NETERIUM

BANKING ON THE CLOUD

A PARADIGM SHIFT FOR FINANCIAL CRIME COMPLIANCE

January 2024

neterium.io

In the rapidly evolving landscape of the financial industry, the adoption of cloud-based solutions, particularly Software-as-a-Service (SaaS), is emerging as a pivotal trend.

While the financial industry may have initially been slower and -rightfully- cautious in its adoption of cloud-based solutions, there are now abundant examples of such successful implementations. Use cases today are extensive and diverse, encompassing areas from document management to reporting and data analytics, as well as customer relationship and risk management, reaching even into the realms of cybersecurity and core banking systems.

Many success stories have underscored the practical and strategic advantages that financial institutions gain by embracing SaaS in the public cloud. However, financial institutions should remain cautious when selecting SaaS solutions and providers, especially in terms of the protection of sensitive customer data and operational controls.
This paper covers the key benefits of leveraging cloud-based SaaS solutions for sanctions screening compliance while also offering ways to contain the related risks.

“Many success stories have underscored the practical and strategic advantages that financial institutions gain by embracing SaaS in the public cloud. This paper covers the key ***benefits of leveraging cloud-based SaaS solutions for sanctions screening compliance*** *while also offering ways to contain the related risks.”*

1) Key advantages of using a SaaS Sanctions Screening solution in the public cloud

Financial institutions can gain a strategic edge by harnessing the power of cloud-based sanctions screening solutions. Here are the key benefits:

Cost-Efficient Scalability. Well-designed and well-run SaaS solutions offer unparalleled scalability. In the public cloud, financial institutions can harness virtually infinite resources to meet dynamic workloads effectively and cost-efficiently, instead of the heavy initial investment in bank-owned operating centers that must be oversized to handle potential volume peaks. This flexibility not only aligns with the volatile nature of financial crime and financial markets but also enables institutions to adapt swiftly to regulatory changes, securing their competitive edge in an ever-changing landscape.

Performance. The public cloud infrastructure ensures high-speed performance, facilitating optimal throughput and low latency while processing vast amounts of data. This is critical for timely financial crime detection. The most advanced sanctions screening solutions can deliver a throughput of 100,000 transactions per second, with a transaction latency of only a few milliseconds, catering to the demand of new use cases such as screening of Instant Payments.

Reduced Implementation Cost and Risk. SaaS solutions in the cloud slashes upfront implementation costs compared to traditional on-premises solutions. There is no need to pay a hefty one-off license nor spend significant resources to install the solution on the bank's hardware. Furthermore, financial institutions can rigorously evaluate the solution on the SaaS provider's sandbox before committing to acquiring it, which strongly minimizes the risk of post-implementation dissatisfaction. This efficient resource allocation improves the quality of financial crime compliance services and, by reducing the financial burden on institutions, provides a faster return on investment.

Continuous Software Updates. With SaaS solutions comes the enjoyable benefit of automatic software updates, ensuring that users always have access to the latest features and security enhancements. This proactive approach eliminates the need for long painful manual updates and ensures that the compliance software remains cutting-edge. Staying current with the latest software versions is not just a matter of convenience but a strategic imperative in the current fast-moving geopolitical and sanctions landscape. It is critical for financial institutions to be equipped with the most advanced tools to respond promptly to new regulatory requirements. Dedicated test environments allow financial institutions to perform extensive feature and non-regression testing before new releases are deployed in production.

Instant Provisioning. With SaaS solutions, screening services are available immediately upon contract signature. Unlike the delays associated with local implementations, instant provisioning in the cloud ensures swift deployment, accelerating time-to-value for financial institutions.

Business Continuity. Best-in-class SaaS solutions leverage the inherent resilience of the cloud for business continuity and disaster recovery to ensure uninterrupted services, even in the face of unforeseen events, providing peace of mind to financial institutions and their clients. SaaS solution providers can cost-efficiently deploy their solutions in multiple regions of a cloud provider, or even across multiple cloud providers, allowing for impressive Service Availability performance and – in case of disaster recovery scenarios – a very short recovery time. Beyond this very important continuity aspect, this resilience safeguards the reputation and trustworthiness of financial institutions.

Enhanced Security. Security is paramount in handling sensitive financial and customer data. Best-in-class SaaS solutions in the public cloud use robust security measures, including encryption, access controls, and continuous monitoring. Notably, large cloud providers like Amazon AWS, Microsoft Azure or Google Cloud can afford to invest substantial amounts in security, a level of expenditure individual banks might find challenging to match. Partnering with major cloud providers not only enhances security but also ensures that financial institutions benefit from the cutting-edge advancements in security protocols and practices, elevating the overall defense against cyber threats.

2) What should you look for in your supplier when choosing a SaaS solution?

When considering a SaaS solution in the public cloud for financial crime compliance services, it is crucial to be mindful of key elements to ensure a successful and seamless partnership. Here are the most important aspects to keep in mind when selecting a SaaS provider:

Service Level Agreements (SLAs). Financial institutions should ensure the SaaS provider's SLAs align with their expectations. Transparent and well-defined service availability (Uptime) and business continuity commitments, along with low latency and responsive support, are critical components of a reliable financial crime compliance service.

Robust SLAs not only create a foundation of trust but also contribute to establishing a clear framework for ongoing collaboration, fostering a strong and mutually beneficial partnership. Best-in-class SaaS providers demonstrate their quality by showcasing public service uptime statistics and transparency about incidents.

Uncompromised Data Privacy. The handling of customer data is paramount. Financial institutions should scrutinize the provider's commitment to data privacy and verify that their SaaS solution adheres to stringent data privacy standards and is fully compliant with regulations such as Europe's GDPR. A strong emphasis on data protection is essential to maintain the confidentiality, availability and integrity of sensitive information. The best providers may offer innovative zero-footprint models, processing data exclusively in memory without ever committing it to storage, which dramatically reduces the risk of data breaches while allowing banks to leverage the full benefits of the cloud.

Adherence to Regulatory Standards. Financial institutions should assess the provider's understanding and commitment to meeting or exceeding regulatory requirements related to financial institutions outsourcing sanctions screening services. A SaaS provider that is in lockstep with regulatory requirements ensures your institution can confidently manage compliance obligations.

Commitment to security. While SaaS providers automatically benefit from the enhanced security of the cloud, they should still be able to demonstrate that they themselves implement best practices in terms of security. Financial institutions should challenge their SaaS providers on their security practices, which best-in-class SaaS providers should be able to independently demonstrate through their ISO27001 certification or SOC2 attestation.

> *Selecting a SaaS provider with these considerations in mind is not just about due diligence; it is about securing a strong and mutually beneficial partnership that will enhance your institution's compliance operations and maintain its integrity in a fast-evolving market environment.*

3) Conclusion

The market trend toward the adoption of SaaS solutions in the cloud is clear.

For financial institutions, the failure to adopt these tools could significantly undermine their ability to effectively and efficiently combat financial crime and deliver high-quality services to their clients. However, given the delicate nature of customer data involved, a cautious approach is paramount when transitioning to these solutions and choosing a provider.

Embracing SaaS in the public cloud is an essential step forward in ensuring competitiveness and achieving excellence in financial crime compliance. The prudent adoption of SaaS solutions, backed by thorough vetting of providers, will empower financial institutions to navigate the complexities of an ever-evolving financial landscape, ensuring operational resilience and steadfast compliance.

CONTACT NETERIUM

https://neterium.io/

/company/neterium/

info@neterium.io

https://twitter.com/neterium