Agenda

• Security and Trends Affecting MFP Security
• Customer Security Needs and Concerns
• Canon’s imageRUNNER ADVANCE Security Features, Software Solutions, and Services for Security
  – Authentication and Access Control
  – Document and Information Security
  – Data Security
  – Logging/Auditing Security
  – Network Security
Security in the News and Trends Affecting MFP Security
Security Breaches are Increasing, and are Risky and Costly

• Concerns:
  – Data Breach
  – Identity Theft
  – Privacy
  – Compliance
  – Mobility
  – Cloud

Security Breaches are more and more frequently heard of in the News!
What are Current Trends Affecting Security Today?

• New solutions for creating, accessing, processing and producing content and documents.
• Users need “untethered” access to document/content resources
• MFPs evolve as “on and off ramp” to cloud solutions.
  – “Scan to” and “print from” cloud solutions
  – Cloud migration impacts the paper to digital conversion

Security and the MFP

- Not thought of as vulnerable
  - Easier to hack without detection
  - Has a hard drive, memory, keyboard, panel, network connectivity = system
  - Requires the tools to have the “who, when, what” usage data
  - Authentication?

- Typical breaches if not in place
  - Stolen or guessing at others’ credentials
  - Capturing data from other users
  - Sending data externally to retrieve or printing documents
  - Backdoor remote access
  - Disabling controls in place, tampering

Customer Concerns and Needs for Security
Can you Find Security Risks Below?

- Printed docs leave a trail
- Device Access is Open
- Visiting staff
- Information in the Bin
- Personal Printers
- Docs left on printer
What you Can Do to Address these Security Risks?

**Audit**: Log all print, scan, fax data operations, content aware data processing

**Authentication & Access**: Restrict access to devices/function

**Data Security**: Secure hard drives

**Authentication**: Secure guest printing (Mobile)

**Destination Restrictions**: Prevent unauthorized document distribution

**MPS**: Reduce personal printers, or Include in Management
imageRUNNER ADVANCE Security Features and Solutions
Security Needs and Requirements for MFP

- HDD Data Confidentiality
- Information and Document Security
- Secure Architecture
- Network Security
- Authentication & Access Control
- Logging/Auditing Security
Your Concerns about MFP Device Security

• How can I ensure privacy and prevent a data breach?
• How can I ensure the privacy of my data after the life of my imageRUNNER ADVANCE?
• How can I ensure security features and settings are consistent across my entire fleet efficiently?
• How can I monitor activity that is occurring at the devices?
• How can I allow access to certain types of activity based on type of user?
• How can I integrate my company’s authentication policy with my imageRUNNER ADVANCE?
• How can I be sure that my document permissions follow my document workflow, from scan and into my Content Management System?
• How can I know and control when my Data is erased?
• How can I prevent my device from being hacked, and data residing on the device accessed?
Security Features Overview

**Document Security**
- Document Scan Lock & Tracking
- Send to Myself (only)
- Adobe® LiveCycle® Rights Management ES2
- Encrypted Secure Print
- Watermark/Secure Watermark
- Copy Set Numbering
- Encrypted PDF (AES 256 support)
- Digital Signature PDF
- Fax Forwarding
- Fax Destination Confirmation
- uniFLOW Secure Print
- AAPrint
- Universal Login Manager
- Therefore Document Security

**Data Security**
- TPM
- HDD Data Encryption
- HDD Data Erase (Standard on Next Generation)
- HDD Initialize (up to 9 times overwrite)
- HDD Password Lock
- HDD Erase Scheduler
- Advanced Box Security
- Mail Box Password Protection
- Job Log Conceal
- Removable Hard Disk Drive*

**Network Security**
- IP/MAC Address Filtering
  - IP + Port Filtering
- SSL Encryption/TSL Encryption
- Network Application On/Off
- USB Port On/Off
- Destination Restriction
- IP Sec (Standard on Next Generation)
- IEEE802.1 x (Wired/Wireless)

**Mail Server Security**
- POP Authentication before SMTP
- SMTP Authentication

**Device Security**
- IEEE2600.1 Common Criteria Certification (for all ADVANCE Next Generation)

**Logging / Auditing Security**
- imageWARE Secure Audit Manager
- imageWARE Secure Audit Manager Express

**Authentication**
- Department ID/Control Card Systems
- Device Level Login
- Active Directory Login
- LDAP Server (Lotus Domino and Novell eDirectory) Login
- Access Management Systems (AMS)
- Function Level Login via AMS
- Authorized Send
- Smart Card Authentication
- Advanced Authentication-Proximity Card

**Disclaimer:** For supported devices and details regarding standard or optional feature or additional solution, please refer to the imageRUNNER ADVANCE and Software Products’ specifications and features.
Authentication and Access Control
Customer Concerns about Authentication and Access Control

• Can anyone walk up and access the device?
• How can I control access and usage of our network communication such as email, scan, fax?
• Can I restrict usage by department or employee?
• Could the use of network device or device feature access cause compliancy violations?
• I need to restrict capabilities by role, do all users have the same privileges?
• If a breach or threat occurs is there a method to track activity and usage to identify the origination?
• I need to customize my login screen to contain pictures of my employees, and my company logo
• How can I be sure to print from my mobile device securely?
• Can I scan documents from my MFP to my cloud applications such as Google Docs securely?
Lock down devices to prevent unauthorized access

Require users to authenticate prior to copying or sending documents

**Authentication – Secure Device for Walk Up Use**

- Various levels of **DEVICE** based authentication
- Proximity and **CAC/PIV CARD** based authentication
• **Authentication**
  – **Device Based**
    • Department IT Management
    • Local Device Authentication
    • Simple Device Log-in (SDL)
    • Single-Sign-On
    • Authorized Send
    • Universal Login Manager
  – **Card Based**
    • Advanced Authentication (AA)PROX
    • Advanced Authentication (AA)CAC/PIV
    • Authorized Send
    • uniFLOW Secure Print
    • Universal Login Manager

• **Access Control**
  – **Access Management System (AMS)**
    • Standard on all imageRUNNER ADVANCE Models
# Authentication: Device Based

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Companies Who Need</th>
<th>What</th>
<th>Benefit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department ID Management</td>
<td>... basic standalone authentication &amp; device usage limitation features.</td>
<td>Define up to 1000, 7 digit numerical IDs &amp; PWs for device authentication.</td>
<td>• Know who accessed devices based on ID</td>
<td>• No AD integration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Usage tracking</td>
<td>• Manually configured via RUI.</td>
</tr>
<tr>
<td>Local Device Authentication Simple Device Log-in (SDL)</td>
<td>... to use personal ID for standalone authentication.</td>
<td>Define IDs &amp; PWs using personal info for device authentication. Max user #:1000</td>
<td>• Messages sent from device include senders email address.</td>
<td>• No AD integration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Manually configured via RUI.</td>
</tr>
<tr>
<td>Single-Sign-On (H)</td>
<td>.... authentication solution with higher level of security and AD integration.</td>
<td>A hybrid of SSO-K and SSOV3, supports NTLM, Kerberos, and local.</td>
<td>• AD Integration</td>
<td>• Has AD integration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Kerberos support.</td>
<td>• Local user#: Max :5000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• AMS V2.0 support</td>
<td></td>
</tr>
<tr>
<td>Authorized Send</td>
<td>....requires authentication to all send features, Scan to Email, Scan to Fax, Scan to Folder, while keeping daily walk-up features such as copy, open</td>
<td>Supports NTLM, Kerberos, LDAP. Supports a wide variety of enterprise systems, authentication servers and LDAP-servers using common protocols.</td>
<td>• AD Integration</td>
<td>• AD Integration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Novell NetWare / eDirectory</td>
<td>• Customizable solution</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Flexibility to authenticate in a variety of ways only at the point of sending is differentiator</td>
</tr>
<tr>
<td>Universal Login Manager (Device or Card based)</td>
<td>...authentication solution that integrates with Access Management Controls that can either be Device based or Card based and also tracks usage at the device</td>
<td>Multiple Authentication Modes: Authenticate at device personalization by selecting photo, or user name, password, or use of a proximity card as well.</td>
<td>• Serverless solution for device authentication</td>
<td>• Has AD integration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• IT administrator can set access permissions and share across devices</td>
<td>• Easy upgrade path to uniFLOW</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Usage Tracking</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Device Personalization</td>
</tr>
</tbody>
</table>
About Universal Login Manager (ULM)

Universal Login Manager is a **Server-less** solution for all iR-ADV devices offering Multiple Device and Card-based login modes and Usage tracking functionality

**Key Features of Universal Login Manager:**
- Provides Prox card, PIN Code or Active Directory Login
- Allows tracking the usage on the iR-ADV devices
- Device personalization (Image based login)
- Integration with Access Management System
- Easy and simple upgrade to uniFLOW Server
IT Administrator: Universal Login Manager

- Server-less solution with easy set up and administration
- Allows integration into company network via AD
- Control physical access to device, per user and function (via Access Management System integration)
- Flexible proximity card support (using MiCard PLUS)
- Fully Customizable login screen
- Simple Reporting and Usage Tracking
- Shares Login credentials to other MEAP applets installed to ensure smooth user experience
Card Based Authentication
## Authentication: Card-Based

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Who</th>
<th>What</th>
<th>Benefit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card-Based</td>
<td>Companies who need ...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| AA PROX             | ... basic standalone authentication & device usage limitation features. | Based on SSOH, Supports Proximity Cards, Integrates with Access Management System | • Know who accessed devices based on ID  
• Usage tracking  
• Sender information sent with scans | • Local Device and AD Integration |
| AA PROX/CAC PIV     | ... government solution for Card based authentication | Based on SSOH, Supports Proximity Cards, Integrates with Access Management System | • Know who accessed devices based on ID  
• Usage tracking  
• Sender information sent with scans | • Specially developed for Government requirements |
| UNIVERSAL LOGIN MANAGER | ...authentication solution that integrates with Access Management Controls that can either be Device based or Card based and also tracks usage at the device | Multiple Authentication Modes: Authenticate at device personalization by selecting photo, or user name, password, or use of a proximity card as well. | • Serverless solution for device authentication  
• IT administrator can set access permissions and share across devices | • Has AD integration  
• Easy upgrade path to uniFLOW  
• Usage Tracking  
• Device Personalization |
| UNIFLOW SECURE PRINT | ...Fleet-wide card based Authentication and Follow-me Printing Capabilities | Enterprise solution for secure follow-me print solution. Supports proximity cards, | • Most robust and modular solution with extended output management capabilities in addition to security | • Server-based Enterprise scale solution  
• AD, LDAP, Usage Tracking, Intelligence Reporting |

**Authentication and Access Control**

**SECURITY**
Card Based Authentication

**Embedded/Serverless**

- AA Prox
- AA CAC/PIV
- ASEND CAC/PIV *(Federal Gov’t)*
- Universal Login Manager

**Server Based**

- uniFLOW Secure Print
What is Access Management System?

A standard device management feature which allow you to assign access restrictions to users/user groups to restrict entire functions or specific features within a function.

<table>
<thead>
<tr>
<th>Job Type</th>
<th>Common Security concern for each iR device job function:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Copy</strong></td>
<td>An internal employee copying a confidential document and taking it off the premise with the intention of unauthorized sharing and distribution.</td>
</tr>
<tr>
<td><strong>Print</strong></td>
<td>An internal employee printing a confidential document and taking it off the premises with the intention of unauthorized sharing and distribution.</td>
</tr>
<tr>
<td><strong>Scan</strong></td>
<td>An internal employee converting a confidential document into electronic format using scan function, for easy unauthorized electronic distribution.</td>
</tr>
<tr>
<td><strong>Send</strong></td>
<td>Information leaks via Universal Send emails that contain confidential information.</td>
</tr>
<tr>
<td><strong>Fax</strong></td>
<td>Internal employees using the fax function to distribute confidential information to unauthorized recipients.</td>
</tr>
<tr>
<td><strong>Web</strong></td>
<td>Internal employees using the web access function to access confidential information.</td>
</tr>
</tbody>
</table>
Access Management System

Limit access to specific functions based on authentication

**AMS (with Device level log-in)**

Unusable functions are lightly displayed and cannot be selected.

Only the usable functions can be operated.

**AMS (with Function level log-in)**

Usage not restricted

Usage requires log-in
Secure Mobile Printing

Canon Direct Print and Scan for Mobile (DPSM)

- Provides mobile printing and scanning for iPhone, iPad, Android tablets/phones, and Blackberry smartphones
- Integrates with any Canon supported authentication method (e.g., AA-Prox, ULM, SSO, Dept. ID. 3rd Party MEAP applications, etc.)
- Supports usage tracking for Mobile printing
- To enable Security and Tracking, the mobile device must scan a Barcode in the DPSM application on the device, or to create a security code to print and release a job (SSL must be activated)
Secure Mobile Printing

**uniFLOW Secure Mobile Printing**

- Supports any Canon’s Authentication methods, and more. Supports Prox card, smart card, magnetic swipe card, username/password or PIN
- Secure print release at any device with a single platform
- Extends mobile printing to all of the output management features and benefits of uniFLOW
Secure Cloud Printing/Scanning

Print securely via Google Cloud Print

Authentication for Apple iPhones/iPADs

QR code on display for easy device Authentication for Google Cloud Print
Document and Information Security
Secure Distribution of Confidential Documents

- Is there a requirement to **secure Prints and Scans** produced through an MFP?
- Do prints with **sensitive information** lay open on the output tray? Are they always picked up?
- Is there a method of reducing the security risk for **scanned documents**?
- Can I **prevent** mistakes or fraud of certain documents and information being distributed externally?
- How can I maintain privacy and security for files being **routed for digital workflows**, and being stored and accessed from a **Content Management System**?
Securing Confidential Documents- Standard Device-based PRINT Solution

SECURE PRINT

• Jobs are held securely at the MFP until released by the user entering the correct password. Prevents documents from being left out in a device tray unattended.

• Secure Print Delete Time can be selected from 10/20/30 minutes in addition to 1/2/3/6/12/24 hours (default: 1 hour).
Securing Confidential Documents – Optional Device Based PRINT Solution

**ENCRYPTED SECURE PRINT**

Two layers of security:
1. Encryption of Document Data itself using AES 256
2. Password Protection

- The encrypted data will not be decoded until the user enters the correct password
- After printed out, the data will be deleted
- Secure Print Delete Time can be selected from 10/20/30 minutes in addition to 1/2/3/6/12/24 hours (default: 1 hour).
Securing Confidential Documents - Device based Serverless SECURE PRINT

### AA Print Serverless Secure Printing
- Print jobs are held at the **Device**, until user walks up and authenticates for Release
- Print Anywhere support, uses Advanced Box of imageRUNNER Device
- Reporting by User/Device Supported
- Simple Implementation
- Meter Reads Supported
- imageRUNNER ADVANCE and SFP Models, MEAP Enabled LBP Supported
- Upgrade to uniFLOW
- Personalization Supported
- Access Management System Integration Supported
- New Bundle of AA-Print with AA-Prox is available to link Authentication and Secure Print Solution together

### uniFLOW Serverless Secure Printing
- Print jobs are held at the **Device**, until user walks up and authenticates for Release
- imageRUNNER ADVANCE and Compact MFPs supported
- Secure Print to device only, doesn’t support Print Anywhere
- Upgrade to uniFLOW
Securing Confidential Documents - Server based PRINT

- Print jobs are held on server until user identifies themselves and releases the job
  - Provides “pull-print” style secure printing
  - Job can be released to any Canon, HP or standard PCL or postscript printer
  - User can see the secure jobs waiting for them on any device they go to

User can change the printing options of the job, including double sided, the number of copies and the page range to print.

SERVER BASED Fleet Wide
Securing Confidential Documents - COPY

- Secure Watermark
  - This embeds hidden text within the backgrounds of documents
  - If a copy is made, the hidden text appears on the resulting pages, making clear that the copy is unauthorized.
Securing Confidential Documents - SCAN and SEND

- E-MAIL
- A-BOX/MAIL BOX/NETWORK FOLDER
- FAX
- CONTENT MANAGEMENT SYSTEM
## Securing Confidential Documents - SCAN and SEND

<table>
<thead>
<tr>
<th>Feature</th>
<th>E-MAIL</th>
<th>FOLDER</th>
<th>FAX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Restriction</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Digital Signature applied to PDF</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>PDF Encryption (Password Protected)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Adobe® LiveCycle® Rights Management ES Integration</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Document Scan Lock &amp; Trace</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Password Protected (Access)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Send to Myself (only)</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send to My Personal Folder (only)</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
</tbody>
</table>

**ATTRIBUTES APPLIED TO THE DOCUMENT AT MFP**
Document Scan Lock (1)

**Ability to embed scan lock information on the document and restrict copy/send/fax job**

- With Prohibit AllRestriction, the copy/send/fax job will be cancelled immediately.
- With Password Authentication, the copy/send/fax job is proceeded when the correct password is entered.
- With User Authentication, the copy/send/fax job is proceeded only if authorized user has been logged in the device with proper User ID and Password.

---

**Description**

- Ability to embed Scan Lock information ((hidden, background Track & Lock code or QR Code) on the copied and printed document to restrict unauthorized copy, send and fax of the document.
- The available restrictions are as follows:
  1) Prohibit All: No one can make any copy/send/fax.
  2) Password Authentication: Allow to make copy/send/fax only if proper password is entered.
  3) User Authentication: Allow to make copy/send/fax only to authorized user with proper User ID and Password.

**Benefits**

- Prevent information leakage by locking copy/send/fax function when the document is scanned/copied.
Document Scan Lock (2)

**Ability to track where the document is originated**

Description:
- Ability to embed hidden Tracking Information such as User Name, Date/Time and Device Name on the background of the copied and printed document.
- Document Scan Code Analyzer for MEAP allows you to track Who, When and with Which device the document was copied or printed by simply scanning the document on the device.
- Only authorized personnel can access the tracking information of the document by entering a required password.

Benefits:
- **Determine the user that created the copied / printed document for tracking and auditing.**
Securing Confidential Documents: Encrypted PDF for PRINT and SCAN (Optional Device-based Security Option with USend Security Feature Set)

File encryption helps prevent data leaks. Data is encrypted prior to being sent from the device.

Employed 256-bit AES encryption to meet with higher encryption needs.

At the PC, users can add passwords and restrictions to their documents.

Similar features are available with scanned documents from the device using Encrypted PDF.

Prevent information leakage to unauthorized users by protecting PDF documents with an encrypted password.
Send to Myself (only)

- Restrict all scan and send activity at the device to allow users once authenticated to send ONLY to their own email inbox.
- Prevents accidental or intentional security breaches of sending information to the unintended recipient.
- Operates with Login/Authentification functionality implemented at the device.
Send to My Personal Folder (only)

- Create Personal Folders on the device for users to Scan documents to a folder on the network unique to their login.
- The folder requires a password in order to access
- Prevents accidental or intentional fraud of scanning sensitive information for the unintended recipient.
Extended Key Chain: Authentication ID/PW Preset

- Ensure consistent security
- Users can associate their device ID and Password with login information from outside servers so no need to re-enter server login info at the device
  - LDAP, SMTP, Adobe LiveCycle Rights Management
- Authentication procedure is simplified to log-into server

User-A

User-B

SMTP
  Sender of e-mail from device will have Individual user’s address.

LDAP
  Information stored in LDAP server associated with user is retrieved without inputting ID/PW of the server

Adobe LiveCycle RM
  No re-entry of ID/PW to give rights management information to scan document

Pre-set User ID/PW with Server Login info
How do you ensure your information is security stored?

- End-to-End Security from Input, through Management, Process, Store and Search to Output
- Fully customizable Access Permissions
- Integrates with Windows Security and LDAP for Single Sign-On
- Maintains Authentication user credentials through entire document lifecycle process
- Track what users have been doing and what processes documents have gone through with Audit Trail
Enable/Disable settings for scan/print with memory media

Administrators can restrict “Use Scan Function” for Memory Media and “Use Print Function” from Memory Media respectively.

Description

- Administrators can restrict “Use Scan Function” or “Use Print Function” from Settings/Registration

Benefits

- Restrict usage of memory media depends on IT policies

When function is restricted, you cannot select “Memory Media”
Data Security
Hard Drive Data Protection – Privacy and Control

• We Need to maintain confidentiality of information during use and retiring of technology equipment
  – What information resides on the hard drives?
  – Can the information on the hard drive be compromised?
  – Can anyone access the information on the hard drive?
  – Is that information properly deleted?
  – Can I control how and when to erase information?
Advanced Control – Standard Security Features

- Privacy and protection.
  - **Standard** security features
    - HDD Erase: Removes latent images from hard drives
    - 9xHDD format: Secure erase of HDD during end of life
    - Trusted Platform Module: Protects passwords and encryption keys
    - IPsec: Ensures information security for Internet Protocol
    - HDD Password Lock
Hard Drive Data Protection

Further enhance the protection and removal of HDD data

**HDD Format (initialization)**
- Overwrite all image data, documents in Advanced Box and Mail Box, address book and device settings.
- Overwriting methods can be selected from User Mode.

**Data Erase**
- **Deletion of job data in a normal process**
  Only management data is deleted after output while the actual data remains on the hard disk.
- **Deletion of job data with Data Erase**
  Each output is overwritten with data or random data.

**Description**
- HDD Format (initialization) feature provides ability to overwrite all user data/settings stored in the hard drive.
- HDD Data Erase function automatically overwrites the image data when the job is completed or deleted from the hard drive. **HDD Data Erase function newly became standard on Next Generation imageRUNNER ADVANCE.**
- Numbers of overwriting while initialization is now increased up to 9 times.

**Benefits**
- HDD Format (initialization)-reduce concern for customer to destroy/remove hard drive to protect information at the end of Lease
- HDD Data Erase-ensure latent images are removed completely from the hard drive after each task
- 9 times overwriting for HDD Format is one of the highest in the industry (as of April 2012)
HDD Password Lock

Further enhance the protection of HDD contents

Description
- HDD Lock feature locks the HDD with password (32 bytes). Password is automatically generated and given by device.
- The HDD Lock ties the HDD to the imageRUNNER ADVANCE device only, rendering unreadable if removed.

Benefits
- to analyze the data stored in the hard drive.
- HDD Password Lock: prevents access to HDD from PC when it is removed from devices.
TPM (Trusted Platform Module)

Provides tamper-resistant capability for confidential information

Description
- TPM (Trusted Platform Module) is a tamper-resistant security chip, equipped in all imageRUNNER ADVANCE models for an enhanced device data security
- TPM generates secure cryptographic keys to encrypt and decrypt confidential information such as password, certification, and encryption key before being stored into or being retrieved from the HDD and other memory components respectively

Benefits
- Prevents leakage of confidential information, since the encryption key to retrieve data on the HDD is stored and controlled in a separate location, within a tamper-resistant TPM chip
- Prevent unauthorized device access and vulnerabilities both on a physical device and network level
Advanced Control – Optional Advanced Security Features

- Privacy and protection.
  - **Optional** security features
    - HDD Data Encryption
    - HDD Password Lock
    - HDD Erase Scheduler
    - Removable Hard Disk Drive
Hard Drive Data Protection

*Further enhance the protection of HDD contents*

**Description**

- HDD Data Encryption encrypts image data before storing to the HDD. Both temporary and permanent data stored in Advanced Box and Mail Box are encrypted to meet with Common Criteria Certification EAL3.

**Benefits**

- HDD Data Encryption: Helps prevent user data from being exposed if an unauthorized person physically removes and attempts to analyze the data stored in the hard drive.
HDD Data Erase Scheduler

Optional MEAP application for scheduling and confirmation of HDD Data Erase.

**Description**
- Set daily, weekly and monthly schedule for overwriting temporary data on HDD.
- Overwrite temporary HDD data on-demand by push of button.
- Print out report upon execution of scheduled or on-demand overwriting.

**Benefits**
- Provides visibility for HDD Data Erasing.
- Similar to competitors’ offerings.

**New Option**
- Set schedule for Data Erase
- Erase Data on push of button
- Printed report upon execution of Data Erasing

**Install MEAP application on device**

**Set schedule for Data Erase**

**Erase Data on push of button**

**Printed report upon execution of Data Erasing**
Removable Hard Drive Disk

Removable HDD Kit enables HDD to be removed and placed in a secure location while the device is not in use.

**Description**

- Provides capability to physically remove the Hard Drive out of the device and place it in a secured location.
- Allows the hard drive to be easily removed for secure storage and easily replaced when needed.

**Benefits**

- Provides another layer of data security for government agencies and corporate offices that need to ensure that data stored on the hard disk is physically secured when the unit is not in use.
Logging/Auditing Security
iW Secure Audit Manager Express

• Main Features:
  – Archives all images from copy, fax, send, and print jobs from the device
  – No Database is required (Easy start, Simple Implementation)
  – Several Search capabilities by using job log attributes or OCR text
  – E-Mail notification capability and system integration with DMS (Document Management System) when used in conjunction with uniFLOW

Audit, Track, and PREVENT FRAUD
imageWARE Secure Audit Manager Express

Simple Data Flow, Simple Operation

(1) When job is executed, iR Agent retrieves the Job Log and Image

(2) Job log and Image are sent to the iWSAM Express Server

(3) Store in a Windows folder after PDF conversion / OCR processing (No DB required).

(4) When information leak occurs, admin searches job log by attributes and keyword

Click to display actual image and OCR text
Higher Level Security Solution

1. When a job is executed, the iR Agent retrieves the Job Log and Image.

2. Job log and Image are sent to the iWSAM Express Server.

3. SAM stores data in the Export Folder after PDF conversion.

4. uF retrieves the log data and checks the document for restricted keywords.

5. Admin is informed if someone copies/prints/scans a restricted document.

6. All log data is sent to DMS for future references.

7. Admin can search jobs by using the search UI on DMS.
Logging and Auditing Security

Security Level

High

• Prevent information from being printed or scanned

• Image Log Archiving for All Jobs
  • Security Audit by Full OCR Text
  • eMail Notification
  • SFP & Multi Vendor Support
  • DMS integration

Low

• Image Log Archiving for All Jobs
  • Security Audit by Attributes
Network Security
Network Security

- Is there a concern that the MFP is the *entrance* to network security vulnerabilities?
- Is there a requirement to limit *device network capabilities* to reduce threats?
Protection against network threats

Provide ability to protect against attack via network

If the device is set as follows;

- **IP:** Reject xxx.xxx.xxx.001 - 100
- **MAC:** Receive ww-ww-ww-ww-ww-ww

then, the only MAC address (ww-ww-ww-ww-ww-ww) can access to the device

- **IP Address Filter:** Authorized IT personnel can permit or reject incoming packets from specific IP addresses or range of IP addresses (Up to 8 IP address or ranges can be set)
- **MAC (Media Access Control) Filter** allows and denies access to/from specific MAC addresses. Up to 100 MAC addresses can be registered. Useful for environments using Dynamic Host Configuration Protocol (DHCP) for IP address assignments.
- **Network Port / Application Access Control** allows to set up only the necessary protocols such as IPP, FTP, SNTP, SNMP, RAW, LPD and others at the administrator’s discretion

**Benefits**

- Helps minimize the risk of data falling into the wrong hands
- Disabling unneeded services, protocols, and ports assists in securing the network by reducing potential path of attack on the system
**Encrypted Secured Print / Secured Print**

Supports robust network protocol to secure the communication over network

**Secured Print**
- *Password*  
- *Enter Password, then print out*

**Encrypted Secured Print Job**
- *Encryption*  
- *Password*  
- *Enter Password, then decode and print out*

---

**Description**
- Encrypted Secured Print and Secured Print features provide the capability to hold a print job until the user enters a specified password at the device to release the job.
- Encrypted Secured Print feature provides an additional layer of security by encrypting the print data prior to sending over the network.
- The printed data is automatically deleted once printing has been completed.

**Benefits**
- Ensure that the user is in close proximity when the document is printed.
- Help prevents printed documents from being left out on the device.
- Help prevent information leakage by unauthorized people taking the printed document out of the device.
Network Security

Supports robust network protocol to secure communication over the network

**IPsec**

- IPsec provides a capability to protect Internet Protocol (IP) communications from lower layer of communications such as TCP and UDP by authenticating and encrypting each IP packet of a data stream across the Internet.

- IEEE802.1x provides ability to authenticate before gaining access to LAN. The client (MFP) needs “Supplicant” which act as the authentication software to communicate with “Authenticator”. Authenticator will block the client from accessing LAN and verify the client’s user ID/password to RADIUS server.

**IEEE802.1x**

- Provides strong security that can be applied to all traffic crossing the network.

---

**Description**

- IPsec is standard on all imageRUNNER ADVANCE Next Generation models.
For More Information

• Please Refer to Canon USA’s Security section of our website:

• Please Refer to Canon USA’s Security White Paper:
Thank you!