

OneGate

Resumen de Producto



Tabla de contenido

1. Introducción	4
2. OneGate – SPOE & SPOA	4
3. Punto Único de Entrada / Single Point of Entry (SPOE)	4
3.1 Un Gateway Unificado para Todo Acceso	4
3.2 Eliminación de Capas de Acceso Fragmentadas	5
3.3 Beneficios Clave – Único Punto de Entrada / Single Point of Entry	5
3.4 Aplicación de la Normativa en Tiempo Real	5
4. Punto Único de Administración / Single Point of Administration (SPOA)	5
4.1 Control Centralizado en toda la Plataforma	5
4.2 De la Gestión Distribuida a la Gobernanza Centralizada	5
4.3 Beneficios Clave	6
4.4 Control Unificado y Consistente	6
5. Arquitectura Avanzada Zero Trust	6
6. Capacidades Básicas	7
6.1 Proveedor de Identidad (IdP) / SSO	7
6.2 Autenticación Multi-Factor (MFA)	7
6.3 Motor de Políticas	7
6.4 Control del Tráfico en Línea	7
6.5 Gestión de Sesiones	8
6.6 Control de Acceso Granular	8
6.7 Federación e Integración	8
6.8 Confianza en el Dispositivo	8
6.9 Administración	8
6.10 Integración de Multi-Directory/Base de Datos de Usuarios	8
6.11 Gestión de Acceso Privilegiado	8
6.12 Auto-Servicio del Usuario	9

6.13	Transformación de Contenido en Línea	9
6.14	Balanceo de Carga y Agrupamiento	9
6.15	Protección contra Amenazas Conductuales	9
6.16	Firma Digital	9
7.	Modelos de Despliegue	9

1. Introducción

OneGate es una plataforma unificada para la gestión de identidades, el control de accesos y la seguridad. Esta solución permite a las organizaciones proteger a usuarios, sistemas y datos mediante una arquitectura moderna, escalable y flexible.

2. OneGate – SPOE & SPOA

OneGate se basa en dos principios fundamentales: un Único Punto de Entrada (SPOE) y un Único Punto de Administración (SPOA). Toda la funcionalidad se ofrece a través de una única instancia física o lógica, proporcionando una puerta de enlace unificada para todos los accesos y centralizando al mismo tiempo la administración y el control.

Este enfoque arquitectónico es lo que diferencia a OneGate de las pilas de seguridad multicomponente tradicionales y es la base del nombre "OneGate": un único punto de entrada para todo el acceso.

En lugar de combinar múltiples sistemas separados, como IAM, proxies, motores de políticas, soluciones de firma y herramientas de seguridad, OneGate consolida todas las capacidades en una plataforma unificada con administración centralizada.

Beneficios clave:

- Un único punto de acceso para todos los usuarios, sistemas y tráfico.
- Un solo punto de administración para todas las políticas y configuraciones.
- Aplicación coherente de las políticas en todas las interacciones.
- Menor complejidad y eliminación de la sobrecarga de integración.
- Operaciones, monitorización y mantenimiento simplificados.
- Mayor seguridad gracias al control total de todos los flujos de tráfico.

Este enfoque unificado garantiza que la identidad, el control de acceso, la aplicación de las normas, la administración y la seguridad se apliquen siempre de forma coherente y en tiempo real, sin depender de arquitecturas fragmentadas.

3. Punto Único de Entrada / Single Point of Entry (SPOE)

3.1 Un Gateway Unificado para Todo Acceso

OneGate proporciona un **Único Punto de Entrada** para todos los usuarios, sistemas y tráfico. Todo el acceso fluye a través de una única instancia física o lógica, lo que garantiza que cada solicitud y respuesta se controle, inspeccione y aplique en tiempo real.

Este principio es la base del nombre "OneGate": un único punto de entrada para todo acceso.

3.2 Eliminación de Capas de Acceso Fragmentadas

Las arquitecturas tradicionales suelen depender de múltiples componentes, tales como:

- Proxies inversos
- Soluciones VPN
- Gateways de Aplicación
- Gateways de API

Estos puntos de entrada fragmentados generan complejidad y una aplicación inconsistente de la ley.

OneGate sustituye este sistema por una puerta de enlace unificada, lo que garantiza que todo el tráfico pase por el mismo punto de control.

3.3 Beneficios Clave – Único Punto de Entrada / Single Point of Entry

- Un único punto de entrada para todos los usuarios, sistemas y tráfico.
- Visibilidad y control total de todos los flujos de acceso
- Aplicación coherente de las políticas en todas las interacciones.
- Reducción de la superficie de ataque mediante la eliminación de puntos de entrada no controlados.
- Arquitectura simplificada sin múltiples pasarelas

3.4 Aplicación de la Normativa en Tiempo Real

Porque todo el tráfico pasa por OneGate:

- Cada solicitud es verificada
- Cada respuesta está controlada
- Toda interacción está sujeta a política

Esto permite una **aplicación real del principio de Zero Trust en línea** en todo el entorno.

4. Punto Único de Administración / Single Point of Administration (SPOA)

4.1 Control Centralizado en toda la Plataforma

Además de ser un único punto de acceso, OneGate proporciona un **Punto Único de Administración / Single Point of Administration**.

Todas las políticas, configuraciones, fuentes de identidad, métodos de autenticación y controles de seguridad se gestionan de forma centralizada dentro de la misma plataforma.

4.2 De la Gestión Distribuida a la Gobernanza Centralizada

Los entornos tradicionales suelen requerir administración en múltiples sistemas:

- Plataformas IAM
- Soluciones MFA
- Configuraciones Proxy
- Sistemas PAM
- Servicios de firma

Esto conduce a:

- Configuraciones duplicadas
- Políticas inconsistentes
- Aumento de los gastos generales operativos

OneGate elimina este problema centralizando toda la administración en una interfaz y capa de control unificadas.

4.3 Beneficios Clave

- Punto único de administración para todas las políticas y configuraciones.
- Definición y aplicación coherentes de las políticas en todos los sistemas.
- Reducción de la complejidad operativa
- Monitoreo y resolución de problemas simplificados
- Cambios más rápidos y mejor gobernanza

4.4 Control Unificado y Consistente

Al combinar la administración en una única plataforma, OneGate garantiza que:

- Identidad
- Control de Acceso
- Aplicaciones de ley
- Políticas de Seguridad

se gestionan de forma coherente, centralizada y en tiempo real.

OneGate no es solo un único punto de entrada para el acceso, sino también un único punto de control para la administración.

5. Arquitectura Avanzada Zero Trust

OneGate se basa en una arquitectura avanzada de Zero Trust, donde cada solicitud de acceso se verifica, controla y aplica continuamente en tiempo real. Ningún usuario, dispositivo o sesión se considera de confianza implícita.

Principios fundamentales:

- Verificación continua - cada solicitud y respuesta se evalúa en tiempo real.
- Control de acceso basado en la identidad - basado en el usuario, el contexto y el comportamiento.
- Control en línea - todo el tráfico fluye a través de OneGate.
- Acceso con privilegios mínimos - se otorga el acceso mínimo requerido.
- Seguridad adaptativa - la seguridad se ajusta dinámicamente en función del riesgo.

Qué lo hace Avanzado:

- Identidad + Política + Aplicación en una sola plataforma
- Control de tráfico en tiempo real
- Transformación de datos en línea
- Detección y predicción de amenazas conductuales
- Punto de control unificado

Impacto en el negocio:

- Elimina la confianza implícita
- Reduce la superficie de ataque
- Detecta y detiene las amenazas en tiempo real.
- Admite entornos híbridos
- Se alinea con marcos de trabajo como NIS2.

6. Capacidades Básicas

6.1 Proveedor de Identidad (IdP) / SSO

Autentica a los usuarios y proporciona inicio de sesión único (Single Sign-On) en múltiples sistemas y aplicaciones. OneGate es compatible con estándares de federación como SAML y OpenID Connect (OIDC), lo que permite una integración perfecta con proveedores de identidad tanto internos como externos.

La solución centraliza la autenticación y elimina la necesidad de múltiples inicios de sesión, mejorando tanto la seguridad como la experiencia del usuario.

6.2 Autenticación Multi-Factor (MFA)

Proporciona una autenticación sólida mediante la combinación de múltiples factores, como algo que el usuario sabe, posee o es. OneGate admite una amplia gama de métodos, incluidos BankID, Freja eID, TOTP, certificados, autenticación push, métodos basados en RADIUS y autenticación adaptativa como WizePass.

La plataforma permite una autenticación flexible alineada con LoA 1–4 y admite métodos sin contraseña cuando corresponda.

6.3 Motor de Políticas

El motor de políticas evalúa las decisiones de acceso en tiempo real basándose en la identidad, los roles, el contexto, el estado del dispositivo y las señales de comportamiento.

Las políticas pueden definirse con gran detalle y aplicarse de forma dinámica, lo que permite a las organizaciones aplicar el principio de mínimo privilegio y adaptar los controles de seguridad en función del riesgo.

6.4 Control del Tráfico en Línea

Todo el tráfico fluye a través de OneGate, donde se inspecciona y controla en tiempo real. Esto garantiza que cada solicitud y respuesta esté sujeta al cumplimiento de las políticas establecidas.

A diferencia de las soluciones tradicionales, la aplicación de la normativa es continua y no se limita a la fase de inicio de sesión, lo que permite una verdadera seguridad de Zero Trust.

6.5 Gestión de Sesiones

Supervisa continuamente las sesiones activas y aplica controles dinámicos a lo largo de todo el ciclo de vida de la sesión.

Esto incluye la finalización de la sesión, la reautenticación (autenticación multifactor / MFA reforzada) y la restricción de acciones en función del riesgo o el comportamiento, lo que garantiza que la confianza nunca sea estática.

6.6 Control de Acceso Granular

Proporciona un control preciso del acceso en múltiples niveles, incluyendo el de aplicación, ruta, función y acción.

Esto permite a las organizaciones aplicar políticas de acceso precisas y minimizar la exposición, garantizando que los usuarios solo accedan a lo estrictamente necesario.

6.7 Federación e Integración

Permite la integración con sistemas externos y proveedores de identidad mediante protocolos estándar como SAML y OIDC.

Admite entornos híbridos y permite a las organizaciones extender el acceso seguro a través de sus límites organizativos sin modificar los sistemas existentes.

6.8 Confianza en el Dispositivo

Valida los dispositivos mediante mecanismos como certificados e identidad del dispositivo.

Garantiza que solo los dispositivos de confianza y que cumplan con la normativa puedan acceder a sistemas confidenciales, reforzando la seguridad más allá de la autenticación del usuario.

6.9 Administración

Proporciona una interfaz de gestión centralizada para configurar políticas, usuarios, integraciones, flujos de firma y ajustes de seguridad.

Esto simplifica las operaciones y reduce los gastos administrativos al consolidar el control en una única plataforma.

6.10 Integración de Multi-Directory/Base de Datos de Usuarios

Permite la integración simultánea con múltiples fuentes de identidad, como Active Directory, LDAP, Entra ID y proveedores de identidad federados.

Permite a las organizaciones autenticar usuarios en diferentes directorios sin necesidad de consolidación, lo que facilita la gestión de entornos de TI híbridos y estrategias de migración gradual.

6.11 Gestión de Acceso Privilegiado

Proporciona control y supervisión del acceso privilegiado a sistemas críticos.

Incluye funcionalidades como acceso justo a tiempo, autenticación reforzada, control de sesión y registro de auditoría completo, lo que reduce el riesgo de uso indebido de cuentas privilegiadas.

6.12 Auto-Servicio del Usuario

Permite a los usuarios gestionar sus propias credenciales y acceder a través de una funcionalidad de autoservicio segura.

Incluye funciones como el restablecimiento de contraseña y la verificación de identidad, lo que reduce la carga de trabajo del servicio de soporte y mejora la productividad del usuario.

6.13 Transformación de Contenido en Línea

Modifica el tráfico y el contenido en tiempo real para adaptar las aplicaciones sin necesidad de realizar cambios en los sistemas de backend.

Algunos ejemplos incluyen la reescritura de URL, la transformación de formatos de datos, la adaptación de atributos de identidad entre sistemas y la posibilidad de utilizar externamente contenido con formato interno, lo que permite una interoperabilidad perfecta.

6.14 Balanceo de Carga y Agrupamiento

Incluye funciones integradas de equilibrio de carga y agrupación en clústeres para distribuir el tráfico entre varios nodos.

Esto garantiza una alta disponibilidad, escalabilidad y conmutación por error automática sin necesidad de infraestructura externa.

6.15 Protección contra Amenazas Conductuales

Analiza continuamente el comportamiento del usuario para detectar anomalías y predecir posibles amenazas.

Basándose en patrones de comportamiento aprendidos, OneGate puede aplicar de forma proactiva medidas de seguridad como la autenticación reforzada, la restricción de sesiones o el bloqueo, todo ello en tiempo real dentro del flujo de tráfico.

6.16 Firma Digital

OneGate incluye soporte para la firma digital, lo que permite firmar transacciones y documentos de forma segura y conforme a la ley directamente dentro de la plataforma.

Admite una autenticación sólida previa a la firma, la integración con métodos de firma basados en eID, como BankID y Freja eID, y el manejo seguro de los flujos de trabajo de firma sin necesidad de una plataforma de firma independiente.

7. Modelos de Despliegue

OneGate admite modelos de implementación flexibles, que incluyen configuraciones en la nube (SaaS o alojadas), locales e híbridas.

Esto permite a las organizaciones cumplir con los requisitos normativos, de seguridad y operativos, manteniendo al mismo tiempo una paridad total de funcionalidades en todos los entornos.