

# secureMFP®



**TOSHIBA**

# TOSHIBA SECURITY

## PRINT SECURITY IS CRITICAL TO EVERY ORGANIZATION

No matter the size of your company, you have confidential data and intellectual property to protect. And between ever-growing government regulations and compliance requirements, many industries find themselves with rigorous mandates to meet. As an organization and employer, it's your responsibility to keep sensitive customer and employee details secure.

From employees' personal details to customers' valuable data to your own intellectual property, your company transmits and prints an enormous amount of sensitive information that would be extremely valuable to identity thieves and competitors. The costs of a breach add up quickly across detection, notification and remediation. And the toll of lost business and brand reputation can be devastating to your organization. Remember, no company of any size or industry is immune.

## DON'T MAKE THE MISTAKE OF NEGLECTING THE SECURITY OF YOUR MULTIFUNCTION PRINTERS

**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

## DON'T OVERLOOK YOUR MFP

As one of the most shared resources in your organization, don't make the mistake of neglecting the security of your multifunction printers (MFPs). As they store and transmit business-critical information, customer records, employee files and more, this centrally located and networked resource is continuously accessed by people inside and outside your organization. That means every sensitive document you print, copy, scan and transmit could be vulnerable to an attack.

## DON'T LET YOUR DEVICE BECOME COMPROMISED

From data on hard drives to unauthorized access to unsecured transmissions to or from the device, there are several points of vulnerability in your print and document environment that need protecting. For instance, networked printers can become hacker gateways making unencrypted data easily accessible. From there, sensitive information can be digitally shared with unknown sources and become physically available to anyone. It's more important than ever to make sure you're protected at every level.

## A HOLISTIC APPROACH TO SECURITY

To best tackle your security vulnerabilities, Toshiba takes a unique, comprehensive approach to safeguarding your print and document environments. We look at security in your environment across three areas: product, process and people. The most important component is indeed product security because that is the hub of all your data and human interactions. Once the device is secured, we focus on understanding the processes and people who interact with the device. This allows us to advise you on not just the equipment, but also on the best security methodologies to put in place in your organization. This powerful combination ensures an end-to-end security strategy for your print environment.

## PRODUCT SECURITY

Starting at the product level, we deliver an in-depth defense across five areas:

secureMFP™

1. INSTALL TO END-OF-LIFE DEVICE SECURITY
2. PHYSICAL AND DIGITAL ACCESS PROTECTION
3. DOCUMENT LIFECYCLE DEFENSE
4. CLOUD SECURITY
5. FLEET-WIDE SECURITY ADMINISTRATION



## DEVICE SECURITY

All devices have a definitive lifecycle, from installation to operation to end-of-life. At Toshiba, we want to ensure their protection is as easy as possible across the entire life of the device. For example, upon installation, we follow strict password rules that make it compliant with the most rigorous IoT laws. Our High Security Mode allows you to automatically set over 70 configurable features to the highest security level; therefore, ensuring high security has never been easier. After setup, we protect your day-to-day operations with tamper-proof layers of software and hardware. We restrict and verify the applications, firmware and operating system so your software is continuously secure. We also protect the hardware by securing the BIOS and utilizing a self-encrypting hard drive with proprietary wipe technology. Our built-in Trusted Platform Module (TPM 2.0) adds another layer of hardware-based security in zero-trust environments. Lastly, Toshiba's well-documented end-of-life policy ensures our MFPs go through a formal data-wipe process, so no data remains on the device when it leaves your facility.

## ACCESS SECURITY

The secret to access security is making sure the right people have access to the right data as well as the right device capabilities. Toshiba achieves this by restricting, managing and monitoring access. Our multi-factor authentication along with roles based access control features ensure that only authorized individuals or sites can access the device physically or digitally; you can even limit access at the feature-level so your security policies can be very granular and customized. Along with restrictions comes the task of managing those boundaries. Toshiba makes it easy with authorizations that can be managed from a centralized active directory so you can apply consistent role-based security rules across the board. And lastly, we offer comprehensive monitoring through steps such as activity logs, real-time notifications and shareable alerts. Toshiba devices also support biometric authentication which adds another layer of access security.





## DOCUMENT SECURITY

The idea of a lifecycle not only applies to the MFP, but also to the sensitive documents it handles. At Toshiba, proper document security starts with the capture phase where we employ built-in security for all input sources, including computer, email, web/cloud and USB on the MFP. Once the documents are in the device, we ensure that documents are safely stored in the hard drive with multilevel encryption and protected policies. To guarantee a secure release from your devices, you have multiple methods to take into consideration. Printing, copying, scanning and faxing each have their own security risks, and Toshiba has many tools, restrictions, verifications and more to ensure you and your company are covered no matter the output method. Our recently launched secure print solution (e-BRIDGE Global Print) further helps release their print jobs on-demand thus securing sensitive documents.

## 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. Toshiba MFPs have several built-in security features to protect from cyber threats. Some of these include hardware root-of-trust via TPM 2.0, identity and access management (IAM) via OAUTH 2.0, integration with leading identity providers such as Microsoft & Google, and built-in anti-malware. These features combined with latest data encryption protocols make Toshiba devices ideal for hybrid workforce.

Finally, Safeguarding the privacy and security of customer data has never been more vital. That's why we ensure all communication between the MFP and our cloud server uses the most up-to-date security protocols and encryption, along with cloud hosting provided by Microsoft Azure or Amazon Web Services (AWS), where security is inherently built in. Additionally, our cloud infrastructure is compliant with ISO/IEC 27001 (Information Security Management) & ISO/IEC 27017/27018 (Cloud Service Security) to ensure your data is properly protected. With Toshiba, you can rest assured knowing your business is safe in the new workplace.

## FLEET-WIDE SECURITY

Whether you are an SMB with two devices, or an enterprise with hundreds, security is an important consideration, and we know you want to be able to set, apply and manage security policies with ease and consistency across your organization. Our Elevate Sky Suite of Services manages your fleet security concerns with a cloud-based application that supports the centralized and remote monitoring and management of security policies on all Toshiba MFPs. With Toshiba Elevate Sky Suite of services, you gain visibility, accountability and peace of mind.

To learn more about Toshiba's Secure MFP Program, visit [business.toshiba.com](https://business.toshiba.com)

[business.toshiba.com](https://business.toshiba.com)