



Entrust IdentityGuard para Empresas

Protección para su empresa

Cuando un empleado o asociado comercial tiene acceso a la red corporativa mediante una red externa, una puerta de enlace de acceso remoto (VPN) o un equipo de escritorio con Microsoft® Windows®, abren la puerta hacia los activos más sensibles, la propiedad intelectual y la información de los clientes de la organización.

La seguridad de la red y de los equipos de escritorio conectados es tan sólida como el método de autenticación implementado, lo que destaca la importancia de la correcta ejecución de ésta.

Proporcionar autenticación de doble factor a la población empresarial completa es un componente esencial en la protección de su organización. Los desafíos presupuestarios y administrativos de implementar ampliamente autenticadores sólidos provocan que las organizaciones busquen soluciones que no sólo son flexibles sino que también asequibles. Sólo una plataforma de autenticación versátil que permite a las empresas elegir múltiples tipos de autenticadores basados en los usuarios y el costo puede cumplir efectivamente con los requerimientos de la empresa.

Sumando las obligaciones que se imponen a la industria como las Reglas de Bandera Roja, la ley Sarbanes-Oxley (SOX) o el estándar de seguridad de datos la Industria de tarjetas de pago (PCI, Payment Card Industry), las organizaciones están siendo impulsadas a aumentar la solidez de la autenticación para un población de usuarios mucho más amplia que antes.

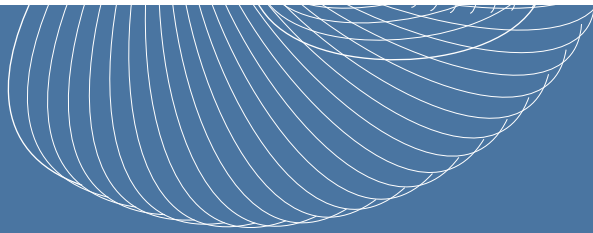
Entrust IdentityGuard: Autenticación segura y asequible para empresas

Como un líder consolidado y global en estrategias de seguridad probadas, Entrust ofrece una plataforma de autenticación versátil y asequible que puede ayudar a las organizaciones a proteger las identidades de los empleados y asociados comerciales que tienen acceso a información confidencial de la empresa.

La plataforma de autenticación versátil de Entrust IdentityGuard permite que las organizaciones igualen los mecanismos y la fortaleza de la autenticación con el nivel del riesgo involucrado, los requerimientos de capacidad de uso y las consideraciones de costo. Esto permite que las organizaciones apliquen una sólida autenticación a través de la empresa, en lugar de sólo a un grupo determinado de usuarios.

Beneficios de los productos

- Plataforma de autenticación versátil que puede implementarse a una fracción del costo de las opciones tradicionales
- La gama más amplia de métodos de autenticación rentables
- Sencillo de implementar y administrar con una arquitectura no invasiva
- Protege aplicaciones líderes como las redes privadas virtuales (VPN) tipo IP-SEC y SSL, aplicaciones de escritorio de Microsoft® Windows® y aplicaciones Web como Microsoft® Outlook® Web Access
- Amplio soporte para plataformas que incluye Microsoft® Windows® Server 2003, Sun Solaris, AIX y Linux



Entrust IdentityGuard se integra sin problemas con los entornos existentes produciendo un impacto mínimo en la experiencia del usuario. Esto presenta una ventaja a los usuarios que tienen acceso a la red mediante acceso remoto, equipos de escritorio con Microsoft Windows o por la red externa, la que puede usarse para aplicaciones líderes como Microsoft® Outlook® Web Access.

Ventajas de Entrust IdentityGuard

Gran gama de opciones de autenticación sólida

Entrust IdentityGuard proporciona la más extensa gama de opciones de autenticación disponibles en el mercado en la actualidad. La variedad de autenticadores de la solución permite la aplicación de una autenticación más sólida en toda la empresa sin la necesidad de implementar una solución de tamaño único que posiblemente no cumpla con los requerimientos específicos de la organización.

Con una versatilidad, eficiencia y asequibilidad sin igual, Entrust IdentityGuard permite la aplicación de una autenticación sólida sin la necesidad de instalar software o hardware en el lado del cliente ni de realizar cambios importantes en la experiencia del usuario.

Algunos autenticadores virtualmente no necesitan interacción del usuario, como la identificación de dispositivos, los certificados digitales y la geolocalización de IP. Las técnicas de autenticación que no necesitan un segundo factor de forma físico incluyen la basada en el conocimiento, el nombre de usuario y contraseña, los tokens de software por SMS, las tarjetas eGrid y los códigos de acceso de un solo uso (OTP) fuera de banda mediante SMS o voz.

La plataforma también soporta entornos de autenticación que requieren un factor de forma, lo que incluye las tarjetas de cuadrículas, los tokens de hardware OTP basados en eventos y en tiempo y los tokens tipo tarjeta delgada.

Entrust IdentityGuard permite un nivel de opciones, flexibilidad y personalización tanto a los usuarios finales como a las empresas. Las organizaciones pueden elegir la forma en que desean que sus usuarios se autenticen dependiendo del tipo de usuario, la evaluación de riesgo y la aplicación que se utilizará, incluyendo acceso remoto, equipos de escritorio con Microsoft® Windows® y aplicaciones instaladas en la red externa.

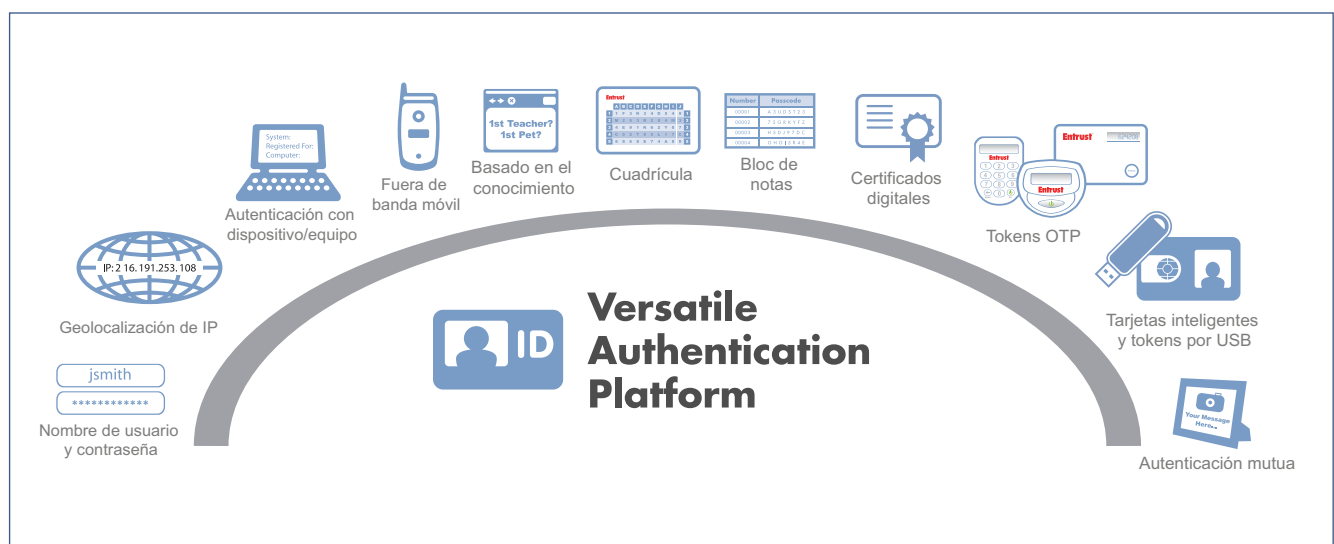


Imagen 1: Entrust IdentityGuard proporciona una de las más amplias gamas de opciones de autenticación disponibles en el mercado en la actualidad.



La plataforma puede extenderse fácilmente a otros canales de entrega, incluyendo sistemas de respuesta de voz interactiva (IVR) y sistemas de servicios de asistencia. Los métodos de autenticación de la solución no requieren de hardware especializado o conexiones de hardware directas con el equipo, por lo que se pueden utilizar a través de distintas plataformas y se pueden usar para realizar varios tipos de transacciones.

La gama de métodos de autenticación proporcionados por Entrust IdentityGuard se basa en una capa administrativa única que permite a las organizaciones administrar a todos los usuarios mediante un punto de aplicación de políticas, al mismo tiempo que pueden personalizar la política de autenticación específica para un usuario o grupo. La seguridad de la plataforma de autenticación versátil Entrust IdentityGuard está construida sobre un motor criptográfico de Entrust validado por el estándar FIPS 140-2.

Fácil de usar

La plataforma brinda la posibilidad de administrar la autenticación diaria en la empresa con un tipo de autenticador y luego usar una opción distinta para las aplicaciones de

servicio automático de recuperación de datos de usuario. Entrust IdentityGuard permite la creación de informes mejorados que posibilitan a los Administradores ejecutar informes del sistema y de los usuarios desde la consola de la plataforma. Esto les permite administrar eficientemente la implementación de Entrust IdentityGuard y mejorar la experiencia del usuario.

Plataforma abierta y no invasiva

La plataforma de autenticación versátil de Entrust IdentityGuard está diseñada para trabajar dentro del entorno de una organización produciendo un bajo impacto a la infraestructura existente.

Entrust IdentityGuard puede ejecutarse como un servidor de autenticación independiente o instalarse en servidores de aplicaciones líderes, incluyendo IBM y BEA, haciendo interfaz con la aplicación de inicio de sesión actual mediante los servicios Web. Esto permite una rápida integración con aplicaciones actuales que estén construidas en J2EE, .NET o en plataformas heredadas.

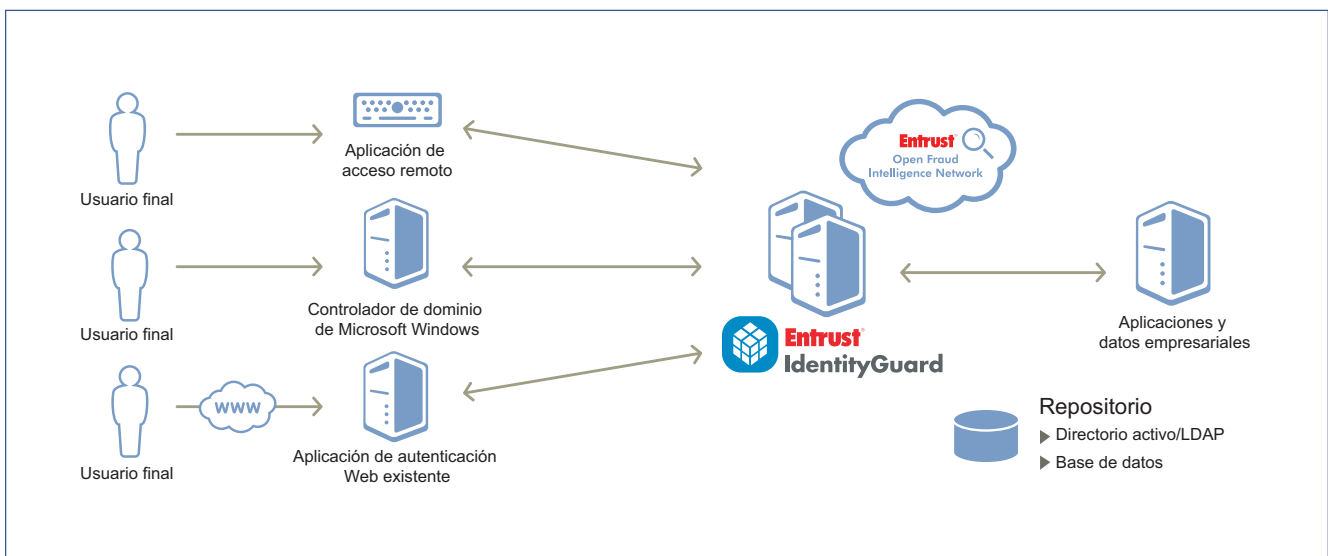


Imagen 2: Arquitectura empresarial de Entrust IdentityGuard



No requiere software de cliente o de servidor adicional para acceso remoto VPN ya que se integra con distintas aplicaciones líderes de VPN tipo SSL e IP-SEC de Cisco, Checkpoint, Juniper Networks, F5 y más. La solución además incluye soporte nativo para 802.1x.

Para las aplicaciones Web, las organizaciones pueden usar API de servicios Web estándar para integrarlas directamente en un portal empresarial o usar un filtro ISAPI estándar para proteger las aplicaciones líderes como Microsoft® Outlook® Web Access.

La solución usa los repositorios existentes para almacenar información de identidad en lugar de necesitar nuevas y costosas instancias, incluyendo soporte a directorios LDAP líderes como Sun One, Microsoft Active Directory y Novell y bases de datos de Oracle, IBM y Microsoft.

Se extiende fácilmente para abarcar la seguridad del consumidor

La característica única de Entrust IdentityGuard es su capacidad de proporcionar autenticación sólida tanto para entornos de empresas como de consumidores. No sólo se puede usar para proporcionar seguridad a aplicaciones empresariales, sino que también se puede extender para proporcionar autenticación sólida, rentable y muy utilizable para implementaciones de varios millones de usuarios que son muy comunes en la actualidad.

Más información

Para obtener más información acerca de Entrust IdentityGuard, comuníquese con el representante de Entrust en su zona al 613-270-3400 (ext. 5) o visite www.entrust.com/identityguard.

Acerca de Entrust

Entrust provee soluciones de seguridad basadas en la identidad, que posibilita a empresas, consumidores, ciudadanos y sitios web en más de 4000 organizaciones en 60 países. El enfoque de seguridad basada en la identidad de Entrust permite el balance correcto entre servicio, experiencia y costo. Para autenticación robusta, detección de Fraude, certificados digitales, SSL y PKI, llame al 613-270-3400 (ext. 5) correo electrónico entrust@entrust.com o visite www.entrust.com.

Entrust® Securing Digital Identities & Information

Entrust es una marca comercial registrada de Entrust, Inc. en Estados Unidos y otros países. En Canadá, Entrust es una marca comercial registrada de Entrust Limited. Los demás nombres de productos y nombres de servicios de Entrust son marcas comerciales o marcas comerciales registradas de Entrust, Inc. o Entrust Limited en determinados países. Los demás nombres de empresas, de productos y logotipos son marcas comerciales o marcas comerciales registradas de sus respectivos propietarios. © Copyright 2010 Entrust. Todos los derechos reservados.