YSOFT SAFEQ®

SECURING THE ENTERPRISE WORKFLOW ENVIRONMENT

INTRODUCTION

Data is everywhere, and daily we are creating more than 2.5 quintillion bytes[1] of it. Data protection tools are developing quickly, but sophisticated hackers are also advancing and evolving. The rapidly growing network of connected devices and Internet of Things (IoT) devices, combined with big data, has created a data explosion that is fueling the drive toward data becoming the new currency.

While data breaches are often the topic of news stories, an organization's enterprise workflow infrastructure must also be considered for the security of private information. In the European Union, the General Data Protection Regulation (GDPR) is a sweeping mandatory legislation relating to the use and protection of individuals' data. It comes with a hefty penalty for certain breaches, in some cases even up to €20m or 4% of a business' global turnover, whichever is greater. These regulations also apply to breaches made within a company's enterprise workflow infrastructure.

This paper looks at the key security considerations for protecting data within your print, copy and scan workflow environment. It will also take a closer look at YSoft SafeQ 6, which has been specifically designed to support security measures and increase the protection of data as part of a comprehensive and secure enterprise workflow solution.

[1] IBM, Ten Key Marketing Trends

For more information about YSoft SafeQ and GDPR, please read GDPR Compliance Guide for YSoft SafeQ 6

ENTERPRISE WORKFLOW SOLUTIONS

ENTERPRISE WORKFLOW SECURITY – THE MFD PLAYS AN INTEGRAL ROLE

According to Quocirca, in 2013, nearly 63% of organizations experienced at least one security breach through printing. However, despite this, a 2015 Ponemon Institute study[2] showed that 56% of organizations exclude printers and multifunctional devices (MFDs) from their security strategies, making it a weak link within the IT infrastructure. The MFD has become an integral piece of office equipment, providing increased productivity and convenience for a huge number of organizations. However, with nearly all MFDs networked over an Internet Protocol (IP) with advanced connectivity and accessibility, the potential security risk also increases. An example of how advanced connectivity and accessibility can pose security risks is an MFD that supports auto-discovery protocols such as Web Services Dynamic Discovery (WS-Discovery) or Universal Plug and Play (UPnP) and advertizes the MFD's existance as an open point of entry to the network. Without proper protection, the MFD can enable unauthorized access to the network risking both corporate and customer data. Achieving a secure enterprise workflow infrastructure is a critical concern for all organizations in order to close the security gap.

[2] Ponemon Institute, "Annual Global IT Security Benchmark Tracking Study", March 2015

ENTERPRISE WORKFLOW SOLUTIONS AND THE MFD – A TIGHT CONNECTION

Since enterprise workflow solutions, including YSoft SafeQ, are typically embedded in MFD's and communicate with third-party systems, the security of the entire system must be considered. Therefore, it is important for close collaboration between an enterprise solution provider, the MFD service provider and an organization's IT department.

There are six key security areas in the enterprise workflow infrastructure/MFD connection, let's take a closer look at each of these.

1. DEVICE AND NETWORK ACCESS

Unauthorized or open access to an MFD creates the potential for a security breach within an organization. Using the YSoft SafeQ Authentication module removes the risk of unauthorized access because the MFD will remain locked until an employee's identity has successfully been verified. User authentication can be verified by use of ID cards, PIN codes, login passwords, or a combination of different identification methods matched against a corporate directory outside of the YSoft SafeQ system.

This authentication process eliminates printed documents left in the print tray since print jobs are not processed unless the user has correctly authenticated at the MFD. It is important to note that where user authentication by password is used, passwords are encrypted before sending them for verification on the server, and only salted password hashes are stored, or the authentication is delegated to an Active Directory server. No password data is stored on the MFD and Active Directory Domain credentials are never stored neither in the MFD or in YSoft SafeQ.

Administrators can also mitigate risk to their networks through the MFD by monitoring and analysing incoming traffic. Print activity to the MFD need only come from YSoft SafeQ; all other traffic can be blocked which limits attack vectors attacking the MFD from other networks.

The YSoft SafeQ mobile application (Mobile Terminal) is another way to authenticate at an MFD. Users can identify a network printer by scanning its QR code, NFC or beacon. The mobile application uses a one-time activation link, which is sent to a user's email when connecting to YSoft SafeQ for the first time.

After successful activation, a mobile terminal token is generated for this specific user and, thereafter, is used for the user's authentication. This procedure protects the domain credentials from an attacker replacing the QR code / NFC / beacon, since it does not require these to be entered in the application. Communication between the mobile terminal and the YSoft SafeQ server is encrypted.

2. SECURE PULL-PRINTING

The ability to send a print job and print it from any MFD in your organization – within a single building or across the world – improves communication and productivity. Obviously, this increases the volume of data being transferred across your network. It is vital, therefore, that your enterprise workflow solution protects your data while also helping your employees carry out their jobs better. Pull-printing also helps decrease the possibility of confidential documents being left in the print tray. The YSoft SafeQ pull-print feature, called Print Roaming®, enables the user to print from any convenient MFD or networked printer anywhere within the print infrastructure, but only when the authorized recipient has authenticated at the MFD.

Within YSoft SafeQ, Print Roaming can be structured as either Near Roaming, Far Roaming or both, depending on the organization's infrastructure:

Near Roaming: When print jobs are sent to YSoft SafeQ on a local server, print job data flows from the user's workstation directly to YSoft SafeQ through encrypted communications.

Far Roaming: When a print job is sent from a user's workstation to YSoft SafeQ on a local server but printed from an MFD in a remote location, communication may go through a server at the remote location. In this case, print job data flows between the local and remote servers through encrypted communications.

3. SECURE MOBILE PRINTING

Workforces are increasingly mobile, and the tools and devices used are rapidly changing and not always secure. The demand to print from any device and bring your own device (BYOD) initiatives has created both flexibility and risk. Employees can now easily connect their personal smartphones, tablets and laptops to the print network. While this is convenient and efficient for organizations, this creates new entry points for potential risks.

The secure Mobile Print module within YSoft SafeQ enables employees and guests to print from any mobile device securely with confidence – supporting the flexibility of BYOD without needing complicated support and IT implementation. Combined with the Authentication module, the Mobile Print module enables organizations to support their mobile workforce printing needs fully while maintaining document security, restricted access and cost savings.

The Mobile Print module provides two options for sending print data to the YSoft SafeQ server. A user can either connect to a web interface and, after identity verification, upload the document, or use email integration, where an email attachment is pulled from the email server via POP3 or IMAP protocol. Both options are possible with SSL/TLS encryption.

Another way to send job data to the YSoft SafeQ server is through Y Soft's Mobile Integration Gateway component, which allows sending jobs from iOS or Android devices via IPPSSL protocol.

4. USAGE REPORTING AND TRACKING

In any organization, employees will inevitably have access to confidential information. To keep on top of potential security risks, organizations need to be able to identify and monitor who is using the MFD, what is being copied, scanned and printed, when and where. Gathering such information from metadata into a report is a useful indicator to highlight potential misuse of the MFD, such as

printing or scanning confidential documents that are outside of an employee's remit. The YSoft SafeQ Reporting module provides administrators with terminal access reports, informing them of the operations performed on any of the MFDs, enabling administrators to ensure the environment is secure and users are adhering to internal usage policies.

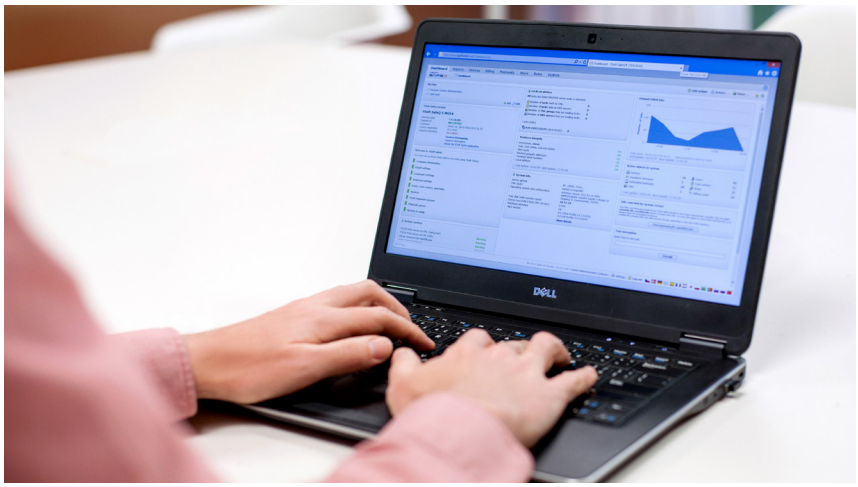
5. MFD HARD DRIVE SECURITY

Organizations should have policies in place with their MFD service provider for the protection of MFD hard drives during daily operation, during servicing or when they are decommissioned. With YSoft SafeQ, no print or copy data is permanently stored on the MFD's hard drive. Traditional scan to email or use of scan workflows may temporarily store data needed to create digital scans but it is then immediately erased after the workflow is completed.

6. DATA ENCRYPTION

Any device that sends or receives data poses a potential security threat. To counter this, data needs to be encrypted, digitally signed and the communicating parties authenticated to protect the confidentiality of transferred information and to ensure the strong integrity of the communication. Customers who have PKI (public key infrastructure) in place may want to use it with YSoft SafeQ to ensure mutual authentication of MFDs and SafeQ servers.

The following section provides additional detail on the communications within YSoft SafeQ and between YSoft SafeQ and other systems.



YSOFT SAFEQ, SECURE BY DESIGN

As mentioned earlier in this paper, we are seeing an explosion of data as well as increasingly sophisticated ways for unauthorized access. Securing data across your network of devices is increasingly complex, but essential to meet the needs of organizations looking for productivity enhancing workflows and capabilities. With data passing between devices, servers, systems, and the MFD, multiple data transfers are taking place over the communication pathways, and YSoft SafeQ secures this data through encrypted communications. Communication pathways use open, standardized encryption implementations (not proprietary) unless an open and standardized implementation is not available. Even in the latter case, open, standardized implmentations of the security algorithms are still used.

There are eight major encrypted communication pathways available in YSoft SafeQ, Figure 1.

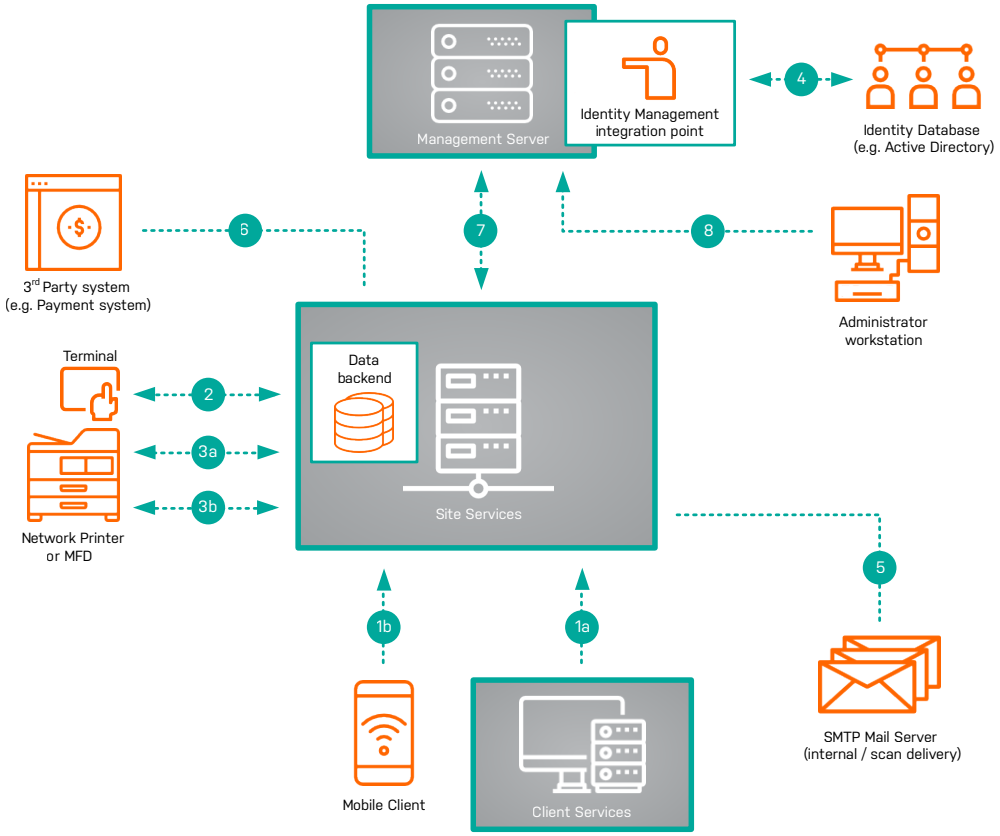


Figure 1.
YSoft SafeQ communication paths

1. Printing – communication from YSoft SafeQ when
   a. A print job is sent from the client's workstation
   b. A job is sent from a mobile client

2. MFD (multifunctional device) authentication — communication from the MFD's terminal/reader to YSoft SafeQ for the purposes of verifying a user's login credentials

3. Communication from YSoft SafeQ to the networked MFD:
   a. A pull-print release of a print job
   b. Authentication verification, authorization, and accounting

4. Integration with the identity management database or identity/authentication provider

5. Connection from YSoft SafeQ to an SMTP mail server or shared network folder for data delivery of digital scans

6. Integration with third-party applications or systems, for example, for delivery of digital scans to a cloud-based document repository

7. Inter-server communication. Depending on an organization's redundancy and fail-over requirements, multiple Site Services tiers or Management Server tiers can be in multiple remote locations. Inter-communications between the tiers at the various locations are required for print release job processing and the transfer of print job metadata for reporting purposes

8. Administrator access to the YSoft SafeQ Management interface

SECURING DATA IN ALL STATES

Print, copy or scan data has three potential states – in use, in transit and at rest.

- **Data in use –** active data being manipulated by the application and stored in non-persistent memory only. A document to print while being parsed by an MFD is an example of data in use.

- **Data in transit or motion –** data being transferred or moved outside of a server from one location to another. An email in the process of being sent from an automated scan workflow, or from a scan to email function are both examples of data in motion.

- **Data at rest –** inactive data that is stored persistently. An example is print job meta data used for reporting purposes stored in a database. Another example is in a multitenant environment, where data of different tenants are stored in isolation in a production database and those who have access to reporting data do not have access to the production database (and vice versa).

Ensuring up-to-date cryptographic protocols are correctly deployed is a vital role in protecting your data. It should be noted that security threats are an ongoing concern for the entire IT community. The Y Soft product security team continually monitors and updates cryptographic protocols and algorithms to ensure that YSoft SafeQ is current with industry security standards in addition to ongoing education to recognize potential vulnerabilities and best practices for secure coding.

In addition, the team performs threat modeling and static code analysis in accordance with Microsoft Security Development Lifecycle methodology. Both design and implementation threats are identified and apply logical countermeasures to mitigate the risk. Specific knowledge of threats ensures an organized approach to security. Proactive security measures allow data at risk to be identified and appropriately protected according to its sensitivity.

BUILT-IN ENCRYPTION

Encryption has risen to the forefront in the battle to secure data and goes hand in hand with a strong firewall. The purpose of encryption is to secure all data in each of the three data states within the entire system and all communication pathways. While encryption itself does not prevent a security breach, it is recognized as a layer of protection. If data does end up in the wrong hands, it is useless as it is encrypted. By encrypting clear data or plain text with a secure algorithm, it is ensured that only those with access to the decryption key can read that data back from the cipher text. For the user, encryption takes place transparently in the background with no input required.

There are two main types of data encryption – symmetric and asymmetric, in practice often combined and being referred to as hybrid encryption. Symmetric encryption uses the same secret key for both encryption and decryption of data. Asymmetric encryption uses two different keys – one private key, which is kept secret and used for signature and decryption, and one public key which is shared freely and used for encryption and signature verification.

Cipher suites and key lengths are chosen and regularly updated to address known vulnerabilities and attacks. The fast-pace of change in this area means that algorithms or just their implementation can become outdated, and this can leave data unprotected if not managed correctly. Keeping on top of the recent developments is possible by following advice from some key organizations such as NIST, Mitre or Apache Foundation.

Each of the three previously mentioned data states presents a different challenge in terms of security, as any unprotected data, regardless of the state, leaves enterprises in danger of an attack.

- **Data in use –** Encryption is not a solution to properly protect data in use as data must be available for processing. There are however, good practices to protect data in use. In YSoft SafeQ, this includes restricting user access, not unnecessarily storing sensitive data, and features such as Authentication and Reporting to support data security in this state.

- **Data at rest –** This information is initially protected by setting the access rights correctly and utilizing firewalls and anti-virus programs, but hard drive encryption can improve the security further. Enterprises can utilize Microsoft Encryption File System (EFS) to encrypt data at rest prior to storage or encrypt the storage drive itself; encryption at the operating system level can provide a secure enclave for storing encryption keys. EFS transparently encrypts files when being stored using the AES algorithm (the current standard for symmetric encryption).

- **Data in transit/motion –** Communication links with sensitive data are protected using standard TLS (Transport Layer Security) protocol and multiple configurable cipher suites, ordered by security level to achieve maximum protection and ability to support legacy devices at the same time. TLS not only ensures confidentiality and integrity, but also prevents replaying previously captured traffic. This also allows for IT to easily enhance protection by changing the cipher suite's configuration values should new security recommendations be made or if the organization's security policy changes, for example, if use of SHA-1 (Secure Hash Algorithm 1) is now discouraged.

PEACE OF MIND AND SEAMLESS USER EXPERIENCE

Protecting your organization's data is not a tick-box exercise. Having data protection ingrained within the culture of your company will enforce its importance. The challenge of protecting data and preventing security breaches is a necessity considering the changing landscape with the Internet of Things, BYOD, data explosion, malware and external devices.

The extreme consequences of a security breach put security and data protection high up on the list of business challenges. The YSoft SafeQ solution reduces security risks by combining print security, document security and device access control. No demands are placed on users, other than simple authentication at the MFD. The seamless backend process also means that users' experience in terms of speed of action are unaltered, like that of using secure online banking.

FREQUENTLY ASKED QUESTIONS

Where is data held in the processing of print jobs, scans and copies?

- **Print jobs –** When using Print Roaming, data is held in the Client Services and Management Server layers of YSoft SafeQ. If using Client Based Print Roaming, the print job is held at the client workstation and only print job metadata is communicated to the Client Services through to the Management Server layer of YSoft SafeQ.

- **Scan to email, scan to file system and Automated Scan Workflows –** Data is temporarily held on the MFD hard drive and erased when the job is completed. If using scan to email, the email from the MFD to the client workstation can be delivered through encrypted communication. For even better security with end-to-end encryption, encrypted PDFs are supported. With Automated Scan Workflows, the digital scan is delivered to a predefined location through encrypted communication.

- **Copies –** Temporarily held on the MFD hard drive and erased when the job is completed.

Can you provide proof of data destruction on the MFD's hard drive?

Any data temporarily stored during scanning is immediately erased. The MFD service provider and the organization should have processes in place for securing the MFD hard drive during use, during servicing and in the event of decommissioning which includes destroying data on the hard drive. It should be noted, however, that the MFD's hard drive is outside of YSoft SafeQ's area of responsibility.

Can you provide compliancy with payment gateway systems?

YSoft SafeQ does not communicate with any payment gateway systems. In the case of the Credit and Billing module of YSoft SafeQ or the Payment Machine, YSoft SafeQ is only notified by the financial institution that payment and the amount has been received.

Can you securely integrate your reporting data into our web portal?

Web portals are typically secured via signed certificates, which are supported by YSoft SafeQ. YSoft SafeQ reporting data can be integrated with a web portal to show print, copy and scan data.

How can data be encrypted throughout its lifecycle?

With YSoft SafeQ, when using the spooling client, IPP over TLS protocol for encryption, authentication, and with integrity of the data transferred to the MFD, the data leaves the workstation only when the job is released. It is also possible for server-based Print Roaming to send the data from the workstation to the YSoft SafeQ server via an HTTPS channel. This is also the case for print data transfer between servers when Far Roaming is active. While at rest on the server, standard Microsoft EFS can be used for print data protection.

Can my organization view documents that have been printed by employees?

When using Print Roaming, an administrator with access to the file system can access the print streams for all jobs held at the YSoft SafeQ Management layer (jobs waiting to be printed, printed or marked as favorites). However, YSoft SafeQ can be configured to automatically delete print jobs after printing. If YSoft

SafeQ is running under a named service account and using Microsoft EFS, the administrator will have to know the service account's password to see the job. Any activity in the named service account is captured in the Windows audit logs. Additionally, Microsoft EFS enables segregation of duties – such as having enterprise administrators who can administer servers and applications without having access to print job data and enterprise administrators who have security clearance to access print job data.

When using Client Based Print Roaming, only the print job's metadata is captured. To see the actual job, access to the workstation would be required.

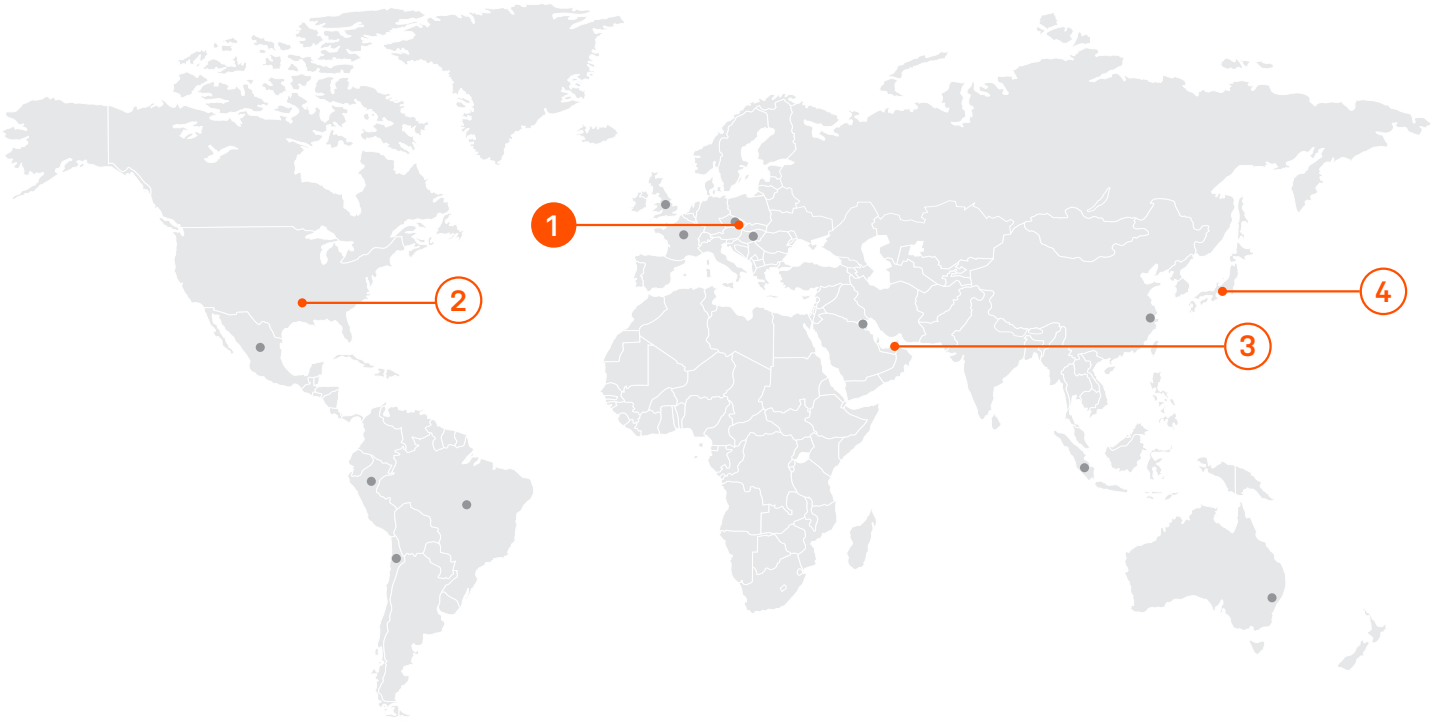
Can users see what documents have been printed by others?
No.

How does YSoft SafeQ help organizations meet GDPR regulations?
Please review the detailed information in the GDPR Compliance Guide for YSoft SafeQ 6.

In short, YSoft SafeQ enables administrators to address an individual's rights pertaining to the data the organization has (the Right to Access), to correct the data (the Right to Rectification), to prevent the processing of the data (the Right to Restrict Processing), and to delete the data (the Right to Erasure).

Can a person's personal identifying data be removed from the YSoft SafeQ system but remain anonymous for reporting purposes?
Yes. A delete query will remove a user's data from the YSoft SafeQ system without removing printing details for reporting purposes. The report will just show a blank user.

LOCATIONS



Company Headquarters	Regional Headquarters
1 Y Soft Corporation, a.s. Technology Park, Technická 2948/13 616 00 Brno Czech Republic	2 North and Latin America Y Soft North America, Inc. 1452 Hughes Rd, Suite 110 Grapevine, TX 76051 3 Middle East Y Soft Middle East Offices 107/108, Makateb 4 IMPZ, Dubai, UAE 4 Asia Pacific Y Soft Japan, Ltd. KFM Building, 10th Floor 658-0032 Koyocho Higashinada Kobe, Hyogo Japan

For a complete list of more than sixteen countries and locations, please visit our website.

YSOFT
BUILD SMART BUSINESS

SFQ-SEC-WP-6-2018