SAFETICA POST-IMPLEMENTATION RECOMMENDATIONS

Safetica Technologies s.r.o.

safetica®

CONTENT

USE OF SAFETICA PRODUCTS

Introduction

Thank you for choosing Safetica to secure your company's data.

Our goal is to reduce the risk of data leakage and, through our products, give businesses the ability to detect security issues, educate employees, and prevent the misuse of sensitive corporate data.

When developing our products, we realize that they can be used in many ways – just like weapons – for personal protection as well as for attacking someone else. That is why we are doing everything we can to minimize the possibility of abuse.

Safetica Data Protection Solutions collects a wide range of information in order to identify risks and incidents within an organization, and therefore it also collects personal information about employees or external partners. Therefore, protecting both data and privacy is an important part of our product development. We develop our functionalities in such a way that we minimize any invasion of employee personal space while at the same time we are able to communicate how and why data is collected in the most transparent way. Developing Safetica's security is one of our top priorities. For more information, see our Secure Software Development Statement.

Use of Safetica Products

Safetica products are developed to protect intellectual property and to reduce our clients' risk of corporate data leaks. They are not intended for any other purpose.

Specific product settings significantly affect how much information the product collects and processes. For privacy, we try to limit product presets to the minimum necessary levels for the purposes described above. However, these limits may vary according to national legislation. Therefore, we strongly recommend that you familiarize yourself with your country's legislative requirements before configuring the product.

Regardless of country legislation, we strongly recommend that you:

- Ensure that all employees are notified of the use of Safetica in advance;
- Set the working hours during which the product will collect data;
- Prioritize restrictive (blocking) functions prior to monitoring;
- Restrict the data collection settings and keep them to the minimum;
- Transparently communicate the use of the product and its settings to employees;
- Use outputs from the product in conjunction with other data sources and check the information before drawing any conclusions.

Safetica products are not designed to collect sensitive data (such as passwords, content of communications, political beliefs, health, etc.). However, due to the complexity of information system operations, it is not possible to exclude the random collection of such data. In these cases, it is strongly recommended to immediately delete any such data and not to process it any further.

It is also important to acknowledge that Safetica software can only control how data is handled in our

consoles and preconfigured views. If you export, copy, or send data from a system (for example, in the form of backups, reports, alerts, etc.), we recommend that you protect it in compliance with the legal requirements. A good example of a legal requirement arises when the retention period expires. When data is deleted from the system, corresponding records that have been exported to other system locations must also be deleted.

While we do our best to broaden Safetica capabilities, it's important to remember that no security is 100 percent. Although it is very important, Safetica is just one of the components of overall security. In the Recommendations Document, you'll find the settings and steps we think are important to ensure the highest level of security.

GLOSSARY OF TERMS

For more information about implementing security measures through Safetica, and on how to prevent security threats, please visit our S.

General Terms

Confidentiality, Integrity & Availability

Applying the concept of the CIA triad ensures that data is always available only to authorized persons, while maintaining the reliability of the data. Therefore, unauthorized persons do not have access to sensitive data and are unable to make changes.

Authentication, Authorization & Accounting

Applying the concept of the AAA triad ensures unambiguous user authentication based on individual access to data. Once an identity is authenticated, access to the server and control access permissions are granted. All these steps must be recorded for later accountability.

The Principle of Least Privilege

In general, it is recommended that only information that is necessary and legitimate for the user's work be provided. This means that user accounts, applications, or processes accessed by the user should be assigned only the minimum possible rights.

Separation of Duties

The basic concept of role-sharing is that no individual should have complete control over a task. According to this principle, no user (including administrators) should have direct access to the 'safetica' system account. As this account has full access to all product features and records, a user with system account rights has unlimited access to the entire system, which can greatly compromise system security and increase the risk of user error.

Securing Access to the Computer Network

IEEE 802.1X provides secure access to the computer network. If a new device is connected to the network, either via a network cable or wireless access, authentication is required using the IEEE 802.1X protocol. The connection point to which the device is connected blocks client data traffic until it is authenticated.

Basic Threats

Malware

Malware is a general designation for malicious code (a program) that is intended to damage or invade a computer system. There are currently countless types of malware programs that need to be effectively protected against. Malware is most commonly spread over the Internet or via email.

Viruses are a subset of malware. The purpose of a virus is to penetrate and infect your computer. There are countless types of viruses that serve to control your computer, steal your data, use your computer for DDoS attacks, and more. A virus can spread to an infected computer without the user's knowledge.

Ransomware is a type of malware program that blocks a computer system or encrypts data, and then demands that a ransom be paid. It is currently the most widespread and dangerous type of malicious program. Because defense against ransomware is very difficult, we recommend that you always have an updated operating system and run an antivirus program.

DoS (Denial-of-Service)

DoS is a type of cyber-terrorist attack on Internet services or sites. The purpose of these attacks is to disable service to other users by overwhelming the service or causing an error. Choosing appropriate hardware, combined with a decentralized security system, can help defend against these attacks.

DDoS is a DoS attack subtype, a distributed one. This type of attack uses a large number of scattered computers that are infected with a malicious code. These stations subsequently overwhelm the target service request, rendering the service unavailable.

Network Communication Security

We recommend using a firewall to ensure the security of network communications. A firewall is a hardware device that can filter inbound and outbound communications. All corporate communications should always go through the firewall. Firewall filtering works on the principle of network traffic monitoring, preventing suspected, accidental, and banned communications.

Communication Encryption

Any communication with the surrounding environment should be encrypted. If communication is not encrypted, it is easy for an attacker to read. We recommend encrypting email communications via electronic certificates and signatures and by using the TSL protocol.

LEGISLATIVE COMPLIANCE

This chapter describes Safetica's ability to identify compliance with laws, to store data, and to respect user privacy. Safetica is deployed to increase security and secure the digital footprint, in accordance with legislation or security guidelines.

Compliance with the Law

Safetica can be used to comply with a variety of different laws. In some cases, you may be legally required to implement some measures before installing the product. Your company can use Safetica to achieve the necessary level of compatibility with laws and standards such as ISO / IEC 27001, HIPAA and others.

GDPR

GDPR (General Data Protection Regulation) is a binding European regulation on the protection of personal data. For more information on how Safetica can assist you in complying with GDPR, please see the documents on our website.

Security Directives

Any company whose employees use information technology should always have a security directive in place that defines the rights and obligations for managing company resources. Safetica can be used to ensure that the rules of such a directive are followed.

User Privacy

Every user has the right to privacy, and every employer should remember this fact. Some Safetica features may infringe on this privacy and should only be used in extreme cases. Users should be informed in the event of such security cases.

- General records in the Auditor module should only be used to take necessary action or resolve situations related to the work, data leakage or user activity. The details regarding sites visited (or apps accessed) should not be used in any other way.
- We recommend turning off the Activity Monitor function outside of working hours.

THE SECURITY ENVIRONMENT

Security is a combination of physical, organizational, digital, personal and legal controls. Threats not only come from the digital world, but there are also environmental errors, problems caused by user inattention (human error factor), etc., and thus it is advisable for everyone to pre-emptively prepare for such threats.

Security Threats and How to Prevent Them

In today's interconnected world, there are an increasing number of cyber-attacks, not only against global services, but also targeted attacks on companies without global reach.

There are countless types of security threats. The most basic ones can be found in the glossary at the beginning of this document. Below are some simple recommendations for how to prevent such threats.

Regular Operating System Updates

For both compatibility and security reasons, we recommend that you always maintain a current operating system, both at the endpoints and on the production server on which the product is running. Third party software also needs to be updated to ensure that Safetica runs properly. For more information, please visit our Knowledge Base.

Windows Firewall

When using the Windows Firewall, both automatic and manual installation of Safetica automatically enable the necessary communication ports. For more information on the network ports needed for proper Safetica component communication, please visit our Knowledge Base.

Security Training for Users

We recommend that you conduct security trainings for your employees, users and any external parties with access to the environment and/or data. Security training gives users a complete overview of security threats, how to behave on the Internet, and how to handle corporate devices, both computers and mobile phones. By increasing security awareness among employees, security protection moves to a higher level and helps to prevent security incidents.

Penetration Tests

Not all security threats come from within your company. We recommend regular penetration tests to protect against outside dangers. Penetration tests focus on detecting weaknesses in your security systems that could potentially be exploited by an attacker.

Application Trust Management

The trust level of the application determines the permissions that are granted access to the ASP.NET security policy. An application that has full credentials can access all types of resources on the server and perform privileged operations. These applications are only affected by the security settings of the operating system.

Applications running on the same server as Safetica should not be set as fully trustworthy due to possible interference with Safetica processes and communications.

Administrative Recommendations

Some Safetica features require regular maintenance. The basic actions to be taken are described below.

- It is strongly advised not to have multiple DLP solutions in one environment.
- All stations should be regularly updated, especially the operating system, the antivirus system and the appropriate components (.Net Framework, IIS server, SQL server, etc.).
- We recommend managing access rights (based on unambiguous access accounts) to local, network, and cloud folders so that confidentiality is maintained and unauthorized access is prohibited.

When installing Safetica on additional computers, servers, or whole organizational units, it is important to monitor their performance, database usage, and interactions with other software.

Working with Sensitive Data

Sensitive data refers to both company data that is protected by Safetica, as well as Safetica records that contain employee personal information.

- Sensitive data should never be available to unauthorized users, or to people who do not necessarily need the data to perform their work.
- Our recommendation is to back up sensitive data on a server where unauthorized user access is restricted and where there is limited physical access.
- If sensitive data is stored and not actively processed, the disks, external media, and other locations where the data is located should be encrypted. We also recommend periodically backing up data in these locations.
- Be aware that sensitive data is stored not only electronically. Also make sure to protect your printed documents, screen-visible data, and physical access to servers, end stations, and other hardware used to transfer, store, or work with data.
- Particular attention should be paid to accessing data such as passwords, encryption keys, and so on.

SAFETICA CONFIGURATION AND SECURITY ARCHITECTURE

Safetica Updates

From a security point of view, we do not recommend using versions of Safetica older than the most recently released version. Download the latest version here.

Recommendations for updating Safetica:

- Download and update the new version of Safetica on the server. You can find current and detailed steps in our Knowledge Base.

- Test the Safetica Management Service after updating.
- Connect Safetica Management Console to Safetica Management Service and ensure that it is working properly.
- Test the display and accuracy of graphs and records in the Safetica Management Console.
- If there is a problem, check the "lastrun" file (*C:\ProgramData\Safetica Management Service\Logs\Service_lastrun.txt*). If the file contains error messages, see upload.safetica.com for a detailed analysis of the cause.
- Distribute the update package to client stations.
- Test that client stations are functioning properly, including proper logging and compatibility with programs in your production environment. Test the functionality of Safetica clients, including data protection and restrictive measures.
- If you encounter any problems during testing, please follow our recommendations in the Knowledge Base.
- If testing did not show any problems, continue to upgrade the stations from the production environment. Start from the least critical parts of the organization and, if any problems occur, immediately stop the update and report issues to support@safetica.com.

Some versions of Safetica convert database data during the update. For this reason, the database server may be temporarily loaded and the Safetica database unavailable. The product functionality at the end stations is not affected in any way. We recommend updating the production server at a time when the database server is not being used by other applications.

Regular Service Inspection

We recommend that you perform regular checks of Safetica, WebSafetica service, endpoints, database status and overall status of the environment.

We recommend installing Safetica on all stations in the company. To achieve this, you can create a rule for distributing Safetica to newly installed stations. For example, we suggest using a domain controller to create a policy that will automatically install the Safetica Agent distribution package. This establishes a connection with the server and ensures that it is ready for the next installation steps.

At regular intervals, we recommend categorizing unknown webpages and applications. By categorizing, you can achieve a more precise aggregation of results by category and also increase security when using rules that can be bound to the categories.

We recommend having automatic updates turned on in Safetica. Updates also include compatibility definitions, updates of category databases and security updates.

Security Recommendations

- Change your password immediately after installing the product. The password should be compliant with password-safe phrases (a combination of uppercase and lowercase letters including digits and special characters, minimum 8 characters, such as "J0hn_th3-k1ng").
- Passwords should be set appropriately for everyone who will use the Safetica Management Console (i.e. choose account passwords as well as privileges for individual views and product features). The recommendation is to use the Principle of Least Privilege.
- We also recommend using the principle of the division of roles. When a user has access to Safetica to

view data and records, he should not have full administrative access, and administrative tasks should be addressed by an administrator, who may not have the right to view employees' records.

- Safetica processes are not active in Windows Safe Mode, so it is possible to uninstall the product without obstacle. For greater security, therefore, it is recommended to disable user access to safe mode.
- Safetica processes are not active when booting the system from external data storage. Therefore, it is advisable to disable such system booting methods for ordinary users.
- From a security point of view, it is inappropriate for regular users to have administrator privileges in the operating system.
- It is not recommended that administrators log on to end stations using their domain accounts during servicing, as there is a risk of passwords being intercepted. For service interventions, we recommend using one-time accounts for local administrators.
- Labeling data only works on the NTFS file system. If the data is copied to another type of file system or is sent in an open form such as email, the tag is lost and thus data security is compromised. The solution is to set the appropriate paths for copying protected files.

Administrative Recommendations

Some Safetica features require regular maintenance. The basic actions to be taken are described below.

- All Safetica features should be regularly reviewed and compared to the organization's current needs. We recommend implementing regular analysis of the company's needs and adjusting policies based on relevant findings.
- Special attention should be paid to DLP policies in informative and restrictive modes. Records available under the DLP protocol should be regularly reviewed and DLP policies or other actions should be optimized and initiated according to the protocol (process changes, incident management, employee discussions, etc.).
- Every change in the organization should be reflected in the product settings. Changes in organizational structure, organizational unit agenda or in IT departments should be immediately embedded in Safetica settings. We recommend implementing business processes to manage these changes.
- Notifications and service warnings sent from Safetica should be reviewed regularly. Database status, terminated processes, and error messages from the Safetica server are particularly important.
- The performance and condition of Safetica Endpoint Agent and Safetica Endpoint Client at endpoint stations should be regularly tested and monitored to confirm proper functionality in the customer environment and to avoid the emergence of security risks.

License

We recommend that you monitor the validity and number of your Safetica licenses. If licenses expire or if you exceed the number of purchased licenses, new licenses must be purchased or existing licenses renewed. When a license expires, you lose access to Safetica records. Safetica will notify customers about expiring licenses. For more information about Safetica licensing, please refer to the product documentation and help in Safetica.

MSSQL

The MSSQL database is used to store all data and records sent to Safetica clients and the Safetica server itself. When the database is full, data consistency cannot be guaranteed. Therefore, we recommend having database maintenance turned on, so that when there is a lack of space the oldest data will be deleted. Older data can be automatically archived and deleted or backed up, see below.

- To ensure that all operations run smoothly, use a supported version of MSSQL Server (MSSQL Server 2012 and higher).
- To ensure full monitoring and DLP functionality, use the full MSSQL server solution. If the full solution is not available, use MSSQL Express 2016 or later. Due to performance enhancements, the newer the version, the better.
- If you are running MSSQL Express Edition, make sure that you have Auto Database Maintenance enabled and backups set to prevent database overload. For more information on automated tasks and MSSQL visit the Knowledge Base.
- If you do not use automatic database maintenance and backups via Safetica MSSQL, we recommend setting up your own MSSQL server backup.
- Communication between MSSQL and Safetica components is encrypted.

MSSQL Encryption

MSSQL Server serves as a repository for sensitive information. This is a necessary step to protect this information. One way to increase information protection on SQL Server is through encryption. Encryption is available in MS SQL Enterprise. The encryption and decryption process takes place when reading the data, and encryption occurs automatically when stored to disk. It is completely automatic and does not require any user intervention. If the encryption key is not known, encrypted data will be illegible and unavailable in case of theft. Of course, you may use other alternative methods of securing your database data.

External Applications

Only listed Safetica compatible applications are integrated in the default Compatibility Mode. If a particular application is used (for example, an unusual design software or an information system), it is necessary to integrate this application manually to ensure that all DLP rules and restrictions work properly. Before completing the full integration of the application, it is recommended to use a test group to verify the compatibility of the Safetica application.

Backup and Archiving

- We recommend that you perform either a physical or a virtual server backup, as well as MSSQL database independent backups. We recommend backing up to a separate server, ideally one that is physically separated from production. Backups should run automatically and at predetermined intervals (day, week, etc.), without the repeated involvement of an administrator. Backups must be secured against misuse by unauthorized persons.
- We recommend automatic and regular archiving and deletion of records. This is so users who access Safetica only see up-to-date records. Archives can be reconnected to Safetica to retrieve specific information.

Safetica does not bear any responsibility for records that are archived and stored outside of Safetica and is not responsible for their accuracy.

Please contact your sales representative for further information. Or visit our website at www.safetica.com.

Prague | Czech Republic | 1. 4. 2018.