SAFEQ Managed™

SECURE PRINT MANAGEMENT IN THE CLOUD

At Y Soft, keeping documents and user data secure is not a new challenge. As the Cloud has matured to a delivery system for business applications, we have addressed the security implications of moving to Cloud and Edge Computing. SAFEQ Managed offers robust print management features and print infrastructure as a reserved cloud subscription.

SAFEQ Managed uses a secure Edge device which addresses the data privacy and residency risks without requiring you to deploy or manage any costly and risky client software. On-premises applications running on end user devices and/or servers increase your maintenance costs and increases your potential security attack surface. The YSoft SAFEQ Managed approach eliminates maintenance costs, and without client software, the security attack surface is reduced.

DESIGNED FOR ZERO TRUST SECURITY

Your print environment is only as secure as its weakest link. Security starts on end user devices and ends in the Cloud and on (multifunction devices) MFDs. SAFEQ Managed has been designed for zero trust environment, without any implicit trust among end user devices, the Edge device, the Cloud and MFDs. All communication is secured using industry standards for data in transit (TLS 1.2/1.3) and data at rest.

EFFORTLESS COMMUNICATION

Industry standard Internet security communication protocols are used for service communication and data security. These include:

- HTTPS with mTLS (HTTP over TLS 1.2/1.3 with mutual-TLS authentication).
- IPPS (IPP over HTTPS).
- MQTT and MQTT over Web Sockets.

Mutual authentication is handled via internal PKI infrastructure which is part of the service (with the option to use customer provided PKI) or OpenID Connect/ OAUTH2.x-based authentication and authorization (full OIDC compatibility is work in progress).

DATA COMPLIANCE

Print jobs processed may contain sensitive and personally identifiable information. The SAFEQ Managed service offers features for keeping business data secure, including strong user access control, GDPR-compliance, and local data protection laws. SAFEQ Managed is offered on Microsoft Azure, the cloud platform with the broadest data protection law compliance in the world.

TRUE SECURE EDGE

Our Edge devices are designed with hardware root of trust. This means we incorporate not only appropriate software security measures, but security is built into the hardware design, manufacturing, and logistics. Security and trust between the Cloud and every single Edge device is established during the manufacturing process and backed by hardware security modules thanks to our integrated engineering and manufacturing capabilities. Attackers cannot tamper with the devices before they arrive to your business, which is not the case for off-the-shelf and 3rd party hardware. True, secure Edge is so much more than an on-prem server disguised as an installable client app or a small box.

PREVENTING SECURITY “MISH-MESH”

The ugly truth of complex, ad-hoc communication infrastructures, such as peer to peer, overlay or mesh networks, is that you need to maintain a lot of node-to-node visibility, which means firewall rules and exposed network ports and less opportunity for security boundaries and network (micro-)segmentation and quarantining. Like fire doors in a building or watertight doors in a ship, boundaries and segments are important tools used to prevent security breaches from spreading.

These boundary and segmentation tools are used by businesses large and small, often automatically. Today, even basic Wi-Fi routers provide advanced features, such as stateful packet inspection and VLAN tagging for segmentation and quarantining of connected devices. Ransomware and other security concerns no longer differentiate businesses based on their size, why should you? We let your security measures do their job without standing in their way.

OUR COMMITMENT TO SECURITY AND PRIVACY

It is our business to help your business communicate effectively, digitally and in print. It is our commitment to keep your business assets and communications highly available to your customers, and highly secure from theft or harm through technical innovation and human integrity.

Y Soft ensures that its internal security information practices, policies and procedures are designed to meet with the ISO 27001:2013 standard, recognized globally as the standard and that which many countries base their own national guidelines. Additionally, our products and services leverage existing standards such as end-to-end encryption, and oauth2/openID connect standards. Learn more about Data Protection / GDPR.