APPGATE SDP
ZERO TRUST NETWORK ACCESS (ZTNA) UNIVERSAL

Visión general de la solución

Appgate SDP es una solución de Zero Trust Network Access Universal (ZTNA) líder en la industria que aborda los retos de seguridad de las fuerzas de trabajo distribuidas modernas. Proporciona un control de acceso granular y contextualizado para infraestructuras en la nube e híbridas, garantizando una seguridad robusta sin comprometer la flexibilidad. Appgate SDP utiliza un modelo de perímetro definido por software, creando conexiones de red dinámicas 1:1 entre usuarios/dispositivos y los recursos específicos que necesitan. Este enfoque ofrece una arquitectura escalable, distribuida y de alta disponibilidad con enrutamiento directo, optimizada tanto para la seguridad como para el rendimiento en entornos híbridos y de nube, permitiendo un acceso granular a los recursos de red "segmento-de-uno".

Componentes clave

1. **Controlador:** Punto de decisión de políticas
2. **Gateway:** Punto de aplicación de la política
3. **Cliente:** Software del dispositivo del usuario final
4. **Conector:** Dispositivo multicliente para la gestión del tráfico de recursos locales

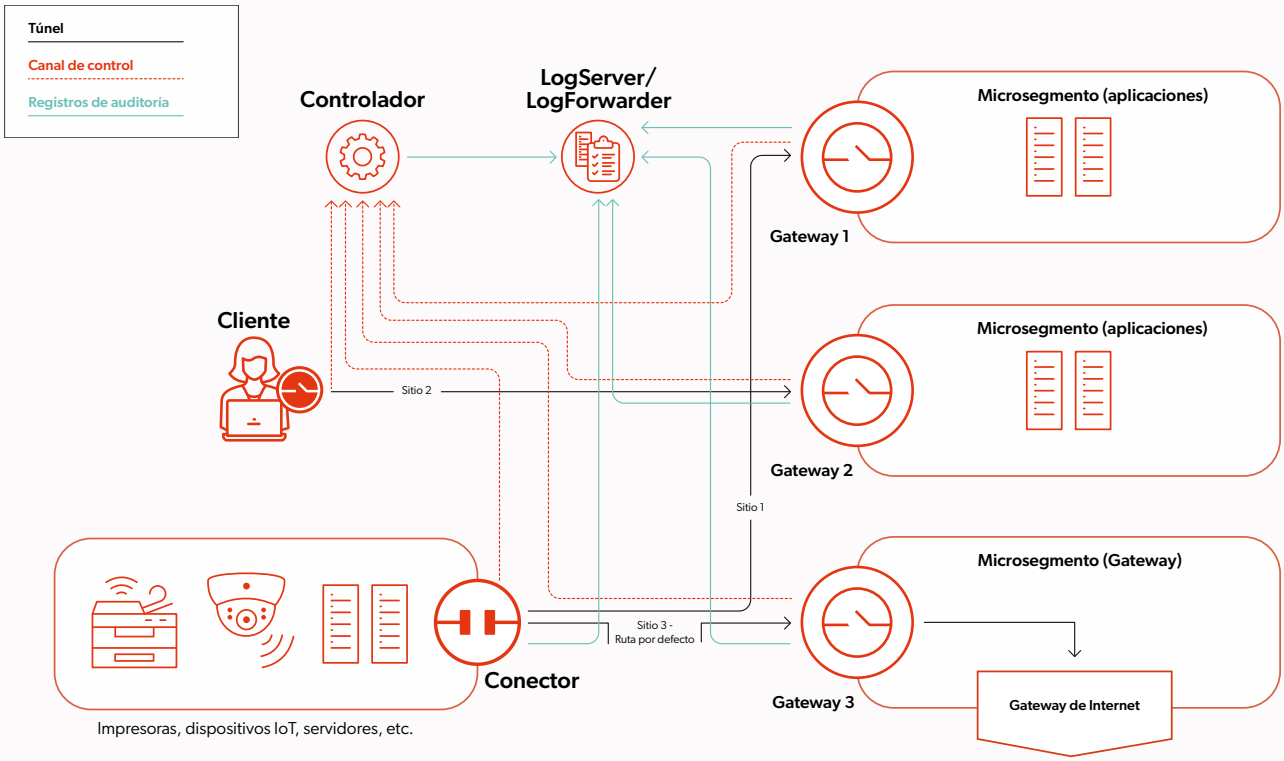
Especificaciones técnicas

- **Authenticación:** Algoritmos basados en PKI para relaciones de confianza entre componentes
- **Control de acceso:** Evaluación de políticas en tiempo real basada en atributos de usuario, entorno e infraestructura
- **Seguridad de red:** Túneles seguros establecidos a través del controlador de red del cliente
- **Compatibilidad:**
  - **Proveedores de identidad (IdPs):** Appgate SDP es independiente de los IdP y admite la autenticación a través de IdP externos LDAP (AD), certificados LDAP, OIDC, RADIUS y SAML.
  - **Soporte OS:** Todos los principales sistemas operativos de escritorio, servidores y móviles
  - **Infraestructura:** Todas las principales plataformas de nube y virtualización

Appgate SDP proporciona ZTNA Universal a todos los usuarios, independientemente del dispositivo o la ubicación, ya sea local o remoto, a través de un modelo de política unificado. La solución crea dinámicamente conexiones individualizadas y seguras entre usuarios y recursos basadas en la identidad y el contexto verificados. Single Packet Authorization (SPA) hace que la red sea invisible cuando no hay puertos expuestos, permitiendo el acceso al canal de comunicación sólo a los usuarios validados criptográficamente con un SPA. Appgate SDP aplica el principio de mínimo privilegio estableciendo micro firewalls basados en sesiones y justo a tiempo para microsegmentar usuarios, cargas de trabajo y recursos. Los derechos dinámicos en tiempo real modifican el acceso en función del contexto y el riesgo. Con Appgate SDP, las organizaciones tienen un control total sobre cómo viajan los datos a través de su infraestructura de red.

CARACTERÍSTICAS PRINCIPALES:

1. **Modelo de confianza avanzado:** Implementa un modelo de confianza único de seis capas, ampliando la seguridad más allá de la autenticación inicial para verificar el acceso en el punto de conexión de recursos.
2. **Control de acceso inteligente:** Utiliza un sistema controlador para autenticar usuarios y dispositivos en función de múltiples factores, emitiendo tokens de derechos para una gestión precisa del acceso.
3. **Acceso basado en navegador:** Ofrece un portal para el acceso sin Cliente a través de navegadores web, manteniendo el mismo nivel de seguridad que el Cliente completo.
4. **Integración de dispositivos IoT y heredados:** Incorpora un componente conector para integrar y gestionar de forma segura el acceso de varios dispositivos, desde sensores hasta servidores.
5. **Microfirewalls dinámicos:** Crea instancias de firewalls individuales para cada sesión, garantizando el control granular y la invisibilidad de los recursos protegidos.
6. **Acceso simplificado a recursos remotos:** Permite una fácil integración de recursos distribuidos a través de conectores, requiriendo únicamente una conexión saliente en el puerto 443.
7. **Auditoría exhaustiva:** Incluye un LogForwarder para un registro de auditoría flexible y potente, compatible con las necesidades de cumplimiento y supervisión de la seguridad.
8. **Despliegue flexible:** Funciona independientemente de los perímetros de red tradicionales, aprovechando la virtualización de software para una integración perfecta en entornos de nube e híbridos.



La arquitectura distribuida de Appgate SDP ofrece la flexibilidad de desplegar dispositivos donde sea necesario; cada dispositivo es una máquina sin estado y puede configurarse para ofrecer diferentes funciones: Controlador, Gateway, LogServer, LogForwarder, Metrics Aggregator, Portal o Conector.

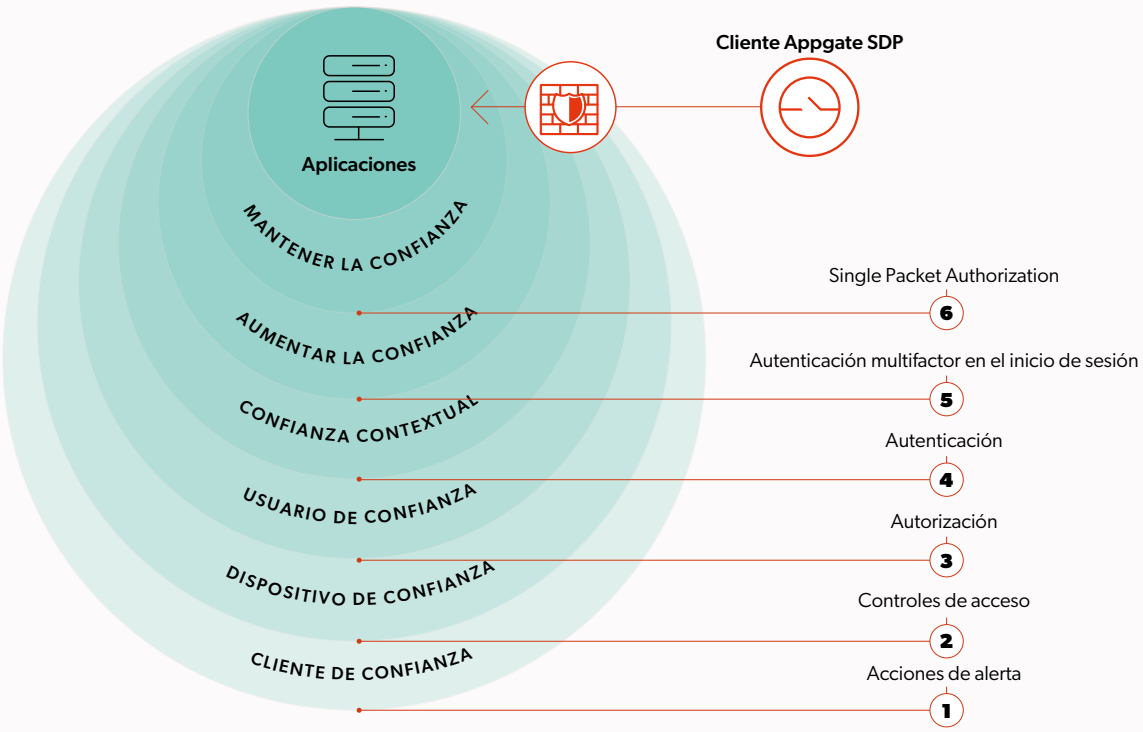
Flujo operativo

1. La autenticación del cliente se envía al controlador.
2. El controlador emite un token firmado criptográficamente con recursos autorizados.
3. El cliente establece túneles seguros y reglas de enrutamiento.
4. El Gateway aplica comprobaciones de acceso condicional en tiempo real.
5. El acceso se concede a través de un túnel seguro: Cliente ⇢ Gateway ⇢ Servidor.
6. LogServer registra todos los eventos de acceso.
7. Opcional: LogForwarder se integra con sistemas SIEM/IDS.

Establecimiento de la confianza: El modelo de seis capas

Appgate SDP utiliza un modelo de autorización multicapa para proporcionar un control en tiempo real y adaptado al contexto sobre todos los intentos de acceso de los usuarios. Los números que aparecen a continuación corresponden a las capas del proceso en el diagrama siguiente.

1. **Single Packet Authorization (SPA):** SPA hace que el sistema Appgate SDP (es decir, los componentes/la infraestructura) sea invisible para los usuarios no autorizados, permitiendo únicamente a los clientes con la clave precompartida.
2. **Autenticación multifactor (MFA) en el inicio de sesión:** El registro del dispositivo de un usuario sirve como segundo factor de autenticación (de confianza), mejorando la seguridad al bloquear intentos de acceso no autorizados con credenciales robadas. Se puede utilizar cualquier MFA configurado y, una vez registrado un dispositivo (o navegador), elimina la necesidad de que los usuarios realicen la MFA en cada inicio de sesión.
3. **Autenticación:** Esta capa valida las credenciales del usuario y del dispositivo frente a fuentes de confianza definidas, como SAML y OIDC.
4. **Autorización:** Los criterios de asignación de políticas evalúan los atributos del usuario/dispositivo, permitiendo asignar un conjunto específico de derechos a cada usuario/dispositivo..
5. **Controles de acceso:** Esta capa compara el tráfico de usuario con los derechos, aplica la política de acceso, verifica las condiciones de acceso y solicita al usuario que actúe (por ejemplo, MFA) cuando sea necesario. Appgate SDP gestiona dinámicamente el acceso para cada usuario/dispositivo basándose en el host, el puerto y el protocolo del recurso protegido definido en los derechos.
6. **Acciones de Alerta:** Esta capa actúa como un sistema de activación que bloquea y registra con una alerta los comportamientos de alto riesgo, como los escaneos de puertos no autorizados, para abordar proactivamente las amenazas potenciales.



El modelo de confianza de seis capas de Appgate amplía la seguridad más allá de la autenticación inicial, verificando continuamente el acceso en el punto de conexión de los recursos.

Especificaciones de seguridad

- **SPA:** Utiliza el cifrado AES-256-GCM para mejorar la seguridad.
- **Certificado de dispositivo:** Generado por el controlador utilizando SHA512 con cifrado RSA, tamaño de clave 4096. Actúa como una autoridad de certificación con restricciones estrictas para garantizar una comunicación segura entre el controlador y el cliente.
- **Cifrado de reclamaciones y tokens de derechos:** Utiliza el cifrado AES-256-CTR para proteger los tokens.
- **Cifrado de bases de datos:** Utiliza el cifrado AES-256-CTR para proteger los datos almacenados.
- **Cifrado de archivos de copia de seguridad:** Protegido con cifrado simétrico GPG (AES-256-CFB) para garantizar la integridad y confidencialidad de los datos.
- **Conformidad con FIPS:** Para clientes de escritorio, Appgate SDP cumple con los estándares FIPS 140-3, aprovechando el módulo wolfCrypt.

Protocolos de comunicación y cifrado

- **TLSv1.3:** Protocolo predeterminado para todas las comunicaciones, con TLSv1.2 como alternativa cuando sea necesario..
- **Comunicación entre dispositivos:** Protegida mediante cifrados TLS13-AES256-GCMSHA384 y ECDHE-RSA-AES256-GCM-SHA384, con autenticación mutua basada en certificados y comprobación de DN.
- **Comunicación entre el cliente y el administrador y el dispositivo:** Utiliza por defecto los cifrados TLS13-AES256-GCMSHA384 y ECDHE-RSA-AES-256-GCM-SHA384.
- **SSH a dispositivo:** Admite los cifrados AES-256-CTR, AES-192-CTR y AES-128-CTR.
- **Túnel de cliente a pasarela:** Utiliza cifrados TLS13-AES256-GCM-SHA384 y ECDHE-RSAAES256-GCM-SHA384 con autenticación mutua basada en certificados.

CAPACIDADES CRÍTICAS

- **Compatibilidad con MDM:** Para gestionar dispositivos móviles de forma segura.
- **VPN multitúnel:** Permite varias conexiones VPN simultáneas.
- **Compatibilidad con IPv6:** Garantiza la compatibilidad con redes IPv6.
- **Servicio Health Check Probe:** Para supervisar y mantener la salud del sistema.
- **Agregador de métricas y exportador Prometheus:** Para recopilar y exportar métricas del sistema.
- **Compatibilidad con protocolos proxy:** Mejora la compatibilidad con servidores proxy.
- **SPA:** Añade una capa adicional de seguridad ocultando la infraestructura de red subyacente.
- **Alta disponibilidad:** Garantiza la fiabilidad y el tiempo de actividad del sistema.
- **Compatibilidad multisitio:** Permite el despliegue de Appgate SDP en múltiples ubicaciones geográficas.
- **Firewall por usuario:** Proporciona un control de acceso granular basado en perfiles de usuario individuales.
- **Equilibrio de carga:** Distribuye el tráfico entre varios servidores para garantizar un rendimiento óptimo.
- **Llamadas REST externas en scripts de criterios:** Permite tomar decisiones dinámicas de control de acceso basadas en datos externos.

Integraciones tecnológicas

- **Endpoint Detection and Response (EDR):** CrowdStrike y SentinelOne
- **Gestión de servicios de TI (ITSM):** ServiceNow
- **Microsegmentación:** Illumio y ColorTokens
- **Gestión de incidentes y eventos de seguridad (SIEM):** Splunk, Sumo Logic, Falcon LogScale, Elasticsearch, OpenSearch, DataDog, Coralogix, Azure Monitoring, AWS Kinesis, así como cualquier herramienta SIEM que acepte el reenvío TCP.

Servicios en la nube de valor añadido

La plataforma Zero Trust (ZTP) de Appgate es una solución nativa en la nube que mejora las capacidades de Appgate SDP, ofreciendo un marco sólido para implementar ZTNA en diversos entornos de TI. Presenta modelos de despliegue flexibles, un motor de políticas unificado con control de acceso centrado en la identidad y una segmentación dinámica de la red que impone el acceso con menos privilegios. ZTP proporciona autenticación y autorización multifactor continua, adaptándose al comportamiento del usuario y a la postura del dispositivo en tiempo real. Con cobertura universal de recursos, ofrece políticas coherentes de Zero Trust en entornos híbridos y multi-nube, mejorando significativamente la postura de seguridad al tiempo que aumenta la eficiencia operativa.

- **Detección de aplicaciones:** Application Discovery ofrece una oportunidad única para que las organizaciones pasen rápidamente del acceso remoto basado en VPN a un modelo ZTNA moderno y seguro. Esta función emplea un avanzado sistema de aprendizaje automático (ML) para observar el comportamiento del usuario y los patrones de acceso a lo largo del tiempo. Al analizar estos datos, Application Discovery genera información procesable que permite a los administradores definir y ajustar las políticas de acceso, garantizando que sólo los usuarios autorizados puedan acceder a recursos específicos alineados con los objetivos de seguridad de la organización. A medida que las organizaciones adoptan despliegues alojados o conectados, el aprovechamiento de Application Discovery puede mejorar significativamente su capacidad para responder a las cambiantes amenazas a la seguridad, preservando al mismo tiempo una experiencia de usuario continua.

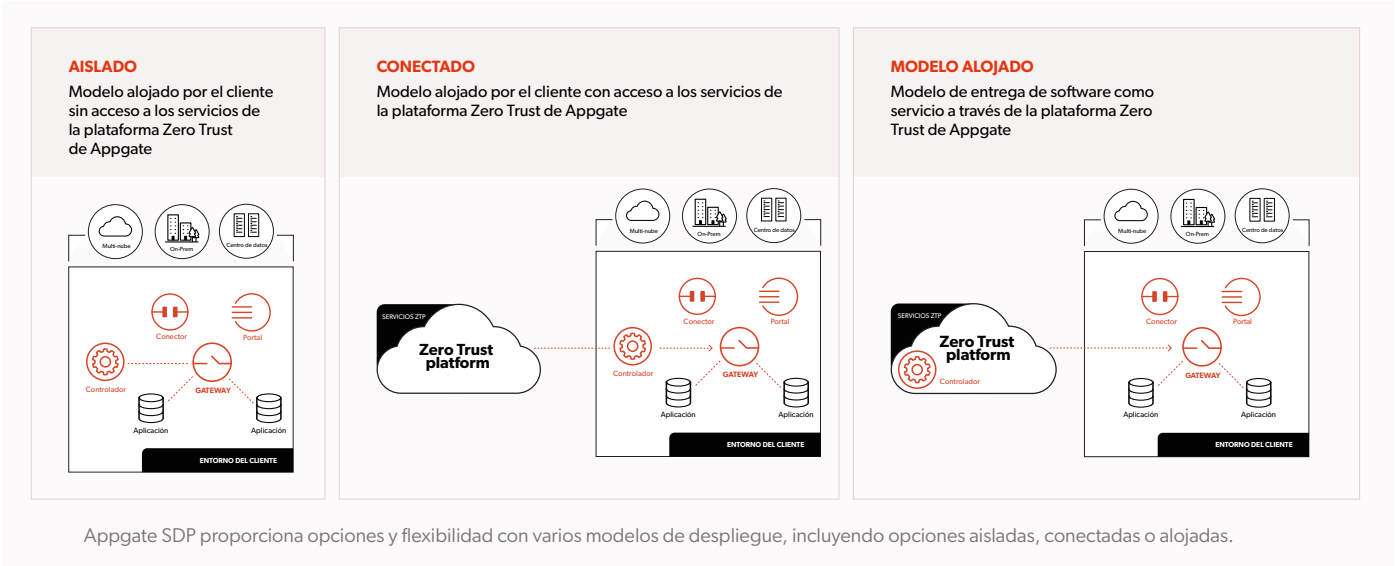
- **Motor de riesgos:** El motor de riesgos mejora las políticas de acceso con información sobre la situación de seguridad recopilada por soluciones empresariales, de seguridad y de TI de terceros. Las integraciones incorporadas con las principales herramientas de seguridad y una interfaz fácil de configurar elimina el costo y la complejidad de las secuencias de comandos API personalizadas.

- **Alertas de riesgo:** El servicio de Alerta de riesgo permite que el motor de políticas dinámicas de Appgate SDP responda a la información procedente de servicios de terceros que indican cambios en la postura de seguridad del dispositivo o del usuario.

- **Analizador de políticas:** El Analizador de Políticas es una potente herramienta diseñada para agilizar el proceso de creación y gestión de políticas. Ayuda a los administradores a reducir la superficie de ataque de su organización, al tiempo que simplifica las operaciones. Al aprovechar los datos y análisis en tiempo real, el analizador de políticas permite a las organizaciones identificar políticas y derechos que pueden retirarse de forma segura, descubre derechos con recursos superpuestos y destaca configuraciones que de otro modo podrían pasar desapercibidas. Este enfoque proactivo mejora la seguridad y simplifica el cumplimiento normativo, por lo que es un activo vital para las organizaciones en transición a un despliegue alojado o conectado.

Flexibilidad de Despliegue

Appgate SDP puede desplegarse en entornos de nube, locales e híbridos, ofreciendo una solución versátil que se adapta a las necesidades específicas de una organización. Su naturaleza definida por software permite una rápida implantación y escalabilidad sin las limitaciones de las soluciones tradicionales basadas en hardware.



Appgate SDP proporciona opciones y flexibilidad con varios modelos de despliegue, incluyendo opciones aisladas, conectadas o alojadas.

Ventajas de Appgate SDP

Maneja Entornos Complejos y Altos Requerimientos de Seguridad: Adapta la arquitectura a retos de red únicos; mantiene el control sin depender de nubes de proveedores; y aprovecha la extensibilidad para construir un ecosistema de seguridad unificado e interoperable.	**Mejora la experiencia del usuario:** Ofrece una experiencia de conectividad coherente para cualquier empleado o tercero autorizado con conexiones multitúnel directas simultáneas que proporcionan un Gateway automático y conmutación por error del sitio.
Refuerza su postura de seguridad: Oculta todos los recursos para hacer invisibles las superficies de ataque; detiene el movimiento lateral a través de un acceso de mínimo privilegio Zero Trust informado sobre el riesgo; consigue una visibilidad completa de la red; y construye una sólida base Zero Trust.	**Minimiza el tiempo de administración de TI y seguridad:** Reduce el tiempo de intervención con un motor de políticas unificado, automatiza el aprovisionamiento de acceso y minimiza las incidencias.
Revoluciona su red: Superpone la experiencia de acceso seguro universal en toda la topología; revoluciona la red con una conectividad segura tipo cafetería; y reduce los gastos operativos al eliminar los costos de conectividad redundante.	**Mejora las inversiones en tecnología:** Se integra perfectamente con una gama de herramientas de supervisión e informes estándar del sector para correlacionar de forma centralizada los riesgos y eventos de seguridad relacionados con el acceso; permite conocer la postura de seguridad mediante servicios de terceros, como la detección y respuesta de puntos finales (EDR); y mejora las políticas dinámicas de control de acceso basadas en el contexto y el riesgo.

Conclusión

Appgate SDP beneficia significativamente a las organizaciones al implementar un modelo ZTNA que autentica dinámicamente y autoriza a los usuarios en función de la identidad y el contexto, minimizando el riesgo de acceso no autorizado. Su arquitectura definida por software reduce la superficie de ataque, mientras que los controles de acceso granular mejoran la segmentación de la red y limitan el movimiento lateral dentro de la red. Las opciones de despliegue flexible en entornos híbridos, la perfecta integración con las herramientas de seguridad existentes y el robusto cifrado de extremo a extremo refuerzan aún más la seguridad y simplifican la gestión, alineándose con las modernas estrategias de seguridad Zero Trust.

Acerca de Appgate

Appgate asegura y protege los activos y aplicaciones más valiosos de una organización. Appgate es el líder del mercado en Zero Trust Network Access (ZTNA) y protección contra el fraude en línea. Los productos de Appgate incluyen Appgate SDP para ZTNA Universal y 360 Fraud Protection. Los servicios de Appgate incluyen análisis de asesoramiento sobre amenazas e implantación de ZTNA. Appgate protege a empresas y organismos públicos de todo el mundo. Más información en appgate.com.

appgate