SANGFOR

Unlocking The Secrets Of Sangfor Athena SASE

Your Ultimate FAQ Guide



What is Sangfor Athena SASE?

Sangfor Athena SASE is a comprehensive Secure Access Service Edge platform that unifies advanced security (ZTNA, SWG, FWaaS, DLP, UWM, and EDR) with wide-area network (WAN) agility, empowering modern businesses to operate securely, efficiently, and seamlessly. It delivers secure, high-performance access to the internet, cloud, and on-premises resources for both in-house and remote users—anytime, anywhere, on any device.

What are the business benefits of using Sangfor Athena SASE?

1. Improved Workforce Productivity: Athena SASE ensures consistent security and high-performance connectivity, enabling business users to work without interruptions or lag, whether at home, in the office, or on the move. By reducing latency and delivering secure connections to on-prem and cloud applications, it eliminates networking and security disruptions, fostering a more empowered and efficient workforce.

2. Accelerating Digital Transformation: The Athena SASE platform is cloud-native by design and offers a unified network and security stack that integrates advanced security features (ZTNA, SWG, FWaaS, DLP, EDR) with wide-area network (WAN) agility. The seamless scalability and flexibility of the cloud-delivered service provide an agile foundation for digital transformation initiatives such as accelerated cloud migration, SaaS adoption, and big data integration.

3. Supporting Geographic Expansion: Athena SASE addresses global expansion challenges head-on, with its global backbone PoP network, advanced security features, data loss prevention, and compliance monitoring, which support new branches, help meet local regulatory requirements, and enable the rapid onboarding of remote employees, partners, and global customers. Athena SASE's Cloud-Native Hyperscale Architecture ensures that as your enterprise expands, your network capabilities scale seamlessly.

4. Comprehensive Data Protection: Athena SASE provides organizations with centralized, real-time visibility into data flows, robust Data Loss Prevention (DLP) controls, insider risk analysis, and support for compliance enforcement to protect proprietary data and ensure adherence to dynamic global privacy regulations.

Is Sangfor Athena SASE suitable for organizations of all sizes and industries?

Yes, Athena SASE is suitable for organizations of all sizes and industries. Its scalable, cloud-native architecture can adapt to the unique needs of each organization, ensuring seamless connectivity and unmatched performance. Its comprehensive security suite and advanced features make it a valuable solution for any organization looking to optimize its network infrastructure and enhance security.



How does Sangfor Athena SASE address the challenges faced by distributed and remote workforces and ensure comprehensive security and consistent protection?



1. Securing Hybrid Workers: Athena SASE platform is designed to provide an optimal and secure experience for users within hybrid enterprises. With cloud-delivered capabilities such as Zero Trust Network Access (ZTNA), Firewall-as-a-Service (FWaaS), and Secure Web Gateway (SWG), it ensures that your employees can connect to internet and intranet resources securely and swiftly. Our global secure access capabilities offer comprehensive threat prevention to all users and devices, regardless of the location they are connecting from. With our solution, geographic barriers diminish, and teams can collaborate in real time without lag or security concerns.

2. Securing Cloud Adoption: Athena SASE's global PoP (point of presence) network ensures that relevant security policies are always enforced on end-user access to private cloud workloads or SaaS applications, regardless of user location or device, without backhauling traffic to data centers. Through our global PoP network, end-user connections to cloud applications and workloads are always secure with blazing fast speed and consistent security policies enforced. Organizations can enjoy the full business benefits of cloud applications without worrying about networking, data leakage, and security.

3. Secure AI Adoption: Athena SASE provides granular visibility and control over generative AI (GenAI) usage across the organization. The platform actively monitors chat content and sensitive data submitted to GenAI tools, delivering comprehensive analytics on AI utilization, organizational use cases, and potential data exposure. By leveraging these granular policy controls, IT teams can establish a structured framework to enable safe, compliant, and efficient AI adoption across the enterprise.

4. Securing Sensitive Data: Athena SASE delivers comprehensive Data Loss Protection for your organization's critical assets against accidental exposure or malicious exfiltration. Utilizing advanced features like AI-powered data loss analysis, data detection and response, endpoint DLP controls, and insider risk management, the platform maintains deep visibility into sensitive data across web, cloud, email, SaaS, GenAI, and internal applications. This unified approach empowers organizations to confidently mitigate data breach risks while seamlessly adapting to stringent PII/PCI data privacy regulations.

5. Cross-Border Connectivity: At its core, Athena SASE employs advanced SD-WAN capabilities, ensuring that data transfers are not only fast but also stable. The solution optimizes paths for data packets, reducing latency and ensuring that applications run smoothly, even in bandwidth-limited environments.



How does Sangfor Athena SASE maintain compliance with data protection regulations and industry standards?



Athena SASE is designed to help organizations comply with data protection regulations and industry standards by implementing advanced data protection security features. These include advanced data loss prevention, data detection and response, insider risk management, automated data identification and classification, and access controls based on zero-trust principles. These features protect sensitive data and ensure privacy, allowing organizations to meet compliance requirements related to PCI DSS and IP data. Athena SASE is a SOC 2 Type 2-certified platform alongside mandatory industry certifications such as ISO 27001.



How is Sangfor Athena SASE recognized by global industry analysts and independent cybersecurity research firms?



Athena SASE has earned notable recognition from leading global technology analyst firms and independent testing organizations. Its market validation reflects strong performance across security capabilities, global networking agility, and customer satisfaction:

1. Gartner® Magic Quadrant™ for SASE Platforms 2026: Featured in the report as a recognized global SASE provider and the only APAC-headquartered vendor to be recognized in the report.

2. Gartner® Peer Insights™: High customer satisfaction scores and positive peer reviews across SASE-enabling components, including ZTNA, SWG, FWaaS, DLP, etc.

3. Frost & Sullivan: Named a leader in the Frost Radar™ for SASE report for market growth, continuous innovation, and AI-driven security capabilities. Recognized by Frost & Sullivan with the Company of the Year Award in the APAC SASE Industry for outstanding strategy, execution, and customer success.



What kind of support and professional services does Sangfor offer to Athena SASE customers?

Sangfor offers dedicated support and implementation services free of charge to help organizations optimize their Athena SASE deployment and maximize the benefits of the solution. The support team is readily available to assist with any technical issues while the implementation services team provides guidance on best practices, configuration, and integration with existing infrastructure. This ensures a smooth transition and ongoing success.





What is Zero Trust Guard and how does it differ from traditional VPNs?

Zero Trust Guard (ZTG) is the Zero Trust Network Access (ZTNA) solution within the Athena SASE platform, designed to provide secure, adaptive application access based on a strict "never trust, always verify" framework.

Unlike traditional VPNs that grant broad, network-level access upon initial login, ZTG limits access strictly to specific, authorized applications based on the principle of least privilege. This application-level isolation conceals internal network infrastructure from public view, neutralizing the threat of unauthorized scanning and preventing attackers or malware from moving laterally across subnets. Furthermore, while legacy VPNs rely on one-time authentication at connection, ZTG continuously monitors user context, behavior, and device health throughout the entire session, dynamically revoking or restricting access if a threat is detected.

From an operational and user experience standpoint, traditional VPNs frequently degrade performance by backhauling user traffic through centralized corporate data centers, creating severe latency bottlenecks. ZTG eliminates this issue by routing remote traffic through Athena SASE's optimized global edge network, delivering low-latency, direct-to-app performance. Finally, ZTG is natively unified within the Athena SASE platform, allowing IT teams to enforce consistent access, security, and data protection policies from a single console, whereas traditional VPNs require fragmented, standalone management.





How does Athena SASE ZTG handle continuous risk evaluation and dynamic session control after the initial user authentication?

ZTG evaluates risk in real time by continuously monitoring user behavior, context changes, and device health posture throughout an active session. If a risk anomaly, device non-compliance, or threat signature is detected, ZTG dynamically enforces step-up authentication, restricts user access privileges, or revokes the session instantly.





How does Athena SASE ZTG protect access across multi-cloud, hybrid data centers, and non-standard legacy applications?

ZTG uses lightweight, outbound-only connectors deployed across multi-cloud and on-premises environments. It proxies both web (HTTP/HTTPS) and non-standard legacy protocols (such as TCP/UDP, SSH, and RDP) directly to the target app, cloaking underlying network subnets and enforcing unified identity-based policies.





What hardware or virtual appliances need to be installed for the ZTG solution?

No dedicated hardware is required. Users only deploy lightweight software agents on endpoints alongside small virtual connectors (lightweight VM nodes) in private data centers or cloud VPCs to bridge app traffic to the Athena SASE edge.





How does Athena SASE SGA inspect encrypted SSL/TLS traffic at scale without creating latency bottlenecks?

Athena SASE Secured Global Access (SGA) inspects encrypted SSL/TLS traffic at scale by leveraging a Single Pass Architecture combined with cloud-native hyperscale performance. Instead of traditional, resource-heavy security stacks that pass traffic sequentially through multiple discrete engines (causing CPU exhaustion and compounding delays), SGA inspects data packets only once. Its parallel engines simultaneously handle URL filtering, application control, intrusion prevention (IPS), and inline threat analysis on decrypted streams. It also incorporates intelligent SSL/TLS bypass capabilities for trusted or privacy-sensitive categories (such as healthcare and financial portals), ensuring compute resources are focused purely on high-risk traffic without impacting user experience.





How does the Athena SASE SGA enforce consistent web security policies for hybrid workers regardless of their location, network, or device?

SGA ensures consistent, cloud-delivered web security policies across all hybrid workers by separating policy enforcement from a user's physical location or network connection type.

1. Identity-Centric, Location-Agnostic Policy Engine: Policies are tied directly to user identity, organizational roles, and device health rather than IP addresses or local perimeters. Whether an employee works from a corporate office, a home Wi-Fi network, or a public coffee shop, the exact same URL filtering, threat protection, and application control rules follow them globally.

2. Single-Pane Centralized Cloud Console: Eliminates policy drift and administrative silos by managing security through a unified cloud management console. IT teams define web security, DLP, and threat inspection rules once, and the SGA platform automatically syncs them across all global PoPs instantly.

3. Distributed Global Edge Network: Diverts user traffic automatically to the nearest low-latency cloud security PoP (out of 70+ global security nodes). This guarantees that hybrid workers experience identical security inspection and low-latency internet browsing regardless of geographic location.





How does Athena SASE SGA discover and provide visibility into unsanctioned Generative AI applications (Shadow AI)?

SGA discovers and governs unsanctioned Shadow AI through deep packet inspection, dynamic application profiling, and centralized user analytics. With an industry-leading database of more than 5,400 AI applications and growing, SGA uses this application signature catalog to detect web traffic, API calls, and browser activity linked to public GenAI tools (e.g., ChatGPT, Claude, Copilot, etc.). SGA also provides visibility into Chat AI prompts, helping admins monitor sensitive prompt and upload trends across the organization.





How can Athena SASE SGA enforce granular, contextual access control for GenAI tools?

SGA enforces granular, contextual access control for Generative AI tools through three targeted capabilities:

1. Inline Context & Action Inspection: Decrypts SSL/TLS traffic using a single-pass engine to distinguish specific user actions—such as prompt submissions, file attachments, and API queries—rather than applying binary allow/block rules.

2. Context-Aware Policy Rules: Enforces flexible policies based on identity, device posture, and role. Security teams can grant read/chat access for approved GenAI applications while restricting high-risk actions like file uploads or code pasting.

3. Tenant & Account Isolation: Differentiates between corporate-managed AI accounts and unmanaged personal sessions, preventing the transfer of work data into personal AI environments.





How does the Athena SASE threat protection engine stop evasive zero-day threats, ransomware, and weaponized downloads in real time?

Athena SASE stops evasive zero-day malware, ransomware, and malicious downloads in real time through a multi-layered, AI-driven security architecture embedded directly into its cloud edge. Key protective mechanisms include:

1. AI-Driven Malware Inspection (Engine Zero): Incorporates Sangfor's proprietary machine learning engine (Engine Zero) directly inline. Rather than relying strictly on static signatures, Engine Zero extracts feature "DNA" from file payloads in real time, detecting unknown zero-day malware and polymorphic ransomware variants with high accuracy before they hit the endpoint.

2. Cloud Threat Intelligence & Dynamic Analytics (Neural-X): Synchronizes constantly with Sangfor Neural-X, a cloud-native threat intelligence and analytics platform. Unknown or suspicious files, URLs, and IP destinations are queried instantly against global threat feeds, blocking active Command-and-Control (C2) communication attempts and zero-hour phishing domains.

3. Network-to-Endpoint Synergy (Built-in EPP): Integrates cloud-edge inspection with Sangfor Endpoint Protection (EPP). If a malicious download bypasses initial network perimeter defenses, endpoint AI engines block execution locally, trigger automated quarantines, and feed threat telemetry back to the SASE cloud edge to protect all global nodes simultaneously.





How does the Athena SASE platform provide unified data protection capabilities across web, email, cloud/SaaS, AI, and endpoint vectors?

Athena SASE Zero Trust Data Protection (ZTDP) delivers unified, 3-in-1 data protection by combining advanced Data Loss Prevention (DLP), AI-powered data classification, and real-time Data Detection and Response (DDR) into a single cloud-native management plane. Rather than deploying disconnected point products, ZTDP uses the Athena SASE's All-in-One agent to enforce a "write once, enforce everywhere" data policy engine across all primary channels: web (internet), email agents, native desktop apps (like WhatsApp and Teams), GenAI platforms, SaaS, cloud, and private apps.





How does Athena SASE DLP prevent data leaks through Generative AI tools and unapproved SaaS applications (Shadow IT)?

Athena SASE prevents data exfiltration across Generative AI and Shadow IT using inline SSL/TLS inspection, continuous SaaS discovery, and Zero Trust Data Protection (ZTDP):

1. Shadow IT & AI Discovery: Identifies unauthorized cloud apps and unvetted GenAI tools (e.g., ChatGPT, Claude) across web, browser, and endpoint traffic.

2. Inline Prompt Inspection: Decrypts outgoing prompt payloads in real time. Admins can define DLP policies for blocking files containing sensitive data such as PII, source code, PCI-DSS data, or intellectual property before submission to public LLMs.

3. Contextual Action Control: Enforces granular AI policies—such as allowing usage of approved apps while blocking file uploads, copying and pasting, or unauthorized tenant logins.





How does Athena SASE ZTDP prevent sensitive data (PII, IP, source code, credentials) from being leaked into public LLM training datasets?

ZTDP prevents sensitive data leaks into public LLMs through real-time payload inspection on endpoints and contextual action controls. It can restrict unauthorized file uploads, block copy/paste prompt submissions containing sensitive data, and alert security teams in real time to enforce compliance.





What advanced detection mechanisms are supported by Sangfor Athena SASE for identifying sensitive data?



Athena SASE ZTDP accurately identifies and classifies sensitive data across structured, unstructured, and graphical formats through a comprehensive set of advanced detection engines.

1. Exact Data Matching Using Regex and Keywords: Define structured databases and exact records (such as credit card numbers, national identification IDs, and customer PII) to detect precise data exfiltration attempts with zero false positives.

2. Source-Based Tracking and Control: Analyzes and tracks sensitive unstructured documents (e.g., source code repositories, legal contracts, IP blueprints, financial statements) to recognize if outgoing files or text payloads are coming from a confidentially marked internal system.

3. Optical Character Recognition (OCR): Scans and extracts text embedded inside images, screenshots, scanned PDFs, and non-editable media to audit sensitive data hidden within non-text visual formats.

4. ML Auto-Classifiers: Utilizes machine learning models to classify unstructured files and context dynamically without relying solely on manual tagging or static regular expressions.

5. AI Auto Classification / Recommendations: Provides automatic classification of files transferred into AI-powered categories, including recommendations, file tagging (Secret, Top Secret, Confidential, etc.), and natural-language summaries for admins about the file content and context.

6. Data Lineage & Content Tracking: Tracks sensitive data movement across endpoints and applications by maintaining content lineage, allowing ZTDP to detect sensitive data even if users attempt to obscure or alter it (such as converting file formats or copy-pasting into unencrypted clipboards).



How does Athena SASE ZTDP protect sensitive data on unmanaged (BYOD) devices or when users are offline/disconnected from the internet?



ZTDP ensures continuous data security across unmanaged (BYOD) devices and offline/disconnected environments through endpoint agent enforcement. On the endpoint, the Athena SASE AIO agent caches DLP rules locally. Even when the endpoint is completely disconnected from the internet or from the SASE cloud tunnel, local policies continue to inspect and enforce data protection rules in real time. This restricts unauthorized physical and local data exfiltration channels offline, including USB mass storage devices, local printing, Bluetooth file transfers, network shares, etc. It also caches incident forensic logs and data leakage alerts locally during offline sessions, automatically syncing telemetry back to the Athena SASE central management console once connectivity is restored.



How does Athena SASE ZTDP simplify compliance enforcement and regulatory reporting (e.g., PCI-DSS, PII, or IP protection)?



ZTDP simplifies regulatory compliance and audit readiness through pre-packaged framework templates and centralized forensic reporting:

1. Out-of-the-Box Policy Templates: Includes pre-built data classification rules tailored for major standards—including PCI-DSS (cardholder data), PII (personal records), and IP protection (source code, schematics)—enabling instant policy deployment without manual setup.

2. Unified Cross-Vector Enforcement: Applies a single compliance policy uniformly across web, cloud apps, email, GenAI, and endpoints, eliminating policy fragmentation.

3. Audit-Ready Reporting: Generates detailed sensitive data movement maps, insights, and log evidence to trace data lineage, user activity, and incident remediation steps. Automatically captures contextual incident logs and visual evidence (e.g., screenshots of unauthorized transfers) while offering regional log storage to comply with strict data sovereignty laws.