MAXimize your MFP security.

Today's organizations have built a strong perimeter of firewalls, intrusion prevention systems, and anti-virus software to protect their digital assets and information. Great attention is given to local network servers, user workstations, and cloud-hosted systems. However, endpoint network printers, mobile-ready printers, and multifunctional digital copier devices have been largely overlooked when it comes to data security.

Leveraging built-in and frequently updated security features, **Datamax MFP Security + Canon** can help you gain high levels of control over these devices, your network communications, and your documents. ***Here are five (5) security topics to consider.***

Controlling Access to MFPs.

MFPs are typically shared among employees within a department and often across departments. They may also be subject to use by authorized guests and even unwanted users.

Establishing measures to authenticate and control access and usage of the device itself, restrict specific functions of the device, and limit the destinations to which information can be transmitted is crucial.

Key Canon features to MAXimize controlled access:

- uniFLOW Authentication
- Access Management System (AMS)
- uniFLOW Secure Print
- Device-native Forced Hold

Transmitted or Stored Information on MFPs.

MFPs today are sophisticated, connected devices that can transmit and receive information over a network, store information, and connect to cloud services.

Such data in motion (or at rest) may include sensitive business information, important client data, or confidential employee details that must be protected.

Key Canon features to MAXimize protection of transmitted or stored information:

- HDD Security Features *(Encryption, Erase, Initialize at end of life)*
- Port Control
- Protocol Version Selection
- Encrypted Secure Print/uniFLOW Secure Print
- imageWARE Secure Audit Manager Express
- Unified Firmware Platform

Cyber Threats to MFPs.

MFPs connected to corporate networks can become a target for hackers attempting to gain access to the device to gain access to corporate data. It's important to implement security measures that allow only known, approved firmware and applications to run on the device, as well as prohibit tampering with firmware and applications.

IT management should also have the ability to monitor activity so that they can quickly identify and recover from potential threats.

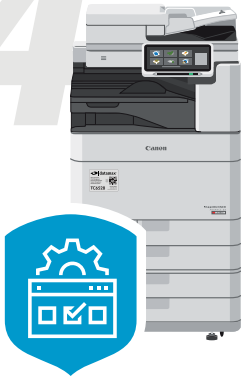
Key Canon features to MAXimize protection from cyber threats:

- Verify System at Start-up
- McAfee® Embedded Control

Datamax MFP SECURITY

Security Settings and Device Activity on MFPs.

4



IT support teams are typically responsible for managing a fleet of MFP devices. This becomes a burden if there aren't proper tools available to ensure that security settings are easily established and deployed universally across the fleet.

Requirements for passwords, such as expiration period, lockout time, and complexity should also be put in place.

Key Canon features to MAXimize protection the management of device security settings & activity:

- Security Policy Settings (with dedicated password)
- imageWARE Enterprise Management Console (EMC) with DCM Plug-in
- SIEM *(Security Information Event Management)* Integration

Regulation, Compliance and MFPs.

5

In today's digital, cyber threat-ridden world, government regulations compel businesses to satisfy compliance or risk facing penalties. The MFP, where sensitive data exists, should be part of your compliance strategy.

Responding to regulatory compliance requirements can be complex. And since an organization's sensitive information are interacting with MFPs, they become a necessary component of compliance initiatives.

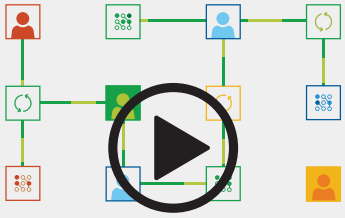
Key Canon considerations for MAXimizing regulatory compliance:

- Align with a partner with a knowledge of relevant compliance regulations and standards.
- Consider industry and government-mandated regulations *(such as GDPR, CCPA, HIPAA, Sarbanes- Oxley, PCI, etc.)* and their impact on how your organization handles information.
- Leverage a dedicated security leader like McAfee and feel more confident that your MFPs are protected from malicious threats and in alignment with information governance.

Need more information or want to **schedule a visit** with a Datamax MFP security specialist?

Please view our imageRUNNER ADVANCE CONTROL Video at https://youtu.be/dMW5_hkAvXo or visit the Datamax MFP Security resource page at https://www.datamaxtexas.com/mfp-security-solutions

Click for Canon imageRUNNER Security Control Video:



Scan QR for MFP Security Solutions Resource Page:

Datamax MFP SECURITY

Canon

McAfee PROTECTED

datamax®