TrustedX

Adaptive Authentication

Descripción

Plataforma de autenticación adaptativa y federación para entornos Web y Cloud:

- Soporta mecanismos de autenticación corporativos, sociales y gubernamentales.
- Autenticación acumulativa. Evalúa el nivel de confianza de la autenticación y lo eleva cuando la aplicación lo requiere.
- Análisis de información contextual. Mejora la seguridad de la autenticación sin alterar la experiencia del usuario.
- Gestiona la confianza en la federación de identidades y proporciona control de acceso único entre aplicaciones.
- Ofrece un sistema de reporting de la autenticación para reacción rápida a problemas de seguridad.

Beneficios

Proveedor de identidad

Actúa como proveedor de identidad, permite la federación con proveedores externos e incrementa la seguridad en la autenticación de los usuarios y grupos existentes. Soporta directorios corporativos (incluido Kerberos), eIDs nacionales e identificadores sociales (i.e. Linkedin, Facebook, etc).

Seguridad por capas

Aporta una capa adicional de seguridad que evalúa de forma transparente el nivel de riesgo de la autenticación en base al perfil, los hábitos y la biometría del usuario. El usuario sigue usando su identidad, solicitándole un paso adicional de autenticación únicamente cuando se supera un determinado umbral de riesgo.

Aplicaciones en la nube

Extiende el control de la autenticación corporativa a las aplicaciones cloud tales como Google Apps, Salesforce y Office 365 gracias a la implementación de protocolos generalizados en entornos Web y Cloud. Soporta SAML 2.0 y OAuth 2.0/OpenID Connect, facilitando la federación de aplicaciones.

Control centralizado y auditoría

Los factores de autenticación se pueden adecuar a cada colectivo de usuarios (empleados, partners, clientes, etc.) y para cada aplicación. La plataforma permite gestionar el Single Sign-On en función del nivel de confianza necesario en cada caso, actuar rápidamente ante incidentes de seguridad y concentrar la información de auditoría, aportando detalles de cada decisión de autenticación.

TrustedX

Adaptive Authentication

Funcionamiento

La plataforma de autenticación actúa de proveedor de identidad frente a múltiples aplicaciones mediante el uso de los conceptos siguientes:

- **Políticas de autenticación adaptativa:** Modelan un flujo de autenticación que puede solicitar un paso adicional (OTPs desplegados, SMS, e-mail, etc.) cuando se supera el umbral de riesgo aceptable.
- **Políticas de análisis de contexto:** Analizan el dispositivo del usuario, la ubicación y los hábitos de conexión para evaluar el riesgo de la autenticación. Cada política es altamente configurable para determinar qué factores se consideran y cuál es su peso**.**
- **Clasificación de mecanismos de autenticación:** Determina el nivel de seguridad alcanzado en cada autenticación.
- **Single Sign-On (SSO):** Agiliza la autenticación de los usuarios en múltiples aplicaciones, respetando las exigencias de seguridad.
- **Autenticación de servidor intuitiva:** Evita que los usuarios sucumban a ataques de phishing y pharming cuando no consiguen reconocer una imagen personalizada en la interfaz de autenticación.

El análisis de contexto presenta las siguientes características:

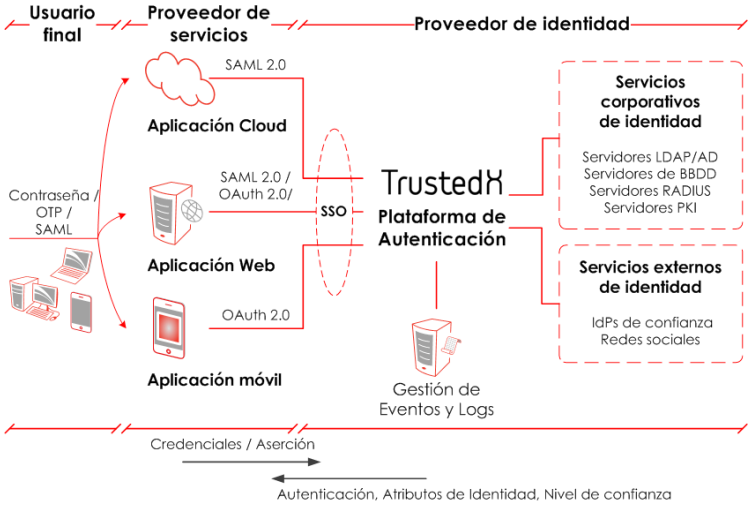
- TrustedX mantiene un perfil de cada usuario, que actualiza de forma progresiva y transparente después de cada acceso. Los perfiles pueden desvincularse de las identidades explícitas de los usuarios, para mantener su privacidad.
- Los usuarios pueden registrar explícitamente los dispositivos que consideran de confianza. TrustedX puede reconocer los dispositivos registrados por un usuario, así como cualquier otro dispositivo que haya utilizado en alguna ocasión.
- TrustedX reconoce la dinámica de tecleo del usuario. Se trata de un factor biométrico que no interfiere en la experiencia de usuario.
- A partir de la información de red, se puede obtener la ubicación geográfica del usuario, reconocer las ubicaciones que ha visitado anteriormente, e incluso cotejar si ha accedido con el mismo dispositivo desde esa ubicación. Además, se puede comprobar que haya podido desplazarse físicamente entre dos ubicaciones consecutivas.
- En la evaluación del riesgo de una autenticación se puede forzar que el usuario supere obligatoriamente un conjunto de factores. La alternativa es evaluar el riesgo mediante una combinación ponderada de varios factores opcionales, que individualmente contribuyen a detectar anomalías menores.
- Para facilitar la configuración de las políticas durante el periodo de preproducción, TrustedX puede operar como observador sin interferir en la autenticación habitual.
- La plataforma ofrece informes detallados y gráficos sobre los factores de autenticación analizados en cada acceso, tanto para facilitar la auditoría como el ajuste fino de las políticas aplicadas en cada caso de uso.
- La captura de todos los factores de contexto se basa en tecnologías de navegador (JavaScript) y servidor que no implican el uso de applets ni plugins, ni la instalación de software en los dispositivos de los usuarios.

Las aplicaciones pueden invocar las funcionalidades de autenticación mediante los protocolos SAML 2.0 (como es el caso de Google Apps, Salesforce y Office 365) y OAuth 2.0 (adecuado, entre otros, para aplicaciones móviles), ambos basados en HTTP. TrustedX incluirá en cada respuesta de autenticación los atributos de identidad necesarios para que las aplicaciones puedan establecer su propia sesión. Además, la plataforma está preparada para que las aplicaciones invoquen a los servicios de firma y cifrado de TrustedX.

Arquitectura

TrustedX media entre las aplicaciones de usuario y los servicios de identidad gestionados por la propia organización o por terceros (consorcios, redes sociales, etc.). La plataforma ofrece distintas estrategias de integración de la autenticación:

- Utilizando la interfaz de autenticación de usuarios finales propia de TrustedX.
- Integrando la autenticación en la interfaz de la aplicación para ofrecer una experiencia de usuario totalmente armónica con las aplicaciones.
- Externalizada en otros proveedores de identidad, complementándola con las funcionalidades de autenticación adaptativa y SSO de TrustedX.



Características técnicas

- **Formato:** Software appliance. Consultar para más información sobre entornos hardware o virtuales homologados.
- **Monitorización de eventos:** Simple Network Management Protocol (SNMP).
- **Acceso a bases de datos y directorios:** Oracle, Microsoft SQL Server o MySQL. Protocolo de acceso a directorio LDAP.
- **Integración con SMS gateways y servidores de correo electrónico** para autenticación adicional.
- **Acceso a servicios de autenticación** basada en LDAP/AD, RADIUS, etc.
- **Integración en aplicaciones** mediante SAML 2.0 y OAuth 2.0. Tecnologías HTML/JavaScript.
- **Clasificación de niveles de confianza (Trust level):** Basada en la OMB/NIST SP 800-63-1 (LoA classification) y estándar ISO/IEC FDIS 29115.

Safelayer Secure Communications S.A.
Basauri, 17 Edif. Valrealty Edif. B Pl. Baja Izquierda Ofi. B
28023 Madrid (Spain)
Tel. +34 917 080 480 Fax +34 913 076 652

www.safelayer.com
World Trade Center (Edif. Sud- 4ª Planta). Moll de Barcelona s/n
08039 Barcelona (Spain)
Tel. +34 935 088 090 Fax +34 935 088 091

SAFELAYER