Safe Software FME

Security Whitepaper

FME Flow & FME Flow Hosted

2023 | V0.1

Table of Contents

1 Introduction

Safe Software's entire business is built on data, and we understand that it is among the most important assets of any organization. The security and privacy of your data is our highest priority. This whitepaper outlines our approach to security and compliance and describes the organizational and technical controls we use to protect your data.

Our security practices and safeguards are embedded across all our technology, programs, and processes. For over 29 years, we have worked with customers in highly regulated industries, such as governments, healthcare, and utilities – each customer willing to trust FME to deliver the power of their data to make better decisions.

In this Whitepaper, we provide an overview of how our security practices have been applied to FME Flow and FME Flow Hosted, what administrators should know about maintaining security of this product and how we can partner with you to ensure security throughout these products' lifecycle.

2 System Architecture

FME Flow, formerly FME Server, is an application that automates the flow of data between applications, as well as other manual data related tasks such as file submission, data download, sending reports, data synchronization, streaming data, and monitoring assets. Workflows can be designed in FME Form and scheduled to automatically run at any time interval, turn it into a self-serve process for others to run whenever they want, or always run in real-time.

FME Flow can be deployed on-premises or your own private cloud.

FME Flow Hosted, formerly FME Cloud, provides an effortless way to run and manage FME Flow without having to provision and look after infrastructure. This hosted solution allows you to use FME Flow without the burden of infrastructure and maintenance.

The main functionalities are:

- Launch instances of FME Flow on dedicated servers (single tenant)
- Monitor the instance and be alerted of issues or events
- Backup and rollback strategy
- Schedule windows during which the Server should run and be charged by the hour
- Control over instance CPU/memory/storage with ability to scale up or down.

The platform is software-as-a-service based and hosted on Amazon Web Services (AWS) infrastructure.

2.1 Network Security

FME Flow is provided as an on-premises solution, deployed by users in their own environment. The application provides secure settings by default where applicable, and configuration options that can be used to enhance the security of an FME Flow instance. Since users have the flexibility to customize the installation and environment FME Flow is installed in, care needs to be taken to ensure the required security controls are in place. For example, if an existing on-premise database is used, we advise users to ensure TLS 1.2 is configured at a minimum to secure the communication.

A check list is available to FME Flow administrators that provides a set of recommended configuration options. We also provide additional recommendations, in the post-installation configuration options article, to assist you in securing your FME Flow instance.

FME Flow Hosted is hosted in AWS which is a public cloud service. We acknowledge that although AWS applies the highest levels of protection to their environment, security is a shared responsibility, and AWS is ultimately a public cloud shared by many other tenants. As such, care is taken to protect data communication at all stages, including those among internal services, using **TLS 1.2** at a minimum.

We follow best practices when it comes to segmentation, separating the FME Flow and FME Flow Hosted components in AWS. Policies and Security Groups are used to separate client workloads, and limit access.

2.2 Access Control

FME Flow supports Role Based Access Control (RBAC). Access to different parts of the system can be controlled via the Security Management GUI or the REST API.

Within an organization, users are grouped into roles. FME Flow ships with five roles by default. New roles can be created for various job functions, and existing roles may be modified. Permissions to perform certain operations are assigned to specific roles.

FME Flow Hosted access control is based on a set of roles that users can have within an account. The roles permissions are defined statically and cannot be modified by users. Permissions are based on actions (read, update, delete) that can or cannot be performed against a category of resources (e.g., Instance, Snapshot, Schedule, etc.).

A member of an account has one of 3 roles (Owner, Admin, Member).

3 Application Security

At Safe Software, we believe that software should be built securely at the outset and throughout the development cycle, enabling us to add protections early and often. We engage in the following activities to ensure our products are built with security in mind.

3.1 Security Requirements

Building applications with security in mind requires a well-defined set of security requirements. At Safe Software, we have adopted the Open Worldwide Application Security Project (OWASP)'s Application Security Verification Standard (ASVS) and adopted a subset of the Level 2 controls based on what is applicable to our system. This ensures our application has the right level of security controls built-in, based on the leading industry standard.

3.2 Automated Security Testing

Static Application Security Testing (SAST) and Software Composition Analysis (SCA) tools are used to scan the **FME Flow** and **FME Flow Hosted** applications for security issues, vulnerable libraries, and supply chain security. The reported issues are triaged and addressed in accordance with the vulnerability management guidelines of our internal policies.

3.3 Threat Modeling

We believe in identifying security issues while we design our systems and understanding how potential attackers could impact our applications so we can put the required protections in place.

To that effect, our team is trained by application and cloud security experts to apply threat modeling while building our products. This includes threat modeling of the system architecture anytime changes are made to the design, as well as identifying abuse cases on all requirements.

3.4 Security Code Review

Our internal policies outline how we build software in a secure manner, including mandatory independent reviews that are conducted to identify potential security issues before integrating new code into our applications.

3.5 Software Supply Chain Security Management

Our Software Supply Chain Security program ensures that all third-party components embedded in or shipped with FME comply with all legal and licensing obligations, as well as our security requirements.

We rely on both automated scanning tools and dedicated personnel to continuously monitor, triage, and track known security vulnerabilities, and to ensure that our third-party components are updated in a timely manner.

Your license of FME Flow includes a Legal Notices file in `<install directory>/Docs/LicenseAgreements/FME Flow Legal Notice.html`, which also applies to Flow Hosted. The Legal Notices file provides a listing of Free and Open Source (FOSS) components used in your particular version of FME. A copy of the legal notices is also available on our website on our FOSS page.

3.6 Vulnerability Disclosure Program

No application is without security flaws, and issues may be discovered at any time. Safe Software welcomes feedback from security researchers and the public to help improve our security. If you believe you have discovered a vulnerability, privacy issue, exposed data, or other security issues in any of our assets, we want to hear from you. Our Vulnerability Disclosure Policy outlines steps for reporting vulnerabilities to us, what we expect, and what you can expect from us.

We value and thank those who take the time and effort to report security vulnerabilities according to this policy. However, we do not offer monetary rewards for vulnerability disclosures.

3.7 Third Party Application Security Assessments

Unlike many organizations who limit their application assessments to penetration testing only and often black-box, we follow OWASP's Security Testing Guide (WSTG) recommendations, and engage third party experts to conduct regular application security assessments, including design review, threat modeling, code security assessment, and annual penetration testing. This is done on both the FME Flow and FME Flow Hosted applications, and threat scenarios that concern both are also considered.

The external team conducting the assessments are former software developers who understand applications and take a software centric approach required to find the more impactful security issues. In addition, those conducting the assessment are rotated each time for additional assurance, following the same process and standards to ensure consistency and maximum effectiveness.

4 Cloud Infrastructure Security (FME Flow Hosted)

We take great pride to secure our systems from an end-to-end perspective, including our cloud infrastructure.

4.1 Automated Cloud Vulnerability Scanning

Our AWS environments are scanned automatically using leading industry scanners and policies that check for CIS AWS Benchmark and other compliance controls. This ensures our systems remain hardened according to best practices, and weaknesses are constantly identified and remediated.

On identifying a threat, we audit our infrastructure to see what is affected, and based on that, assess the security risk and assign a severity level.

If there is a vulnerability and it is high risk, we will immediately create a patch. Before patching, we will send an email out to the emergency contact of affected customers. If it is a lower severity issue, then we will prepare a patch and communicate the issue via the in-app notifications on the FME Flow Hosted dashboard. When we deploy lower severity patches, we aim to strike a balance between risk and ensuring the impact on your production workflows is minimal.

4.2 Third Party Cloud Infrastructure Security Assessments

We engage our external third party security partner to conduct annual Cloud security focused penetration testing aligned with the CIS AWS Benchmark and other industry standards. Other third party assessment activities conducted periodically include design review and threat modeling of our cloud infrastructure.

The team conducting the assessments consists of former software developers with AWS certified experts to find the more impactful security issues. In addition, those conducting the assessment are rotated each time to ensure new sets of eyes review the system, following the same process and standards to ensure consistency and maximum effectiveness.

5 Security Operations

5.1 Security Updates

The versions of our **FME Flow** software are continuously being updated to resolve vulnerabilities. Critical vulnerabilities are addressed quickly and generally released in our micro releases to ensure our customers' systems remain protected. Vulnerabilities with lower severity, or vulnerabilities which are not exploitable due to our software architecture, are generally updated on our main development trunk and therefore are not available until the next major or calendar release of the product depending on the assessed risk, e.g., FME 2023.0, 2023.1.

FME Flow Hosted uses some services that are managed by AWS, and others that are self-managed by Safe. AWS ensures the latest versions of components are provided for all managed services we use, and we do our part to apply the required updates where we use unmanaged services.

Both the operating system and database are upgraded and patched as releases become available. Patches are applied to the staging environment first to ensure they do not cause issues.

5.2 Data Governance and Privacy

FME Flow instances should be installed by your staff on your machines within a computing environment exclusively within your control. In this scenario, your data is under your complete control, and we do not host or access your data in any manner. Please see our Privacy Policy for more information.

If you choose the cloud option, we make sure your data is only accessible to your users. Your business data resides in the **FME Flow Hosted** instance storage, which is encrypted with AES-256 bit encryption. Only your authorized users have access to data or workspaces stored on an FME Flow Hosted instance. Safe Software employees and other customers do not have access to your data. The only exception is a small and controlled number of Safe Software system administrators who have access to the entire system. These administrators can only access your data under very controlled circumstances. You will receive an automated email whenever an administrator accesses your instance, and all operations are logged.

FME Flow Hosted does not receive, process, or store customer credit card information in its infrastructure. Our billing page integrates with a third-party payment processing service that is fully PCI DSS compliant.

Safe Software monitors metrics on system utilization and performance, including disk usage, network throughput, server load, and application monitoring. By checking the performance and reliability of the server, we can alert you if there are any problems.

5.3 Data Lifecycle Security

It is important to protect data at all stages including creation, processing, storage, and destruction. For **FME Flow Hosted**, we apply encryption to all data we store, protect it using TLS while it is communicated across all environments, and apply best practices to protect how we process data.

Upon termination of your **FME Flow Hosted** account, assuming there is no outstanding balance, Safe Software destroys all data stored on instances associated with your account.

5.4 Backup and Disaster Recovery

FME Flow instances hosted by customers provide the functionality to schedule configuration export for backup purposes or on demand. In addition, data is stored in customer-owned databases. As such, it is the responsibility of customers to implement the appropriate backup and disaster recovery controls.

FME Flow Hosted database backups are taken every 24 hours and will be kept for 30 days. This only covers the core FME Flow Hosted application, and not any of the customer data for FME Flow instances hosted in AWS (see above).

For instances hosted in FME Flow Hosted, we provide the following features:

- Backup created automatically every 24 hours while the instance is running.
- Backup created automatically after an instance is stopped.
- Backup created automatically before an instance configuration changes (such as a change in instance type).
- The last 2 up to a maximum of 10 automatic backups are kept. The number of backups to keep can be modified by the user.
- Backups can be triggered manually by the user. These are kept indefinitely until the instance is terminated or the user deletes them.

If the need ever arises to rebuild an instance, users can restore an instance from previous backups. Once an instance is terminated, all data associated with the instance is immediately destroyed, with backups available for 30 days.

5.5 High Availability

FME Flow on-premises deployment offers a High Availability (HA) deployment option that can be used by customers who have such requirements.

FME Flow Hosted services are deployed in different availability zones in AWS to provide high availability to our customers. All components for an instance of FME Flow deployed in FME Flow Hosted are hosted in a single virtual machine with no HA option.

5.6 Incident Reporting

Safe Software is committed to reporting any incident that may impact the customer as soon as possible, especially when customer data could be involved. Critical security advisories that affect our customers will be sent to the Emergency Contact specified for the FME Flow Hosted account. Of course, it is our hope that we never have to notify you of such a reason.

If you believe you have discovered a security vulnerability in our products, please get in touch via email at security at safe dot com. We ask that you not publicly disclose the issue until it has been addressed.

5.7 Inventory Management of Enterprise Software

Our Information Technology team manages our inventory of enterprise software and services. Our Vendor Compliance Review process ensures the following risks are assessed before entering a business or contractual relationship with a vendor: compliance risk, reputational risk, operational risk, country risk, credit risk, and information technology risk.

5.8 Logging and Monitoring

FME Flow instances provide important application log data, such as successful and failed authentication attempts, and allows users to incorporate this information with other security telemetry to get a complete picture of attacks and better identify actual incidents.

FME Flow Hosted takes care to ensure malicious activity is detected early on before attackers can exploit our systems. Safe Software has put logging and monitoring controls in place as follows:

- All logs for the FME Flow Hosted application and infrastructure are centrally aggregated and monitored. This does not include the application logs from customer specific FME Flow instances whose log collection and monitoring are the customer's responsibility.
- AWS logs are stored in a centralized ops account with limited access.

6 Staff Security

As important as it is for organizations to implement technical security controls, humans are often known to be of the weakest links in security and used to bypass costly technical security controls. As such, Safe Software takes appropriate measures to ensure all access is managed appropriately, and staff have the right training in place to address security issues before they become a problem for the organization. In addition, our recruitment process includes extensive verification steps, with additional background screening for sensitive roles.

6.1 Account Management and Access Control

Safe Software requires that all access to its infrastructure, application, and data be controlled based on business and operational requirements. The right to access is restricted based on employee role and regularly audited for continued need.

Safe Software follows the Principle of Least Privilege. Staff are granted the minimum level of access for their defined job function, and use of shared identities is restricted.

Our password policy exceeds the U.S. National Institute of Standards and Technology (NIST) password guidelines and emphasizes the importance of password length. Additionally, we require multi-factor authentication for accounts wherever possible.

6.2 Security Training

Safe Software conducts security awareness training programs annually and upon hire for all employees. Programs are reviewed and updated annually to reflect the latest cyber threats and confirm understanding of organizational policies. Additionally, throughout the year staff are continually reminded to stay vigilant and aware of social engineering threats such as phishing.

We also conduct a secure software development training program dedicated to Product and Software Development teams.

Our e-learning platform provides security modules including those that cover common application security issues aligned with OWASP Top 10, and all team members are required to review this material on an annual basis.

6.3 Endpoint Security

Our endpoints are protected and managed by a suite of device management, monitoring, and endpoint protection software. Full disk encryption has been enabled on staff devices to protect data at rest. Events are monitored by a dedicated Security Operations Center team, staffed by analysts that maintain 24/7/365 vigilance, from alert validation through in-depth forensics and analysis of our internal network and users.

In addition to our regular security reviews and compliance audits, we partner with trusted third-party security companies to perform penetration tests across our internal network.

7 Regulatory & Compliance

Safe Software complies with industry-standard certifications and global privacy regulations, such as ISO/IEC 27001, the European Union's General Data Protection Regulation (GDPR), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), and the Payment Card Industry Data Security Standard (PCI DSS).

Our Security and Compliance Program is based on the ISO 27001 Information Security Management System (ISMS). We have defined policies that govern our security policies and processes and continually update our security program to be consistent with applicable legal, industry, and regulatory requirements. We also undergo regular independent third-party audits and strive for continuous improvement by constantly working to expand our coverage.

If you have any questions, feel free to contact us at security at safe dot com. If you are a current FME customer, please create a Support Case so we can better assist you with your inquiry. If you purchased FME through a Partner, please contact the Partner directly.