

QAX Secure SD-WAN

Empowering Cybersecurity with Cutting-Edge Innovations

As businesses expand with more branches, the complexity of networking between these branches and the headquarters increases. This also makes security operations particularly challenging, leading to increased costs for customers.

QAX Secure SD-WAN enables flexible and secure networking between branches and headquarters using cost-effective internet access. Centralized administrators at headquarters can efficiently manage and control devices across all branch locations.

QAX Secure SD-WAN

QAX Secure SD-WAN provides wide area security networking solution for users in multi-branch, data center interconnection, hybrid cloud and other scenarios with Network as a Service (NaaS) and Security as a Service (SaaS).

QAX Secure SD-WAN consists of two parts, secure network routing gateway and control platform. The control platform is centrally deployed in the enterprise headquarters or data center, and is responsible for the unified control and management of the security gateway.

Through flexible, convenient and on-demand network connectivity and elastic deployment security capability, it makes network more secure and security more intelligent.

"QAX secure SD-WAN helped us a lot by zero-configuration deployment, centralized management platform for unified configuration distribution, achieving consistent operation and management of all network devices, which has been extremely beneficial for us. I am impressed by the experience with this solution as it makes management more convenient and reduces operational costs."

Wei Yao—Senior Director of infra Security, Overseas Chinese Town Corporation Limited.

Benefits

Improve Business Experience

Utilizing intelligent features based on automated deployment to automatically optimize network paths as needed, enhancing business continuity.

Ensure Business Security

Comprehensive authentication and permission control for users, businesses, etc., providing network attack protection, intrusion defense, virus protection, and URL filtering.

Reduce TCO

Zero-configuration deployment, automated operations, and optimized management console can significantly enhance operational efficiency, leading to a substantial cost reduction.

How It Works



Self-Organizing Networks

Utilizes PrivateEX enhanced isolation technology to help enterprise customers establish secure and available corporate networks as needed.



Intelligent Path

Utilizes WKSP intelligent routing technology to achieve multi-path protection, multi-path load balancing, and application-based path selection.



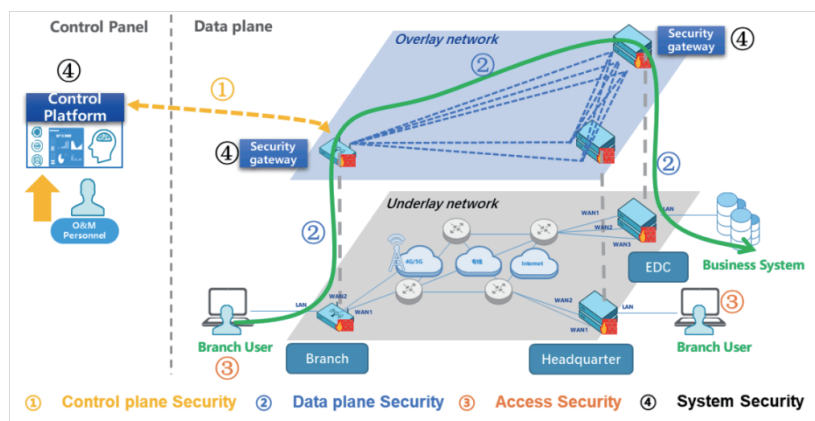
Comprehensive Inspection

Provides deep application identification and threat analysis, supporting advanced security functions such as vulnerability protection, CC protection, virus protection, URL filtering.



Centralised Management

Enables unified management, automated operation and maintenance, with centralised visual management for network, business, and threat management.



QAX Advantages

On Demand Customization

Customized for security on demand and allow flexible changes, issuing network-wide security access control policies from a unified control platform.

Security Integration

Integrates networking technology with security capabilities, leveraging rich security big data to provide secure protection and assurance for enterprise business system access and data security.

Efficient Protection

Utilizes patented application identification technology to achieve precise business awareness, combining business quality requirements and link quality monitoring, and adjusting traffic as needed.

Smooth Transition

Compatible with traditional standard IPsec VPN networking environments, minimizing the business impact of network transformation.

About QAX

QAX, the largest cybersecurity company in China, is a leader in global cybersecurity industry, offering next-generation enterprise and national-level solutions. As the official cybersecurity and antivirus software sponsor for the Beijing 2022 Olympic and Paralympic Winter Games, QAX successfully ensured the event's security with unprecedented "Zero Incident" record.

System Requirements

Hardware system architecture support

X86&ARM

Virtualization Technology Support

KVM&Xen&Hyper-V&VMware