Metomic

Navigating SaaS Data Security

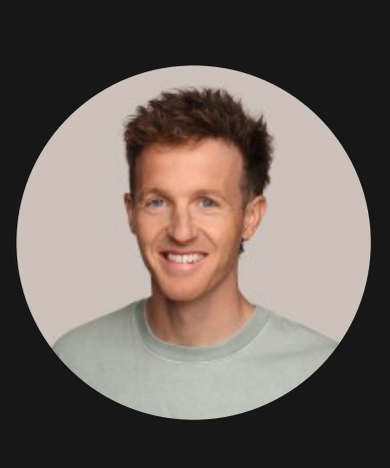
In the Financial Sector

Introduction

SaaS data security is becoming increasingly important as financial services deepen their reliance on SaaS applications and cloud providers, posing new data protection and compliance challenges.

In this guide, we'll examine the risks to data stored in SaaS applications, such as cyber threats and regulatory issues. We also explore practical strategies and best practices for companies in the financial services sector when it comes to keeping data safe and compliant by implementing SaaS data security solutions.

Rich Vibert
CEO of Metomic



Common SaaS Applications in Finance

Popular SaaS Tools in Finance and Associated Date Risk

Cloud Accounting
Streamlines financial operations, real-time data access.

CRM Software
Enhances customer relations, data-driven insights.

Payment Gateways
Simplifies transactions, secure processing.

Project Management
Organises workflows, collaborative tools.

Data Breach Vulnerability
Exposure to unauthorised access.

Compliance Issues
Challenges in meeting regulatory standards.

Data Corruption
Risk of accidental or malicious data alteration.

Unauthorised Access
Potential for unauthorised user entry.

SaaS applications play a vital role in the day-to-day function of the financial sector, housing critical and sensitive information and data that come with their own set of risks needing diligent management.

A few examples of SaaS applications used in the finance sector include:

1. **Cloud-Based Accounting Platforms:**
These tools hold sensitive financial data, including transaction histories and corporate financial statements, with the primary risk being exposure to data breaches that could compromise confidential information.

2. **CRM Software:**
These systems contain personal client information, sales data, and interaction logs, posing risks related to compliance with data protection regulations.

3. **Payment Gateways:**
They process payment details, transaction records, and authentication data, where the main risk entails data corruption that could disrupt transaction integrity.

4. **Project Management Tools:**
These applications store project plans, communications, and internal documentation, with unauthorised access being the key risk that could lead to data leaks or manipulation.

Considering the pivotal roles that data stored in these applications play in financial operations and business continuity, it is clear that a strategic approach to data security is beneficial and essential. Ensuring the confidentiality, integrity, and availability of this sensitive data is a multifaceted challenge that leads us to explore the layers of security infrastructure and policies necessary to protect these digital assets.

Unravelling the Anatomy of Financial Cyber Attacks

Far from being random, cyber attacks in the financial sector are executed through a phased approach, each designed to escalate the attacker's influence over the compromised infrastructure.

Step 1. Reconnaissance
Attackers gather information on potential vulnerabilities within SaaS applications used in finance. This includes scanning for weak spots in public cloud-based accounting systems, CRM tools, and other SaaS offerings of cloud vendors that manage sensitive financial data.

Step 2. Initial Penetration
Using identified vulnerabilities, cybercriminals often deploy social engineering—from generic phishing scams to highly targeted spear-phishing attacks—to gain initial access. This step may involve manipulating users or exploiting weak authentication processes despite the presence of security measures like Multi-Factor Authentication (MFA) and Single Sign-On (SSO).

Step 3. Expansion of Access
Once inside, attackers aim to broaden their access. They may capture session tokens or exploit SSO configurations, allowing them to store data and traverse interconnected SaaS platforms seamlessly.

Step 4. Entrenchment
At this point, attackers solidify their presence by targeting high-level users, like system administrators, through platforms like LinkedIn. They might also initiate supply chain attacks, striking at centralised vulnerabilities that ripple through interconnected systems.

Step 5. Exploitation
With a firm grip on the systems, attackers can unleash harmful activities through such attacks as ransomware, which encrypts critical data, crippling financial operations and business processes and causing extensive damage ranging from financial losses to legal team's regulatory repercussions.

Compliance Challenges and Solutions

Identify Requirements
Understand legal and industry standards.

Risk Assessment
Evalutate vulnerabilities and threats.

Implement Controls
Apply necessary security measures.

Monitor and Audit
Regularly review and update practices.

Compliance Roadmap in SaaS Usage

Tips:

Data Encryption
Protect sensitive information with Metomic.

Employee Training
Raise awareness about security protocols.

Regular Updates
Keep all systems up-to-date.

Compliance Issues with SaaS Apps

The integration of SaaS solutions in finance has its compliance hurdles. Issues like data sovereignty, data encryption, standards, and third-party risk management are at the forefront, necessitating a careful approach to ensure regulatory conformity:

Data Localisation and Sovereignty:
Many regulations require storing financial data within certain geographical boundaries. Often hosted globally, SaaS tools can inadvertently breach these rules by storing data in locations not compliant with national regulations.

Access Controls and Identity Management:
Compliance with standards like the GDPR and HIPAA demands strict control over who can access sensitive data. SaaS tools must have robust identity management and access control systems to prevent unauthorised access and breaches.

Encryption and Data Security:
Regulations like PCI DSS require that sensitive data, especially payment information, be encrypted in transit and at rest. Ensuring that SaaS providers comply with these encryption standards is a significant challenge.

Audit Trails and Activity Monitoring:
Compliance frameworks often necessitate detailed audit trails of data access and modifications. SaaS applications must be capable of providing comprehensive logging and activity monitoring to satisfy these requirements.

Third-Party Risk Management:
When third-party SaaS providers handle financial data, institutions must ensure these vendors comply with relevant regulations. This includes managing the risks associated with vendor security practices and data handling procedures.

Incident Response and Reporting:
In the event of a data breach, regulations like the GDPR require prompt incident response and reporting. SaaS solutions must have quick detection, response, and notification mechanisms per these legal requirements.

Financial institutions must understand these security issues and develop comprehensive strategies to address each, ensuring a secure and compliant SaaS environment.

Practical Approaches to SaaS Data Security Posture Management

Establish Comprehensive Data Governance
A robust data governance framework is key for financial firms using SaaS and cloud applications everywhere. This involves setting clear policies on data access, usage, and storage, ensuring alignment with regulatory standards. It also includes classifying data based on sensitivity and applying appropriate controls, a critical step in managing data risk effectively.

Enhance User Access Management
Tightening user access controls is a vital practice. This means implementing stringent identity verification processes, like multi-factor authentication (MFA), and managing user permissions meticulously to ensure that only authorised personnel can access sensitive financial data.

Regular Security Audits and Vulnerability Assessments
Regular security audits and vulnerability assessments of the SaaS environment help identify and address potential security gaps. Financial institutions should schedule these audits periodically to ensure their cloud infrastructure and SaaS tools remain secure and compliant with evolving security standards.

Develop a Comprehensive Incident Response Strategy
Having a well-defined incident response plan for potential security breaches is essential. This strategy should include procedures for immediate response, communication, disaster recovery plans, and steps for post-incident analysis to prevent future occurrences.

Promote Security Awareness and Training
Investing in regular security training and awareness programmes for employees is crucial. This ensures that all staff members know the potential security risks associated with SaaS applications and are equipped to identify and prevent security threats.

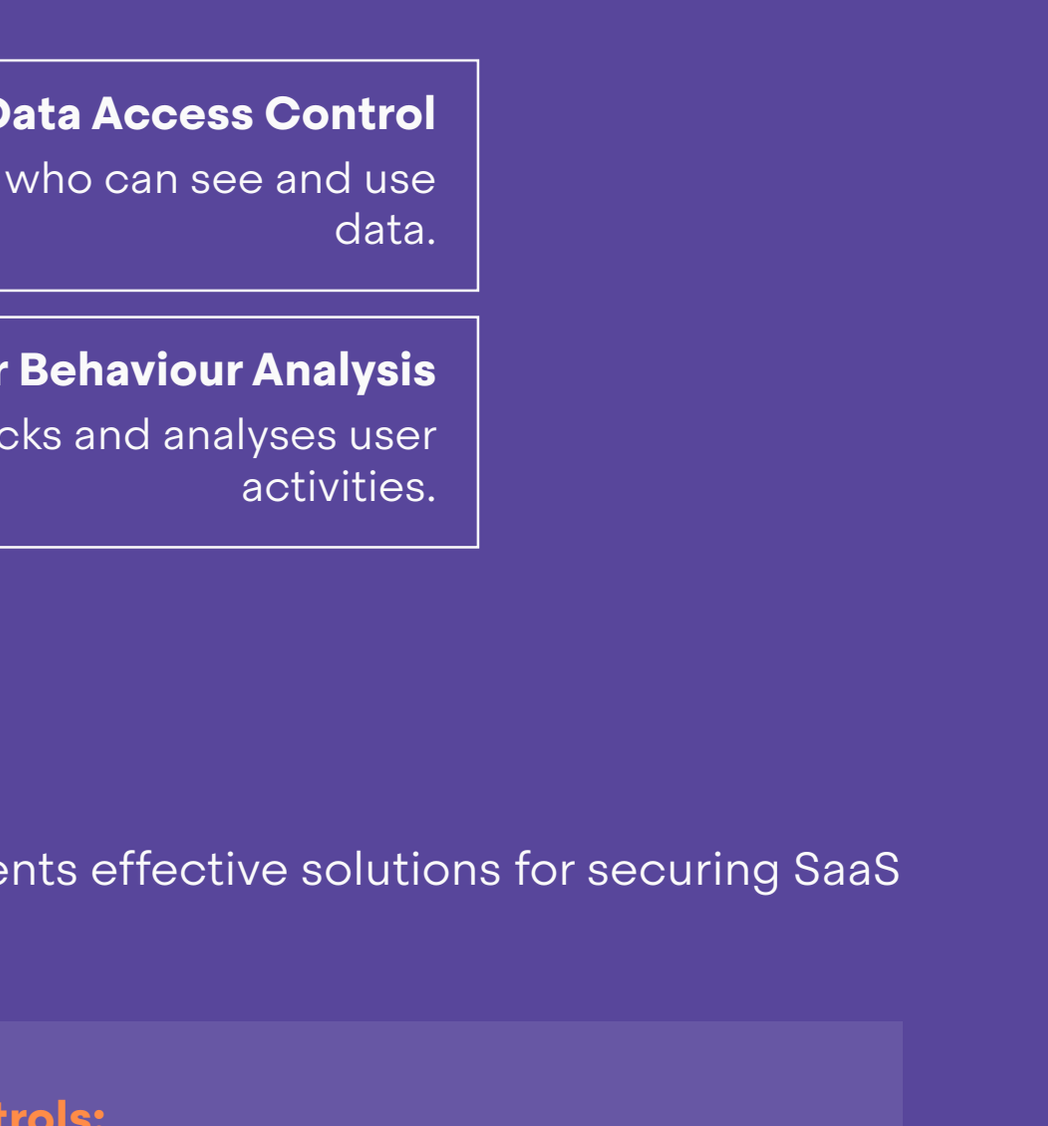
Leverage Advanced Analytics for Threat Detection
Advanced analytics and machine learning algorithms can enhance threat detection and response capabilities. This proactive approach allows financial institutions to identify and mitigate potential insider threats before they escalate.

Integration of Security Information and Event Management (SIEM) Systems
Financial institutions should integrate Security Information and Event Management (SIEM) systems to enhance real-time security monitoring. These systems aggregate and analyse activity from various resources across the IT infrastructure, providing a comprehensive view of security events. By using SIEM, firms can quickly detect, analyse, and respond to potential security incidents, significantly reducing the impact of breaches.

Deployment of Advanced Endpoint Protection
Advanced endpoint protection is critical to defend against sophisticated malware and emerging threats. This involves using next-generation antivirus solutions beyond traditional signature-based detection, employing behavioural analysis and machine learning techniques. Given the remote access nature of SaaS applications, ensuring that all endpoints - mobile devices to laptops - are secured against these advanced threats is essential.

For Organisations Without Dedicated Security Teams
Safeguarding SaaS applications can be challenging for smaller financial organisations or those without dedicated security teams. In such cases, it is vital to leverage external resources and expertise. These organisations should consider partnering with trusted security consultants or service providers who can offer guidance and support in implementing effective security measures.

Additionally, adopting standardised security policies and frameworks and engaging the security team in regular training and awareness programmes can empower employees to recognise and mitigate potential security breaches and risks in their daily operations.



Leveraging Metomic for Enhanced Security

Popular SaaS Tools in Finance and Associated Date Risk

Real-Time Monitoring
Continuous surveillance for threats.

Automated Compliance
Ensures consistent regulatory adherence.

Data Access Control
Manages who can see and use data.

User Behaviour Analysis
Tracks and analyses user activities.

How Metomic Can Protect Your Data

With the growing need for reliable robust data security in financial services, Metomic presents effective solutions for securing SaaS applications in the following ways:

Automated Data Discovery:
Metomic's automatic data discovery software seamlessly integrates with an organisation's SaaS applications. It provides deep visibility at an individual data point level, which is crucial for financial institutions handling sensitive customer data. This feature helps identify where critical data resides across various SaaS platforms, facilitating better control and protection.

Data Loss Prevention (DLP):
Metomic offers DLP capabilities integral to financial data security. The platform can automatically prevent sharing sensitive information across apps or within isolated areas. This is particularly valuable in preventing accidental disclosures or leaks of financial data, such as credit card numbers or transaction details.

Real-Time Alerts and Human Firewall:
The Human Firewall feature enables real-time employee notifications upon policy violations, fostering a proactive security culture. This immediate feedback loop helps educate users about security best practices and reduces the risk of data breaches due to human error.

Advanced Access Controls:
With Metomic, financial firms can control who accesses what data and when. This capability is essential for minimising data exposure and managing internal risks, especially in environments where data access needs to be tightly regulated.

Insider Threat Detection:
Metomic provides visibility over anomalous activities within any SaaS application, an essential feature for identifying and mitigating insider threats. This functionality ensures that unusual or unauthorised data access is quickly detected and addressed.

Compliance with Global Regulations:
Metomic aids in aligning SaaS applications with various global regulations like HIPAA, PCI DSS, and GDPR. Our platform's features assist in maintaining compliance, which is a significant concern for financial institutions operating in a heavily regulated environment.

By integrating Metomic into their security strategy, financial services firms can enhance the protection of their customer data and achieve a higher degree of operational efficiency and regulatory compliance. The combination of advanced technology and user-friendly interfaces makes Metomic a powerful ally in the quest for effective robust data security in the SaaS-dependent financial sector.

Metomic

Book your Risk Audit with our team

To see how Metomic can help improve your Data Security posture, book a demo with our team today.