KATUN® ARIVIA

Security Threats, Measures & Features

The following are recognized as security threats for office MFPs from the viewpoint of data breach, data tampering, and unauthorized data access.

1. Unauthorized operations by other users
2. Eavesdropping and tampering of communication data
3. Unauthorized access to administration functions
4. Software tampering and unauthorized rewriting of software
5. Audit log tampering
6. Breach of document data stored on the device (at return after lease end or device disposal)
7. Data breach caused by careless mistakes of system administrators or user

Table 1. Security Threats and Measures for Office Multifunction Devices

Security threats to office devices	Security measures implemented
1. Unauthorized operations by other users When individual users perform operation on a device, documents stored on the device and related data will be compromised or tampered if appropriate protection (data access permissions, operation controls, etc.) is not implemented for document data to be handled.	**A) User authentication and permissions** • **User authentication** You can identify and manage individual users. • **Restriction in use of functions** Manage each user's usage. • **Automatic logout** Prevent unauthorized use of MFPs by users other than the logged-in person. • **Secure Print / Private Charge Print** You can print confidential documents without exposing them to third person.

A) User Authentication and Permissions

Authentication Feature

Operations by users who have no permission to use the device and unauthorized access can be prevented under operation with the authentication feature. It also allows you to account usage by user from job history.

Remote Server Authentication

By registering smart card information with Active Directory or the LDAP* server, you can use user information managed by the server for user authentication when operating the device or printer.

* Light Weight Directory Access Protocol

25-06-0039-kbs ©2025 Katun Corporation

KATUN®
SUCCESS MADE SIMPLE.

KATUN® ARIVIA

Security Threats, Measures & Features

Feature Access Permissions

Function Access Control is a function of user authentication that restricts MFP functions. All function buttons such as copy or fax can be controlled. Only system administrator can set via the control panel or MFP setting software.

There are 3 types of function control.

1. Device Access control

Control panel operation can be controlled. When the MFP is started up, Log-in UI appears firstly.

2. Service Access control

The following services can be controlled. Hiding the service icons can also be set

- Copy
- FAX/ internet FAX
- Scan to Folder
- Scan to PC
- Scan to Email
- Folder Operation
- Job Flow
- Print by media
- External Access
- Print

3. Access control per user

Function access and print & copy quota control can be set per user.

The system administrator sets copy & quota limitation per user via the control panel and MFP setting software.

When print or copy volume exceed the registered number, the user can no longer use the function. System administrator should clear the counted number.

Access Control to Documents in MFP Folder

You can set a password to an MFP Folder where scanned / faxed documents are stored to protect them. Access to document data by a person who does not have any right can also be controlled by using the authentication mode, which enables user identification.

Automatic Logout

Automatic Logout is a function to prevent another user from accessing the MFP functions as a user previously logged in. If the device is not in use for a certain period, automatic logout is performed, and the device goes back to the initial state.

Secure Print

Secure Print helps prevent unauthorized viewers from gaining access to documents by holding jobs in the device until you enter a password.

* Operation in Authentication mode is required.

25-06-0039-kbs ©2025 Katun Corporation

KATUN®
SUCCESS MADE SIMPLE.

Table 2. Security Threats and Measures for Office Multifunction Devices

Security threats to office devices	Security measures implemented
2. Eavesdropping of communication and tampering of data Eavesdropping of communication or tampering of data may occur when it is exchanged between a PC or file server used for device operations (print, scan, etc.) and the device on the network.	**B) Protection of communication and data** • **SSL/TLS and IPSec** Encrypt communication between PC / File Server and MFP for information protection. • **SMBv3, SFTP** Encrypt communication between PC / File Server and MFP for information protection. • **Digital certificate verification** Verify certificate chain, certificate revocation, and validity period. Certificate update (including the newly issued one), which has been manually performed by an administrator, and associated setting update processing can be automated. • **Disabling setting by network protocol or port** Prevent unauthorized access and data breach. • **Encrypting scanned documents** Prevent data breach with password / public key. • **Direct print of encrypted documents** You can print directly by decrypting encrypted PDF files. • **E-mail encryption and e-mail signature** Reduce the risk of eavesdropping and tampering during e-mail delivery. • **Data breach prevention between different interfaces** Prevent attacks on MFPs or internal network via fax line, wireless LAN, USB port, and malicious programs inside USB memory)

 ©2025 Katun Corporation

KATUN®
SUCCESS MADE SIMPLE.

KATUN® ARIVIA

Security Threats, Measures & Features

B) Protection of Communication and Data

Encrypted Communication between Server or Client PC and MFP (SSL/TLS/IPSec)

You can prevent data breach and tampering in the communication between the device and server or client PC on the network by encrypting communications, assuming if someone attempts unauthorized access on the network. The following are examples of communications that can be encrypted. By default, only TLS1.2 is enabled*, however, TLS1.3 can be supported by changing the settings.

* TLS1.0/TLS1.1/TLS1.3 are disabled by default.

- **Print job using IPP port (print)**
Encrypt the communication path of IPP (Internet Printing Protocol) that is used for exchanging print data to prevent eavesdropping on authentication information and print data.

- **Secure communication using HTTP**
Perform secure HTTP communication when accessing the Internet Services on an MFP from your PC or when accessing an external server from an MFP.

- **Communication with LDAP server (Address Book search / authentication)**
Encrypt the communication path with the LDAP server to prevent eavesdropping on authentication information and Address Book data.

- **Communication with SMTP server (e-mail)**
Encrypts the communication path with the SMTP (e-mail transmission) server to prevent eavesdropping on authentication information and e-mail data.

- **Communication with POP server (e-mail)**
Encrypts the communication path with the POP (e-mail reception) server to prevent eavesdropping on authentication information and e-mail data.

- **Communication with SFTP (scan / file transfer)**
when transferring data to the server by FTP transfer in the job flow, communication path encryption / authentication is performed using the secure shell method to prevent eavesdropping on authentication information and data.

Caution about FTP: Please note that FTP, as it transmits authentication information and data in plaintext, is an insecure protocol. If it is necessary to use FTP for any reason, please ensure that the FTP environment is properly established. For instance, restrict network access to only authorized users, and protect the data and systems from unauthorized access. Whenever it is possible, it is recommended to use SFTP instead.

- **Communication with SMB (scan / file transfer)**
In SMBv3, a communication encryption function has been newly added, and it allows you to send files securely to the destination.

- **Encryption of IP communication by IPsec**
You can prevent tampering and eavesdropping in units of IP packets between devices in which connection by IPsec has been configured. In client communication using certificates, SSL server authentication and IPSec PKI authentication prevent spoofing.

- **Network device authentication using IEEE802.1X authentication**
An authentication standard that regulates the connection of devices to the network when devices connect to each other on the network. As it supports IEEE802.1X authentication, you can securely connect an MFP to the network that is restricted by connected devices.

 ©2025 Katun Corporation

KATUN®
SUCCESS MADE SIMPLE.

KATUN® ARIVIA

Security Threats, Measures & Features

Digital Certificate Validation

Certificate validation is a function to check a certificate used in a communication such as certification chain, revocation checking and validity period. Reliable verification and management of certificates can be carried out with trust anchor certificate management.

It supports automatic certificate delivery feature offered by Network Device Enrollment Service (NDES) of Windows Server. Certificate update (including the newly issued one), which has been manually performed by an administrator, and associated setting update processing can be automated by using SCEP (Simple Certificate Enrollment Protocol).

Encrypting Scanned Document with a Password

With this feature, when storing a scanned document to PC or sending it by email, you cannot only convert the document to a PDF file but also specify "file encryption" with a password. The security functions of applications such as printing and editing restrictions are also supported, let alone password setting for opening files. It reduces the risk of data breach and tampering of scanned documents.

Note: Acrobat Reader / Adobe Reader is required to open encrypted PDF files. However, as the document may not open in older versions, please use the latest Acrobat Reader.

Digital Signing and Public Key-based Encryption for Scanned Documents

Digital signature is available when sending a scanned document in PDF by importing a certificate and private key into an MFP, allowing the detection of data tampering by third parties.

Direct print of encrypted documents

Using a password previously registered in the MFP, the encrypted PDF files stored in USB memory, etc. can be decrypted and directly printed.

E-mail encryption and e-mail signature

E-mail encryption (S/MIME): Encrypt e-mail (including attached documents) by the user's digital certificate so that only the user can open it. It reduces the risk of data breach by eavesdropping during e-mail delivery.

E-mail signature (S/MIME): Sends an e-mail (including attached documents) by attaching the user's signature with a digital certificate of an MFP. It reduces the risk of tampering during e-mail delivery, and objectively prove the sender, allowing recipients to use it with peace of mind.

Preventing Attacks, Eavesdropping, and Data Breaches via Fax Line

Regarding access via fax line (telephone network), only fax protocol communication can be accepted. Therefore, malware in fax data will not affect MFP behavior and unauthorized command will not be executed.

All data received is handled as fax image format data. In case there is malformed data that does not follow the fax protocol standard, it will be processed as image data error such as decoding error.

Images and original documents stored in MFP Folder can be retrieved by polling communication from remote sites. However, no unauthorized data acquisition (breach) will occur by implementing strict password management to MFP Folder.

 ©2025 Katun Corporation

KATUN®
SUCCESS MADE SIMPLE.

KATUN® ARIVIA

Security Threats, Measures & Features

Preventing Attacks, Eavesdropping, and Data Breaches via Wireless LAN (Wi-Fi) Port

The optional wireless LAN converter is a wireless terminal connected with a wired LAN cable. The wireless LAN kit is wireless terminals that perform wireless LAN communication when connected to the MFP.

These wireless terminals support countermeasures to WPA/WPA2's vulnerability known as KRACKs. The Wireless LAN Kit allows users to securely use the device , as it supports WPA3-SAE, which was formulated by Wi-Fi Alliance.

Furthermore, as these wireless terminals do not have a routing function, they do not perform communication between each network interface (TCP/IP).

Accessing an MFP Folder and unauthorized access countermeasures are the same as those for Consequently, information leakage due to unauthorized use of these wireless terminals is averted.

Preventing Attacks, Eavesdropping, and Data Breaches via USB Port

With print jobs imported via USB port, data is handled as printer job language (PJL) and image data. If data other than PJL and image data is received, the job will be suspended due to a job error.

In addition, the relay function establishing a connection to communication lines including network and fax line from USB port is not implemented.

Preventing Attacks, Eavesdropping, and Data Breaches via Virus-infected Files on USB Memory

For the following reasons, MFPs and PCs on the network connected to MFPs are virus-free at execution of scan jobs and print jobs with USB memory.

1. With scan jobs, no access will be attempted to the files on USB memory.
Due to this, MFP will not be infected by virus even if the files on the memory are infected.

2. With print jobs, the files on USB memory are handled as image data.
Assuming the files have been infected, that print job will be suspended due to an image processing error as the format does not match that of image data. Malicious programs will not automatically run.

3. Since MFPs will not be infected by virus as described above, PCs on the network will not be infected by virus via MFPs.

4. Communication method directly connecting to PCs on the network from USB memory is not implemented.

 ©2025 Katun Corporation

KATUN®
SUCCESS MADE SIMPLE.

KATUN® ARIVIA

Security Threats, Measures & Features

Listing of all open ports in the factory default state and their purposes

The corresponding ports and services are as follows and ports other than these will be opened by enabling them individually from User Interface.

Name	Port	Description
	TCP	
IPv4 DHCP Server with WiFiDirect	68	Available when WIFI direct is enabled
LPD	515	
Port9100	9100	
IPP/IPPS	631	
HTTP	80	HTTP including: Web User Interface, UPnP Discovery, Web Services for Products (WSD), WebDAV
HTTPS	443	
HTTPS for XCP (eXtensible Customizing Platform)	58501	Only application on device uses.
	UDP	
SNMP	161	
NetBIOS-NS(WINS)	137	Not supported on SFP
mDNS	5353	
WS-Discovery	3702	

25-06-0039-kbs ©2025 Katun Corporation

KATUN®
SUCCESS MADE SIMPLE.

KATUN® ARIVIA

Security Threats, Measures & Features

Table 3. Security Threats and Measures for Office Multifunction Devices

Security threats to office devices	Security measures implemented
3. Unauthorized access to administration functions Unauthorized operations may be performed if identity authentication to distinguish authorized users cannot work on the rules (security policies) set for document data to be handled and functions that manage user information on the device.	**C) Protection of administration functions** • **System administrator's password** When operating with the default value, a warning message prompts you to change the password. • **Account Lock** To be performed in case of consecutive administrator login failures. • **Customer Engineer Operation Restriction Function** Prevent attacks such as setting changes of MFPs.

C) Protection of Administration Functions

Security Warning Message for Default System Administrator ID & Password

To use the device with higher security, a warning message appears to prompt the administrator to change the password when he/she log in as the system administrator mode with default setting of system administrator ID and password.

Account Lock in case of Consecutive Administrator Login Failures

The function to handle the authentication failures is provided for the system administrator authentication which is performed before accessing the system administrator mode. In case the system administrator fails to login for the predetermined number of times, login attempts can be blocked until the device is restarted.

Customer Engineer Operation Restriction

Operations performed by a customer engineer having special permissions can be restricted with settings configured by the system administrator. A password can be set to enter the customer engineer mode to prevent unauthorized access to the device by a person impersonating a customer engineer.

Table 4. Security Threats and Measures for Office Multifunction Devices

Security threats to office devices	Security measures implemented
4. Software tampering If tampering of software occurs, security policies defined may not be executed properly. With no mechanism to verify that the update program of the product is legitimate, unauthorized software or system files may be uploaded and it leads to disabling the encryption function or installing unauthorized applications.	**D) MFP Software Integrity** • **Vulnerability detection and software update** Regularly performed • **Ensures the integrity when updating software** Prevents unauthorized controller software and add-on applications from being installed on MFPs. • **Ensures the integrity at startup** Prevents unauthorized controller software from being executed at startup. • **Ensures the integrity during operation** Prevents unauthorized operation by monitoring the operation of the controller based on the White List.

 ©2025 Katun Corporation

KATUN®
SUCCESS MADE SIMPLE.

D) MFP Software Integrity

Ensures the integrity when updating software

When updating the controller software, the digital signature verification function prevents the software from being rewritten to the unauthorized one created by a malicious third party. If tampering is detected, the event is recorded in the audit log without starting up the MFP.

As a security level enhancement, you can disable the software updating function from the network to prevent unauthorized software updates over the network.

Furthermore, you cannot update the software from the fax line.

Ensures the integrity at startup (tampering detection function at startup by secure boot function)

When booting the MFP, it verifies the electronic signature of the controller software, and if a falsification is detected, it recovers automatically from golden master (resilience).

Achieves more robust security (HW Root of Trust) by using immutable hardware at the reliable starting point.

Ensures the integrity during operation (tampering prevention function during operation using White List)

Protects normal applications and prevents unauthorized operation by monitoring the operation of the controller based on the White List to prevent suspicious applications from being executed.

Also, unexpected access can be blocked by controlling the network communication destination using the IP address restriction function.

Table 5. Security Threats and Measures for Office Multifunction Devices

Security threats to office devices	Security measures implemented
5. Audit log tampering If the audit log obtained for tracing unauthorized activities is not protected, the log may be tampered or deleted.	**E) Audit log, protection of the log, and other log related functions** • **Audit Log** You can trace the history by using the function to record stop / start of the MFP, configuration changes, and job progress status. • **Audit Log Protection** You can disable viewing, editing, and deletion of audit logs by unauthorized persons. • **SIEM linkage of audit logs** Collective management and analysis of audit logs become possible by linking MFP's audit logs with SIEM products using the Syslog protocol. • **Restrictions on job information display** You can also set to hide job log record that indicates job execution result from other users. • **You can print document-specific identifier "UUID"** You can trace a specific user in the event of data breach.

 ©2025 Katun Corporation

KATUN®
SUCCESS MADE SIMPLE.

E) Audit Log, Protection of the Log, and Other Log-related Functions

Audit Log

You can download “audit log” from Internet Services via web browser. This log shows you detailed history including system data changes, user login/logout, power on/off and job progress status to help you enhance system management and trace the history of unintended changes. It is also useful to raise users’ awareness about security.

Operations related to the following items are recorded on the audit log:

- Status Change: Power on/off of the device, start/end of user operation, etc.
- Login Status: User login, logout, authentication lock of the system administrator, etc.
- Job Status: Job completion, etc.
- Setting Change: Time setting, Security setting change, user information setting, opening Folder, etc.
- Data Change: Certificate change, Address Book change, etc.
- Configuration Change: Storage replacement, ROM version change, etc.
- Communication Result: Communication error, etc.

Audit Log Protection

Audit Log should not be viewed/edited/removed by third parties because of its objective. The following measures are applied for its protection.

- There is no interface to edit/delete the audit log.
- Only administrators can access it. And encrypted communication with SSL/TLS is required to download it.
- Also the audit log information can be protected with the Storage encryption feature even when it is replaced/removed from MFP.

SIEM linkage of audit logs

Early detection and analysis of security threats are supported, as it becomes possible to collectively manage and analyze MFP’s audit logs by using the function to transfer MFP’s audit logs to the outside using the Syslog*1 protocol and linking with SIEM*2 products.

*1: Syslog is a standard protocol that transmits chronological records (logs) through an IP network.

*2: SIEM (Security Information and Event Management) is security software / services that collectively stores and manages records (logs) of the operating status of devices and software, and quickly detects and analyzes events that pose security threats.

Restriction on Job Information Display

This feature allows you to configure settings for restricting information to be displayed such as making it impossible for unauthenticated users to view information on jobs in execution, awaiting, or completed states.

Display restriction can be also set for authenticated users so that they can view only their own jobs and cannot view those of other users. You can enjoy privacy protection and data breach prevention.

Printing Job Log Identifier UUID

This feature allows you to print a document-specific identifier called “Universal Unique Identifier (UUID)” on copy, print or fax documents. You can use it when searching for or identify a certain document. As it shows “when” “by whom”, and “how” documents were handled for check, it helps you identify a certain user in the event of data breach.

 ©2025 Katun Corporation

KATUN®
SUCCESS MADE SIMPLE.

KATUN® ARIVIA

Security Threats, Measures & Features

Table 6. Security Threats and Measures for Office Multifunction Devices

Security threats to office devices	Security measures implemented
6. Breach of document data stored on the device (at return after lease end or device disposal) Document data used for print, copy, or fax are temporarily or permanently stored to the storage . That data may be compromised from the device when it is returned after lease end or it is disposed. This document data may be restored if it has not been physically deleted, even if it seems that access to the data cannot be made on the surface.	**F) Protection of document data stored on the device** • **Encrypting data stored on Storage** Prevent third parties from analyzing the storage removed from an MFP. • **Batch deletion of data in MFP Storage** Batch deletion of the setting information and document information can be performed before reusing an MFP at another organization or disposing it, so that prevent the leakage of information in the MFP.

F) Protection of Document Data Stored on the Device

Encrypting Data Stored on Storage*1

When data is written to the storage, it is encrypted with a very robust method*2 to prevent unauthorized access to stored data. In addition, it prevents the data from being analyzed by a third party when carrying out the MFP.

This cryptographic key itself is not stored in non-volatile memory but generated for use every time the MFP is booted. For this reason, this key will not be compromised even if non-volatile memory is removed from the storage.

In addition, in some models, the encryption key used to encrypt the data stored in the storage is further encrypted with the root encryption key inside the security chip (TPM: Trusted Platform Module) independent of the storage. The root encryption key is securely protected without being read from the outside due to the tamper resistance of TPM.

*1 SSD *2 AES-256

Batch deletion of data in MFP Storage*1

The administrator can delete all information registered and set in the MFP when disposing of or moving it to another department. It prevents the leakage of data in the MFP at the time of disposal.

For SSD-equipped machines, data is erased by formatting (Secure Erase). When the data accumulated in the SSD storage is encrypted, the encryption key is also deleted by performing batch deletion. By deleting the encryption key, you cannot decode (read) the encrypted data accumulated in the SSD storage, so it has the same effect as when the data itself is deleted (Cryptographic Erase).

*1 SSD (Secure Erase)

 ©2025 Katun Corporation

KATUN®
SUCCESS MADE SIMPLE.

KATUN® ARIVIA

Security Threats, Measures & Features

Table 7. Security Threats and Measures for Office Multifunction Devices

Security threats to office devices	Security measures implemented
7. Data breach caused by careless mistakes of system administrators or users Even if system administrators or users think that they configured settings or performed operations with no mistakes, wrong operations lead to unexpected data breach.	**G) Preventing configuration / operation mistakes and improving the awareness of document handling** • **A security warning message for global IP address** Encourage the administrator to change the IP address or use the user authentication mode. • **Scanned documents to be delivered to / stored in fixed destination** You can prevent users from sending data to wrong destination / data breach by limiting the communication destination (including fax) to a specific destination. • **Suppressing erroneous fax transmission** Suppress mistakes by reentering destinations, manual redialing, etc. • **Block Fax Reception** Prevent annoying direct mails. • **Print Lockout Duration** You can prevent printouts left unattended. • **Suppress data breach from printed documents**

G) Preventing Configuration/Operation Mistakes and Improving the Awareness of Document Handling

Security Warning Message for Global IP Address

In case a global IP address is assigned to the MFP and [No Login Required] is set as the [Login Type], a warning message appears when a system administrator logs in. This function encourages system administrators to change the IP address or to apply user authentication modes.

Scan to Fixed Destination

This feature allows to automatically fix the destination address or sender to the authenticated user's own email address. You can use it to prevent wrong email transmission and external email transmission in an effective way.

The document storage location can be fixed to a folder on your PC and moreover, once you store a scanned document on the device, you can send an email with the URL of the storage location attached to the authenticated user. It will be a great help also for reducing loads on network or mail server as well as for secure mail delivery to the authenticated user itself.

* Operation in Authentication mode is required.

25-06-0039-kbs ©2025 Katun Corporation

KATUN®
SUCCESS MADE SIMPLE.

KATUN® ARIVIA

Security Threats, Measures & Features

Preventing End Users from Sending Faxes Wrongly

Sending a fax to a wrong destination - anyone could make this mistake. However, it could lead to catastrophic consequences. Some functions including the following have been enhanced to prevent wrong fax transmission. These functions are compliant with "FASEC 1*", which is the guideline for security functions of fax for business use.

- Re-entry of FAX Destinations: Enter the destination twice for verification

- Manual Redial: Send a fax by selecting a destination from the list of transmission history

▪ **Fax number re-entry**
Avoids input error by entering the destination number twice.

▪ **Prohibition of sending faxes to fax numbers that are not in the Address Book**
Restricts users from sending faxes to numbers not listed in their address book.

▪ **Forced prohibition of direct faxing**
Prohibits fax transmission from PC.

▪ **Display of a fax number confirmation window**
Displays the confirmation screen before sending fax and allows you to delete the destination if it is wrong.

▪ **Fax number confirmation and unnecessary fax number deletion when sending faxes to multiple recipients**

Allows you to delete or correct destinations for broadcast fax.

▪ **Manual redial**
Records the destination once a fax is sent to a destination. Ensures correct fax transmission with a text fax transmission in advance.

Furthermore, the following functions are also applicable against wrong fax transmission.

▪ **Wrong fax transmission can be avoided by prohibiting broadcast fax.**

▪ **The relay broadcast and transfer functions can be prohibited for fax transmission.**

Block Fax Reception

Annoying fax prevention function
Prevent receiving junk faxes by an incoming call rejection function.

You can reject senders from whom you do not want to receive faxes or faxes sent from unknown fax numbers. Eliminate useless print by junk faxes unspecifically sent.

▪ **Block Fax Number: Register G3 ID (phone number) that rejects fax reception. You can register up to 50 fax numbers.**

▪ **Block Unknown Fax Numbers: You can block faxes whose G3 IDs (phone numbers) are unknown.**

Block faxes received from senders other than those registered in the Address Book

You can block faxes received from senders other than those registered in the MFP's Address Book with settings configured by a customer engineer.

25-06-0039-kbs ©2025 Katun Corporation

KATUN®
SUCCESS MADE SIMPLE.

KATUN® ARIVIA

Security Threats, Measures & Features

Print Prohibited Time Period

This feature allows you to specify a time zone when printing is disabled and it prevents uncollected printed and faxed documents when no one is at the office.

Even while printing is disabled by Timers, user can change it to be enabled.

Annotations

You can add a stamp such as “DO NOT COPY” to your document when copying it to inform others of the significance of the document.

Force Annotation

With this feature, it is possible to forcibly print user ID, output year/month/date. etc. on copied, printed, or received fax documents. It allows you to identify “when”, “who”, output the document in an easy way and set four layout template patterns by associating them by print job. It facilitates adequate paper document handling in an easy and hassle-free manner as you can enjoy this feature on the device without any optional functions.

Copy Managemen (Analog Watermark)

You can output a document by printing a control number or watermark on its background. When copying the document, they appear on the surface and it helps to prevent data breach by unauthorized copying. This encourages users to deal with the printed documents more carefully.

The contents, product specifications and other details in this documents are subject to change without notice for improvements.

 ©2025 Katun Corporation

KATUN®
SUCCESS MADE SIMPLE.