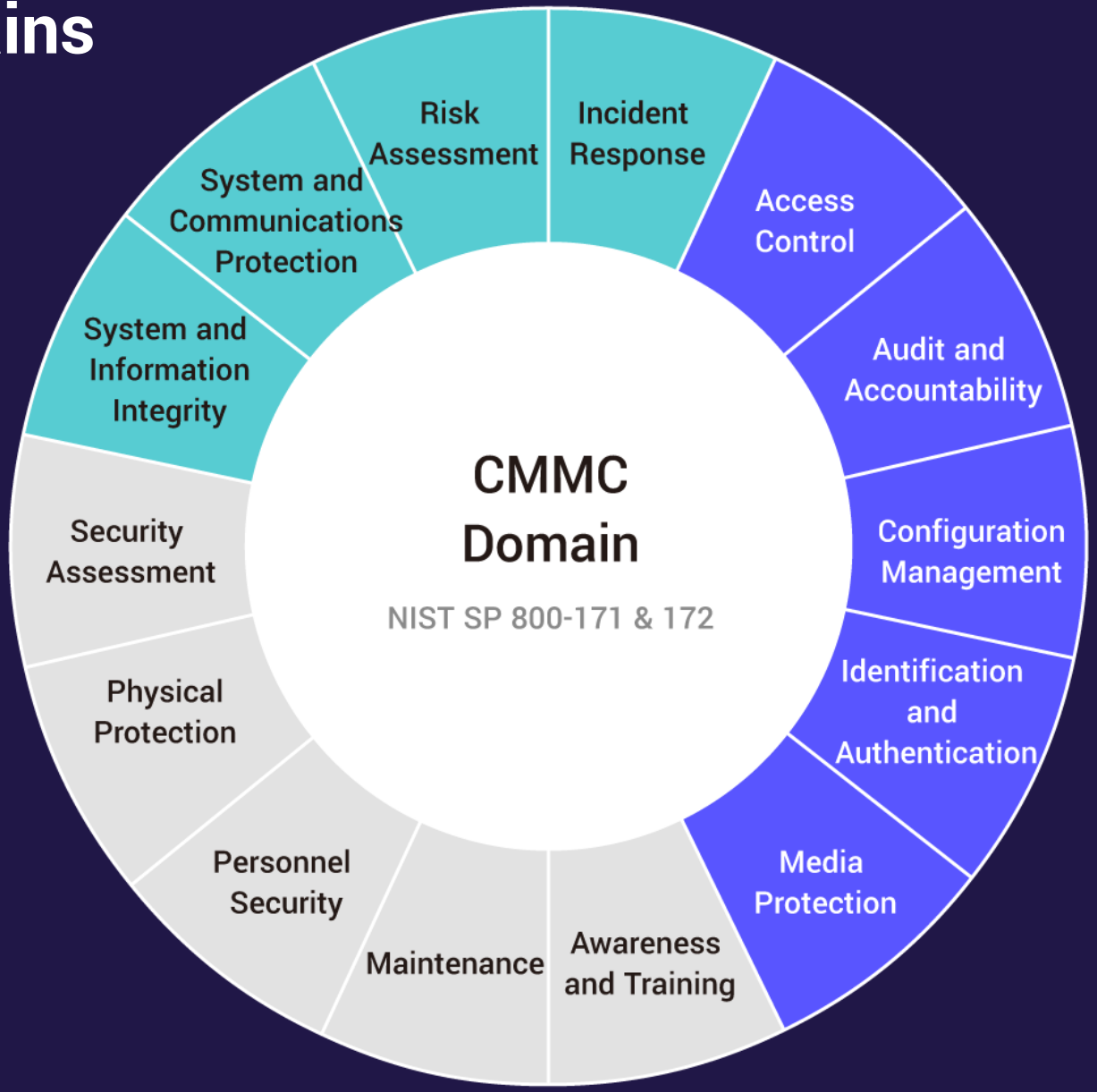
外洩無門：CMMC下的資料外洩防護對策
CMMC compliance : How DLP solutions can help?

Alden Chen

alden@fineart-tech.com

FineArt

CMMC Domains



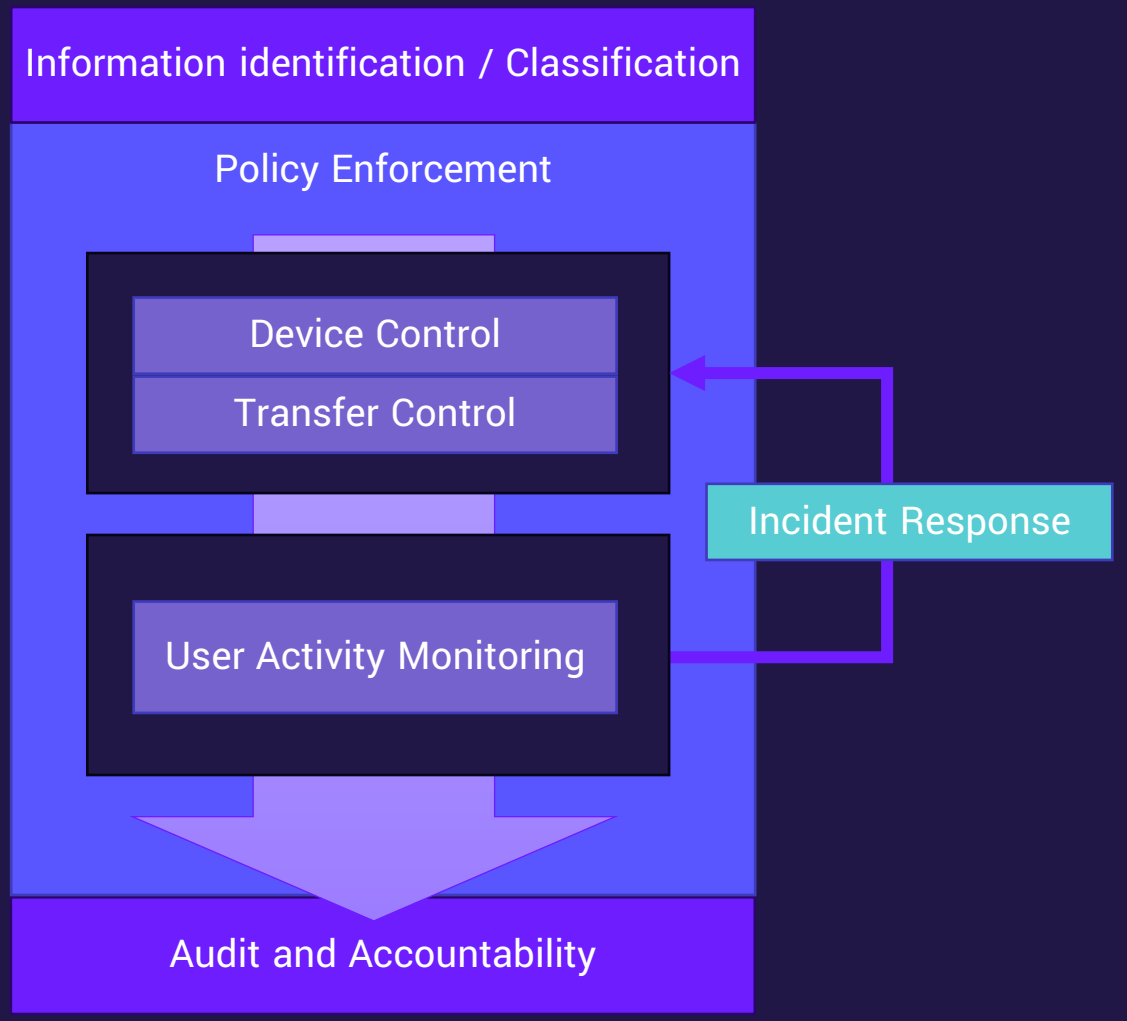
Endpoint DLP tool
Other Security tool
Administrative Process

X-FORT

Data Protection in DLP

Data Protection in DLP

- Information identification / Classification
  - Inventory / Discovery
  - Tagging and annotation
  - Encryption
  - Access control
- Device control
- Information transfer control
- Audit and accountability
- User activities monitoring
- Policy enforcement
- Incident response



X-FORT

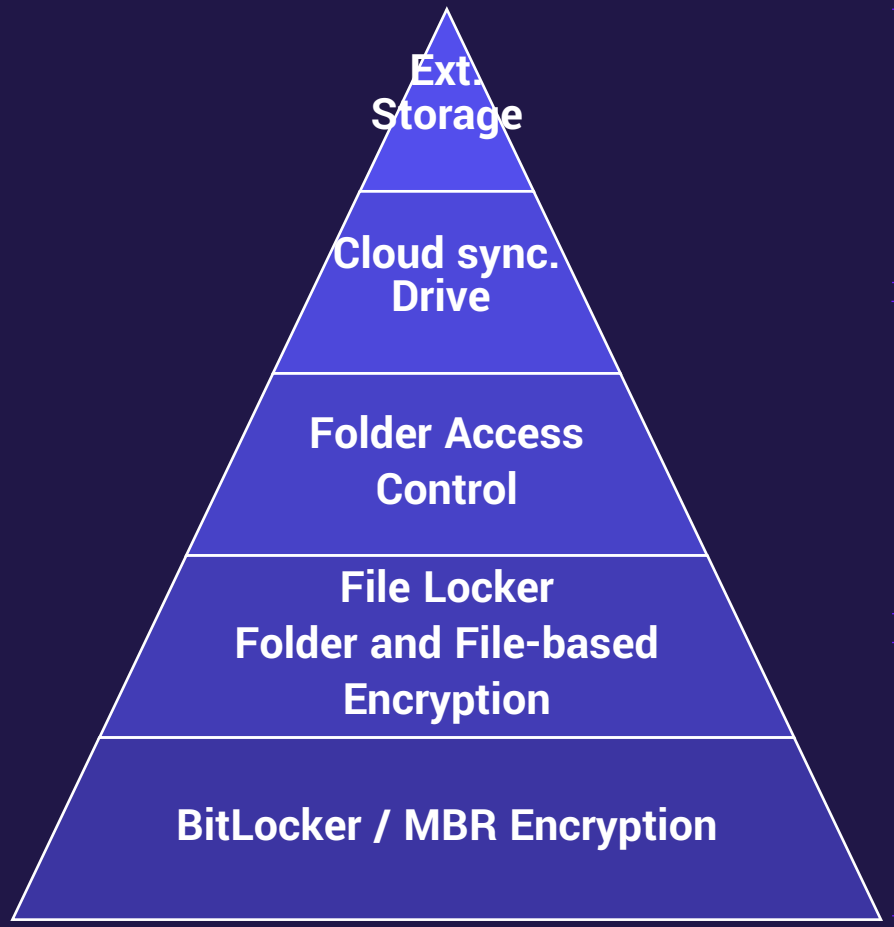
Information identification / Classification

- Identify and safeguard CUI by monitoring data flows, enforcing policies, and preventing unauthorized access or disclosure.
  - Regular expression
  - Out-of-box information type pattern
- Inventory /Discovery
  - Local storage on endpoint
- Classify data and establish access controls based on data classification.
  - Outlook Context / attachment
  - Instant Messaging / Net Meeting file upload
  - External /Removable storage
  - Web access / Upload Files
  - Web Mail context / attachment
- Tagging and annotation
  - Local DB
  - Matched summary
  - Record activities with classification tags and shadow files (evidence)
- Mandate the encryption of data based on its classification or other attributes.

X-FORT

Data encryption

Protecting data in transit and at rest



3

Data in transit

File upload (Web), external storage, IM/FTP
File transfer

2

Data in use

Authorized /Trusted processes
Application whitelisting (AWL)

1

Data at rest

File system-based protection

X-FORT

Device control

- Inventory Management: Know your asset (which access CUI)
  - Hardware
  - Software
  - Managed peripherals
- Zero trusted control
  - Device lockdown
  - Preventing connections from unknown devices
  - Register identified/trusted device

X-FORT

Information transfer control

Transfer Channel

- Webmail
- IM / Net meeting
- Transfer to External Storage
- Copy to, upload files to website

Reaction

- Content filtering
- Attachment
- Blocking
- Tagging
- Shadow file

X-FORT

User Activities Monitoring

- File operation
  - Create, Rename, Delete, Move, Copy items
  - Folder/ Files access by restricted apps
  - Copy to clipboard

- Network activities
  - Browsing
  - Copy to network share
  - Restricted network connection

- Application activities
  - Execution / Process
  - Network access
  - File access protection

- Data transfer
  - Copy to USB removable device
  - Upload to a restricted cloud service
  - Paste to supported browsers

- Printing
  - Watermark
  - Pages and Files shadows

- Desktop session recording
  - Application
  - Web access
  - Instance Message / Net meeting
  - Office open/save/clipboard
  - Copy to Clipboard
  - Unconditional

X-FORT

Incident Response

Based on user operations and activities, Detecting

- USB / External device
- User activities
  - File operation
  - Web access
  - Printing
- Network share access
- Communication port
- RDP in /out

Response and Reaction

- Blocking
  - Shutdown
  - Disable network connection
  - Disable USB external storage
- Dynamic adaptive policy
  - Replace User/Computer security policy
  - Enable file operating audit log
  - Enable printing control
- Notification and alert
  - Screen watermark
  - E-mail, Teams, Line

X-FORT

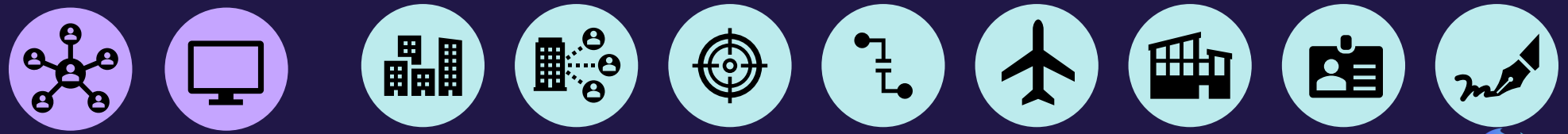
Policy enforcement

Endpoint Security Policy

- Role-Based Policing
  - User / OU / Group
  - Computer / Group (Unconditional)
- Dynamic (Conditional) deployment
  - Auto
  - Network segment
  - Incident responsed
  - Out of field ?
  - Temporary
  - Baseline
  - Unauthenticated

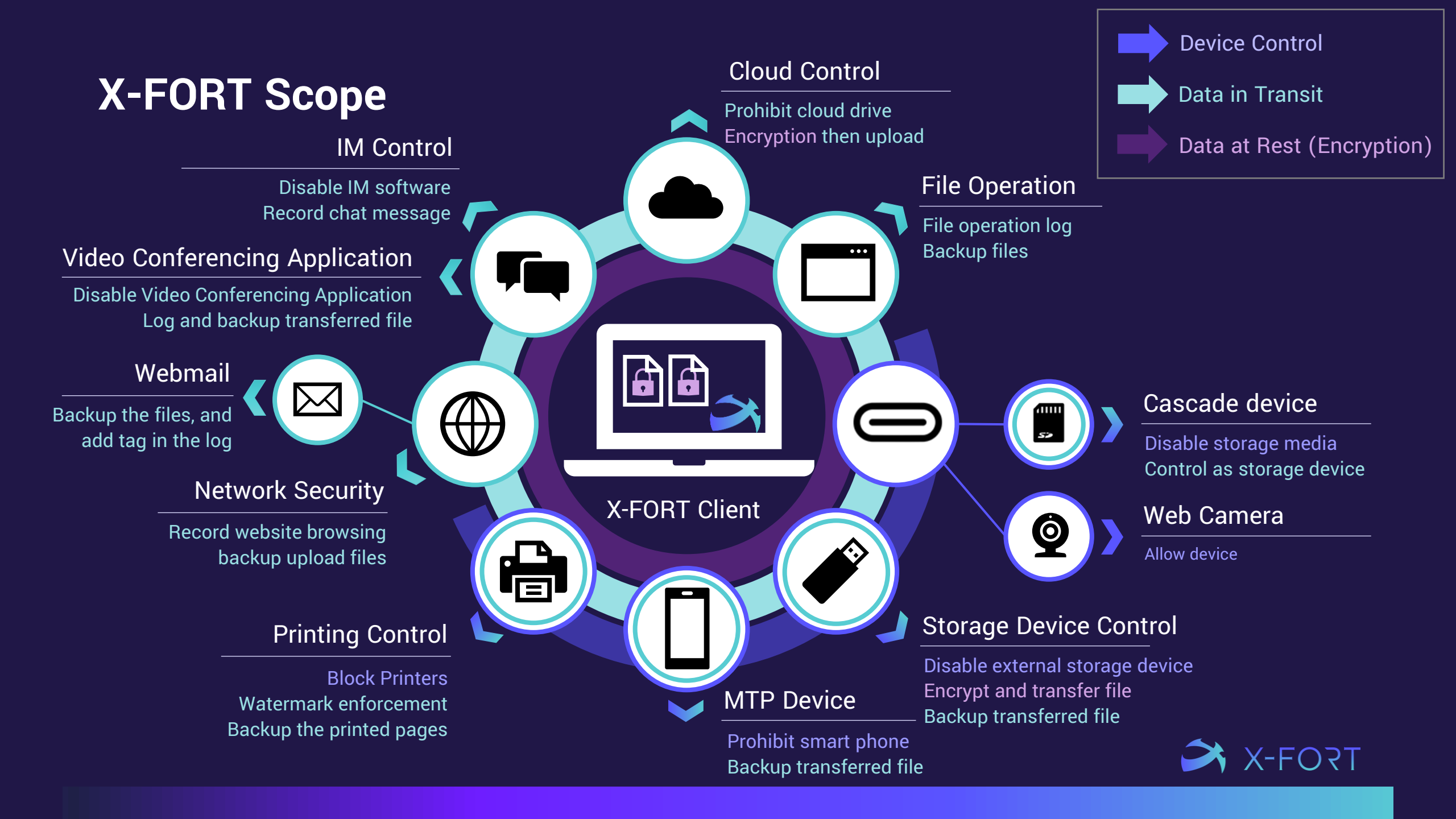
Practice

- Best (PEP, Policy Enforcement Point)

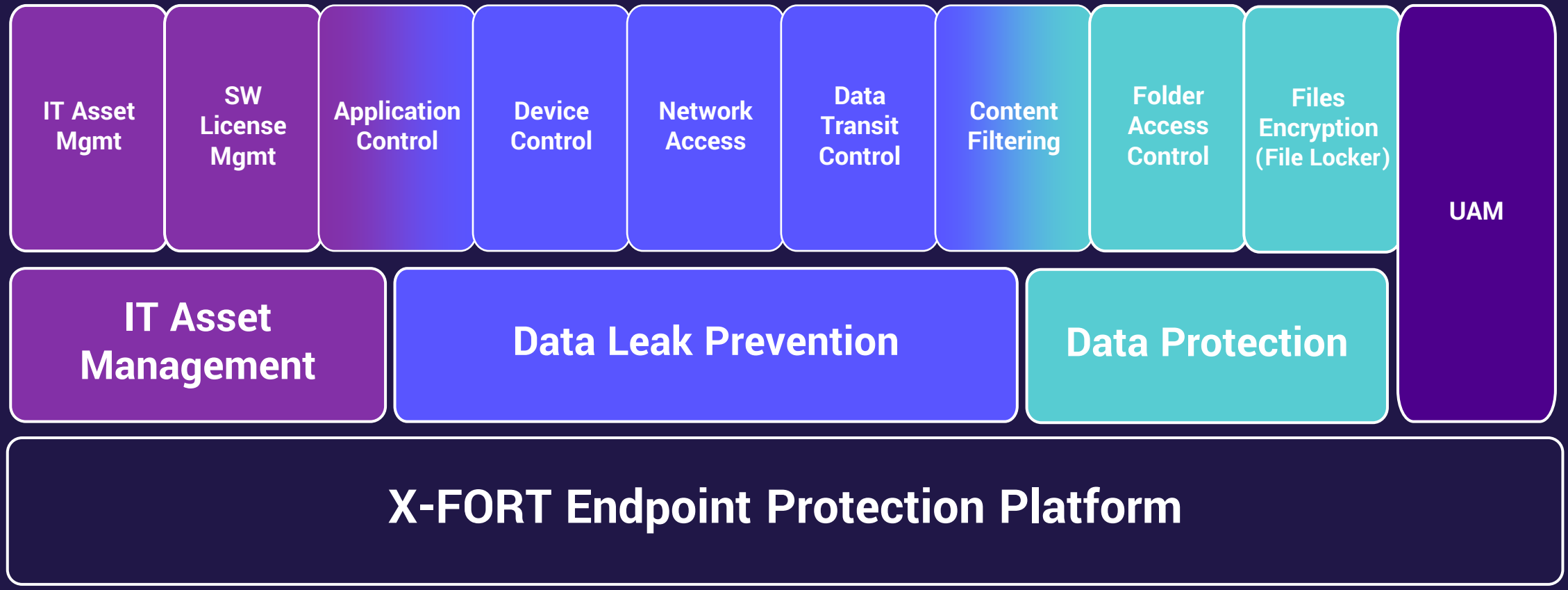


X-FORT

X-FORT Scope


Device Control
Data in Transit
Data at Rest (Encryption)
Cloud Control
Prohibit cloud drive
Encryption then upload
IM Control
Disable IM software
Record chat message
File Operation
File operation log
Backup files
Video Conferencing Application
Disable Video Conferencing Application
Log and backup transferred file
Webmail
Backup the files, and
add tag in the log
Network Security
Record website browsing
backup upload files
X-FORT Client
Cascade device
Disable storage media
Control as storage device
Web Camera
Allow device
Printing Control
Block Printers
Watermark enforcement
Backup the printed pages
MTP Device
Prohibit smart phone
Backup transferred file
Storage Device Control
Disable external storage device
Encrypt and transfer file
Backup transferred file
X-FORT

X-FORT endpoint data protection



X-FORT

Ultimate Security for Business Longevity

www.fineart-tech.com

FineArt