



Niveles de suscripción a Appgate SDP

Para ofrecer más opciones y valor al cliente, Appgate SDP, la solución de Zero Trust Network Access (ZTNA) universal líder del sector, dispone de tres niveles de suscripción. Los niveles Essentials, Advanced y Enterprise permiten a nuestros clientes elegir las funciones de vanguardia, las opciones de despliegue, los servicios y el soporte que mejor se adapten a las necesidades de su organización sin sacrificar los estándares de seguridad. Es más que una suscripción... es una asociación que desbloquea un valor inigualable, permitiendo a los clientes de Appgate SDP prosperar en el dinámico panorama empresarial y de ciberseguridad actual.

Essentials

Essentials es para organizaciones que desean reforzar la seguridad del acceso remoto sustituyendo las VPN por ZTNA dinámica.

Este nivel proporciona políticas dinámicas de Zero Trust, compatibilidad con la integración de proveedores de identidad, autenticación multifactor (MFA) integrada y dos sitios, con más disponibles para la compra. La suscripción también incluye un servicio de descubrimiento de aplicaciones de 30 días que automatiza las necesidades de políticas de seguridad y acelera el camino hacia Zero Trust. Essentials utiliza un modelo de implantación alojado y actualizaciones automáticas de versiones para reducir la sobrecarga operativa, de modo que los administradores puedan gestionar identidades y políticas en lugar de la infraestructura. Se incluye asistencia al cliente estándar y se requieren servicios de implementación (Service Delivery).

Advanced

Advanced es para organizaciones que desean ampliar la implementación de ZTNA más allá de la sustitución de VPN para abordar casos de uso como el acceso de usuarios con privilegios, la protección de entornos en la nube e híbridos y mucho más.

Este nivel incluye todas las funciones de Essentials más compatibilidad con MFA por hardware, compatibilidad con clientes siempre activos y multiusuario, scripts de extensión y cinco sitios, con más disponibles para la compra, además de compatibilidad con dos proveedores de identidad. También incluye el descubrimiento de aplicaciones de servicios en la nube siempre activos y el motor de riesgo dinámico. Se asigna un Customer Success Manager dedicado y se requieren servicios de implementación (Service Delivery).

Enterprise

Enterprise es para organizaciones con requisitos de seguridad de red complejos que desean ampliar ZTNA a todos los casos de uso, incluida la sustitución de SD-WAN y NAC y la eliminación de MPLS.

Este nivel incluye todas las funciones avanzadas, además de soporte ilimitado de sitios y proveedores de identidad. También añade alertas de riesgo de servicios en la nube y un analizador de optimización de políticas, además de recuperación automática del sitio para eliminar las interrupciones del servicio, conectividad del sitio más cercano para reducir la latencia y optimización de la red local para eliminar el "hair pinning". El servicio ampliado de atención al cliente incluye un Customer Success Manager dedicado y, opcionalmente, un Technical Account Manager y un Ingeniero de Soporte. Se requieren servicios de implementación (Service Delivery).

¿Por qué Appgate SDP?

Appgate SDP proporciona ZTNA Universal a todos los usuarios, independientemente de su dispositivo o ubicación, ya sea local o remoto, a través de un modelo de política unificado. La solución crea dinámicamente conexiones individualizadas y seguras entre los usuarios y los recursos basándose 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 único paquete.

Appgate SDP hace cumplir el principio de mínimo privilegio estableciendo micro firewalls basados en sesiones justo a tiempo para microsegmentar usuarios, cargas de trabajo y recursos. Los derechos dinámicos en tiempo real modifican el acceso casi en tiempo real en función del contexto y el riesgo.

Transforma tu red, fortalece las ciberdefensas, reduce costos y aumenta la eficiencia operativa con ZTNA Universal de enrutamiento directo diseñado para entornos complejos.





Appgate SDP

Guía de empaquetado

Características	Essentials	Advanced	Enterprise
Funciones básicas			
Políticas dinámicas de Zero Trust	✓	✓	✓
Integración de proveedores de identidad	✓	✓	✓
MFA integrado	✓	✓	✓
MFA por hardware	✗	✓	✓
Cliente siempre activo	✗	✓	✓
Cliente multiusuario	✗	✓	✓
Scripts de extensión	✗	✓	✓
Sitios	2 (se pueden comprar más)	5 (se pueden comprar más)	Ilimitado
Proveedores de identidad	1	2	Ilimitado
Servicios en la nube			
Detección de aplicaciones (objetivo para finales de 2024)	30 Días	✓	✓
Motor de riesgos	✗	✓	✓
Alertas de riesgo (objetivo para principios de 2025)	✗	✗	✓
Analizador de políticas (objetivo para principios de 2025)	✗	✗	✓
Nota: Los servicios en la nube sólo están disponibles para los tipos de despliegue Alojado y Conectado.			
ZTNA universal			
Redireccionamiento automático	✗	✗	✓
Conectividad del sitio más cercano	✗	✗	✓
Optimizador de red local	✗	✗	✓
Soporte colectivo múltiple	✗	✗	✓
Tipos de despliegue			
Alojado	✓	✓	Opcional
Conectado	✗	Opcional	✓
Aislado	✗	Opcional	Opcional
Asistencia y servicios			
Asistencia al cliente	Estándar	Estándar	Estándar
Customer Success Manager asignado	✗	✓	✓
Technical Account Manager dedicado	✗	✗	Opcional
Ingeniero de soporte dedicado	✗	✗	Opcional
Servicios de implementación (Service Delivery)	Obligatorio	Obligatorio	Obligatorio



Glosario

Componentes de Appgate SDP

Appgate SDP gestiona las políticas de seguridad que controlan el acceso de los usuarios a recursos protegidos como aplicaciones y servicios. Los usuarios pueden definirse localmente con el proveedor de identidad local de Appgate o integrarse con SAML, OIDC, LDAP o RADIUS.

Appgate SDP proporciona acceso basado en el contexto utilizando el proveedor de identidad y las políticas establecidas en el controlador Appgate SDP.

Cliente

La licencia de usuario permite a un único usuario conectarse con varios dispositivos Cliente diferentes simultáneamente y utilizar una sola licencia.

Controlador

El Controlador actúa como punto de decisión de políticas (PDP) y es el “cerebro” del sistema. Se pueden desplegar hasta seis Controladores para alta disponibilidad (HA) sin costo adicional. Los clientes se autentican en el controlador, que a su vez emite tokens para los clientes.

Sitio

Un Sitio es un concepto dentro de Appgate SDP que se refiere a un grupo de redes lógicamente relacionadas que están protegidas por un Gateway (o un grupo de Gateways). Por ejemplo, un Sitio puede contener todas las redes dentro de una nube privada virtual (VPC) y los servicios alojados en ella.

Gateway

Los Gateways actúan como puntos de aplicación de políticas (PEP) que controlan y protegen el acceso a los servidores, aplicaciones y recursos protegidos. Pueden desplegarse múltiples Gateways por Sitio para una alta disponibilidad sin costo adicional. Los clientes establecen una conexión segura con un Gateway en cada emplazamiento.

Portal

El Portal Appgate SDP Clientless ofrece una forma alternativa para que los usuarios se conecten a los recursos de red protegidos desde sus dispositivos no gestionados. El Portal ofrece acceso basado en navegador (sin cliente) sin necesidad de instalar el Cliente completo en su dispositivo. La licencia de usuario del Portal permite a un único usuario iniciar sesión a través del Portal.

Conector

Un conector protege los recursos no gestionados actuando como Gateway entre los recursos conectados y la red. Se puede acceder desde los dispositivos de un grupo de recursos.

Grupo de recursos

Un grupo de recursos es un grupo lógico de recursos gestionados por una política de acceso única dentro de un conector (o un par de conectores de alta disponibilidad). Los recursos pueden ser dispositivos (por ejemplo, dispositivos IoT, impresoras, cámaras IP) o usuarios (que no tienen instalado el software Appgate SDP Client). Por ejemplo, un Conector puede contener tres Grupos de Recursos -uno para impresoras, uno para cámaras y uno para usuarios- y cada Grupo de Recursos recibirá un conjunto único de derechos de acceso a los servicios. Cada licencia de Grupo de Recursos permite establecer una única Política de acceso.

Capacidades de Appgate SDP

Integración del proveedor de identidad

Los usuarios pueden definirse localmente con el proveedor de identidad (IdP) local de Appgate SDP o con un IdP OIDC, SAML, LDAP o RADIUS integrado. SDP proporciona acceso basado en el contexto utilizando el IdP y las políticas establecidas en el controlador SDP de Appgate.

NOTA: Los colectivos alojados soportan integraciones OIDC y SAML.

Capacidades de Appgate SDP (cont.)

Políticas dinámicas de Zero Trust

Verifique y evalúe constantemente la identidad, el contexto y el riesgo como criterios para las políticas de acceso quirúrgico.

MFA integrado

El proveedor de OTP por tiempo integrado funciona con las aplicaciones de autenticación por tiempo de OATH, como Google Authenticator o Authy.

MFA por hardware

El proveedor FIDO2 integrado funciona con dispositivos (USB) compatibles con FIDO2.

Cliente siempre activo

Permite que el dispositivo de un usuario se conecte a la red aunque dicho usuario no haya iniciado sesión.

Cliente multiusuario

Conectividad segura desde equipos multiusuario, como servidores de terminales.

Scripts de extensión

Permite al sistema interoperar con innumerables sistemas externos y entornos de red.

Servicios en la nube Appgate SDP

NOTA: Los servicios en la nube SDP de Appgate enumerados a continuación requieren implementaciones alojadas o conectadas.

Application Discovery

Application Discovery ofrece una oportunidad única para que las organizaciones pasen rápidamente de un acceso remoto estilo VPN a un modelo ZTNA moderno y seguro. Esta función utiliza un sistema avanzado de aprendizaje automático (ML) para observar el comportamiento del usuario y los patrones de acceso a lo largo del tiempo. Mediante el análisis de estos datos, Application Discovery proporciona información procesable que ayuda a los administradores a definir y perfeccionar las políticas de acceso, garantizando que sólo los usuarios adecuados accedan a los recursos adecuados alineados con los objetivos de seguridad de la organización. A medida que las organizaciones migran a un despliegue alojado o conectado, la utilización de Application Discovery puede mejorar significativamente su capacidad para adaptarse a los cambiantes retos de seguridad, manteniendo al mismo tiempo una experiencia de usuario continua.

NOTA: TPara acelerar la configuración inicial y la adopción de Appgate SDP, a los clientes con el nivel Essentials se les proporciona acceso al servicio Application Discovery durante 30 días.

Motor de Riesgo

El motor de riesgos mejora las políticas de acceso con información sobre la postura de seguridad recopilada por soluciones de TI, seguridad y empresariales de terceros. Las integraciones incorporadas con las principales herramientas de seguridad y una interfaz que se configura con un clic eliminan el costo y la complejidad de las secuencias de comandos de API personalizadas.

Alertas de riesgo

El servicio de alertas de riesgo permite que el motor de políticas dinámicas de Appgate SDP responda a la información 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 una organización, al tiempo que reduce la complejidad operativa.



Servicios en la nube de Appgate SDP (cont.)

Al aprovechar datos y análisis en tiempo real, el analizador de políticas permite a las organizaciones identificar políticas y derechos que pueden retirarse, descubrir derechos con recursos solapados y configuraciones que de otro modo podrían pasar desapercibidas. Este enfoque proactivo no sólo mejora la seguridad, sino que también simplifica el cumplimiento de los requisitos normativos, lo que lo convierte en un componente esencial para las organizaciones en transición a una implantación alojada o conectada.

Zero Trust Network Access (ZTNA) Universal

Zero Trust Network Access (ZTNA) Universal garantiza la aplicación coherente de los principios de Zero Trust para todos los usuarios, independientemente de su dispositivo o ubicación, ya sea local o remoto, mediante un modelo de política unificado. La adopción de ZTNA Universal simplifica la gestión del acceso seguro al consolidar y sustituir tecnologías tradicionales como VPN, MPLS y NAC en diversas infraestructuras y entornos de red. Esto permite a las organizaciones mantener la seguridad de la red sin introducir complejidad para los usuarios finales y obtener eficiencias administrativas al tiempo que se reducen los gastos operativos y de capital. El nivel Enterprise es ideal para organizaciones que persiguen casos de uso universales de ZTNA, ya que hay un ROI significativamente mayor y beneficios añadidos por aprovechar Appgate SDP para asegurar simultáneamente conexiones remotas y locales.

Reducción automática de cobertura

La función Automatic Site Fallback reduce la posible interrupción del usuario final cuando falla la conectividad entre el usuario y un sitio.

Conectividad al sitio más cercano

La función de sitio más cercano asigna automáticamente a los usuarios finales el dispositivo Gateway primario más cercano a su ubicación geográfica actual.

Optimizador de red local

La función Local Network Optimizer detecta cuándo un usuario final se conecta desde dentro de la red corporativa y configura túneles seguros sin necesidad de hair-pinning.

Soporte colectivo múltiple

El software cliente puede conmutar automáticamente por error a un Colectivo secundario sin que el usuario tenga que realizar ninguna acción cuando se produce un fallo en el Colectivo primario.

Tipos de despliegue de Appgate

Hosted

Este tipo de despliegue proporciona un valor significativo a las organizaciones que desean los beneficios de la solución SaaS y la conectividad de enrutamiento directo. En este modelo, Appgate es responsable de alojar, supervisar y gestionar el plano de control (dispositivos controladores duales).

Tipos de despliegue de Appgate (cont.)

El cliente es responsable del aprovisionamiento, supervisión y gestión de la infraestructura subyacente utilizada para operar los dispositivos SDP de Appgate en sus instalaciones o en su nube. Appgate es responsable de actualizar todos los dispositivos, independientemente de dónde estén alojados. Los clientes pueden optar por implementar una única instancia de LogServer por cada colectivo alojado sin cargo adicional.

Conectado

Este tipo de despliegue es para organizaciones que se beneficiarán de Appgate SDP y de los servicios en la nube de valor añadido, al tiempo que se adhieren a requisitos empresariales o normativos específicos que actualmente no están disponibles con la opción alojada. En este modelo, el cliente es responsable de todos los aspectos de su Appgate SDP Collective, lo que incluye el despliegue, la gestión, la supervisión, el funcionamiento y la actualización. Appgate conserva la responsabilidad operativa de todos los servicios en la nube.

Aislado

En este tipo de despliegue, la organización es totalmente responsable de todos los aspectos de su infraestructura y dispositivos SDP de Appgate. Los colectivos aislados no pueden conectarse a los servicios en la nube. Este modelo es ideal para organizaciones con necesidades de seguridad, privacidad de datos y normativas muy estrictas.

Soporte y Servicios Appgate

Soporte estándar

El soporte estándar está disponible por teléfono, correo electrónico o Web durante el horario contratado. El "Soporte 24/7" se limita a problemas de Nivel de Gravedad Crítico o Mayor fuera del horario laboral normal. Todos los demás problemas de nivel de gravedad se tratarán durante el horario laboral normal.

Technical Service Account Manager

Asesor técnico premium de confianza del cliente que actúa como la voz del cliente centrándose en la salud y eficacia de la implementación de Appgate SDP. Un TSAM es un socio técnico centrado en la prestación continua de servicios tras la puesta en marcha de la implementación base o en la asistencia técnica añadida a nivel de cuenta para la prestación continua de servicios o el enriquecimiento de la experiencia de la cuenta.

Ingeniero de Soporte Dedicado

El Ingeniero de Soporte Dedicado (DSE) añade un enfoque personalizado en el éxito de la experiencia del cliente y la gestión técnica del entorno del cliente. El DSE asignado para cumplir con la prestación del servicio se mide por el éxito de su comunicación con el cliente y su trabajo proactivo para mantener estable el entorno del cliente.

El recurso DSE se dedica a un único cliente y dedica aproximadamente el 80% de su tiempo a trabajar con el cliente en su solución (reservando el 20% para reuniones Appgate, formación, esfuerzos de documentación, trabajo con Desarrollo, etc.). El recurso se asigna por un mínimo de un año.

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 threat advisory analysis e implementación de ZTNA. Appgate protege a empresas y agencias gubernamentales en todo el mundo. Obtén más información en [appgate.com](https://www.appgate.com).