X-FORT

Enterprise Electronic Data Surveillance System

Control · Manage · Monitor · React · Audit

Version 7

www.fineart-tech.com

DATA SECURITY EXPERT

X-FORT is a comprehensive data security solution that includes Data Leak Prevention, Data Protection, and IT Asset Management—preventing confidential information from breaching or losing and providing management tools of applications, computer assets and remote control.

Data Leak Prevention **Data Protection** **IT Asset Management**

X-FORT

Data Leak Prevention

- External Storage
- MTP Device
- CD/DVD
- Printing
- Device Control
- Folder Sharing Control
- Connection Control
- Web Browsing
- Cloud
- E-mail
- IM Software
- SVT (Secure Virtual Tunnel)

Data Protection

- File Encryption
- Content Filter and Classification
- File Activity Monitoring

IT Asset Management

- Asset Management
- Software Security
- Application Whitelisting
- Remote Management
- File Deployment
- Help Desk

User Behavior Analytics

- Operation Log
- Log Analysis / Audit

X-FORT Enterprise Electronic Data Surveillance System

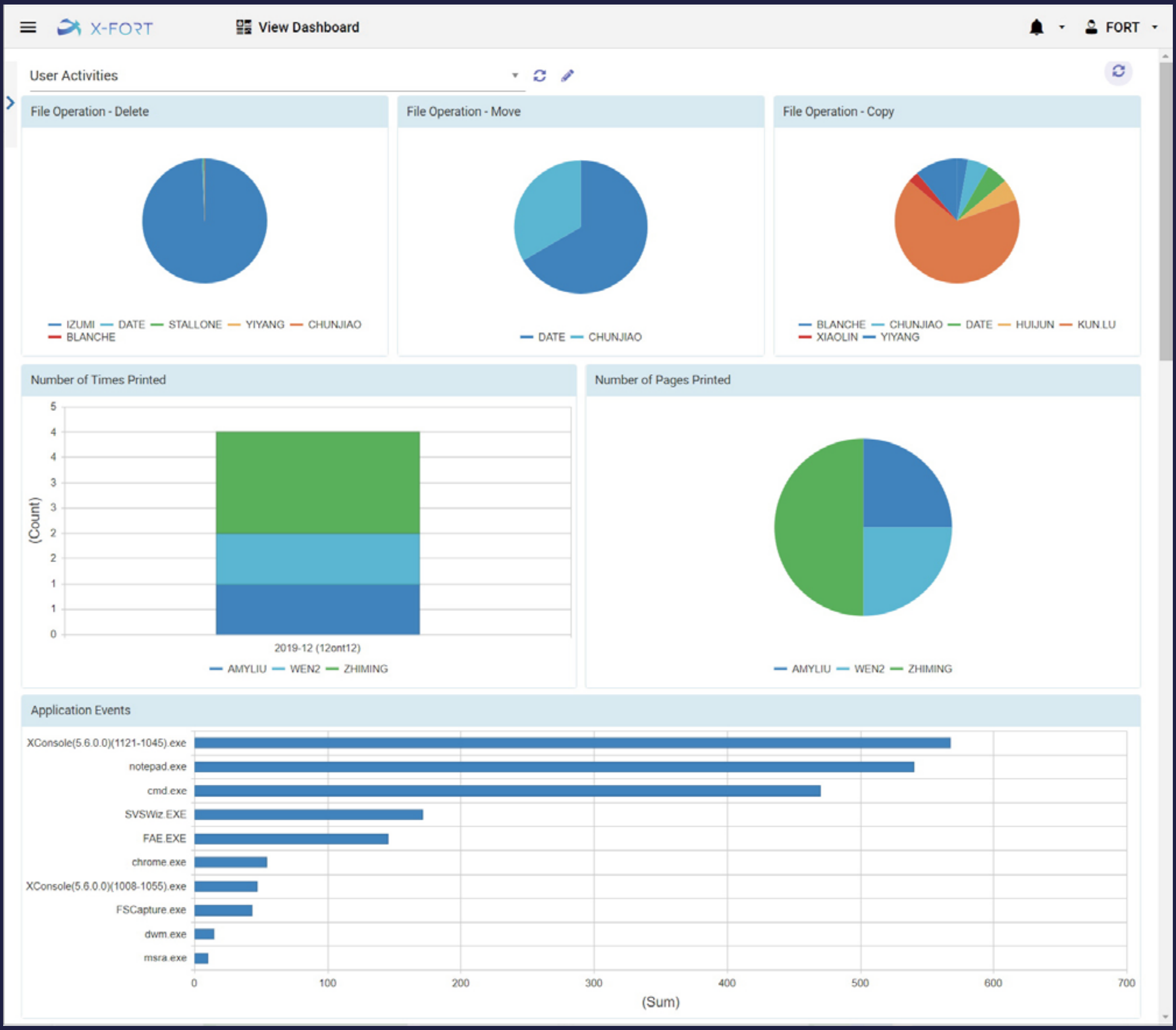
Keeping corporate information safe and compliant has never been easy. Organizations are taking steps to make the information safer by increasing security budgets, educating employees on company-wide best practices, and looking for data leak prevention solutions. Each year, data breaches are responsible for costing companies millions of dollars and continues to happen.
X-FORT is a client-server solution that provides a comprehensive endpoint security solution includes Data Leak Prevention, Data Protection, IT Asset Management, and Endpoint Detection & Response. It protects confidential information against insider threat and malicious behavior; besides, it can detect and respond to abnormal events.

Functions include Control, Manage, Monitor, React, and Audit.

- Control removable devices and any connected peripheral devices.
- Monitor network activities, such as web application, instant message, SMB shares, email, and FTP.
- Manage hardware assets, software license, and application whitelist.
- Provide file encryption to strengthen the protection.
- Get comprehensive endpoint activity log for analysis and forensic.
- Monitor and detect irregularities, and response proactively to reduce risk.
- Real-time and interactive dashboard help audit and investigate potential threats.

Features

- One agent protects everywhere.
- Role-based access control and management.
- Efficient and easy to deploy and use.
- Function module required on demand.



Client Agent Function

Category		Module	Function	Description	Opt.
DLP	Local Security	Storage Device Control		● Flexible control mode: Disable, read-only, plaintext, encryption ● Support external HDD, USB drive, SD card, MP3, etc. ● External storage device registration method: Hardware, software, serial number ● MTP (smart phone) control ● MBR and BitLocker disk protection: Protecting data from access HDD by other system	O
		Adv. Storage Device Control		● Copy file to external storage device with supervisor approval ● Limit size of daily copy or single file to an external storage device	O
		CD/DVD Control		● Disable disc recorder (CD / DVD / HD DVD / Blu-ray) and disable burning applications ● X-BURN：(1)Burned into ciphertext or plaintext with comprehensive log & alert (2)Burn CD/DVD with supervisor approval	O
		Printing Control		● Configure printing policy for each local or network printer ● Watermark enforcement ● Backup the printed pages or file ● Allow temporary printing or cancel watermark with supervisor approval	O
		Operation Log*1		● System file activity & operation record: Record system file deletion and rename event (includes command mode operation) ● User activity & operation record: (1) Application execution and operation (2) Web browsing (3) OS login & logout (4) File operations includes create, copy, move, rename and delete	O
		Adv. Operation Log		● Microsoft Office file access control and log (open, save, save as) ● Clipboard log (copy, paste text) ● Record CMD and PowerShell input and output text	O *1 Req.
		Other Control		● Device lockdown: Prevent using unauthorized device ● Port and tools protection: IrDA transceiver, Bluetooth, file transfer software, PrtScr key, remote control, GHOST, VMware, Virtual Box, Hyper-V, P2P software, SHARE tools, registry editor, sound card, etc. ● Disable the built-in or USB wireless network card ● General device control: Disable devices in Windows Device Manager ● Control Windows virtual devices, e.g., mobile phones, digital cameras, MP3 phones	O
		X-DISK		● Private encryption virtual drives: Store important files, and record user's behavior on X-DISK	O
	Network Security	Folder Sharing Control		● Network folder sharing control: Disable, access record, backup files transfer ● Email notification while network traffic and the number of file deletion exceed the threshold	O
		Connection Control		● Enable or disable communication ports, e.g., FTP, HTTP ● Allow to use communication port with supervisor approval ● Application access control & network access control	O
		Transfer Control		● IM control: Disable IM software, disable file transfer, disable screen snapshot, disable desktop sharing and record chat message. (Support Line, Skype, Tencent QQ, WeChat, AliWangWang) ● Video Conferencing Application control: Disable file transfer; log and backup transferred file (Support Microsoft Teams, WhatsApp, Zoom, Webex Meetings, Webex Teams, DingTalk, BlueJeans, GoToMeeting, Slack, Chatwork, Telegram, Viber) ● FTP: Disable FTP or record & backup FTP transfer ● Wireless access: (1) Disable 3G / 4G & dial-up application (2) Disable WiFi service	O
		Web Browsing Control *2		● Web access control: - Record user browsing behavior, search term and tag visited destination country - Allow user to browse website during specific period (e.g., browse Facebook after hours) - HTTPS control: Support user defined blacklist and whitelist, and record blocked website browsing ● Advanced web access control:Disable open file, save as, printing, keyboard, copy, paste, drag & drop, backup upload files ● Network traffic monitoring: Daily upload and download traffic alerts ● Allow web access with supervisor approval	O
		Cloud Control		● Control sync application and URL of cloud drive ● Control web based cloud service ● Control application using HTTPS connection (TLS / SSL) ● Control Microsoft Office save as to cloud drive	O *2 Req.
		Web Content Log		● Record content of web page ● Support HTTPS/HTTP	O *2 Req.
		Webmail Log		● Retrieve webmail text content of Outlook.com, Yahoo! Mail, Gmail and Openfind Mail2000 ● Backup the attachment of Yahoo! Mail and Openfind Mail2000	O *2 Req.
		E-mail Control*3		● Allow specified SMTP mail server ● Record and backup e-mail content ● Support Outlook client	O
		Outlook Attachment Encryption		● Auto encrypt the attachments while sending e-mail ● Send the decryption password with supervisor approval ● Prohibit email sending with specified domain name or keywords, and record blocked activity	O *3 Req.
		Secure Virtual Tunnel		● Only allow client with X-FORT agent to access protected servers ● Only dedicated users, devices, or software can connect to protected servers ● The communication uses TLS encryption to prevent MITM	O

Category		Module	Function	Description	Opt.
ITAM	IT Asset Management	Software Security	Application Execution Control	● Record prohibited and unmanaged application execution ● Allow to execute specified application during specific period ● Allow application execution with supervisor approval	O
			Folder Access Control	● Isolate files in safe zone to prevent malicious access, e.g., ransomware ● Only specified software allow access safe zone	
			Advanced Application Control	● Disable the function of specified application: open file, save as, printing, keyboard, copy, paste, drag & drop, and backup upload files ● Gradient style screen watermark: Avoid color absorption by background	
		Hardware Assets		● Hardware asset management ● Hard drive utilization information & alert ● Procurement management of computer hardware and peripherals	O
		Software Assets		● Software asset management: (1)Software license management and allocation (2)Software suite and alias management ● Hotfix management and Registry management ● Enforce remotely uninstall software	O
	Remote Management	Remote Function		● Remote wake-up, logout, reboot and shutdown the client ● File deployment: Support for immediate or scheduled delivery, file transfer, transmission bandwidth management, and seeding delivery ● Message broadcast ● Remote view and control computer ● Online help desk and service satisfaction survey ● Remote scan and find the files with specific keywords ● X-Monitor: (1)Support multi gridview on one screen (2)Supervisor can Live monitor the computer screen	O
		Screen Capture		● Capture screenshots at predefined time intervals ● Capture screenshots while execute specific application ● Adjustable image quality and interval time ● Screen capture with specific operation, e.g., switch windows, copy to clipboard, Microsoft Office operation	O
DATA PROTECTION	Document Management	Content Filter and Classification		● Filter by regular expression and keyword ● Filter content of file while writing file to external storage device, sending file on IM software, and emailing attachment in Outlook; When match the rule, block the actions, backup the files, and add tag in the log ● Webmail: filter mail content and attachment, when match the rule, backup the files, and add tag in the log	O
		File Locker		● User decides to encrypt the files, support encrypt single file or batch ● User-friendly: double-click file to auto decrypt file; auto encrypt when file close ● DEF (Document Encryption Folder) - Auto encrypt all files in the DEF folder, and auto encrypt new files - Applicable root directory and cloud sync folder (Server OS is not applicable)	O
EDR	EDR	Incident Response		● Monitoring and detecting irregularities ● Proactive response to mitigate risk, including screen watermark, alert, restrict network access, block untrusted storage, and block printing ● Record various violations, response actions and remediation	O
MGMT	System Management	Client		● Self-protection: Prevent agent destroyed by malicious user or application ● Support Windows safe mode and AD user profile roaming ● Security incidents alert and notification	S

Server Function

Category		Module	Function	Description	Opt.
MANAGEMENT	Server	Main Server		● Support database backup and restore ● Optimized server and client data exchange bandwidth ● File encryption with PKI & AES-256, support HSM key management ● Single server supports more than 1,000 Clients ● Support Microsoft Azure, private cloud, public cloud, and hybrid cloud ● Store backup files on relay server	S
			Console	● Multi-language support: English/Japanese/Traditional Chinese/Simplified Chinese ● Role-based management: Administrators, group managers, auditors, and others ● Compliant with password complexity, password length requirements, and password change enforcement	
		Backup Server		● Multi-server support active-active load balance, assign client to specified server based on network segments	O

System Requirement

Server	Windows Server 2022, 2019, 2016
Database	Microsoft SQL Server 2022, 2019, 2016, 2014
Client	Windows 11, 10, 8.1, 7 & Windows Server 2022, 2019, 2016

Ultimate Security for Business Longevity

FineArt

E sales@fineart-tech.com T +886-3-5772211 A 8F, No.18, Puding Rd., HsinChu City 30072, Taiwan