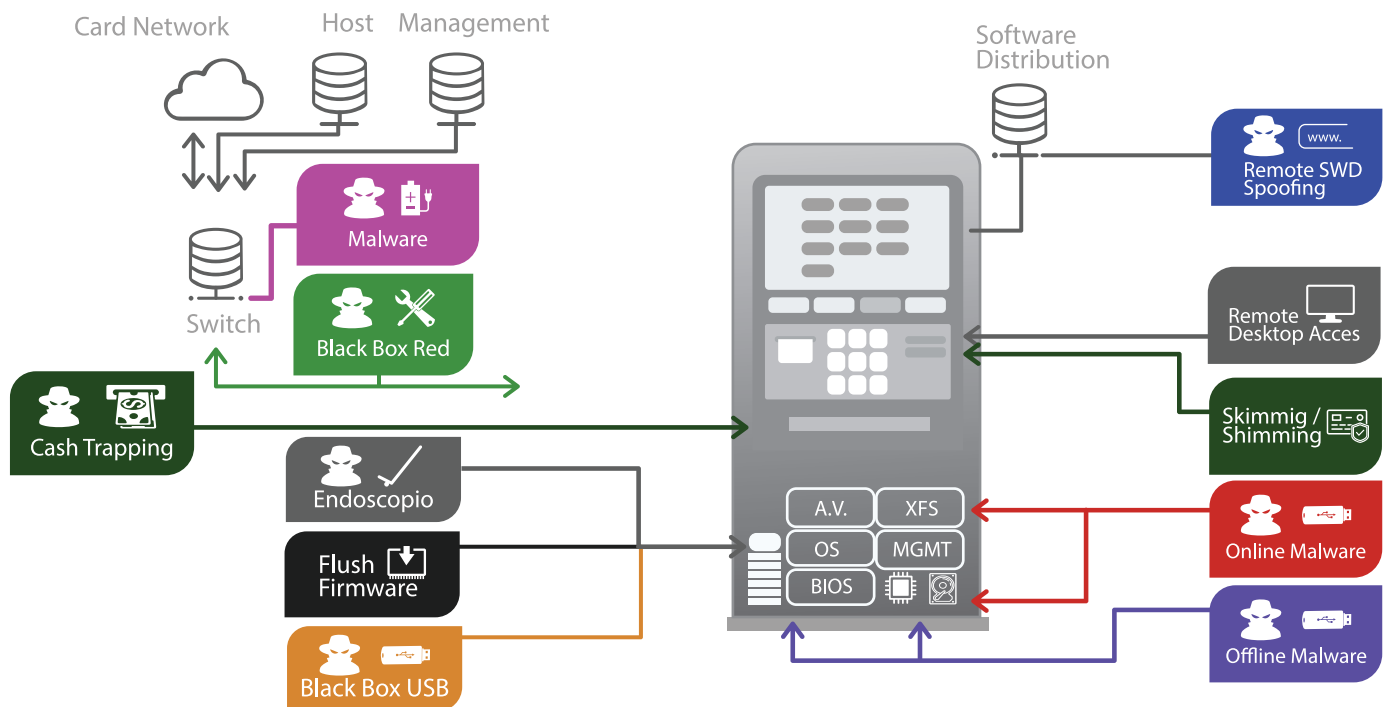
“Application Auditing” PoketPoS or Mobile+PoS

“Secure Development of Payment Solutions” QR or Biometrics

























“Implementation of Security Solutions” for PoS networks and monitoring solutions


ATMS ATTACKS

Attack vector map of the possible types of vulnerability that can occur in an attack on ATMs of any manufacturer, brand, or model.



CYTTEK GROUP SOLUTIONS APPLIED TO ATM NETWORK RISK AND ATTACKS

NOMBRE DE ATAQUES	DESCRIPCIÓN	SOLUCIONES
● Transactional switch commitment	Malware infection of the transaction software.	
● Red Black Box	Deploy equipment to intercept transaction communications and listen to or inject dispensing messages.	 
● Cash Trapping	Capture money before it is presented from the motorized band, or before it is presented at the dispenser.	 
● Reverse Transaction Fraud Types I and II	Conducting errors on transactions that the card issuer does not accept during the transaction to avoid being discounted while the ATM delivers the money.	 
● Endoscope Attack	Inserting an endoscope or USB cable extension through the presenter to attack a vulnerability in the dispenser.	 
● Black Box USB	Inserting a PC, laptop or mini PC that can interact with the dispenser and have Cash Dispenser functions without the need of the ATM banking application.	 
● Hard Drive Theft	Removing the hard drive to install malicious software and run software without control.	
● Violation of Bios, Boot and Intel AMT passwords	Attempt to boot other operating systems containing malicious software to operate the ATM, also used to boot USB or other operating systems into the ATM.	
● XFS Malware	Compromise the operating system by installing software that can operate the ATM perimeters.	 
● Skimming, Shimming, NFC Skimmer	Attackers attempt to clone cardholder information by implementing equipment on top of the reader or internal to the reader.	 
● Committed Software Updates	The attacker manages to infect software packages of the manufacturer before the network or USB from technicians that the bank did not approve its operation.	 
● Engagement through remote access	The attacker attempts to gain access to the ATM remotely by intercepting communication cables.	
● Firmware flush or parameter misconfiguration de seguridad de dispensador	Attacker attempts to install firmware from previous versions with lower security or to misconfigure dispenser security settings.	  
● Gas Attacks, Explosions, ATM theft	The Attacker(s) attempt(s) to insert gas or break the security vault, or remove the atm anchor to steal the entire ATM.	

-  In the event of any software error, slowness or operational problems that require operating system or software solutions, the ATM can be installed and returned to a completely remote state, in addition to protecting attacks that do not require an operating system.
-  Obtain all types of security, operation, transaction and operational error reports, error status and message queries from the ATM, Switch and other devices connected to the ATM for real-time visibility with unlimited reporting, as a financial institution needs visibility tailored to its needs.
-  Software-based security solution to protect the operating system layer from an attack, and to control information filtering.



WWW.CYTTEK.COM