Secure

Secure - Top-Notch Security Features

HCD-PP/IS0 15408 Compliant

- Protection Profile for Hardcopy Devices
- Evaluation criteria for international security standards for digital MFPs
- Developed as security requirements that **must** be met by Japanese and U.S. governments when procuring MFPs
- Manufacturers are required to meet ***extremely*** strict conditions when verifying the effectiveness of encryption of data storage and communication security
  - Validated the ability of bizhub to prevent firmware modification
  - Substantiated bizhub's ability to successfully manage security risks
    - Preventing document data stored in a leased MFP from being leaked after MFP is returned or disposed
    - Protecting against unauthorized modification of firmware
- Proves that Konica iSeries incorporate high-level security measures to protect users against the latest threats

Secure - Top-Notch Security Features

GDPR Ready

- European Data Protection & Privacy Regulation for all citizens
- Addresses the transfer of personal data within as well as outside of Europe

Self-Encrypting SSD

- SSD data encrypted by entering a 20-character alphanumeric passphrase
- 256-bit Authentication Key generated from passphrase and unique device specific data (MFP internal value) using a Konica Minolta unique key generation algorithm *each* time the power is turned on
- Self-Encryption provides increased performance compared to software encryption since CPU is freed up from encryption/decryption calculations

Encryption Algorithm Enhancement

- Unique Key Generation algorithm created each time MFP power is turned on

Secure - Top-Notch Security Features

HTTP/2 Network Protocol

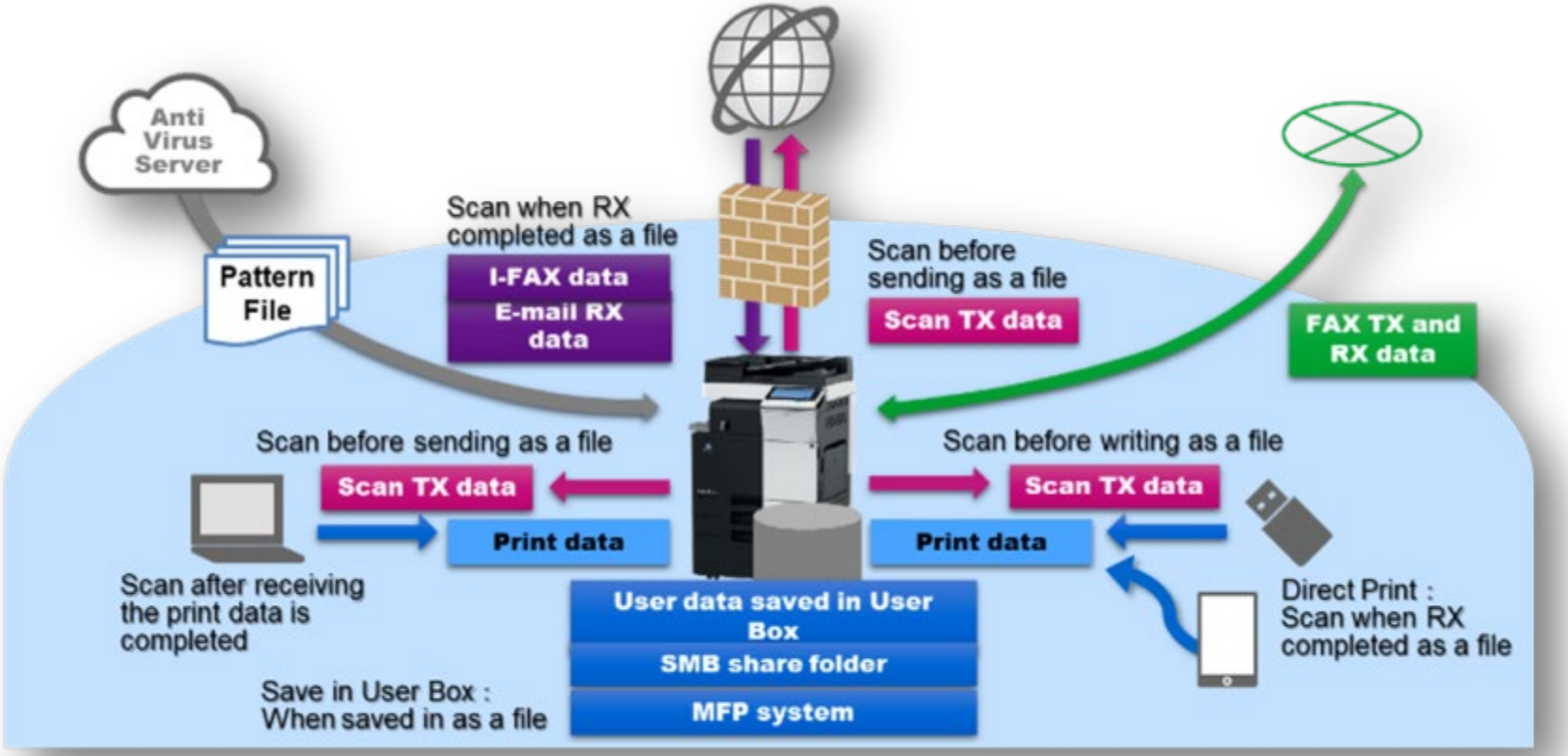
- Major revision of the HTTP Network Protocol used to access the Web
- Offers a more Secure Communication Protocol

bizhub Secure Services

- Manages bizhub Security Settings
- Versatile Services Available
  - bizhub Secure
    - MFP Security Settings
    - Storage Media Security Settings
  - bizhub Secure Platinum
    - MFP Security Settings
    - Storage Media Security Settings
    - Network Protocol Security Settings
  - bizhub Secure Healthcare – Advanced Security for Healthcare
    - MFP Security Settings
    - Storage Media Security Settings
    - Network Protocol Security Settings
  - bizhub Secure Education – Advanced Security for Education
    - MFP Security Settings
    - Storage Media Security Settings
    - Network Protocol Security Settings

Secure – LK-116 Anti-Virus i-Option

Optional LK-116 Anti-Virus



Real Time
Virus Scanning performed as jobs are executed.

Example: Print data, Scan-TX data, i-FAX TX/RX data

Scheduled
Virus Scanning is scheduled for specific time/day

Example: HDD (User Box, SMB)

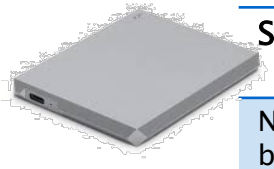
Manual Scan
Virus Scanning is performed by manual initiating the function at the control panel

Scan data in MFP according to instructions in administrator settings

Secure - Top-Notch Security Features

Solid State Drive vs. Hard Disk Drive

- New Technology vs. Old Technology
- SSD does not present same security concerns as a magnetic storage device (HDD)



SSD	HDD
No potential of magnetic traces/variations being left behind	Data stored as magnetic information
Built using NAND Flash Memory; NAND Flash Memory contains “floating-gate-field effect transistors” as memory cells	Data bit is 0 or 1 based on magnetic orientation of each “cell”
No potential of magnetic traces/variations being left behind as in a common HDD. This Flash memory works by adding (charging) or removing (discharging) electrons to and from a floating gate. When the electrons are present on a floating gate, the current is unable to flow through the transistor, rendering the bit state at level (zero) 0. This is considered the normal state for a floating gate transistor when a bit is programmed	Slight possibility that overwriting the cells *may* leave remaining magnetic traces / variations of data on the HDD which in turn, could be used to restore the data. This is where the different overwrite modes becomes effective. By running the magnetic orientation or overwrite patterns multiple times any remaining traces/variations of data will be neutralized.

All SSL communications are encrypted through a more secure encryption algorithm based on the U.S. National Security Agency (NSA) standard