ZTNA de Seqrite

SEQRITE

Asegurando el acceso de los usuarios a
las aplicaciones empresariales
en espacios de trabajo sin fronteras.

www.seqrite.com

¿Por qué deben las organizaciones proteger el acceso de los usuarios a través de espacios de trabajo sin fronteras?

En las empresas sin fronteras de hoy en día, los perímetros empresariales tradicionales se están desvaneciendo a medida que las colaboraciones en múltiples nubes se convierten en algo habitual. Salvaguardar los datos confidenciales frente a las amenazas en evolución supone un reto importante para los responsables de seguridad, a medida que los espacios de trabajo híbridos se convierten en la nueva norma.

Las medidas de seguridad convencionales, como las VPN y los perímetros empresariales, son inadecuadas para las exigencias de colaboración de las fuerzas de trabajo modernas. El BYOD y los dispositivos no gestionados introducen nuevas vulnerabilidades, agravadas por los datos dispersos entre plataformas. Los privilegios de acceso en la configuración actual se convierten en el vector de amenaza más importante para cualquier organización, lo que exige la adopción de un modelo de seguridad moderno que se adapte a los lugares de trabajo híbridos y verifique el acceso independientemente de la ubicación, el usuario o el dispositivo.

Presentamos el ZTNA de Seqrite

El ZTNA de Seqrite es una solución Acceso a la red SaaS de confianza cero que proporciona a los empleados acceso remoto seguro a las aplicaciones y servicios corporativos,contratistas y personal de proveedores a través de espacios de trabajo sin fronteras.

Enfoque holístico de confianza cero: ¡seguridad para un mundo nuevo!

01 **Tenga en cuenta el acceso de los usuarios en espacios de trabajo sin fronteras– Con el acceso a la red de confianza cero de Seqrite**

Permite a su organización aplicar un paradigma de acceso a la red de confianza cero a cualquier empleado, contratista o proveedor con acceso a sus sistemas y aplicaciones, ya sea desde dentro o fuera de la red corporativa. Utiliza políticas contextuales, procesos y un enfoque tecnológico para detener el acceso no autorizado.

02 **Adopte el conocimiento de confianza cero**

Autentica cada intento de acceso realizado por empleados, contratistas o proveedores a las aplicaciones críticas de la empresa. Aprovecha la aplicación basada en atributos de usuario, dispositivos, ubicaciones, detalles de red y otros identificadores antes de dar acceso a las aplicaciones empresariales.

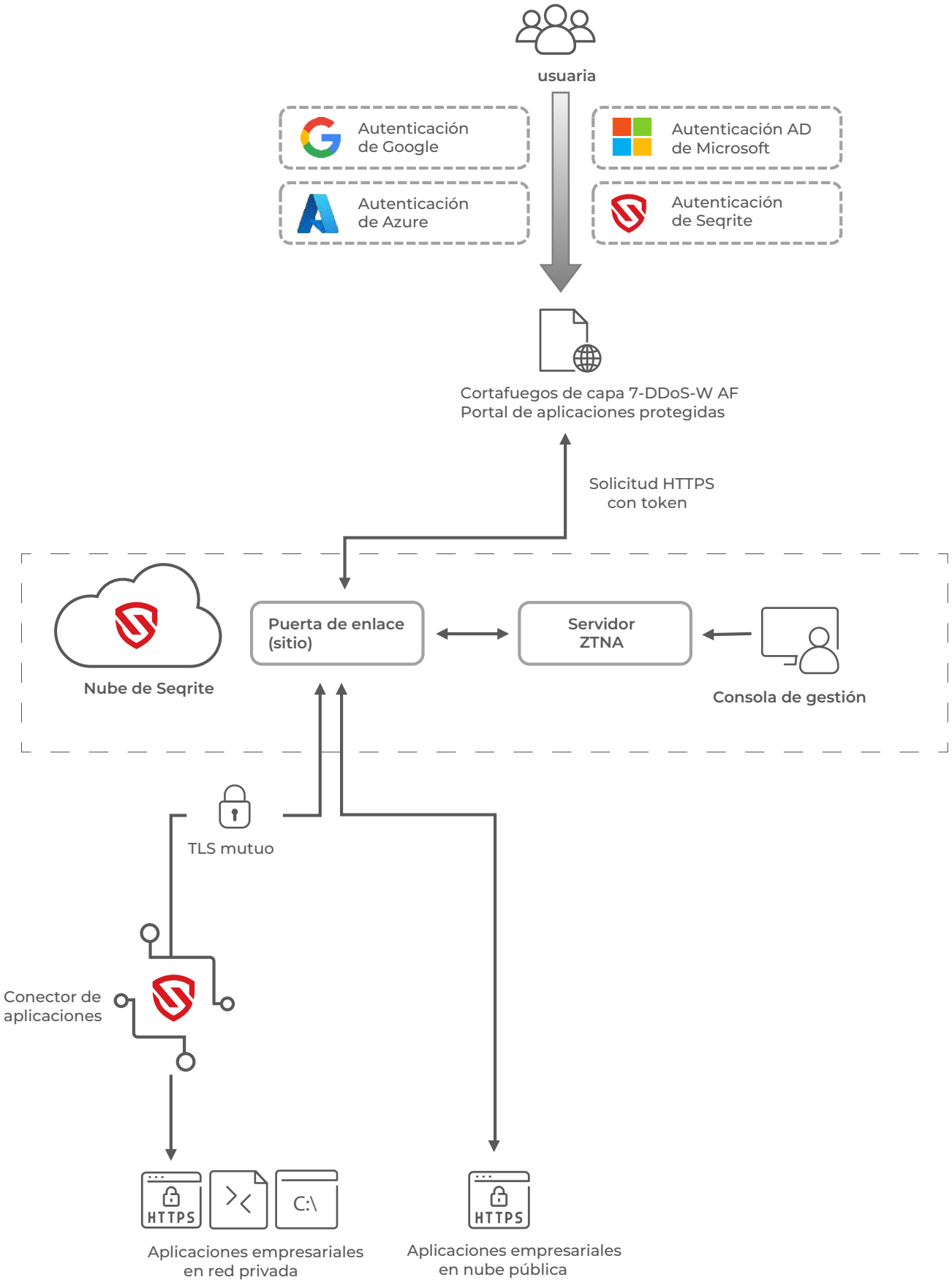
03 **Adopte el principio del menor privilegio**

Se adapta al mundo actual del «trabajo desde cualquier sitio». Aprovecha el principio del menor privilegio y desplaza el centro de atención de la seguridad de las redes al acceso de las aplicaciones con menos privilegios a los usuarios autenticados.

04 **Adopte una postura de seguridad integrada**

Se integra con soluciones a través de su pila de seguridad para fortalecer eficientemente la postura de seguridad integrada de su organización. Los clientes existentes de la plataforma CSM de Seqrite, es decir, Privacidad de datos, XDR y Nube EPP, pueden utilizar el ZTNA de Seqrite para proporcionar acceso seguro a las aplicaciones a sus usuarios finales.

Cómo funciona el ZTNA de Seqrite



¿Por qué su empresa necesita el ZTNA de Seqrite?

Incorporación rápida y sencilla:

- Prepárese para la implantación en pocos minutos.
- Empiece con unos pocos usuarios y aplicaciones y amplíelos gradualmente.
- Integración sencilla con la infraestructura de TI existente para la gestión de identidades.

Cero confianza visual para administradores:

- Vistas gráficas enriquecidas para demostrar cómo acceden los usuarios a las aplicaciones corporativas.

Gestión de políticas simplificada:

- Utilice etiquetas empresariales aplicadas a usuarios y aplicaciones para definir políticas que faciliten el proceso de cambios de usuario en su empresa.

Aumente la eficiencia de su sucursal:

- Mejore el rendimiento de su sucursal sin arruinarse.
- Al eliminar gradualmente la conmutación por etiquetas multiprotocolo (MPLS) y cambiar al acceso a aplicaciones a través de Internet como medio de transporte, puede disfrutar de una solución rentable sin sacrificar el rendimiento.

Reduzca la complejidad y mejore la seguridad:

- Simplifique su infraestructura tecnológica y minimice la deuda técnica adoptando un modelo de acceso seguro centrado en usuarios y aplicaciones.
- Con esta innovadora solución, puede agilizar sus procesos, reducir la complejidad y mejorar la seguridad, al tiempo que minimiza los costes.

Lo más destacado del producto

Gestión de identidades

- Intégrese con sus IdP de nube existentes, como Google Workspace, Microsoft Azure.
- Conéctese con servidores Active Directory 2012/16/19/ADFS o Gestión de Usuarios Locales a través de la Gestión de Seguridad Centralizada de seguridad centralizada de Seqrite.
- Autenticación basada en contraseña sin OTP para la base de datos de usuarios local.

Acceso a aplicaciones

- Opciones de acceso sin agente y con agente para aplicaciones con protocolos: HTTP, HTTPS, RDP, SSH, Telnet, VNC, FTP, SMB, etc.
- Autenticación segura de aplicaciones y acceso a aplicaciones SaaS como Office365, Google Workspace, Zoho, Zoom, Salesforce, etc.
- Acceso sin fisuras a aplicaciones de red que incluyen compatibilidad con los protocolos TCP y UDP. (Disponible como paquete de licencia adicional)

Políticas de Confianza Cero.

- Política de Confianza Cero para definir qué usuario(s) tiene(n) acceso a qué aplicación(es) con un enfoque de denegación por defecto.
- Política de cortafuegos de capa 7 para bloquear el tráfico procedente de IP/países no deseados y permitir sólo el necesario.
- Política DDoS de Capa 7 para permitir sólo un cierto número de peticiones en cada periodo de tiempo y denegar el resto.
- La Evaluación de la postura del dispositivo se basa en múltiples factores para conceder acceso a los dispositivos correctos.

Controles granulares sobre las aplicaciones

- Disposición para restringir las sesiones de escritorio remoto a una aplicación limitada; otorgando acceso a aplicaciones remotas en lugar de exponer todo el servidor.
- Restricciones de acceso al portapapeles y transferencia de archivos.
- Consulte la actividad del usuario mediante grabaciones de sesiones de la aplicación.
- Reglas WAF para proteger aplicaciones críticas para el negocio de ataques de capa 7, como inyecciones de SQL, secuencias de comandos entre sitios, inyecciones de comandos del sistema operativo, acceso a recursos del sistema e inyecciones de plantillas del lado del servidor.

Modelo de licencia para el ZTNA de Seqrite

Característica Nombre	EDICIÓN DE PRUEBA 30-días	EDICIÓN ESTÁNDAR 1 años/3 años	EDICIÓN EMPRESA 1 años/3 años
Descripción	Pruebe el acceso remoto seguro GRATIS durante 30 días Conecte sus propios usuarios, aplicaciones y servicios.	Acceso remoto seguro para pequeñas y medianas empresas	Acceso remoto seguro para grandes empresas
Precio	GRATIS durante 30 días	Suscripción anual $	Suscripción anual $$$
Acceso remoto:			
Portal de administración de la nube	SÍ	SÍ	SÍ
Número de sitios	1 sitio	1 sitio	1 sitio
Número de grupo del conector de aplicaciones	1 grupo	Hasta 3 grupos	Ilimitada
Admite acceso remoto seguro sin agente y basado en agente	SÍ	SÍ	SÍ
Compatibilidad con aplicaciones de red (incluye ambos protocolos TCP-UDP)	NO	Complemento	Complemento
Configuración:			
Admite un dominio personalizado para el portal en la nube de aplicaciones de usuario	SÍ Requiere verificación DNS por parte del cliente	SÍ Requiere verificación DNS por parte del cliente	SÍ Requiere verificación DNS por parte del cliente
Número de aplicaciones y servicios	Hasta 10 aplicaciones y servicios	Hasta 100 aplicaciones y servicios	Ilimitada
Admite la grabación de sesiones de aplicaciones para WebRDP, WebSSH, WebTelnet y WebVNC	NO	Complemento	Complemento
Número de usuarios para el portal de usuarios en la nube (empleados, contratistas, proveedores)	Hasta 10 usuarios	Hasta 1000 usuarios	Ilimitada
Número de puntos finales con agente ZTNA	Hasta 30 usuarios	Hasta 500 usuarios	Ilimitada
Retención de registros:			
Número de días durante los cuales nube, sistema y registros de aplicaciones se conservarán	Hasta 30 días	Hasta 180 días	Hasta 180 días
Número de días que se conservará el rastro de auditoría	Hasta 180 días	Hasta 180 días	Hasta 180 días

Acerca de Seqrite

Seqrite es un proveedor líder de soluciones de ciberseguridad empresarial. With a focus on simplifying cybersecurity,Seqrite delivers comprehensive solutions and services through our patented, AI/ML-powered tech stack to protect businesses against the latest threats by securing devices, applications, networks, cloud, data, and identity. Seqrite es el brazo empresarial de la marca mundial de ciberseguridad Quick Heal Technologies Limited, la única empresa de productos y soluciones de ciberseguridad que cotiza en bolsa en la India.

En la actualidad, más de 30 000 empresas de más de 76 países confían sus necesidades de ciberseguridad a Seqrite.

SEQRITE | Quick Heal Technologies Limited
Teléfono: 1800-212-7377 | info@seqrite.com | www.seqrite.com |
/seqrite

Todos los derechos de propiedad intelectual, incluidas las marcas comerciales, los logotipos y los derechos de autor, pertenecen a sus respectivos
Copyright © 2024 Quick Heal Technologies Ltd. Todos los derechos reservados.