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, 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

- **Improved Workforce Productivity:** Sangfor 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 resources, Athena SASE eliminates networking and security disruptions, fostering a more empowered and efficient workforce.

- **Accelerated Digital Transformation:** Sangfor Athena SASE is cloud-native by design and offers a unified network and security stack that integrates advanced security features (ZTNA, SWG, FWaaS, DLP, and EDR) with wide-area network (WAN) agility. The consistent and autonomous cloud-delivered network and security infrastructure provides an agile foundation for digital transformation initiatives like accelerated cloud migration, SaaS adoption, big data integration, etc.

- **Optimized TCO:** Sangfor Athena SASE consolidates multiple networking and security products into a single, converged, cloud-delivered platform. Customers can save on hardware, licensing, and maintenance costs as they no longer need to integrate, maintain, and troubleshoot multiple product footprints or handle multiple contract renewals and billing cycles. Try our SASE ROI calculator today and understand how Sangfor Athena SASE adds business value to your organization.

- **Seamless Geographic Expansion:** With its global backbone POP network and advanced security features, Sangfor Athena SASE enables smooth expansion to new branch locations, meeting local regulatory requirements and quickly onboarding remote employees, partners, and global customers. Sangfor Athena SASE's Cloud-Native Hyperscale Architecture ensures that your network capabilities scale seamlessly with business growth.

How does Sangfor Athena SASE ensure comprehensive security and consistent protection for users?

Sangfor Athena SASE provides comprehensive security coverage that includes data protection, threat prevention, and secure access for all users, regardless of their location. The all-in-one agent combines Zero Trust Network Access (ZTA) and Endpoint Detection and Response (EDR) capabilities, ensuring seamless and secure access to resources while maintaining device-level security.

How does Sangfor Athena SASE address the challenges faced by distributed and remote workforces?

Sangfor Athena SASE tackles the challenges faced by distributed and remote workforces by providing a unified platform that enables secure, consistent, and reliable access to applications and resources regardless of location. By implementing Zero Trust Network Access (ZTA) and Endpoint Detection and Response (EDR) capabilities, Sangfor Athena SASE ensures that remote workers have seamless and secure access to the resources they need while maintaining device-level security. This helps organizations maintain a high level of productivity and collaboration, even with a distributed workforce.

In what ways can Sangfor Athena SASE help organizations improve their overall security posture?

Sangfor Athena SASE improves the overall security of organizations by providing a comprehensive security suite that integrates multiple layers of protection. This includes a next-generation firewall, intrusion prevention, a secure web gateway, and advanced threat protection. This all-inclusive approach minimizes potential vulnerabilities and attack surfaces - reducing the likelihood of security breaches. Moreover, Sangfor Athena SASE delivers real-time threat prevention with AI-driven capabilities to ensure that organizations stay ahead of emerging cyber threats and maintain business continuity.

Can Sangfor Athena SASE be integrated with other security solutions and tools?

Yes, Sangfor Athena SASE can be integrated with various security solutions and tools - such as SIEM (Security Information and Event Management) systems and third-party NGFW via GRE Tunnel. This integration ensures better visibility, enhanced threat detection, and streamlined security management.

How does Sangfor Athena SASE support remote and mobile workers?

Sangfor Athena SASE provides secure and reliable access to cloud resources and applications for remote and mobile workers through its Zero Trust Network Access (ZTA) and Endpoint Detection and Response (EDR) capabilities. This ensures seamless and secure access to resources while maintaining device-level security, allowing employees to work efficiently from any location.

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

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

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

Yes, Sangfor 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. The comprehensive security suite and advanced features provided by Sangfor Athena SASE make it a valuable solution for any organization looking to optimize its network infrastructure and enhance security.

How does the Sangfor Athena SASE TLS/SSL decryption capability help me?

• **Increased Visibility:** Encrypted traffic, such as HTTPS or TLS, can hide potential threats and make it difficult for security solutions to detect and mitigate them. The platform has a decryption feature that allows you to inspect encrypted traffic to provide better visibility of the data flowing through your network. This allows you to identify and address malicious activity or security risks hidden within encrypted traffic.

• **Enhanced Security:** With its decryption capabilities, Sangfor Athena SASE can also inspect encrypted traffic and apply various security features. This includes a next-generation firewall, intrusion prevention, a secure web gateway, and advanced threat protection. By being able to analyze encrypted traffic, Athena SASE effectively detects and blocks threats - ensuring the safety of your critical assets and data.

• **Compliance and Data Loss Prevention:** In some industries, organizations are required to monitor and control the flow of sensitive information to maintain compliance with regulations. Sangfor Athena SASE's decryption capability allows you to inspect encrypted traffic for sensitive data, helping you to enforce data loss prevention (DLP) policies and maintain compliance with industry regulations.

• **Improved Network Performance:** By decrypting and inspecting traffic, Sangfor Athena SASE can optimize network performance by identifying and prioritizing business-critical applications, ensuring low-latency and reliable access to cloud services and applications.

How does Sangfor Athena SASE support SD-WAN applications and integrate with Sangfor Next Generation Firewall and third-party NGFW solutions for gateway connectivity between headquarters and branch offices?

Sangfor Athena SASE is designed to provide a comprehensive and flexible solution for SD-WAN use cases to ensure seamless connectivity between headquarters, branch offices, and local PoPs. The platform supports integration with both Sangfor's Next-Generation Firewall and other third-party Next-Generation Firewalls (NGFW) as gateways. This allows organizations to leverage their preferred security solutions without compromising network performance or security.

By integrating with Sangfor Next-Generation Firewall or third-party NGFW solutions, Sangfor Athena SASE can optimize network traffic routing, enhance application performance, and deliver consistent security across all locations. This ensures that organizations can effectively manage their distributed network infrastructure while maintaining a high level of security and performance across all branches and headquarters.

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

Sangfor Athena SASE is designed to help organizations comply with data protection regulations and industry standards by implementing advanced security features. These include data encryption, intrusion prevention, secure web gateway, and zero-trust network access. These features protect sensitive data and ensure privacy, allowing organizations to meet compliance requirements such as ISO27001.

What's the difference between Zero Trust Guard (ZTG) and Secured Global Access (SGA)?

- **Different Features:** ZTG and SGA are two different modules within Sangfor Athena SASE. While ZTG is a Zero Trust Network Access solution focused on providing secure remote access to corporate applications and resources including Web Apps, Cloud apps, TCP/UDP Apps, SGA is mainly for security of Internet traffic, including Web security, Internet access control, threat protection, and more.
- **Different Deployment Methods:** SGA is a pure cloud-based deployment solution, which means that users can directly connect to the SGA service within Athena SASE and then securely access the Internet through software clients or gateway devices. While ZTG is a hybrid solution that is hosted as a service in cloud, it also requires additional connectors (software) to establish connectivity to private applications hosted in an organization's data center or cloud (IaaS or PaaS).
- **Different Security Policies:** The security policies of SGA and ZTG are also different. SGA is mainly focused on Internet security based on Web threat (SWG), Internet threat intelligence, FWaaS (cloud IPS), and behavioral analysis to defend against threats. However, ZTG mainly provides security protection to internal applications hosted in an organization's data center or cloud (IaaS or PaaS) through granular user access control and application segmentation - to avoid horizontal proliferation of threats.
- **Different Uses:** SGA is suitable for organizations that need to protect Internet traffic - including branch offices, mobile users, and more. ZTG is more suited to organizations that need to provide secure remote access to internal applications and services - including ERP, CRM, financial systems, and more. Note that SGA and ZTG can be used as standalone product components or together as an integrated solution to provide more comprehensive security protection.

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

Zero Trust Guard (ZTG) is a cloud delivered Zero Trust Network Access (ZTNA) solution that works on the principle of "Never Trust Always Verify". It enables secure and adaptive access to private applications that are hosted in public clouds or enterprise data centers. While traditional VPNs provide broad network access based on location or device, ZTG grants access to specific applications based on user identity, device posture, and context. By following the principle of least privilege, it reduces the risk of lateral movement within the network while enhancing user experience and simplifying IT management.

How does Zero Trust Guard (ZTG) simplify network and security infrastructure of an organization?

• **Centralized Policy Management:** ZTG provides an intuitive cloud-based centralized security infrastructure that allows for the creation of security policies across the entire network, making it easier to manage and update security protocols.

• **Quick and Flexible Deployment:** ZTG is a cloud-native service offering one-click provisioning and easy scalability to accommodate flexible business needs without any significant infrastructure changes.

• **Ecosystem Integration:** ZTG is designed to complement and integrate with existing security tools such as IAM systems, VPNs, single sign-on (SSO), multi-factor authentication (MFA), and security information and event management (SIEM) systems.

How does ZTG enhance security compared to traditional network security models like VPN and helps to meet regulatory standards?

• **Reduced Attack Surface:** ZTG hides applications and resources from unauthorized users, making it harder for attackers to find and exploit vulnerabilities.

• **Continuous Verification:** ZTG continuously monitors and verifies user credentials, device posture, and environment reducing the risk of compromised accounts being used for malicious activities.

• **Granular Access:** ZTG enforces strict context-aware access controls by providing access only to specific isolated application or resources, limiting the lateral movement of the attacker. Even if an attacker gains access, they cannot easily move to other applications or resources.

• **Meet regulatory standards:** ZTG helps organizations meet compliance requirements by ensuring secure access control, maintaining detailed audit logs, and providing tools to enforce and monitor security policies in line with standards like GDPR, HIPAA, and PCI DSS.

How does ZTG improve the remote access experience of devices that are corporate managed or BYOD?

ZTG is designed to provide best in class end-user experience by enabling fast, secure access to applications without the need for complex VPN connections. It routes traffic efficiently via Sangfor Global POP Infrastructure and reduces latency.

• ZTG supports a variety of devices and operating systems, well-suited for remote and mobile users, offering secure, consistent access to applications from any location and any device managed or BYO.

• ZTG supports seamless authentication and single sign-on (SSO) for ease of use. It dynamically adapts to the context of each access request, ensuring secure connections without compromising user experience.