mobilityguard®
Unified Access Management

Para Acceso de Cualquier Escenario – Solo Una Solución

¿Por qué MobilityGuard OneGate?

El VPN SSL sin cliente incluido en el MobilityGuard OneGate es una tecnología avanzada que ofrece un valor empresarial real, permitiendo a los usuarios acceder a las aplicaciones e información desde cualquier lugar, utilizando cualquier dispositivo, sin necesidad de instalar ningún software cliente.

Escenarios

1 Acceda desde cualquier lugar
2 Identifique sólidamente los usuarios
3 No más notas de recordatorio con ingreso simple
4 Administración de Acceso en “solo tres clics”
5 Encapsule Sistemas Inseguros
6 Colaboración Organizacional
7 Gestión de acceso como un servicio
8 Asegure sus servicios y negocios electrónicos

Sin Cliente

Para máxima productividad, el acceso sin cliente de MobilityGuard permite a las empresas ofrecer acceso interno o remoto a la información y aplicaciones de misión crítica. Estas incluyen correo electrónico, intranet, extranet, aplicaciones cliente/servidor, herramientas de colaboración, terminales de servicios y muchos más, manteniendo un alto nivel de seguridad. Los usuarios sólo requieren una conexión a Internet y un navegador web para obtener acceso instantáneo. MobilityGuard OneGate no requiere ningún hardware o software adicional en el dispositivo cliente, lo que hace que sea fácil y asequible de implementar y mantener. Un cliente VPN opcional también está disponible con MobilityGuard OneGate, de ser necesario.

Autenticación Sólida de Usuarios

Más de 15 métodos de autenticación diferentes (se incluye la autenticación de dos factores) se incluyen en el MobilityGuard OneGate que ofrece a las organizaciones una solución eficiente y económica única para identificar con seguridad a cualquier usuario. La solución ofrece soporte tanto para usuarios internos, por ejemplo: empleados; y grupos de usuarios externos por ejemplo: socios, proveedores, clientes, etc. Todos los métodos de autenticación disponibles pueden ser utilizados simultáneamente por lo que la solución se adapta perfectamente a las necesidades de las organizaciones empresariales.

Encriptación Sólida

Al utilizar la encriptación estándar de la industria, los datos de usuario y las transacciones están protegidas del acceso no autorizado. MobilityGuard utiliza el cifrado de 128 a 256 bits utilizando algoritmos de encriptación aceptados militarmente como AES (Sistema de Encriptación Avanzado)

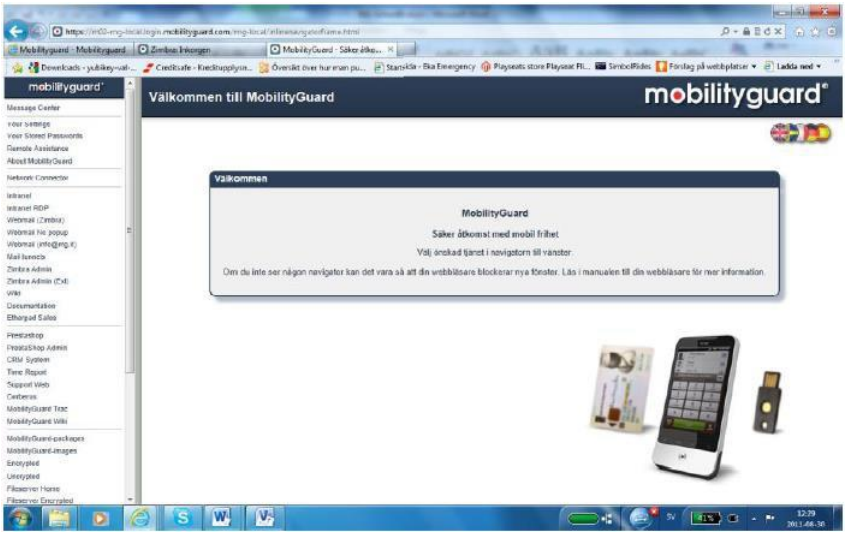
Aplicaciones Amigables con el Usuario

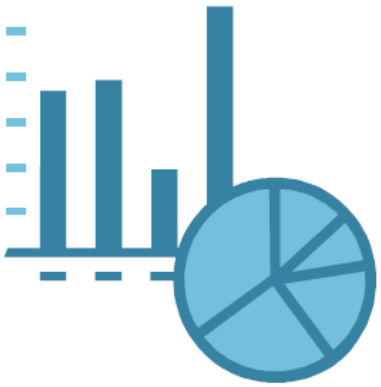
Usando cualquier navegador web, el lanzador de MobilityGuard OneGate simplifica enormemente la experiencia del usuario entregando las aplicaciones y la información en las manos del usuario. Cuando se combina con la tecnología Inicio de Sesión Única de MobilityGuard, los usuarios ya no tendrán que introducir su nombre de usuario o contraseña para cada una de sus aplicaciones una vez que hayan iniciado sesión en MobilityGuard.

ABOX C. Provença 102, 4ª planta, 08029 Barcelona
Tel: 902160145, abox@abox.com

El Lanzador MobilityGuard OneGate es totalmente personalizable permitiendo a los administradores ofrecer menús individuales basados en el usuario conectado, donde el usuario se conecta desde el nivel de autenticación utilizado, y mucho más. El Portal también puede detectar automáticamente el dispositivo cliente y adaptar la interfaz de acuerdo al usuario. Las opciones son ilimitadas.

El interface de Aplicaciones proporciona a los usuarios acceso personalizado a aplicaciones rápida y fácilmente.





La funcionalidad de alta disponibilidad de MobilityGuard proporciona escalabilidad y alto rendimiento que garantiza el acceso 24x7.

Soporte para cualquier aplicación

MobilityGuard soporta virtualmente todas las aplicaciones incluyendo servidores Web, cliente/servidor, mainframe, servidores de terminales, Servidores bi-direccional (VoIP, herramientas de colaboración en línea) y de archivos. Como solución de software, MobilityGuard OneGate es exclusivamente personalizable para apoyar prácticamente cualquier tipo de aplicación.

Escalabilidad y Rendimiento

Mediante la conexión de múltiples MobilityGuard OneGate, la solución es fácilmente escalable para soportar incluso los más grandes entornos de red e implementaciones interregionales.

Alta Disponibilidad Incorporada

Cualquier cantidad de MobilityGuard OneGate pueden ser instalados en su red sin costo adicional, para garantizar el acceso 24x7.

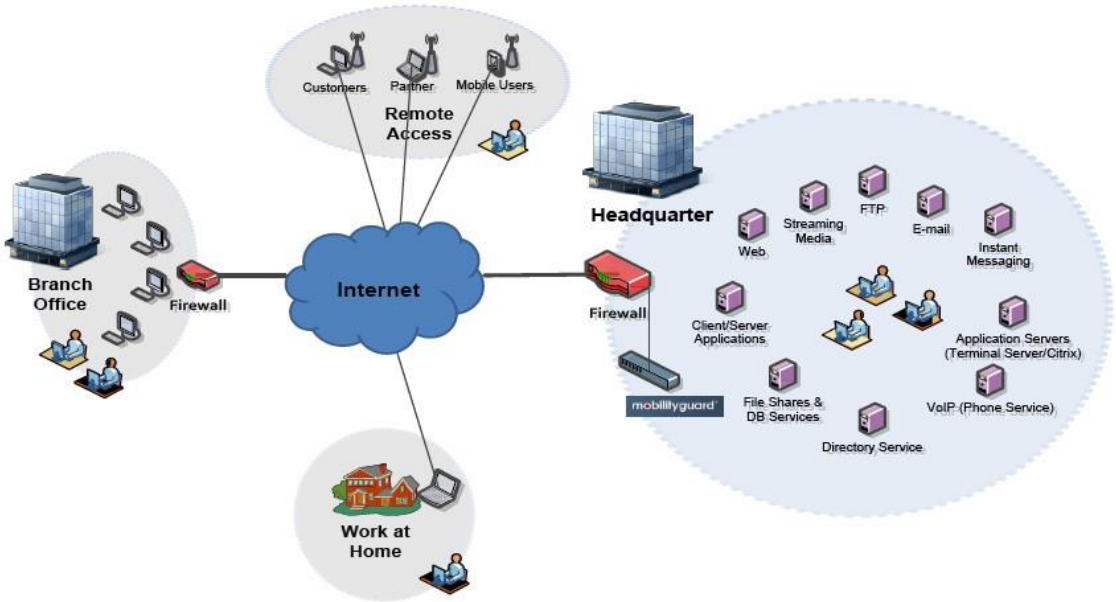
ABOX C. Provença 102, 4ª planta, 08029 Barcelona
Tel: 902160145, abox@abox.com

Acceso desde cualquier lugar

Brinde a cualquier categoría de usuario acceso seguro a los recursos
¿Cómo pueden los usuarios obtener acceso seguro a las aplicaciones, independientemente de la hora, el lugar y el dispositivo que utilicen? ¿Cómo simplificar la variedad de métodos de acceso remoto para la las personas involucradas o en el hogar, así como los ubicados en las oficinas de la sede central o sucursales? Con MobilityGuard OneGate los usuarios autorizados pueden acceder de forma segura a todo tipo de sistemas internos e información sensibles, independientemente del tiempo y lugar. Los usuarios típicos pueden ser empleados, socios y clientes. Quienes pueden estar ubicados en la oficina, en casa o en el campo de acción utilizando cualquier equipo que este a su disposición.

Sólo se necesita un navegador web
Los usuarios sólo requieren una conexión a Internet y un navegador web estándar para obtener acceso instantáneo. MobilityGuard proporciona una movilidad muy alta, ya que no hay necesidad de instalar software cliente en el equipo de conexión. MobilityGuard incluso tiene soporte para dispositivos móviles, como teléfonos inteligentes y tabletas.

No se requiere hardware ni software adicional
MobilityGuard OneGate no requiere ningún hardware o software adicional en el dispositivo cliente, lo que hace que sea fácil y asequible de implementar y mantener.



Acceda a cualquier aplicación
Para máxima productividad, el VPN MobilityGuard sin cliente permite a las organizaciones ofrecer acceso remoto o interno a la información de misión crítica y aplicaciones, manteniendo un alto nivel de seguridad. Esto incluye correo electrónico, intranet, extranet, aplicaciones cliente/servidor, herramientas colaborativas, servicios de terminal, y mucho más. No se requiere personalizar las aplicaciones, lo que significa que la instalación y configuración de MobilityGuard OneGate normalmente se puede completar en una hora.

Todo en una caja
MobilityGuard OneGate ofrece Identificación de Usuario Sólida, Control de Acceso Dinámico, Centro Único de Acceso, y un Motor de integración de cualquier portal web o aplicación. La Solución OneGate está disponible como dispositivo físico o lógico que se ejecuta en VMware, Hyper-V o XEN-servidor.

Cero "huellas" en el dispositivo de conexión
No se dejan "huellas" en el equipo cliente que se conecta después de su uso. Esto significa que ningún otro usuario de la computadora cliente puede obtener acceso a la información recibida de la aplicación. Por ejemplo, un correo electrónico con información confidencial no será visible para otros usuarios que puedan tener acceso a la misma PC.

Filtrado de código malicioso por Manejo De Sesión Segura
Mediante el uso de la tecnología "Verdadero SSL-VPN" con el manejo de sesión segura, MobilityGuard OneGate proporciona un primer nivel de protección contra código malicioso instalado en el equipo que se conecta.

Identifique Sólidamente sus Usuarios

Diferentes categorías de usuarios y muchos escenarios de acceso

Los diferentes usuarios tienen diferentes maneras de identificarse con seguridad a sí mismos antes de acceder a las aplicaciones.

Diferentes situaciones de acceso también requieren diferentes métodos de identificación. Un empleado puede utilizar métodos seguros de identificación o dispositivos tales como los tokens de hardware proporcionados por la organización. Pero ¿cómo se puede gestionar mejor las categorías de usuarios que están conectados libremente a la organización, como socios, clientes e incluso los contratistas?

La Implementación de métodos de Identificación Segura o dispositivos no suele ser la solución preferida para muchas organizaciones debido a los costos y gastos de gestión. Sin embargo, hoy en día estos usuarios necesitan la mejor protección de la seguridad y una solución que los identifique sólidamente cuando acceden a sus aplicaciones.

Combine más de 15 métodos incorporados de autenticación seguros

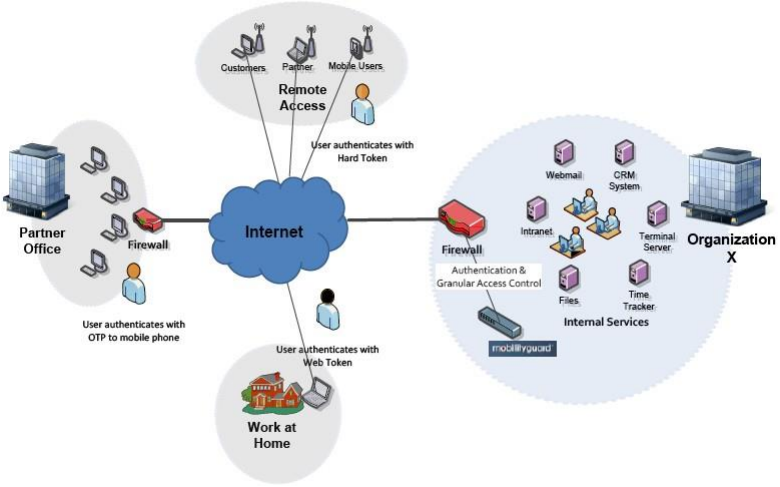
Con la solución MobilityGuard OneGate tendrá acceso a más de 15 métodos de autenticación seguros. Esto incluye, entre otros, el método de autenticación de dos factores a través de un identificador de hardware basado en software único conocido como el Token Web MobilityGuard.

Otro método integrado de autenticación segura es el SMS Token MobilityGuard que proporciona una contraseña de una sola vez enviado al teléfono móvil del usuario como un mensaje de texto SMS. Los teléfonos móviles de los usuarios se convierten en una señal de hardware físico.

Reduzca los costos y resuelva el enigma de la identificación

Usando los métodos de autenticación incorporado de OneGate, se reduce la necesidad de soluciones de terceros adicionales, como tokens duros físicos.

También se pueden combinar diferentes tipos de métodos de autenticación como los tokens duros, incluyendo RSA y Vasco, ID electrónica, certificados locales, Matriz de Código Enigma y llaves USB.



Acceso granular basado en el método de autenticación utilizado

¿Cómo diferenciar los niveles de acceso en función de cómo ha sido sólidamente identificado el usuario? Tradicionalmente esto funciona más bien como un interruptor de encendido y apagado. Si se identifica apropiadamente, el usuario tendrá acceso a toda la red.

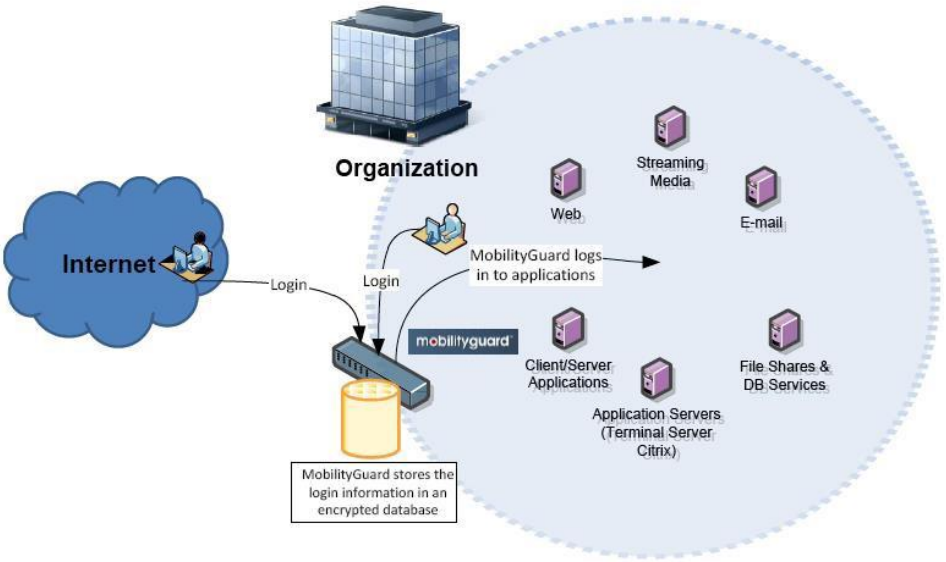
Sin embargo, MobilityGuard OneGate incluye un mecanismo para proveer acceso granular a cualquier sistema basado en un conjunto de políticas, que clasifica los métodos utilizados para su identificación.

En la práctica esto significa que si el usuario se identifica con un método de autenticación más sólido, entonces tendrá automáticamente el acceso a un conjunto más amplio de aplicaciones.

No más Notas de Recordatorio

Los usuarios olvidan su contraseña

Con frecuencia, los usuarios olvidan sus contraseñas, simplemente porque hoy en día se tiene un gran número de contraseñas que recordar. Entonces, ¿cómo los usuarios pueden resolver este problema? ¡A menudo utilizan la misma contraseña para aplicaciones sensibles y no sensibles, algunos crean un sistema organizado para recordarlas y otros incluso recurren a las notas amarillas Post-it pegadas a sus computadoras!



Acceso Único Centralizado

Mediante el uso de la función dinámica centralizada Sign-On/Sign-Off de MobilityGuard, sus empleados tienen un método simple y seguro para iniciar sesión en todas las aplicaciones que necesitan.

La simplicidad es la clave del éxito

MobilityGuard OneGate crea un inicio único de sesión (SSO) de entrada de forma automática, la primera vez que el usuario inicia sesión en la aplicación.
MobilityGuard almacena esta información de SSO en una base de datos cifrada central y la utiliza la próxima vez que los usuarios son autorizados y solicitan acceso a la aplicación.
La solución MobilityGuard OneGate ofrece la opción de permitir o no permitir fácilmente Inicio Único de Sesión para la aplicación sobre la base de la política de seguridad.
La política de seguridad se define simplemente por cinco criterios de seguridad en el Centro de Control OneGate.

No más notas de recordatorio

Mediante el uso de MobilityGuard OneGate puede eliminar el uso de las notas amarillas “Post-it" para recordar las contraseñas.

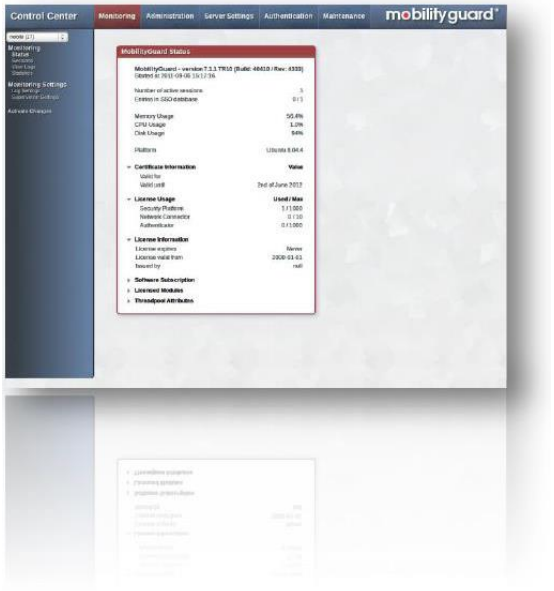
Administración de acceso en tres clics

El acceso seguro complejo limita su empresa
¿Cómo proporcionar acceso seguro a su entorno de IT?
Muchas organizaciones tienen entornos muy complejos. Con el fin de gestionar los usuarios y facilitar el acceso a las aplicaciones, la organización debe implementar varias soluciones para entregar el acceso requerido. Múltiples soluciones a menudo significan también que es necesario tener acceso a múltiples interfaces de administración y esto no es rentable.
También son muy complejas de configurar, difíciles de manejar y mantener los niveles de seguridad.

Punto único de administración
Usando MobilityGuard OneGate, la cual es una plataforma de seguridad centralizada, usted tiene un único punto de administración para todos los métodos de acceso que usted necesita apoyar.
Con sólo tres clics del ratón usted puede distribuir de forma segura aplicaciones de base WEB, servidor de terminal e incluso aplicaciones cliente-servidor a cualquier usuario en cualquier situación.

Tres pasos para el desarrollo de su negocio
Una opción de acceso típica se configura a través de estos tres pasos:

1. Defina su aplicación
2. Cree una lista de control de acceso
3. Cree una entrada en el menú



Todas las funciones de seguridad en una única solución
MobilityGuard OneGate proporciona una gama completa de funciones de seguridad en una única solución. Algunos ejemplos de la funcionalidad son:

- Ingreso Seguro con autenticación de dos factores
- Comunicaciones seguras con el manejo de sesión segura
- Único acceso inteligente y centralizado
- Control de autorización dinámica para acceso granular
- Apoyo para la fácil integración con cualquier aplicación o portal web
- Federación de Identidades de usuario para colaboración
- Funciones de autoservicio para los usuarios; por ejemplo restablecimiento de contraseña
- Firma Digital de la información electrónica

Extienda su negocio
Implementar un Dispositivo MobilityGuard OneGate, significa que los problemas de seguridad y control de acceso ya limitan la expansión de su negocio.
MobilityGuard OneGate está disponible como:

- Servidor Rack de 19 ", Series 3000 -, 4000 - y 6000-; escalable hasta 3000 usuarios concurrentes por dispositivo
- Dispositivos lógicos: VMware, Hyper-V y Xen-Server

Encapsular Aplicaciones Inseguras

Encapsular cualquier aplicación o servicio no seguro
No es habitual que las aplicaciones se diseñen pensando en la seguridad desde el principio. Sin embargo, es importante tomar en cuenta la seguridad desde el principio en la planificación de cualquier proyecto nuevo.
La seguridad es fundamental, independientemente de si el proyecto es para uso interno o un servicio electrónico prestado a los usuarios externos o anónimos, pero es mucho más difícil de tratar de añadir seguridad a las contramedidas en las últimas etapas de un proyecto de seguridad de IT.

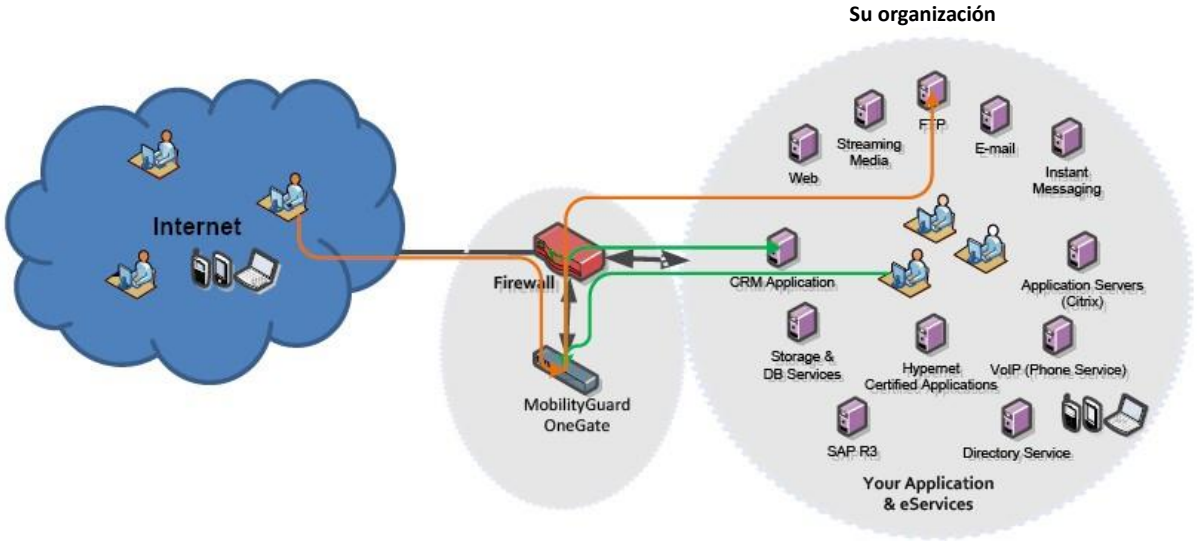
Seguridad Shell
MobilityGuard OneGate resuelve este problema de seguridad, ya que permite crear un shell seguro en torno a una aplicación ya desarrollada o implementada.
La Shell es una manera fácil de asegurar que la aplicación está totalmente protegida con las medidas de seguridad necesarias, sin la necesidad de cualquier rediseño o modificación de la propia aplicación.

Todas las funciones de seguridad en una única solución
MobilityGuard es una solución única que protege cualquier aplicación o servicio electrónico con:

- Comunicación con seguridad
- Identificación sólida del usuario
- Control de acceso dinámico

Todas las funciones de servicio se configuran mediante unos pocos clics y sin necesidad de hacer cambios a las aplicaciones de destino.

Tenga una visión más amplia
Es importante tener una visión holística de la red y la seguridad de las aplicaciones. Es muy fácil centrarse demasiado en la obtención de un único servicio y perder de vista las otras debilidades de seguridad importantes de la red en otros lugares.
MobilityGuard OneGate ofrece un entorno informático seguro y homogéneo que proporciona el rendimiento más alto de seguridad para todos, en lugar de aplicaciones individuales.
OneGate logra su objetivo de proporcionar una visión holística segura del entorno IT con el menor costo total de propiedad.



Organización Colaborativa

Haga Colaboración Fácil y Segura

¿Encuentras dificultades con IT y los problemas de seguridad IT al establecer la colaboración con socios de su negocio? ¿Ve la necesidad de conexiones VPN (Red Privada Virtual) complejas que son difíciles de administrar, a fin de mantener el nivel de su seguridad?

Al conectar los socios comerciales de su entorno IT a través de VPN usted puede exponer involuntariamente la red interna a la red de sus socios. Sólo es posible mantener los niveles de seguridad necesarios para la VPN a través de la administración avanzada y una gran cantidad de trabajo.

MobilityGuard OneGate hace que sea mucho más fácil y seguro colaborar con sus socios a través de una funcionalidad integrada de federación de identidades.

¿Qué es la Federación de Identidades?

La base de las Identidades Federadas es la confianza. Confianza significa que una organización se apoya en otra organización para identificar a los usuarios de una manera segura y confiable.

Una vez que usted o su socio de la red colaborativa ha verificado la identidad del usuario, la aplicación requerida se podrá acceder por ellos. Mediante el uso de la Federación de Identidades, incluso se puede crear una solución transfronteriza-organizativa para Único Acceso (SSO) que simplificará enormemente el acceso a los usuarios.

El acceso a las aplicaciones internas y externas es transparente y los usuarios no tienen necesidad de saber dónde se encuentran los recursos.

¿Por qué utilizar la Federación?

La Federación MobilityGuard OneGate proporciona una manera fácil de colaborar con sus socios. Los beneficios incluyen:

- No hay que establecer conexión VPN
- Niveles de seguridad mejoradas
- Mínima administración y el costo de gestión
- Funcionalidad ampliada
- La perfecta integración con su red y servicios de socios de negocios
- Fácil uso de los "Servicios en la Nube" ampliamente disponibles, como Google Apps y los servicios basados en Internet de Microsoft.

Un poco acerca de la Tecnología

La tecnología de Federación MobilityGuard OneGate se basa en SAML (Lenguaje de marcado de aserción de seguridad) versión 2, el cual es el protocolo estandarizado para la Federación Europea de identidad,

MobilityGuard OneGate puede actuar como el proveedor de identidad o alternativamente como el proveedor de servicios dentro de una configuración federación de identidades.

Gestión de Acceso como un Servicio

¿Por qué la seguridad tiene que ser tan difícil y complicada?
La creación de soluciones de acceso seguro y fácil por lo general implica una gran inversión, también son complicadas y requieren operaciones y gestión costosas.
La edición MobilityGuard Datacenter le permite ofrecer facilidad de administración de acceso "como un servicio" a sus clientes finales.
Por medio de la Gestión de Acceso puede administrar toda la operación y la gestión de las funciones de seguridad que sus clientes finales y socios necesitan.

Cinco beneficios principales
Los 5 beneficios clave del Datacenter MobilityGuard son:

- Bajo costo inicial ya que no hay ninguna inversión en hardware o software
- Instalación muy rápida y mínimo tiempos configuración.
- Apoyo continuo y programas de mantenimiento que brindan acceso a los últimos estándares y tecnologías de seguridad
- Presupuesto fácil con un mínimo de costo adicional
- Los cargos se basan sólo en el uso efectivo

La gama completa de servicios de acceso seguro
La edición de MobilityGuard Datacenter incluye una amplia gama de servicios de seguridad:

- Sesión segura con autenticación sólida por lo general con SMS o certificados
- Comunicación segura con el manejo de sesión segura
- Único acceso inteligente y centralizado
- Control de autorización dinámica
- Apoyo para una fácil integración con cualquier aplicación o portal web
- Federación de identidades de usuarios
- Autoservicio para los usuarios, por ejemplo, restablecimiento de contraseña
- Firma Digital de cualquier información electrónica

Dispositivos de Datacenter
La solución de "Access como servicio" está disponible como un dispositivo completamente configurado:

- Las Series de MobilityGuard 3000, 4000 y 6000, dispositivos de servidores de rack de19 ", escalables hasta 5000 usuarios concurrentes por dispositivo
- dispositivos virtuales que se ejecutan en VMware, Hyper-V o XEN-Server

ABOX C. Provença 102, 4ª planta, 08029 Barcelona
Tel: 902160145, abox@abox.com

Asegure sus Servicios y Negocios Electrónicos

¿Cómo se puede entregar sus servicios y comercio electrónico de forma segura?
¿Cómo puedo ofrecer servicios electrónicos, web y no web basados en una forma segura de cualquiera de mis clientes y socios?
¿Cómo puedo hacer frente a la gestión de todas las cuentas de usuario y todos los problemas de seguridad en el equipo que se conecta a mi aplicación o servicio?
¿Cómo puedo proteger mi red contra el código malicioso de dispositivos conectados remotamente?
¿Cómo puedo manejar las funciones necesarias de seguridad para la identificación de usuarios, comunicaciones fijas y otros problemas de seguridad que surgen de mi servicio electrónico o aplicación de comercio electrónico?
¿Cómo puedo proteger mis servicios y soluciones de comercio electrónico de una manera rentable?

Asegure todo en un solo producto
MobilityGuard OneGate resuelve todos los problemas de seguridad de sus servicios y negocios en un solo producto.
Con MobilityGuard OneGate su empresa está protegida con todas las funciones necesarias. Al mismo tiempo OneGate permite una cooperación más estrecha y mejor con sus clientes o socios a través de la funcionalidad de la federación de identidades, firma digital Único Acceso, etc.

Haga que suceda
La solución OneGate está disponible en forma de aparatos físicos o virtuales. Los aparatos físicos están disponibles en tres modelos (MOG3000, MOG4000 y MOG6000) diseñados para organizaciones pequeñas, medianas y grandes.
Los dispositivos virtuales MobilityGuard OneGate se entregan para entornos virtuales, como VMware, Microsoft Hyper-V y Xen Server.

Despegue dentro de una hora
No se necesitan modificaciones en la aplicación de comercio o servicio electrónico o para que esté listo para despegar en una hora.

¿Por qué no hacer un vuelo de prueba?

ABOX C. Provença 102, 4ª planta, 08029 Barcelona
Tel: 902160145, abox@abox.com