

Securing Digital Banking & Financial Services with Sangfor Athena SASE

Trusted, compliant, and resilient access for the modern financial enterprise



BFSI Digital Transformation Is Reshaping Security Requirements



Banks and financial institutions are modernizing operations to improve agility, productivity, and responsiveness. Yet in a highly regulated environment, sensitive financial data must remain protected, traceable, and compliant wherever it is accessed or used. As SaaS adoption, cloud workflows, hybrid work, and AI tools move regulated activities beyond traditional offices, branches, and data centers, traditional perimeter-based security models struggle to provide consistent visibility, compliance control, data protection, and secure connectivity.

Sangfor Athena SASE for Modern Financial Services

Sangfor Athena SASE helps banks and financial institutions secure modern operations with a cloud-native Zero Trust platform that unifies secure access, data protection, threat prevention, and operational visibility. Delivered through purpose-built security PoPs and a global private backbone, Athena SASE enables low-latency, secure access to private applications, public GenAI tools, SaaS platforms, cloud services, internet resources, and sensitive financial data — helping BFSI organizations reduce risk, simplify operations, and support compliance.

BFSI Use Cases and Athena SASE Solution

Use Case & Requirement	Key Challenges	Athena SASE Solution
Secure Access to Private Apps and Networks for Remote Users Enable remote workers, contractors, and partners to securely access authorized applications and data based on least privilege principles.	- VPNs grant broad network access, which facilitates lateral movement and exposes sensitive internal resources. - Static access policies fail to account for device risk, behavioral anomalies, or session context, increasing theft and compliance risks.	Zero Trust Network Access - Enables zero-trust, application-specific remote access without exposing the broader corporate internal network. - Continuously evaluates conditions like user identity, device security posture, user behavior, and session risk to enforce access permissions dynamically.
Secure Internet, SaaS, and GenAI Access Enable authorized, secure access to Internet, SaaS apps, and public GenAI without exposing sensitive data, users, and endpoints to internet-borne threats anywhere, anytime.	- Remote users are exposed to malware, viruses, and malicious websites when working outside corporate security controls. - Unsanctioned SaaS & AI usage creates visibility gaps and increases security and compliance risk.	SWG + FWaaS + Secure Workspace - Provides firewall protection or a secure isolated workspace for internet and chat AI access across users, branches, offices, and remote locations. - Enforces SWG controls & monitoring for Web, SaaS, and public GenAI tenants to evaluate risky users, applications, and websites.

Use Case & Requirement	Key Challenges	Athena SASE Solution
Prevent Data Loss and Support Regulatory Compliance Prevent unauthorized exposure, transfer, or misuse of sensitive data (e.g., PII, PCI, transaction records, customer information) while supporting regulatory compliance requirements.	• Sensitive data can leak through SaaS, GenAI uploads/chat, cloud, endpoints, and unsanctioned desktop apps. • Limited visibility and control over how regulated data is accessed, shared, and transferred increases compliance risk.	Athena SASE DLP + Secure Workspace • Prevents sensitive data like PII/PCI/IPs from being entered into or uploaded to SaaS, public GenAI platforms, web, cloud, email, endpoints, and unsanctioned desktop apps. • Provides centralized visibility into sensitive data movement, ensuring comprehensive tracking and streamlined reporting for regulatory compliance audits.
Simplified Administration & Experience Reduce administrative overhead and gain end-to-end visibility while enabling a seamless end-user experience.	• Multiple point solutions result in admin overhead, integration challenges, and visibility gaps. • Multiple endpoint agents are complex to manage and result in a poor user experience.	Athena SASE AIO Agent • Provides a single-pane-of-glass unified admin portal with end-to-end visibility. • The all-in-one agent enables easy rollout and upgrades, delivering a seamless end-user experience for better productivity.

Athena SASE BFSI Business Outcomes

01



Reduced Business & Cyber Risk

Reduces the risk of service disruption, financial loss, regulatory scrutiny, and reputational damage from ransomware and data breaches.

02



Faster, Safer Digital Growth

Accelerates SaaS and hybrid-cloud modernization, branch rollout, and remote work to improve service delivery and operational agility.

03



Higher Workforce Productivity

Utilizes local PoPs to reduce latency and improve employee productivity with an AIO agent for reliable access to time-sensitive financial systems and data.

04



Stronger Compliance Assurance

Meets regulatory demands on data privacy (PII/PCI), AI visibility, and Zero Trust mandates through built-in reporting and evidence.

05



Lower Operating Costs & Complexity

Consolidates standalone security tools into a unified cloud-native model delivered using one unified agent, reducing licensing costs and operational overhead.

As financial institutions move toward cloud-first, distributed operating models, Sangfor Athena SASE provides a unified foundation for secure access, data protection, threat prevention, and compliance. By consolidating networking and security into a scalable cloud-native platform, Athena SASE helps reduce complexity, improve performance, and support secure financial services innovation.