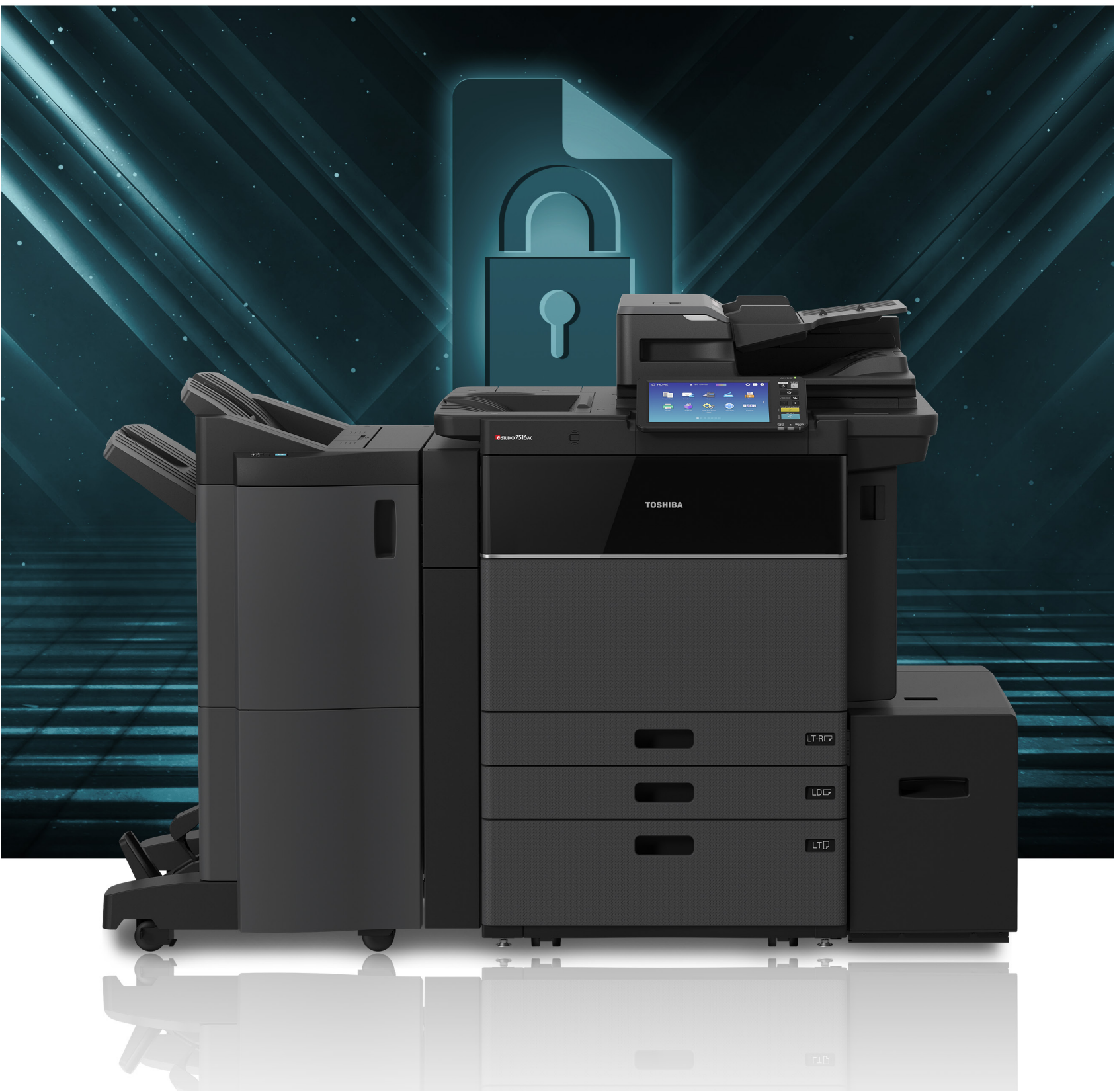
TOSHIBA

WHITE PAPER: TOSHIBA'S BEST PRACTICES FOR PRINT SECURITY



TOSHIBA

TABLE OF CONTENTS

TOSHIBA

WHITE PAPER: TOSHIBA'S BEST PRACTICES FOR PRINT SECURITY

This document provides an overview on the importance of data security in print environments for small to medium-sized businesses and how companies can proactively manage those security risks, thus avoiding costly expenses related to data breach across their businesses.

1. OVERVIEW

Information security is essential to organizations of all sizes. However, due to their lack of processes, security breach technology safeguards and dedicated IT teams, small to medium-sized businesses (SMBs) are particularly vulnerable to attacks. According to a recent study, 76% of SMBs have been impacted by at least one cybersecurity attack in 2022, a considerable increase compared to 55% in 2020. Also 73% of SMBs agree that their organization has reached a tipping point where cybersecurity concerns demand action. Another study by IBM found that organizations with 500-1,000 employees had an average data breach cost of $3,533 per employee, compared to $204 per employee in larger organizations. For industries that require regulatory compliance, including HIPAA, FERPA, SOX and GLBA, the costs are even higher. Although the consequences of data breaches are severe, there are steps SMBs can take to mitigate costs and potentially reduce their overall security risk.

76%

of SMBs have been impacted by at least one cybersecurity attack in 2022

73%

of SMBs agree that their organization has reached a tipping point where cybersecurity concerns demand action

The IBM study above also found that 60% of companies that had a data breach say the root cause was a negligent employee or contractor. Unsecured computing devices coupled with negligent employees within the company's print and document environment pose a major threat to the SMB's document security. Additionally, multifunction devices are some of the most shared resources in any organization, with unhindered access to every document printed and scanned. These documents may include company confidential information, sensitive user information and customer data, which is essential to the survival of the company. Most modern print devices are also accessible through mobile devices and the cloud, making them vulnerable to external attacks.

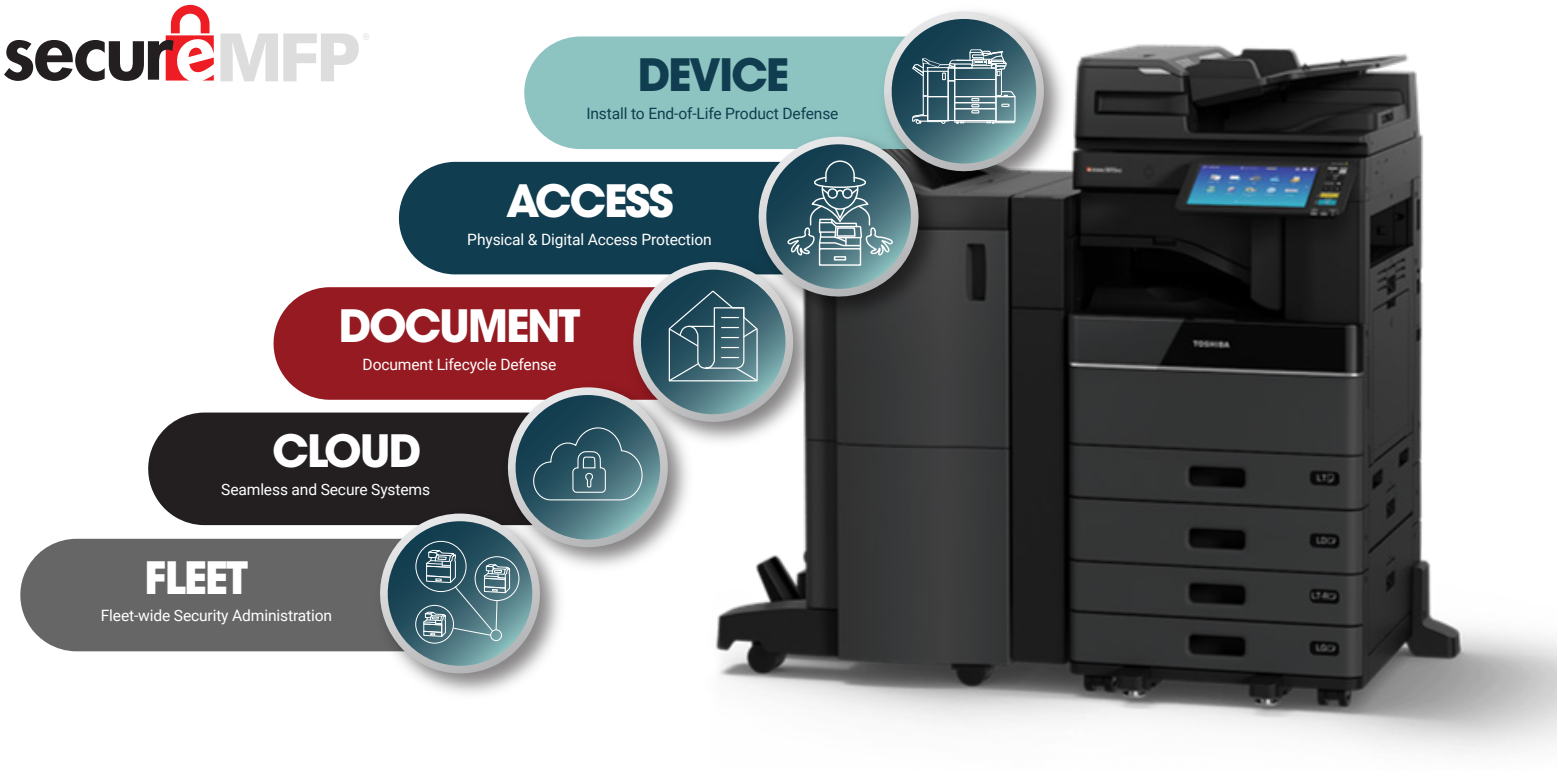
With recent attacks on multifunction devices making the headlines, businesses are becoming increasingly aware of the threats and the potential vulnerabilities that can impact them. That's why Toshiba offers best-in-class multifunction devices for end-to-end print security. By creating security awareness and providing training and best practice guidelines, Toshiba acts as a trusted partner for its customers.

2. WHY PRINT SECURITY

Every business has sensitive information that is essential to its survival. Ensuring the privacy of customer data and protection of employee personal data is as essential as protecting proprietary intellectual property and company financial records. Complicating matters even more are the increasingly stringent (and extremely punitive) government regulations and standards for managing information. Generally, organizations focus on sensitive information stored in the database underlying their operations, yet most organizations do not offer enough attention to the document imaging process and its entire lifecycle within and outside the organization, thus opening their data to potential theft and breaches.

When it comes to print security, just having a secure device is not enough either. Any security solution for the print environment must ensure that security is built into the entire hardware, software and the application stack including cloud services. Additionally, effective management of security settings and policies across the entire fleet of print devices is crucial as well.

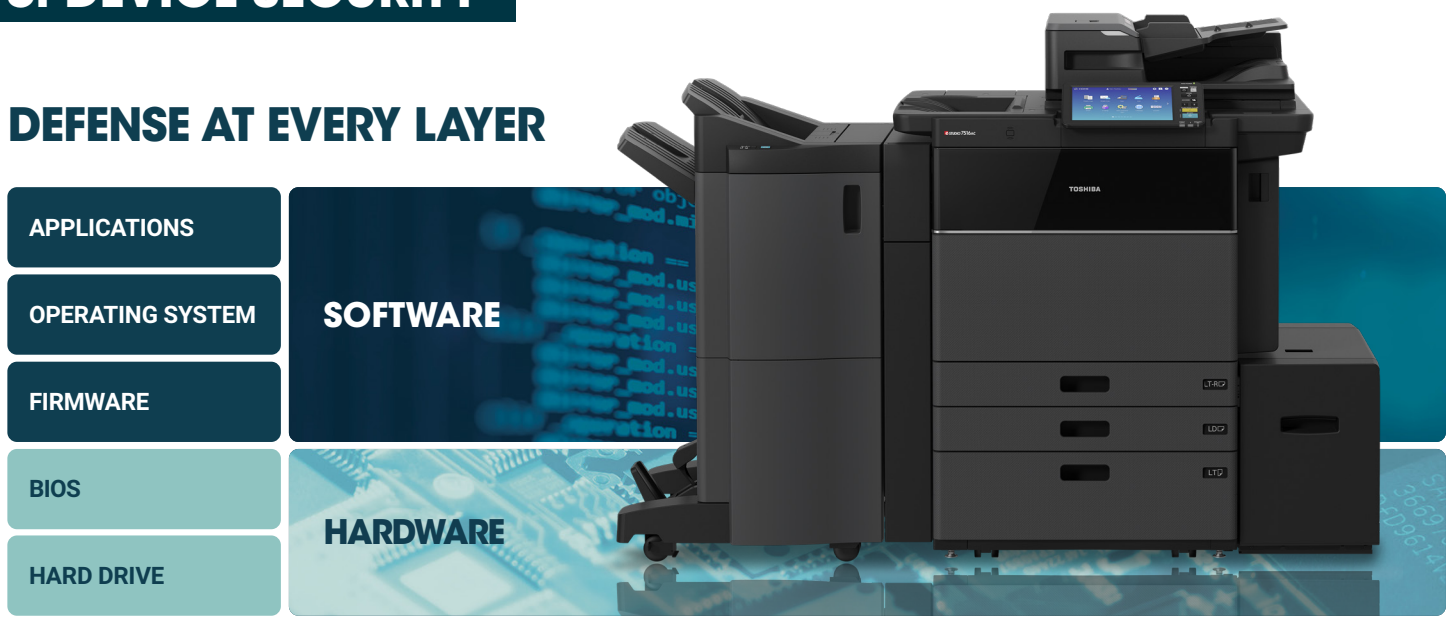
OUR IN-DEPTH PRINT SECURITY APPROACH



As shown above, overall print security can be broadly divided into five different categories: device, access, document, cloud and fleet security. Device security focuses on the built-in securities in the device hardware, controller and software and ensures end-to-end equipment protection from installation to end-of-life of the device. Access security ensures that the right people have access to the right features, functionality, and data on the print device. Any intrusion is proactively monitored and managed. Document security protects all documents and information within those documents from being eavesdropped while the document is stored or in-transit. Cloud security pretty much protects the MFP from any cyber threats, ransomware, phishing etc. Finally, fleet security helps manage security settings and policies across the entire fleet.

3. DEVICE SECURITY

DEFENSE AT EVERY LAYER



Device security protects the device hardware, controller software and software applications from security threats throughout the entire lifecycle of the print device, from the day it's installed through day-to-day operations to the end-of-life process. Some of the key device features include:

BIOS Protection

Device BIOS is a set of instructions in the device hardware which controls input and output operations on the device. Only the authorized BIOS from the manufacturer should be allowed to be loaded to the device. Additionally, it is recommended that system BIOS must be encrypted so that any unauthorized BIOS can be strictly prohibited.

Hard Drive Encryption

Hard drives can be the target of security attacks because print devices may temporarily store copies of documents scanned, copied and printed on those hard drives. If the hard drive on the print device is compromised, then any sensitive documents stored on the drive are at risk. Therefore, the data on the hard drive must be encrypted, so that even if the storage media containing sensitive documents is lost or stolen, the document still can't be retrieved from the disk. As an additional precaution, the storage media should also be automatically rendered useless when removed from the print device.

OS / Firmware / Application Whitelisting

Recently, security defects in several embedded systems used in print devices have created entry points for ransomware and spyware and have disrupted corporate networks. Companies must ensure that the embedded systems on their print devices have gone through thorough security vulnerability tests and are frequently updated with security patches. Additionally, the device must also protect itself from any attempt to install unauthorized software. All device firmware and software applications running on the print device must be digitally signed by the manufacturer and all others rejected so that malicious firmware cannot be installed on the device.

4. ACCESS SECURITY

Access security ensures that the right people have access to the right data and functions on the print device—from physical access to digital access including network access and access from mobile devices and the cloud. Administrators must be able to restrict access, manage and enforce security policies, and monitor any unauthorized access in real time. Some of the key features in this category include:

Authentication & Directory Access

Organizations must have a standard process to make sure that only authenticated users are able to access the print devices. These authentication methods may include any combination of user credentials, badge readers, PIN codes or even biometric authentication. Additionally, user roles and access privileges must be managed via a central company directory to avoid illegal access. SMBs, specifically in regulatory compliance industries, must also consider multi-factor authentication to add another layer of security to the authentication process.

Password & Access Policy Management

40 percent of SMBs say their companies experienced an attack involving the compromise of employees' passwords in the past year. Enforcing a strict password policy is one of the simplest measures that companies can take with the most positive impact on the security. A good password policy must enforce minimum password length, password expiration and account lockout, at the very least. The policy should also disallow frequently used password strings or default passwords.

Physical & Network Port Blocking

Print devices must also have built-in protections from unauthorized access physically as well as across the network through USB port disable, network port blocking and IP/MAC filtering. These ensure that only authorized personnel and devices are allowed to communicate with the print devices, thus blocking any unauthorized access.

Monitoring & Intrusion Detection

System-wide audit logs for all access and activities on the print devices are highly recommended to provide visibility to administrators with regards to when and how the device or document was accessed. Some regulatory, stringent industries even require this functionality on imaging devices. Additionally, companies should also monitor system and security logs from print devices via external Antivirus or SIEM (Security Information & Event Management) software to detect any intrusion in real time. Therefore, print devices should seamlessly communicate with those third-party systems.

5. DOCUMENT SECURITY

When it comes to document security, companies must ensure that documents and the information within those documents, such as social security numbers, credit card details and other personally identifiable information (PII), are secured through the entire lifecycle of the document, from its inception to disposal. Documents typically go through the following three key processes in a print environment: capture, store and deliver.

5.1 CAPTURE

Typically, during a document capture process, a physical document is converted to a digital, searchable format via an optical character recognition (OCR) process. Scan to email, scan to self, scan to network share and scan to cloud storage are some of the methods used in almost every organization to capture physical documents and convert them into digital format.

Data Capture Security

By ensuring that the print devices use the secure print protocols (Secure IPP) and encrypted transmission channels for scanning documents, administrators can stay assured that document data cannot be eavesdropped. In fact, at a minimum, communication devices should be configured with TLS 1.2 or higher, HTTPS and WPA2 for wireless security. Unsecured or unused wireless communication (Wi-Fi, NFC, Bluetooth) should be disabled on the print devices. Furthermore, companies using fax communications should consider password protecting the incoming faxes and holding or scheduling fax jobs to be printed during a specific time of the day to avoid unauthorized access to those faxes.

Whitelist Scan Destinations

By whitelisting the scan destinations, organizations can ensure that sensitive documents can be scanned to only specific scan destinations. By prohibiting users from sending documents outside specific scan destinations, you can rest assured that documents can only be delivered to the rightful owner/destination and will not end up in the wrong hands, even by mistake.

5.2 STORE

After documents are captured, they are typically stored inside a file system, cloud storage system, document management system or even on storage media inside the print device. Security measures must be taken to ensure that the storage locations are monitored, audited and protected from hackers. Here are a few recommendations to ensure that your business-sensitive documents are stored securely:

Document Encryption

On occasion, the hard drive on the print device is used for e-filing. At a minimum, companies must ensure that their business documents are encrypted, and password protected when they are stored or shared, so in case a document falls into the wrong hands, they are not able to open the documents.

Security Stamps

Adding security stamps to stored documents once printed, copied, e-filed or even faxed helps organizations determine the source of the documents thus avoiding any tampering. These stamps may include a username, department name and timestamp. This feature also discourages internal and external users from tampering with documents and storage locations.

5.3 DELIVER

Every business has document workflow processes (e.g., order processing, HR recruiting, accounts payable, etc.) that require stored documents to get delivered to an external destination or an output device, such as mobile or print. Therefore, organizations must ensure that their document delivery process (external or internal) is fully secure to avoid eavesdropping and man-in-the-middle attacks. Here are a few steps that companies can follow to secure their document delivery process in print environments:

Secure / Private / Hold Print

In addition to the authentication on the device, organizations must implement secure print release solutions for their printer fleet. Secure print release ensures that confidential documents are held in a secure print queue until the owner of the print job authenticates and releases the print job at the printer. If the recipient is someone other than the person sending the document, private print enables users to password protect their print jobs in order to similarly ensure that documents are not released until the person with the correct password releases the job at the printer. The user may release their confidential print job by entering their password at the panel. These defenses ensure confidential documents are not left waiting unattended at the printer.

Secure Document Exchange

With widespread use of cloud and mobile technology, organizations must also ensure that documents shared over network, internet and Wi-Fi/mobile infrastructure are fully secure. When documents are exchanged with external audiences, it must be ensured that only the intended recipient can access the file. Access monitoring and an audit trail of such access is key to the security of the document when shared with any external audience.

Document Copy Protection & Tracking

Certain document types, such as paychecks or classified documents, should never be copied or scanned. Therefore, print devices must provide a mechanism to protect such documents from copy, print or scan. Hardcopy security features within multifunction devices protect classified documents from illegal copies being made. Additionally, any such illegal action should be logged and reported to the administrators.

6. CLOUD SECURITY

Cloud technologies and services are prevalent in almost all workplaces today. With hybrid work environments, the print devices may be located at a home office or may need to be accessed anytime and from anywhere. Hence, it's even more important that the MFP is protected against any threats originating inside or outside of the organizations network.

Convenience of cloud comes with the need for better security framework to protect your data. Some of the key areas of cloud security involve hardware root-of-trust, data security, identity and access management (IAM), data security, built-in anti-malware, and data governance policies to prevent, detect, and mitigate threat.

Hardware Root-of-Trust

While network and access security are mandatory, it is not sufficient to protect against attackers who target BIOS and other low-level elements in the MFP. Hence, the print devices must have built-in hardware-based security, a starting point that is implicitly trusted. Trusted Platform Module (TPM) is one such technology where security begins at the silicon chip. TPM starting to become prevalent in zero-trust security frameworks. Recently Microsoft requires TPM for Windows 11 hardware.

Data Security

Cloud services should only collect any user identifiable data or customer data such as documents, copy, fax, and scan data from the MFP fleet when it is absolutely necessary. Any data if collected should be obfuscated and encrypted with at least AES 256. Additionally, all communication between the MFP and the cloud servers is authenticated and encrypted using at least TLS1.2 or higher.

Identity & Access Management (IAM)

Multi-factor authentication must be standard for all authentication and authorizations.Token based OAUTH2.0 should also be used across different hardware and software platforms to avoid user credentials being transmitted across the network. Biometric authentication also adds another layer protection for users within an organization. The administrators should also consider utilizing a single IAM provider without replicating their users across different systems.

Anti-Malware

Ransomware, phishing attacks are all around when it comes to cloud. Bad actors may not be interested in the data within the print devices, rather they try to exploit the print device as a point of entry into your network. Hence, built-in anti-malware in print devices adds another layer of protection. It stops any malware attacks in real time protecting your network environment from Denial-of-Service (DoS), and Remote Code Execution type of attacks.

7. FLEET SECURITY

Last but not least, whether you are an SMB with two devices, or an enterprise with hundreds, you want to be able to set, apply and manage your security policies with ease and confidence across your entire organization. For added convenience, you also want to be able to manage and monitor your devices remotely without having to access the device physically. Therefore, a successful print security solution must include a fleet management tool that supports centralized monitoring and management of security policies across the fleet of print devices. At a minimum, this tool should allow administrators to create security policies and deploy them across a fleet of any size. Any violations to these policies should be notified and possibly corrected automatically. It's preferable that this management tool be cloud-based for added convenience and management.

8. WHY TOSHIBA

Toshiba offers best-in-class multifunction devices for end-to-end print security. In addition to all the security recommendations described above, Toshiba brings uniquely distinguishing features for its customers.

- Toshiba is the only print device OEM that manufactures its hard drives and has full control over how data is encrypted on the hard drives. Toshiba devices are HCD-PP compliant when equipped with our optional FIPS 140-2 validated self-encrypting drives—a requirement for regulatory compliance for hard drive security.
- In addition to being HCD-PP certified, Toshiba multifunction devices also comply with the different industry standards, such as HIPAA for healthcare, GLBA and SOX for finance, FERPA for education and SB-327 for IoT device security compliance in California.
- We support multi-factor authentication for all Toshiba cloud apps. e-BRIDGE Cloud Login service follows a standard OAUTH authorization scheme so that the user login credentials are communicated directly to respective cloud identity providers. No user credential is shared with our cloud thus protecting user identity and access.
- We offer a suite of cloud applications and services that can integrate with customers identity provider such as Microsoft or Google. As a result, the customers can maintain their user information at one location without replicating them across different applications.
- All Toshiba devices are equipped with controls that allow the entire hard drive to be wiped at the end of the lease period. Our strict decommission process also ensures that customer data never leaves their premises.
- Toshiba's Data Overwrite ensures that any leftover temporary data is wiped immediately after the scan/copy function is complete. Hence, customers can stay assured that the device does not store any sensitive document information that may be accessed for inappropriate use. Some of the competitive devices that offer this feature only wipe data periodically, rather than immediately, which leaves a window of vulnerability in the device.
- Toshiba makes security easy. A single code on the device can turn on all the security features on the device (over 70 functions), thus enabling the device to be put in High Security Mode. It's very effective for high-security print environments that wish to maximize security.

- Toshiba's policy driven Elevate Sky Services platform helps customers create and deploy security policies across their fleet quickly and also allows them to monitor and automatically remediate any violations.
- As a cloud service provider, data Governance is extremely important to Toshiba.
- All our cloud services are also hosted on industry-leading hosting providers Amazon Web Services (AWS) and Microsoft Azure, which are designed with security in mind. We also comply with ISO/IEC 27001 (Information Security Management) & ISO/IEC 27017/27018 (Cloud Service Security) with periodic penetration testing and vulnerability scanning using 3rd party security tools.
- But most importantly, Toshiba understands that data security within an organization's print environment is a multi-dimensional phenomenon involving people, process and product. Each of these dimensions must work together to implement a successful strategy for print security.

For an in-depth look at Toshiba's approach and details on the security features within our devices, please contact your Toshiba representative or refer to *White Paper: Toshiba's Holistic Approach to Print Security*.

TOSHIBA

business.toshiba.com

Inv. Code: 22371 Toshiba Print Security White Paper 8/21