

TOSHIBA



END-TO-END SECURITY

Elevate Sky[®] Workflow

April 2025

How to use this paper.

This white paper provides an overview of the security features built into Toshiba MFPs and Elevate Sky® Workflow, helping answer common IT and compliance-related questions.

Let's keep your data protected—at every step.



Table of Contents

Preface	4
1.1 Before Reading This Document	5
1.1.1 Considerations and Limitations	5
1.2 General Use Cases	5
1.3 Data Chain: Data Captured at the MFP (Representative Functions)	7
1.3.1 Secure Data Chain at the MFP	7
Elevate Sky® Workflow – Product Overview	8
2.1 Operation & Management	8
Elevate Sky® Workflow – Security	9
3.1 Access Controls and Authentication	9
3.2 Identification	10
Secured User Interaction	10
3.2.1 Backend Verification	11
3.3 Data Acquisition	12
3.4 Data Structuring	12
3.5 Data Sharing	13
3.6 Data Encryption	14
Key Security Aspects of ESW Data Encryption	14
3.7 Data Retention	14
3.7.1 Job Data Retention	15
3.7.2 Company Data Deletion Actions (After License Invalidation)	15
3.7.3 User Data Retention (Transactional)	16
3.8 Network Security	16
Additional Information	17

Preface

Securing applications used for **data acquisition** ensures that sensitive data, including personally identifiable information (PII), remain protected from unauthorized access, breaches, and cyber threats. Strong encryption, access controls, and secure transmission protocols safeguard data both in transit and at rest, while maintaining compliance with industry standards. **For customers, secure multi-function printer (MFP) applications provide peace of mind** by preventing data leaks, ensuring document integrity, and protecting confidential business information. In general, MFP security enhances trust, reduces risk, and supports compliance, making it essential for organizations handling sensitive documents.

1.1 Before Reading This Document

Disclaimer: The information provided in this document is intended solely for informational and educational purposes. It is not designed to serve as a definitive security architecture, nor should it be relied upon for establishing formal security requirements, compliance frameworks, or risk management strategies. While every effort has been made to ensure accuracy, security best practices continuously evolve. Organizations should conduct independent assessments, consult with qualified security professionals, and tailor solutions to their specific operational and regulatory needs. The guidance presented herein does not constitute a guarantee of security and should be interpreted as a general description of features and recommendations, rather than prescriptive measures.

1.1.1 Considerations and Limitations

- Consumers of the ESW product should institute their own safeguards to further harden security.
- The utilization and monitoring of security logs will serve as complementary best practices for the ESW and any service-based application.
- ESW Administrator/User roles are implemented as Role Based Access Control (RBAC), rather than Attribute Based Access Control (ABAC) commonly applied within Identity and Access Management (IAM) implementations.
- ESW or affiliate partners such as AWS do not provide compliance guarantees. The responsibility for security best practices always resides with the customer and end-user.

1.2 General Use Cases

ESW is designed as a hub-and-spoke architecture, with the hub representing a cloud solution and the spokes representing client-functioning embedded applications.

- An administrator manages a company within the administrative dashboard and grants access to individuals authorized to utilize ESW. The administrator may also be responsible for establishing document templates, which individuals within the company use to perform workflow activities based on template data.
- The end-user accesses ESW by entering their credentials to launch the application. Additional login options, such as PIN authentication, may be enabled at the enterprise level (rather than configured on individual MFDs). Users can update their access PIN at any time. Once logged in, the user uploads documents, triggering a data acquisition process that supports data-driven workflows.

ESW supports two primary use cases.

- In the first use case, an end-user uploads a source document directly at the MFP. A limited amount of data processing takes place on the device via the embedded ESW application and its Integrated Platform. The data is encrypted and sent to a cloud-based instance of the Integrated Platform, where full processing and job execution occur.
- In the second use case, the data originates from external connected sources rather than the MFP. Similar to the first use case, the data is encrypted and sent to the cloud-based platform for processing and job execution.

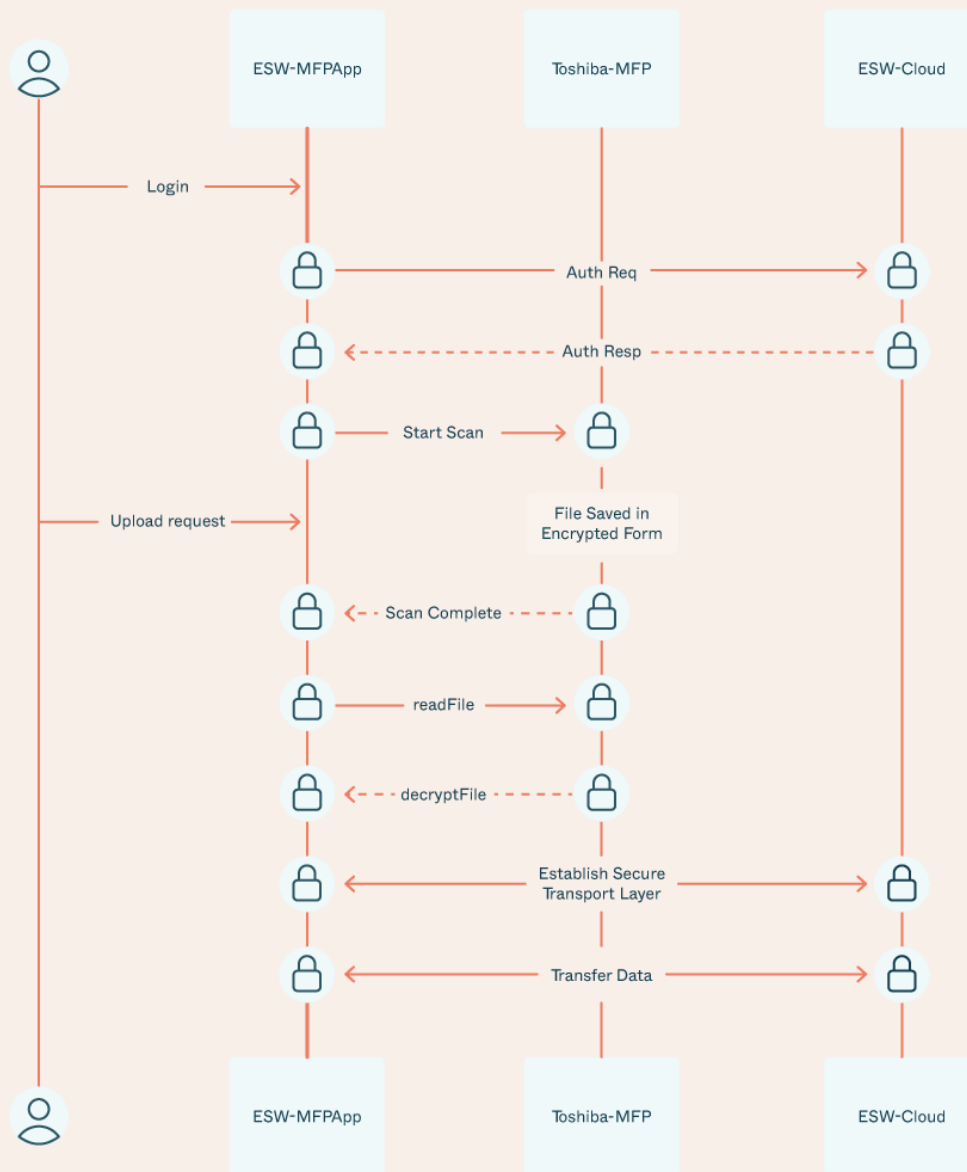


Figure 1: ESW data sequence depicting data from source to cloud

1.3 Data Chain: Data Captured at the MFP (Representative Functions)

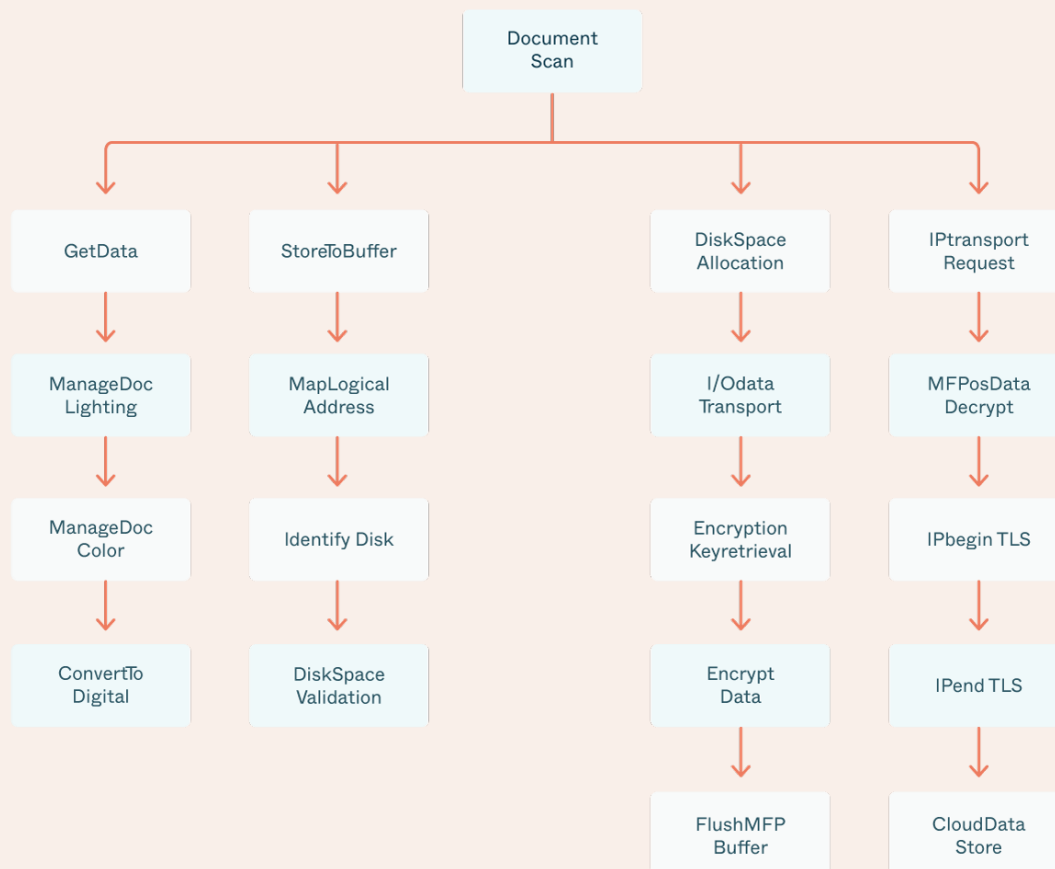


Figure 2: ESW Functional Decomposition (FD) representing the ESW data chain

1.3.1 Secure Data Chain at the MFP

The Toshiba MFP performs a capture function (*GetData*) in which a scan process initiates the scan of a document. Some basic functions that follow the *GetData* function include managing document lighting (*ManageDocLighting*), managing document color (*ManageDocColor*), and others before performing an analog-to-digital conversion (*ConvertToDigital*) of the source document.

Data captured at the MFP is temporarily stored in nonvolatile memory (*StoreToBuffer*). Native Toshiba MFP logic identifies the logical location (*MapLogicalAddress*) where the data is temporarily stored. The disk volume is verified (*IdentifyDisk*) as a target location where the temporary data will be stored. The available storage space is verified (*DiskSpaceValidation*) to ensure temporary storage retention.

Disk space is allocated (*DiskSpaceAllocated*) on the encrypted disk of the Toshiba MFP. The I/O controller of the Toshiba MFP transports the temporary data (*I/OdataTransport*) from nonvolatile memory to the Toshiba encrypted disk (volatile memory). The Toshiba encrypted disk automates an encrypted key retrieval (*EncryptedKeyRetrieval*) process to encrypt the data at rest. The plain text of the source document is automatically encrypted (*EncryptData*) on the Toshiba encrypted disk. Upon encryption of the data, buffers that contained the temporary data are flushed (*FlushMFPBuffer*).

The ESW app sends a transport request (*IPtransportRequest*) with the intent of moving data originating at the Toshiba MFP to the ESW cloud. The request from the ESW app begins a decryption process (*MFPposDataDecrypt*) in which the encrypted data is converted back to plain text before transport. The ESW app establishes a secure transport via Transport Layer Security (TLS) v1.2 between the Toshiba MFP and the ESW cloud, ensuring the complete security of data, while encrypting data-in-transit to the ESW cloud (*CloudDataStore*).

Elevate Sky® Workflow – Product Overview

Elevate Sky® Workflow (ESW) is a cloud service that automatically ingests documents obtained from a multi-function printer (MFP), personal computer (PC) and a mobile device with various business applications.

2.1 Operation & Management

ESW operates on AWS® (Amazon Web Services), leveraging a trusted and robust security infrastructure that complies with globally recognized standards, including ISO/IEC 27001 for Information Security Management, ISO/IEC 27017 for cloud service security, and ISO/IEC 27018 for the protection of personally identifiable information (PII) in the cloud. Additionally, AWS® meets SOC1, SOC2, and SOC3 requirements, ensuring adherence to strict controls over data confidentiality, integrity, and availability. These certifications validate that the underlying infrastructure behind ESW is designed and maintained with best-in-class security measures.

To further strengthen system security, ESW undergoes rigorous and comprehensive vulnerability audits both before release and on an ongoing basis. These assessments include automated vulnerability scans, manual penetration testing, and the remediation of any identified risks to ensure a secure operating environment. This proactive approach helps mitigate potential threats while maintaining compliance with evolving security standards—ultimately delivering a highly secure and reliable platform for users.

Elevate Sky® Workflow – Security

Ensuring security and data integrity throughout the lifecycle of a workflow is critical in any system. This document outlines key security aspects across access control, identification, data acquisition, data structuring, and data sharing, each playing a vital role in protecting sensitive information and maintaining compliance.

Access Control	Establishing and enforcing role-based and attribute-based permissions ensures that only authorized users can perform specific actions, reducing the risk of unauthorized access or privilege misuse.
Identification	Secure authentication mechanisms, including token-based verification, help validate user identities and prevent unauthorized entry.
Data Acquisition	Protecting data at the point of collection is essential; secure transmission protocols (e.g., TLS encryption) and validation processes ensure data integrity from its source.
Data Structuring	Organizing and securely storing data received from scans, as well as storing data securely using encryption, access policies, and structured formats, enhances data protection and prevents unauthorized modifications.
Data Sharing	Secure integration with external services requires API security and controlled data access to prevent data leaks and unauthorized sharing.

ESW addresses security principles, utilizes security-centric design to mitigate risks, ensures data confidentiality, and maintains trust by delivering a secure workflow solution.

3.1 Access Controls and Authentication

ESW enforces strong security by requiring user login, ensuring that only authorized individuals can access the ESW platform. Validation is required as part of company registration, which ensures entitlement compliance and restricts usage to legitimate users. ESW allows integration with services like Google™ and Microsoft®, while requiring separate credentials with secure authentication methods (e.g., OAuth 2.0) to ensure data ingress/egress requests are granted only to approved accounts. The ESW access controls and authentication measures uphold data integrity, prevent unauthorized access, and enable fine-grained controls tailored to ESW users.

ESW security provides safeguards in four (4) core areas of the document workflow.

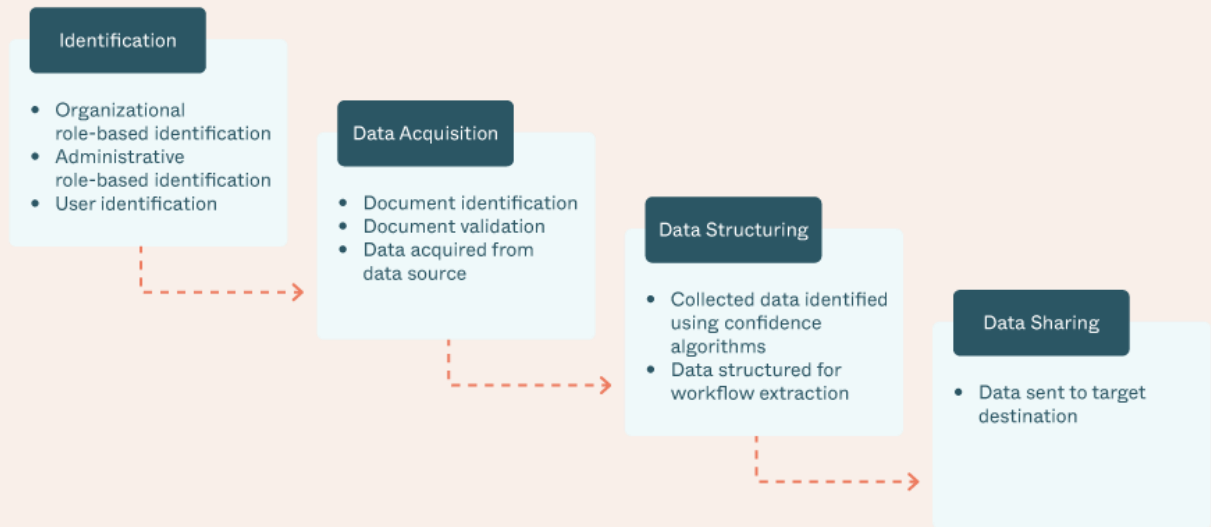


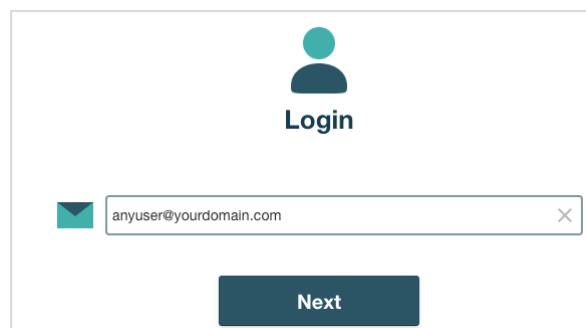
Figure 3: ESW Data Flow

3.2 Identification

ESW performs secure user interaction between the user and the ESW cloud, then verifies access using backend processing.

Secured User Interaction

ESW provides a secure web portal that enables users to manage their data workflows and gives administrators the tools to oversee business activities. Users log in through a branded, ESW-specific interface using their email and password. The connection between the user and the ESW service is established over HTTPS (Hyper Text Transfer Protocol Secure), ensuring a secure communication channel. All data transmitted is encrypted using Transport Layer Security (TLS) version 1.2, protecting it from unauthorized access and ensuring confidentiality during transmission.



The login form features a user icon and the word "Login" at the top. Below this is an email input field with a teal envelope icon on the left, the text "anyuser@yourdomain.com" in the center, and a close button (X) on the right. At the bottom of the form is a dark blue button labeled "Next".

Figure 4: ESW login prompt / login data entry

3.2.1 Backend Verification

ESW leverages a robust user pool authentication system to provide secure, fine-grained access control. By utilizing backend attributes and token claims, ESW ensures modern, scalable authentication that protects user data and system integrity.

- ESW user credentials are validated against a managed user pool
- Federated users are validated against the respective Identity Provider (IdP) (e.g., Microsoft®, Google™)
- ESW support for federated identities maps external identities to ESW

Credential Management

Prior to the ESW backend performing verification, ESW users provide the appropriate credentials via the web portal. The credentials provided by ESW users are hashed using hashing algorithms (e.g., bcrypt or equivalent) during the login request, then encrypted using TLS 1.2.

Token-Based Security

Upon successful authentication of the ESW user via credential management, token-based security is utilized in the form of three (3) JSON Web Tokens (JWT):

- **ID Token:** Contains ESW user information such as an email address
- **Access Token:** Used to authorize various API calls
- **Refresh Token:** Used to obtain new tokens without requiring reauthentication

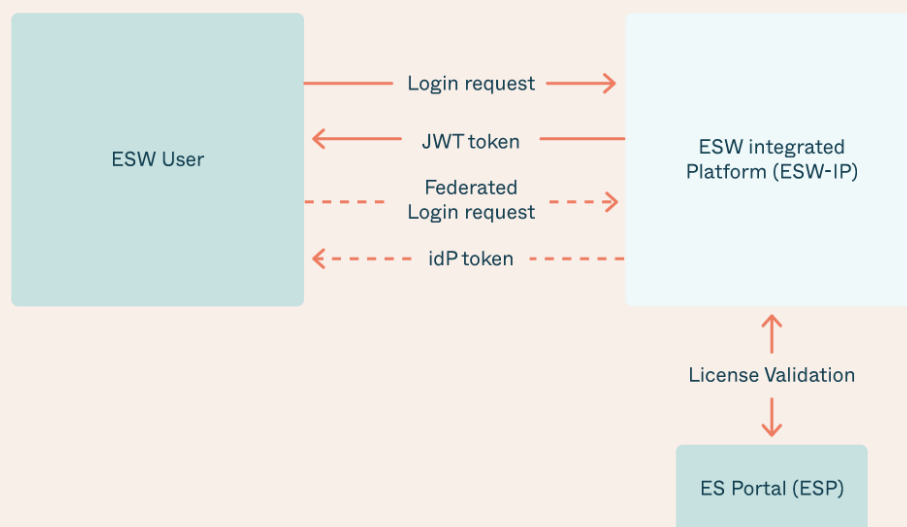


Figure 5: ESW identification & authorization block diagram

3.3 Data Acquisition

ESW cloud services are accessed directly from Toshiba MFPs through the installed ESW embedded application. When launched from the MFP control panel, the embedded application functions as a client application of the ESW cloud. The ESW services running on the MFP, via the embedded application, securely connect to the ESW cloud using standardized protocols (e.g., HTTPS, OAuth 2.0).

Once initiated, the application facilitates data acquisition from source documents and begins data processing in the ESW cloud environment. To access the service, users must enter their unique PIN, which is authenticated against ESW's cloud-based identity service. Upon successful verification, the MFP receives an OAuth 2.0 access token, enabling the user to securely utilize ESW functionality from the device.

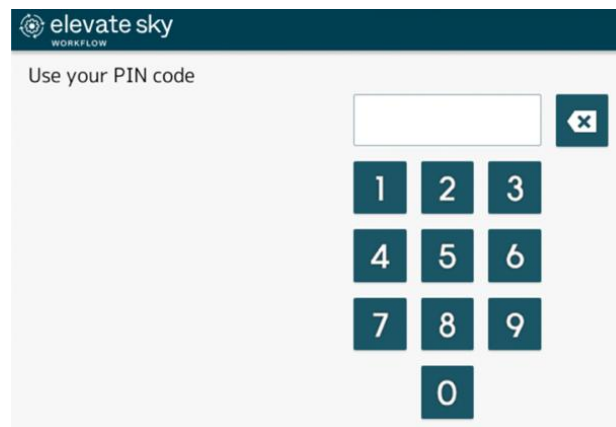


Figure 6: ESW PIN login from MFP

ESW enforces role-based access control at the MFP to ensure that only authenticated users can retrieve or manage scanned data. When a document is scanned, the acquired data is temporarily stored on the device before being securely transmitted to the ESW cloud. There, it is routed to integrated systems for OCR processing. Because OCR is not performed locally on the MFP, the risk of exposing sensitive data at the device level is significantly reduced, enhancing overall data security.

3.4 Data Structuring

Once data is captured through ESW, it is parsed into logical groupings and stored in secure cloud environments. Access to this data is tightly controlled, ensuring that only authorized entities can interact with it.

Within the ESW portal, only the processed and analyzed OCR output—such as extracted text and confidence scores—is displayed. Fully scanned documents are not exposed, reducing the visibility of sensitive information and ensuring that only essential data is presented to the user.

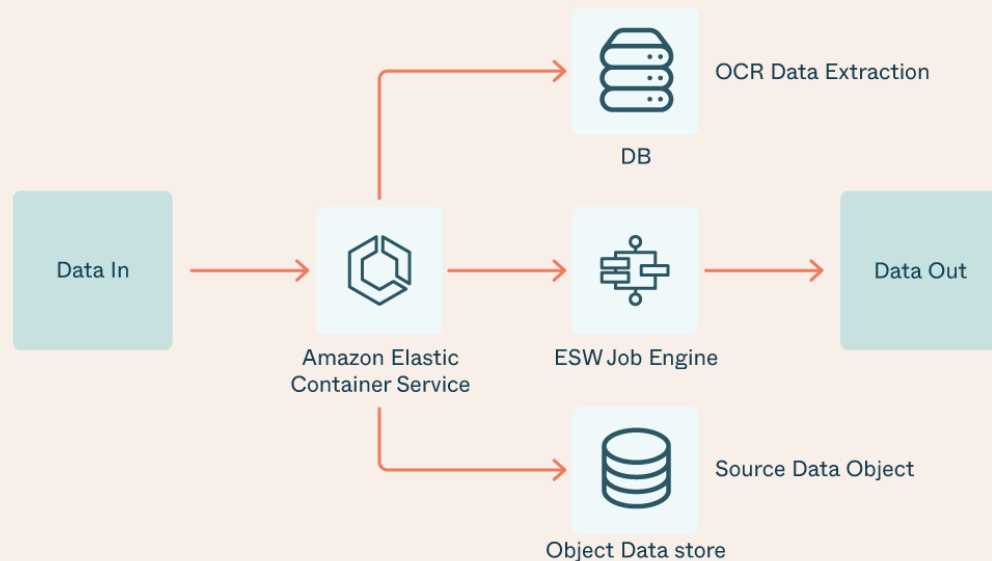


Figure 7: Abbreviated view of the ESW Data Store Environment

3.5 Data Sharing

ESW supports integration with external services through two built-in connectors: the “Popular Cloud Connector” and the “Internet Platform as a Service (iPaaS) Connector”.

- The **Popular Cloud Connector** enables secure connections to widely used data storage services such as Google Drive™, Dropbox®, SharePoint®, OneDrive®, and Box™. These integrations leverage OAuth 2.0 for use cases such as document retrieval.
- Similarly, the **iPaaS Connector** supports workflow automation by connecting to services like Make.com and Zapier®, allowing seamless interaction with various third-party platforms.

Before any connection is made, ESW users must grant explicit consent for selected third-party service. Once approved, ESW retrieves access tokens—never user credentials—to authorize API calls securely, maintaining strong data protection and user privacy.

When data is shared with external services or automation platforms, ESW ensures security through robust encryption protocols—both in transit (e.g., HTTPS, TLS) and at rest. Access is restricted through strong authentication methods such as OAuth or API keys, ensuring only authorized users and systems can interact with the data. Additionally, secure integration with external services and automation tools includes endpoint validation, limiting data exposure, and applying the principle of least privilege to limit access only to data necessary for the workflow.

3.6 Data Encryption

ESW cloud data storage is secured using server-side encryption, which automatically encrypts data at rest using keys managed by the AWS Key Management Service (KMS). The AWS KMS service ensures that data is protected without requiring any action from the ESW user. ESW's integration with AWS offers scalability, compliance with global security standards, and seamless integration with various AWS services, making it a robust solution for secure data storage.

Key Security Aspects of ESW Data Encryption

- Automatic encryption for data at rest and in transit
- Encryption algorithms such as AES-256
- Compliance with standards such as GDPR, HIPAA, and SOC

3.7 Data Retention

ESW follows a strict data retention policy to enhance security and reduce the risk of unauthorized access. Sensitive OCR-processed data is retained only as long as necessary to support system functions, minimizing exposure to potential breaches and unauthorized access. Through its integration with AWS, ESW leverages native data lifecycle and retention policies within AWS S3 and AWS DynamoDB. These capabilities help automate data deletion, reduce reliance on manual processes, and improve overall security posture. Additionally, ESW's use of AWS S3 lifecycle rules support automatic archiving or deletion based on predefined conditions, while AWS DynamoDB utilizes Time to Live (TTL) functionality, which automatically removes expired data to maintain optimal performance and efficiency. Together, these tools ensure that data is only stored for as long as it is needed—supporting a balance between security, compliance, and cost optimization.

3.7.1 Job Data Retention

To maintain performance and keep stored data relevant, ESW enforces short retention periods for job-related data. This prevents data accumulation, improves system efficiency, and ensures operational focus. Once an ESW job is completed, the data is deleted after the following conditions are met:

Job State	Retention Period
Incomplete job	Data removed after 7 days
Jobs uploaded successfully	Data removed after 14 days
Jobs uploaded unsuccessful	Data removed after 14 days
Job execution log data	Data removed after 90 days

Table 1: ESW job data retention lifecycle

3.7.2 Company Data Deletion Actions (After License Invalidation)

To further enhance security and ensure compliance, ESW automatically decommissions associated AWS systems after the license expiration period. This process helps prevent unauthorized access, minimizes the risk of data breaches, and aligns with licensing agreement requirements. All company-related data is scheduled for removal two months after the official license expiry date, including:

Data Type	Data Resource Removed (Purged / Unallocated)
User data	AWS Cognito
Company data (and workflow template data)	AWS Cognito & AWS Dynamo DB
User group data	AWS Cognito & AWS Dynamo DB
Device data	AWS Dynamo DB
Company connection data	AWS Dynamo DB

Table 2: ESW company data deletion actions performed after expiry period

3.7.3 User Data Retention (Transactional)

When a user is removed from ESW, all associated data is immediately deleted to maintain security and ensure data hygiene. This includes:

- User connection data
- User PIN code

3.8 Network Security

ESW employs a multi-layered network security strategy to protect against unauthorized access, data breaches, and cyber threats.

A Web Application Firewall (WAF) is implemented to monitor, filter, and block malicious traffic in real time. The WAF helps prevent common web-based threats such as SQL injection, cross-site scripting (XSS), and denial-of-service (DoS), ensuring that only legitimate traffic reaches the ESW platform.

All communication between ESW and connected devices—including MFPs, PCs, mobile devices, and integrated business applications—is encrypted using HTTPS with TLS v1.2 encryption, providing end-to-end protection. This ensures data confidentiality and integrity during transmission, safeguarding against interception or tampering.

ESW also enforces strict certificate validation and secure handshakes to authenticate all endpoints before any data exchange occurs. This robust encryption framework aligns with industry best practices and helps protect sensitive information in transit.

Additional Information

Toshiba is committed to the ongoing security and reliability of the Elevate Sky® Workflow platform. If you have any questions not covered in this document, or if you believe you have identified a potential security issue, please contact us at security@tabs.toshiba.com



All product names, logos, and brands referenced in this document are the property of their respective owners. Use of these names, logos, and brands does not imply endorsement. Microsoft®, SharePoint®, QuickBooks®, Salesforce®, Zapier®, and other third-party marks are trademarks or registered trademarks of their respective holders.