TOSHIBA

secureMFP

Security built into every layer.

Protect your documents, data, and devices with Toshiba's SecureMFP® Program.

Five layers of protection:

- Device
- Access
- Document
- Cloud
- Fleet

Print security is critical to every organization.

No matter your size or industry, your organization handles sensitive data that must be protected. With growing regulations and compliance requirements, the pressure to secure customer and employee information is higher than ever.

From personal details and proprietary business content to confidential customer records, your organization prints and transmits data that can attract identity thieves and competitors alike.

A single breach can escalate fast—detection, notification, and remediation costs add up quickly. But the biggest damage often comes later: lost trust, lost business, and a damaged brand.

The reality? No organization is immune. Strong data protection isn't optional—it's essential.

Your MFPs are part of the front line.

Multifunction printers (MFPs) are among the most shared and connected devices in your organization—used daily to print, scan, copy, and transmit sensitive information. That makes them a critical part of your security strategy.

From customer records to internal business data, every document passed through your MFPs carries risk if not properly protected. With compliance demands increasing and cyber threats evolving, it's essential to secure your print environment as part of your broader IT defense.

Stop threats before they start.

Your printers shouldn't be your weakest link. Toshiba technology protects every point of vulnerability—from stored files and user access to cloud connections and data in transit.

Our built-in security features work together to lock down networked devices, encrypt data, and keep confidential information secure at every touchpoint.

Security that covers every layer.

Toshiba takes a holistic approach to print and document security—covering your devices, your data, your people, and your workflows.

By aligning with Zero Trust principles like "trust but verify" and least-privilege access, we deliver consistent, end-to-end protection from product design through end-of-life.

The risk is real.

94% of SMBs experienced a cyberattack in 2024.

78% are concerned a severe attack could shut them down.

Yet many organizations still overlook their print environment.
Toshiba helps you close that gap with powerful, easy-to-deploy protections.

Source: ConnectWise, The State of SMB Cybersecurity in 2024

Toshiba SecureMFP® Program

Our SecureMFP® Program brings together all layers of security—devices, access, documents, cloud, and fleet—under a unified framework.

It includes built-in protections, expert guidance, and best practices to help organizations of all sizes safeguard information, meet compliance standards, and reduce risk exposure.

Install to end-of-life device security

Physical & digital access protection

Document life-cycle defense

Cloud data protection

Fleet-wide security administration

Trusted. Certified. Compliant.

ISO/IEC 27001 Certified
Information Security Management

Common Criteria
EAL Certified

Compliant with NIST SP 800-171

ISO/IEC 27017 Certified
Cloud Security Controls

Supports
CAC/PIV

Supports
Microsoft 365 GCC High Environment

Device Security

Toshiba MFPs are secured throughout their lifecycle—from day one to decommissioning.

High Security Mode enables 70+ security settings in a single step

Tamper-resistant design protects hardware and software

Firmware, OS, BIOS, and applications are validated and secured

Solid-state drives (SSDs) boost both security and reliability

Trusted Platform Module (TPM 2.0) adds hardware-based protection

End-of-life sanitization ensures no data is left behind when devices are retired

Access Security

Toshiba ensures only authorized users have access—at the right level, at the right time.

- Multi-factor authentication and role-based access controls
- Feature-level restrictions enforce precise security policies
- Centralized management through Active Directory
- Real-time alerts and activity logs provide complete visibility

Integration with cloud identity providers such as Microsoft® Entra ID strengthens centralized authentication and supports the “Trust but Verify” principle of Zero Trust.

Support for CAC/PIV (Common Access Card / Personal Identification Verification) authentication provides an extra layer of secure ID verification for government and public-sector environments.

Document Security

Documents are secured from the moment they’re captured, printed, or shared

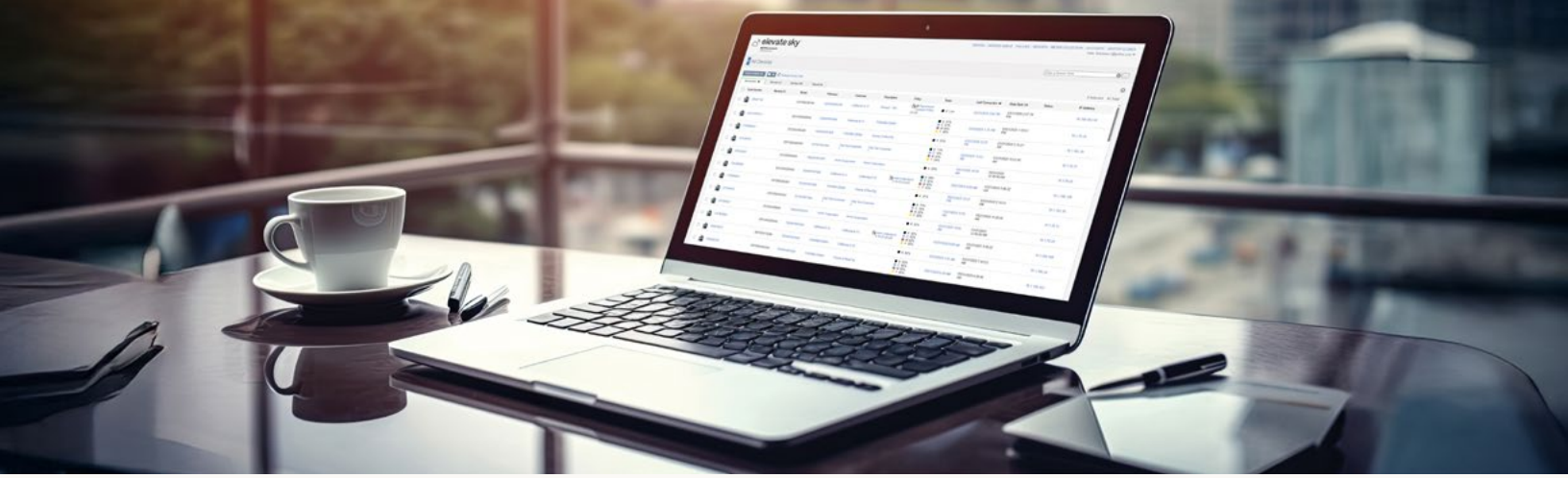
Tools and restrictions for print, scan, fax, and copy functions

Multi-level encryption for stored and in-transit documents

Automated redaction and workflow tools help reduce human error and support compliance

Controlled release ensures output only reaches authorized users

Documents stay protected throughout their lifecycle, with safeguards for every output method and access point



Cloud Security

As hybrid work expands, cloud protection is essential. Toshiba MFPs are built for secure cloud-based environments—without adding risk.

- TPM 2.0 hardware root-of-trust and OAuth 2.0 identity management
- Advanced encryption and anti-malware protection
- Integration with Microsoft® and Google™ identity providers
- Secure hosting on Microsoft Azure® and AWS®, certified to ISO/IEC 27001, 27017, and 27018
- 24/7 monitoring by Toshiba's global Product Security Incident Response Team (PSIRT), ensuring protections stay effective and vulnerabilities are addressed in real time
- Alignment with post-quantum cryptography standards (NIST IR 8547) to stay ahead of emerging threats

All communication with Toshiba's cloud servers uses the latest secure protocols—keeping your data protected, wherever your devices are deployed.

Fleet-Wide Security

With Toshiba's Elevate Sky® MFPConnect, managing security across your fleet is simple—whether you have two devices or two hundred.

- Centralized, cloud-based management
- Consistent security policy enforcement
- Full visibility across all locations
- Streamlined updates and monitoring

Your entire print environment stays secure, scalable, and easy to control.

Ensuring transparency and trust with comprehensive security auditing.

Toshiba's commitment to security extends beyond prevention to Auditing, Accounting, and Controls (AAC). Our comprehensive auditing capabilities ensure immutable records of activity across applications and MFPs, providing full transparency into who did what, where, and when.

The Toshiba Difference

Comprehensive Coverage

We protect every layer of your print and document environment—from the device to the cloud—so no security gap goes unaddressed.

Expert Guidance

Our security specialists help you align with regulatory requirements, industry standards, and Zero Trust strategies.

Peace of Mind

Your devices, data, and documents are safeguarded at every stage, so you can focus on your business. not your vulnerabilities.

Let's lock down your print environment.
To learn more about the SecureMFP® Program, visit business.toshiba.com/security

Technical data is subject to change without prior notice. All company and/or product names are trademarks and/or registered trademarks of their respective manufacturers in their markets and/or countries. All rights reserved. We are constantly making efforts to deliver the latest status of data to our partners. Specifications for some models may change in the time between the production and the release of this documentation.

Corporate Office 25530 Commercentre Drive, Lake Forest, CA 92630
Tel: 949-462-6000

©2025 Toshiba America Business Solutions, Inc. Electronic Imaging Division. All rights reserved.
Inv. Code: 22366 Security Brochure 10/25

TOSHIBA