Unlocking The Secrets Of Sangfor Access Secure

Your Ultimate FAQ Guide

What is Sangfor Access Secure?

Sangfor Access Secure is a Secure Access Service Edge (SASE) solution that combines network security and SD-WAN (Software Defined Wide Area Network) capabilities into a single, cloud-based service. It aims to provide secure and efficient access to cloud resources, applications, and services for both on-premises and remote users.

What are the key features and benefits of using Sangfor Access Secure?

Some of the key features and benefits of Sangfor's Access Secure platform include:

• **Comprehensive Security Suite with an All-in-One Agent:** The Sangfor Access Secure platform offers a robust, all-inclusive security suite that includes a next-generation firewall, intrusion prevention, secure web gateway, advanced threat protection, and more. For BYOD users, Sangfor Access Secure features an all-in-one agent that combines Zero Trust Network Access (ZTA) and Endpoint Detection and Response (EDR) capabilities to ensure seamless and secure access to resources while maintaining device-level security.

• **Enhanced User Experience with Sangfor's Digital Experience Monitoring (DEM):** Sangfor Access Secure prioritizes user experience by leveraging its cutting-edge Digital Experience Monitoring (DEM) technology. This powerful solution continuously monitors and optimizes network performance, ensuring low-latency and reliable access to cloud services and applications.

• **80% TCO Reduction with Proven Cost Savings:** Sangfor Access Secure significantly reduces the Total Cost of Ownership (TCO) by up to 80%. By consolidating multiple network functions and security services into a single platform, organizations can save on hardware, licensing, and maintenance costs.

How does Sangfor Access Secure ensure comprehensive security and consistent protection for users?

Sangfor Access Secure platform 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 Access Secure address the challenges faced by distributed and remote workforces?

Sangfor Access Secure 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 Access Secure 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's Access Secure platform help organizations improve their overall security posture?

Sangfor Access Secure 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 Access Secure 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's Access Secure platform be integrated with other security solutions and tools?

Yes, Sangfor Access Secure can be integrated with various security solutions and tools - such as SIEM (Security Information and Event Management) systems and other 3rd party NGFW via GRE Tunnel. This integration ensures better visibility, enhanced threat detection, and streamlined security management.

How does Sangfor Access Secure support remote and mobile workers?

Sangfor Access Secure 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 Access Secure customers?

Sangfor offers dedicated support and professional services to help organizations optimize their Sangfor Access Secure 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 while using Sangfor's Access Secure platform.

Is Sangfor Access Secure suitable for organizations of all sizes and industries?

Yes, Sangfor Access Secure 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 Access Secure make it a valuable solution for any organization looking to optimize its network infrastructure and enhance security.

How does the Sangfor Access Secure 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 Sangfor Access Secure 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 Access Secure 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, Sangfor's Access Secure platform can effectively detect and block 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 Access Secure'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 Access Secure 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 Access Secure maintain compliance with data protection regulations and industry standards?

Sangfor Access Secure 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.

How does Sangfor's Access Secure platform 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 Access Secure 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 Access Secure 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.

What's the difference between Enterprise Private Access (EPA) vs Secured Global Access (SGA)?

• **Different Features:** SGA is mainly for the security of Internet traffic, including Web security, Internet access control, threat protection, and more. EPA, on the other hand, is mainly for the security of on-premises applications and services - such as multi-cloud connectivity, application access control, application health check, and more.

• **Different Deployment Methods:** SGA is a cloud-based deployment pattern which means that users can directly connect to cloud SASE services and then securely access the Internet through software clients or gateway devices, Sangfor PoPs around the world can provide security protection for users. EPA also requires additional application connectors (software) to connect to the organization data centre or cloud (IaaS or PaaS) to provide protection within the organization.

• **Different Security Policies:** The security policies of SGA and EPA are also different. SGA is mainly based on Web threat (SWG), Internet threat intelligence, FWaaS (cloud IPS), and behavioural analysis to defend against threats. However, EPA mainly provides internal security protection 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. EPA is more suited to organizations that need to protect internal applications and services - including ERP, CRM, financial systems, and more. Note that SGA and EPA can be used as standalone product components or together as an integrated solution to provide more comprehensive security protection.