TOSHIBA

e-BRIDGE® Global Print

WHITE PAPER:
e-BRIDGE® GLOBAL PRINT & SECURITY

TABLE OF CONTENTS

TOSHIBA

WHITE PAPER: TOSHIBA'S e-BRIDGE® GLOBAL PRINT & SECURITY

The purpose of this document is to provide an overview of the importance of security, flexibility and ease-of-use when meeting the needs of modern work environments to encourage productivity and collaboration.

1. OVERVIEW

As modern work models continue to evolve, your employees seek more flexibility. Toshiba's e-BRIDGE® Global Print meets this challenge by making it easy to work from anywhere. Employees can send their print jobs directly to your company's fleet of cloud-connected Toshiba MFPs, from any remote location, and then release them directly from any MFP touch panel.

e-BRIDGE® Global Print is a completely cloud-native application, so users no longer need to know the IP Address of a particular printer or whether they're on the same network as the printer they want to use. Once your employees simply install the Toshiba universal print driver onto their computer and register with e-BRIDGE® Global Print, they can send print jobs from anywhere to the company print queue in a secure manner. All print jobs are encrypted from a user's workstation all the way through to the MFP where the job is released and printed. To further ensure sensitive documents are not left unsupervised at the document tray, users must employ a simplified secure authentication process at the MFP control panel.

2. e-BRIDGE® GLOBAL PRINT

e-BRIDGE® Global Print is a hosted application that connects your fleet of Toshiba MFPs directly to the cloud with industry-leading security. In a traditional print environment, print servers and ports can be vulnerable to hackers gaining access to sensitive information.

2.1 SECURITY MISSION & DESIGN PHILOSOPHY

Toshiba understands that you've trusted us to safeguard your information. We take this responsibility seriously and have designed e-BRIDGE® Global Print with security top of mind. From the backend server down to the end-user experience at the panel, our design and implementation heavily rely on a zero-trust security framework. We ensure that the workstation app, MFP app, and cloud server authenticate each operation.

One of the main tenets of a highly secure environment is network segmentation. With this in mind, we improve upon traditional print environments.

- To be secure, resources shouldn't be able to contact one another. Unfortunately, with a traditional print environment, your printers must be open to incoming traffic, which allows the possibility of an MFP breach granting access to other resources on your network. In contrast, e-BRIDGE® Global Print allows an architecture whereby your MFPs can be on a different network than your employees. This architecture eliminates the possibility of an MFP breach granting access to user data on your network.

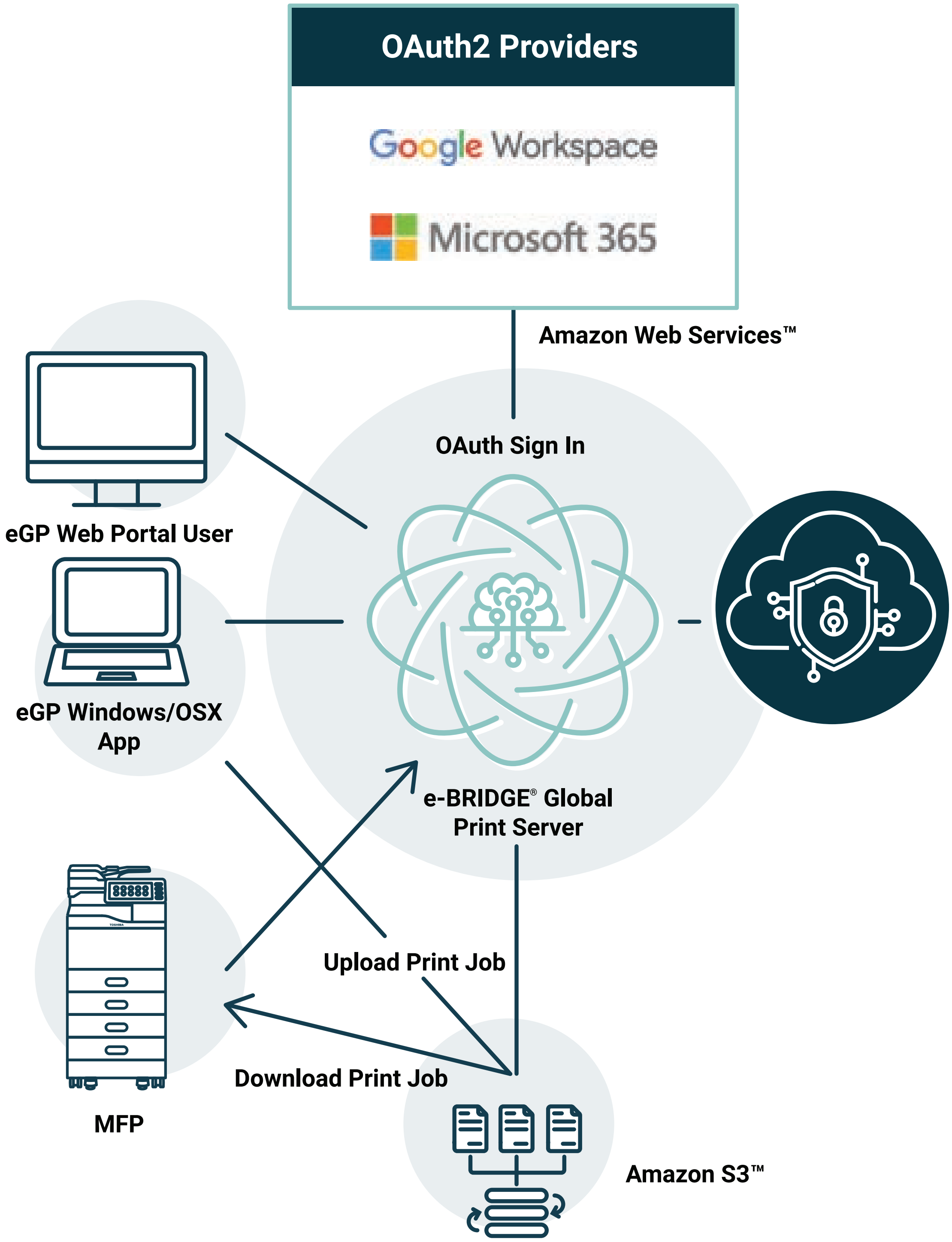
- In a traditional print environment, print requests are initiated from a print server, which, again, requires you to have your printer ports open, thereby increasing the security threat. In contrast, e-BRIDGE® Global print requests are initiated by the user at the MFP or at their client devices (desktop or laptop), so the need for open ports on the MFPs is eliminated.

Another security measure is to validate each element on the network and not assume that actors inside the network are trusted or secure. With e-BRIDGE® Global Print, each operation between the print driver, the cloud, and the MFP requires a specific, secure token to maintain security with each operation.

secureMFP
CLOUD
Seamless and Secure Systems
FLEET
Fleet-wide Security Administration
DOCUMENT
Document Lifecycle Defense
ACCESS
Physical & Digital Access Protection
DEVICE
Install to End-of-Life Product Defense

2.2 NETWORK TOPOLOGY & GEOGRAPHY OF DATA

The illustration below shows the basic data flow for a user accessing the e-BRIDGE® Global Print service. The client app (Toshiba Universal Print Driver) communicates with our cloud server over a secure HTTPS (TLS) connection. If registration is needed, the user is sent to a third-party authentication provider to log in, which responds back to our server once validation is successful. Next, the client receives and stores a secure, per-user token. This token is used to authenticate requests to submit print jobs to the e-BRIDGE® Global Print queue. Once submitted, the user can go to any MFP and log in, and a secure, per-session user token is used to access the server and grant user access to release their print jobs.



3. DEVICE LEVEL SECURITY

3.1 MFP SECURITY

Toshiba takes a holistic approach to security when it comes to our MFPs. There are security features built into each layer such as hardware, firmware, application, and cloud.

For information about Toshiba's holistic approach to security, please review the following white paper:
https://business.toshiba.com/media/tabs/downloads/products/White%20 Paper_Toshiba%20Holistic%20Approach%20to%20Print%20Security.pdf

In addition to built-in security, e-BRIDGE® Global Print includes several added security features as well.

3.2 EMBEDDED MFP APP SECURITY

Toshiba has built a secure, user-friendly embedded app that resides on the MFP and integrates with e-BRIDGE® Global Print. This touch screen app allows users to view, delete, and print those jobs in his/her queue in a secure manner. Toshiba designed the app to ensure that users can't use the app to access another user's data—even administrators are prevented from accessing users' content. Personal information, user passwords, and print jobs are never permanently stored in the app or on the MFP.

It should be noted that this app and all Toshiba MFP apps are built with security in mind. All apps are validated using a signing policy to prevent the MFP from installing unverified content. Additionally, apps cannot talk to one another or share data in an unauthorized way.

3.3 CLIENT SECURITY

Toshiba follows modern security protocols including OAuth 2.0 and JWT, and TLS to ensure that all user data is secure and protected against both man-in-the-middle attacks and access from unsecure embedded browsers. Toshiba stores a per-user token on the client (desktop, laptop) to access the cloud server. This token can only be used to access print jobs for that specific user, and once printed, jobs are deleted from the cloud server.

4. ACCESS SECURITY

Access security ensures that the right people have access to the right data and functions on the print device.

4.1 USER AUTHENTICATION

The same user accounts you already have associated with Google Workspace™ or Microsoft 365® will be used for e-BRIDGE® Global Print, and the password policy you have in place with your Google Workspace™ or Microsoft 365® account will be used once your users register with e-BRIDGE® Global Print.

As both a security measure and a usability benefit, you can specify up to five private company domains to be used for auto registration. Users with an email address that uses a specified company domain will be registered with e-BRIDGE® Global Print automatically.

4.2 AUTHENTICATION METHODS

Toshiba gives you the ability to choose which authentication method works best for the customer. You can choose PIN or badge authentication. For added security, PINs are auto-generated, so no two users share the same one.

4.3 USER SECURITY

e-BRIDGE® Global Print minimizes the amount of sensitive data stored on Toshiba servers, such as security tokens, obtained from authentication providers. When Toshiba must store confidential information, it is always encrypted, and, when possible, only the salted hash is stored (not the actual data).

5. DOCUMENT SECURITY

Toshiba ensures your documents are secure as they pass through our applications, cloud server, and MFP. Toshiba takes every precaution possible to safeguard print jobs stored in the global print queue while they wait to be released at an MFP, and documents are deleted from the queue afterwards, with all documents automatically deleted after four days whether they were released or not. Users' print jobs are backed-up and encrypted in transit. Toshiba uses Amazon S3™ architecture to ensure that documents are available with the highest uptime and protection available.

Additionally, all data and documents are programmatically separated across individual customers. Print job data is also separated from the application data, so that application users may not eavesdrop on customer print jobs.

6. CLOUD SECURITY

e-BRIDGE Global Print

ALL data between ALL parts of the system is encrypted and transmitted using HTTPS protocol.

6.1 CLOUD INFRASTRUCTURE

All cloud components and services communicate with devices over a secure channel using HTTPS (TLS 1.2). Because Toshiba uses highly available cloud services, you never need to worry about a local database outage, server updates, or hardware resources.

6.2 ROLE-BASED ACCESS CONTROL

Toshiba employs role-based access control to ensure that no one user can access another user's content. Each role has a strict hierarchical scoping to ensure a user account is only seen by its company admin, and that a company account is only seen by its reseller and distributor. Toshiba understands our customers work closely with their reseller, so the data shared between them is kept private; outside resellers and software providers will never be able to see customer account information, and your dealer will never be able to see individual user data.

6.3 GOVERNANCE

Toshiba uses Microsoft® Azure® and Amazon Web Services™ (AWS) to bring you a robust, immediately scalable, and secure cloud print ecosystem. For more information on the compliance and regulatory frameworks available to Toshiba via our hosting partners, see the links below. While these certifications are not specific to their application, things like SOC 2 and ISO 20000-1 are provided by the infrastructure on which their application resides.

Azure Compliance Documentation: **https://docs.microsoft.com/en-us/azure/compliance/**
AWS Services in Scope by Compliance Program: **https://aws.amazon.com/compliance/services-in-scope/**

7. COMMON SECURITY THREATS & RESPONSES

7.1 ACCESSING PRINTED DOCUMENTS

One of the easiest ways of keeping a physical print job out of the wrong hands is to use secure print release. This is the main method of printing with e-BRIDGE® Global Print. Users submit print jobs from their computer, and then release them from the MFP. Print jobs are only released when a user has logged into the MFP, so there's no mad dash across the office to get a sensitive printout before someone else grabs it off the tray.

7.2 UNAUTHORIZED DEVICE ACCESS

For added security, e-BRIDGE® Global Print provides a way for users to revoke a device's access should the device be lost or stolen. For example, a user can simply log into the e-BRIDGE® Global Print web portal and revoke the client device (like desktop) token associated with the lost device. Once revoked, the device can no longer be used to submit print jobs or access any data until the user re-registers the device.

7.3 DATA INTERCEPTION

Client-initiated requests prevent a hacker from listening to network traffic, intercepting network data, and accessing user credentials. When the MFP requests a print job, the job is downloaded within the time-based user session. ALL data between ALL parts of the system is encrypted and transmitted using HTTPS protocol.

8. CONFIGURATION & BEST PRACTICES

8.1 USER COMMUNICATION

Toshiba recommends that your users get comfortable with their client apps and MFP experience. As an administrator, you will receive a welcome email from e-BRIDGE® Global Print when your organization is setup. To onboard users, we suggest using a Google Workspace™ or Microsoft 365® deployment tool or sending an email to your users with instructions for getting started by doing the following:

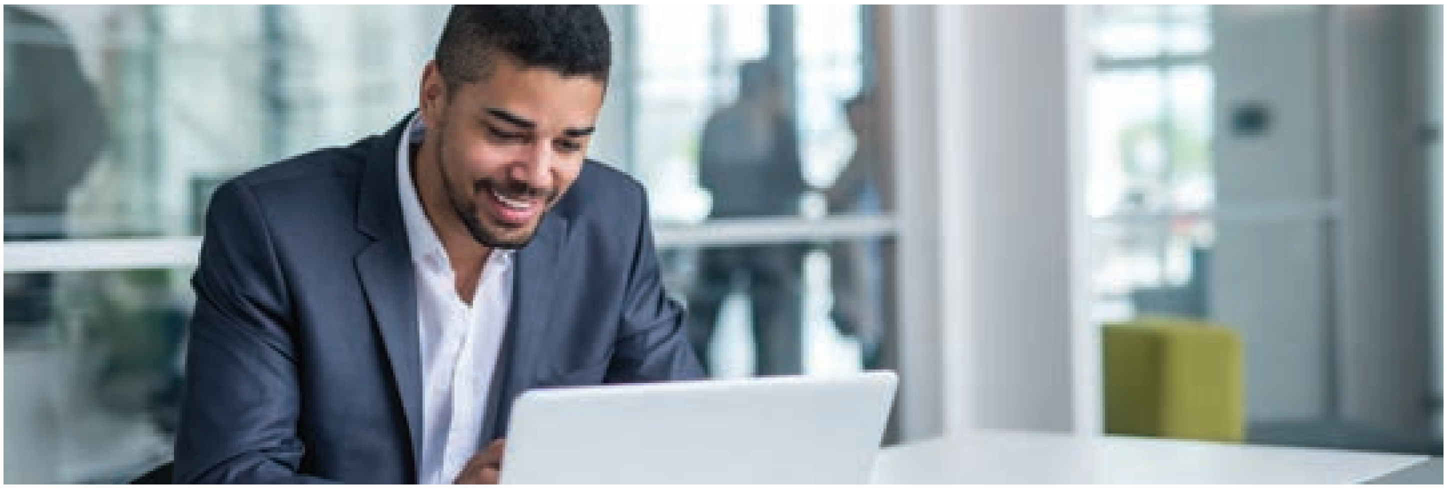
- Install the e-BRIDGE® Global Print plugins or Chrome extensions, so users can print from any application to the global print queue.
- Access the e-BRIDGE® Global Print web portal, so they can obtain their PIN code or card registration to log into the MFP.

8.2 SECURE PRINT RELEASE

In compliance-heavy industries, such as Education, Finance, and Healthcare, the organization must take necessary steps to safeguard PII (Personally Identifiable Information) data. This includes any sensitive data in paper documents within print and document environments. Toshiba's e-BRIDGE® Global Print solution ensures that documents are released to the correct authenticated user from the MFP to reduce the likelihood of documents falling into the wrong hands. Since the printing experience with e-BRIDGE® Global Print is so simple and easy, Toshiba recommends you adopt this workflow to increase security and to reduce waste.

8.3 CONTACT

Toshiba is constantly working to test and secure our service. If you have any specific questions that aren't covered here, or if you believe you've uncovered a security concern with the product, please contact Toshiba at **security@tabs.toshiba.com**



TOSHIBA

business.toshiba.com

Inv. Code: 22409 Toshiba's e-BRIDGE® Global Print & Security White Paper 5/22