Cifrado nativo de Alcatel-Lucent OmniPCX Enterprise Purple

Cifrado de software de las comunicaciones y plataforma reforzada contra los ciberataques

La digitalización está en marcha desde hace tiempo. Hoy en día, los empleados pueden colaborar desde cualquier lugar con la posibilidad de comunicarse en tiempo real. Pero no todas las herramientas de comunicación proporcionan el marco necesario para abordar la **disponibilidad continua**, **la seguridad**, **la confidencialidad** y **el cumplimiento**.

Alcatel-Lucent Enterprise (ALE) ha estado trabajando con organizaciones y clientes de todo el mundo para entender los nuevos retos a los que se enfrentan y proporcionar **soluciones de comunicaciones unificadas seguras** que permitan a los trabajadores trabajar desde cualquier lugar y con cualquier dispositivo.

En este documento describimos cómo **ALE protege sus comunicaciones de los ciberataques**, con una plataforma de comunicación segura por diseño, abierta a la nube con una arquitectura híbrida, con los mejores mecanismos de cifrado nativos, proporcionando un control total a su equipo de TI y el cumplimiento de sus políticas de seguridad y mejores prácticas.

Alcatel·Lucent
Enterprise

El panorama actual de la ciberseguridad

El cambio a un entorno digital ha provocado un rápido aumento de los ataques de phishing y ransomware. Se trata de una grave preocupación para el creciente número de trabajadores a distancia en el espacio y para todas las organizaciones (públicas y privadas). Con el aumento de las ciberamenazas, las empresas deben trabajar más que nunca para proteger a sus empleados y a sus clientes.

Un aspecto importante es el hecho de que el paso a la nube aumenta la "superficie de ataque", lo que significa que los hackers podrían explotar la apertura no segura de los servicios basados en la nube o el software como servicio (SaaS). Es necesario que el equipo de TI establezca requisitos estrictos para los acuerdos de nivel de servicio (SLA) de los proveedores.

Enfoque de seguridad por diseño de ALE

Un análisis exhaustivo del panorama actual permite a las empresas determinar las estrategias de protección que necesitan para sus activos de TI. Por ejemplo, ALE ofrece a las empresas las soluciones que necesitan para cumplir las normativas y estándares regionales o verticales, como el Reglamento General de Protección de Datos (RGPD), HDS o HIPAA (para el mercado sanitario), y la Directiva NIS 2 en los países de la Unión Europea.

ALE también ofrece una conectividad segura en la nube, con elementos de autenticación y cifrado mutuos , mejor comunicación confidencialidad en las reuniones, así como privacidad y control de los datos dentro de la nube. Una solución integral para cubrir el entorno de seguridad empresarial en evolución garantiza que los equipos puedan prosperar con seguridad en cualquier nuevo entorno.

La privacidad y la fiabilidad de los servicios en la nube a veces se ponen en duda. Los servicios en la nube de ALE ofrecen una estricta política de privacidad de datos con centros de datos en diferentes lugares para una cobertura de servicio mundial. ALE tiene puntos de presencia en países preocupados por la privacidad, como Francia, Alemania, Estados Unidos, Canadá, Singapur y Australia. Según los términos del contrato, los datos personales de los usuarios no se utilizan con fines comerciales o de marketing, y ALE garantiza el cumplimiento de las normativas locales sobre privacidad de datos, como el RGPD en los países europeos. Los servicios en la nube de ALE también cuentan con la certificación ISO 27001 relativa a la gestión de la seguridad de la información y CSPN de la entidad reguladora francesa ANSSI.

Los servicios en la nube de ALE también pueden aprovechar los servidores de comunicación del cliente. Los clientes pueden mantener los sistemas críticos de comunicación empresarial en sus instalaciones y conectarse a la nube para obtener aplicaciones y servicios de colaboración innovadores.

Arquitectura híbrida de comunicaciones unificadas

La plataforma de colaboración y comunicaciones unificadas es una importante herramienta fundacional para la empresa. Sin embargo, el retorno de la inversión solo se hace evidente con la inscripción de cada grupo de trabajo. Para ello, hay que consultar a las partes interesadas, y tener en cuenta y abordar sus preocupaciones, incluido el equipo de TI encargado de las políticas de seguridad.

Con demasiada frecuencia, las medidas de seguridad obstaculizan el uso regular de nuevos servicios innovadores. Cuando se trata de trabajo colaborativo, la experiencia del usuario debe seguir siendo intuitiva. Por parte de la administración , es importante verificar la compatibilidad de las plataformas en función de los entornos aprobados por el departamento de TI, incluyendo, por ejemplo, la admisión de aplicaciones móviles para smartphones y tabletas Android e IOS. Además, la solución colaborativa y el servidor de comunicaciones deben dialogar a través de APIs abiertas para facilitar la gestión y el control de los servicios telefónicos y las centrales en tiempo real. Esta evolución está llevando a los equipos de TI a un mayor control de las fases previas.

Alcatel-Lucent Enterprise ofrece soluciones integrales de **comunicaciones y colaboración en las instalaciones** y **basadas en la nube** para abordar la transformación digital.
Las soluciones de comunicación de ALE permiten la continuidad de las llamadas desde cualquier lugar, en cualquier situación y desde cualquier dispositivo.

Funciones clave de ALE para proteger las comunicaciones:

- **Conectividad segura** entre el sistema de comunicación de ALE en las instalaciones (IP-PBX y teléfonos) y la infraestructura de la nube, operada por ALE, con autenticación mutua, cifrado y controlador de límite de sesión (SBC) para proteger el acceso a la red pública y a los trabajadores remotos equipados con dispositivos y clientes SIP
- **Conexión sin fisuras** dentro y fuera de la organización. La infraestructura de comunicaciones subyacente conecta a los trabajadores híbridos con los empleados de administración y de primera línea, sin importar cuáles sean sus dispositivos, a través de una variedad de tecnologías estándar como PSTN, TDM, IP, SIP, VoWiFi y DECT, y proporciona las métricas para que la TI supervise la calidad de servicio (QoS)
- **Alta disponibilidad** que alcanza los 5x9 con arquitecturas espacialmente redundantes, desplegadas en las instalaciones del cliente o alojadas en una nube privada, 100 % basadas en software y totalmente virtualizadas, con protección contra ataques de denegación de servicio (DoS), seguridad integrada con dispositivos y sistemas operativos reforzados.
- **Privacidad y protección de datos** con control de acceso basado en funciones y encriptación de los datos almacenados. Esto asegura que todos los datos cruciales que se recogen en el entorno laboral, que está en constante evolución, esten totalmente protegidos de extremo a extremo y bajo su control.
- **Confidencialidad en las comunicaciones** con unos robustos mecanismos de cifrado basados en estándares del sector implementados nativamente en la solución, sin que afecten a la calidad y el rendimiento de la voz, y proporcionando la experiencia que esperan los clientes y los empleados.

Las comunicaciones son susceptibles de ser interceptadas y escuchadas por cualquiera, a través de la red corporativa (LAN o WLAN) y aún más a través del Internet público. Múltiples contramedidas a nivel de infraestructura de red minimizan el riesgo de interceptación (entorno de LAN conmutada, segmentación de VLAN, gestión de ACLs entre VLANs, protección contra el ARP spoofing o flooding), pero la única forma de garantizar una protección completa es que la conversación esté totalmente cifrada en tránsito: incluso si es interceptada por una persona malintencionada, la conversación de voz seguirá siendo inaudible porque el descifrado no es posible.

Alcatel-Lucent OmniPCX® Enterprise Purple (OXE Purple) ofrece un cifrado nativo **integrado** para garantizar el cifrado completo de cualquier comunicación a través de la red (Internet privada y pública).

Principios de cifrado nativo OXE Purple

OXE Purple ofrece soluciones de comunicación empresarial diseñadas para la era digital. Conecta a toda la empresa y le proporciona la **libertad**, la **agilidad** y la **seguridad** que necesita para hacer crecer su negocio con confianza.

OXE Purple ofrece la:

- **Libertad** para conectarse en cualquier momento con clientes y compañeros. Les permite conectarse en la oficina, en los edificios industriales, en la carretera o en casa, utilizando un smartphone, un ordenador o un teléfono específico.
- **Agilidad** para automatizar las operaciones de comunicación empresarial mediante una nube privada e integrar las interacciones en tiempo real en los procesos de negocio.
- **Seguridad** para cualquier interacción dentro y fuera de la empresa, ya sea la conexión con un colega, un socio, un cliente o un agente del centro de contacto. Las interacciones pueden realizarse por teléfono, en una aplicación del ordenador o el smartphone, videoconferencias y desde un sistema de mensajería seguro en la nube.

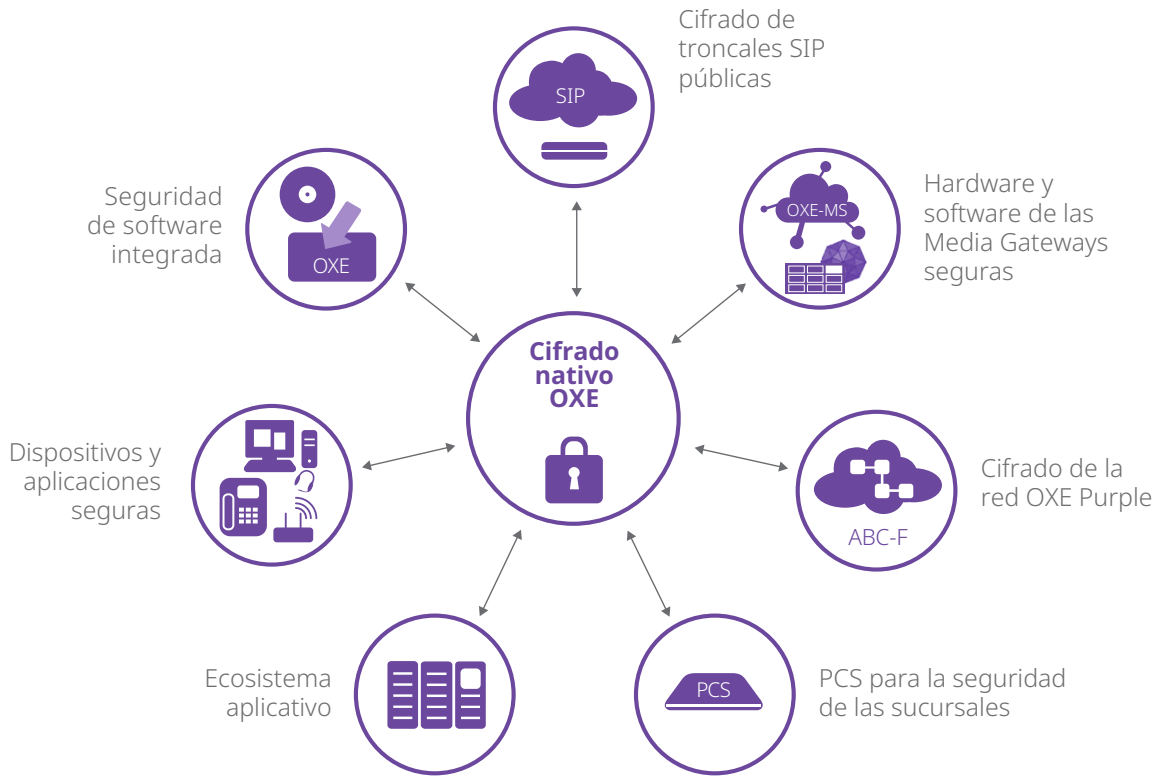
Esta tecnología puede desplegarse de forma segura en cualquier entorno: en las instalaciones o alojada en una nube privada. Está **basado al 100 % en software**, admite **virtualización** y ofrece una **alta disponibilidad de 5x9s** con redundancia en caliente de los componentes principales.

Proporciona confidencialidad con estándares de cifrado de última generación con cifrado completo en tránsito para todas las conversaciones sea cual sea el dispositivo o la aplicación de software. Dispone de una arquitectura flexible, que permite identificar a los usuarios sensibles de entre todos los empleados, que utilizan dispositivos IP o no IP.

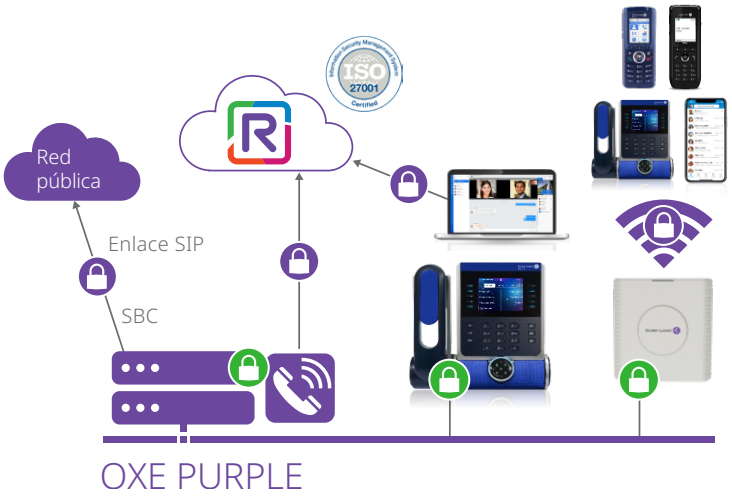
Componentes de cifrado nativo OXE Purple

El cifrado nativo OXE Purple ofrece:

- **Cifrado del flujo de señalización** mediante los protocolos Datagram Transport Layer Security (DTLS) o Transport Layer Security (TLS). Esto se aplica a los flujos de señalización intercambiados entre el servidor de comunicación OXE Purple y los dispositivos y aplicaciones IP compatibles con DTLS/TLS.
- **Cifrado del flujo de voz** mediante el protocolo SRTP. Esto se aplica a los flujos de voz intercambiados entre dispositivos y aplicaciones IP compatibles con DTLS.
- **Autenticación mutua** como opción entre servidor y dispositivos/clientes.
- **Media Gateways IP seguras** (basadas en software puro o en hardware propietario) para el procesamiento de medios cifrados, incluidos los teléfonos no IP conectados a placas de hardware (digitales y analógicas).
- **Cifrado de las comunicaciones** a la red pública a través del enlace SIP público hasta el elemento fronterizo del proveedor de servicios utilizando SIP TLS.
- **Cifrado de las conversaciones** mediante la aplicación del cliente de Rainbow (en escritorio, web, smartphone android e iOS) a través de la pasarela Rainbow WebRTC para comunicaciones internas (a un dispositivo u otra aplicación gestionada por el servidor de comunicación OXE Purple) o a la red pública.
- **Cifrado de las comunicaciones** en una red de servidores de comunicación OXE Purple.
- **Compatibilidad con la georredundancia** del servidor de comunicaciones OXE Purple y del servidor de comunicaciones pasivo (PCS) para la sucursal segura en modo de supervivencia.
- **Autoridad de certificación (CA) y almacén de confianza integrados** para la autenticación basada en certificados, con la posibilidad de que el cliente personalice el certificado con una infraestructura de clave pública (PKI) externa para lograr una privacidad total.



El cifrado nativo OXE Purple es compatible con la mayoría de los dispositivos y aplicaciones IP conectados al servidor de comunicación (incluidos los teléfonos de escritorio, softphones y estaciones base IP DECT). También admite el cifrado completo en tránsito para un usuario equipado con un equipo no IP (por ejemplo, un teléfono analógico o digital) conectado a una pasarela de medios de hardware gestionada por el servidor de comunicación OXE Purple. Además, la función es compatible con la aplicación de colaboración basada en la nube Rainbow™ de Alcatel-Lucent Enterprise.

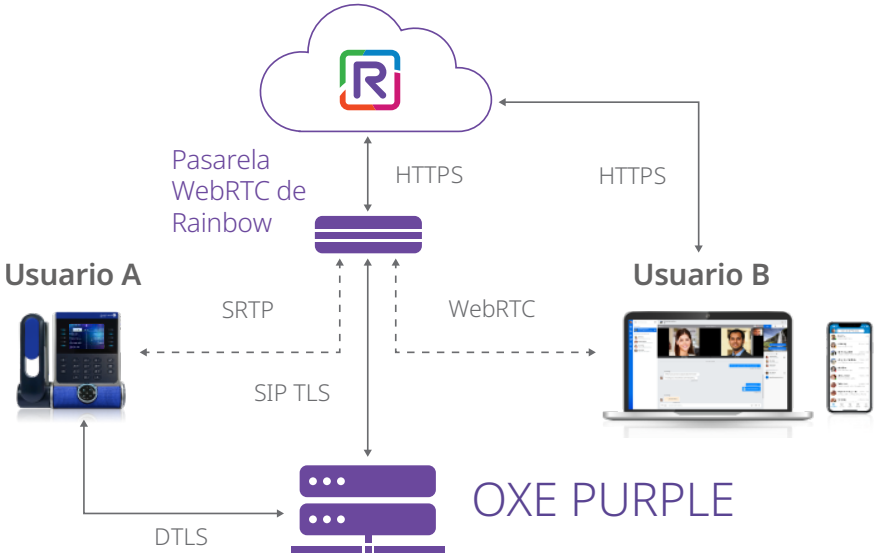


La conexión entre el servidor de comunicación OXE Purple y los servicios en la nube de Rainbow está garantizada por el componente de software de la pasarela Rainbow WebRTC.

La pasarela Rainbow WebRTC genera un par de claves asimétricas y exporta una solicitud de firma de certificado (CSR) para que sea firmada por una autoridad de certificación (CA) que puede ser la autoridad de certificación (CA) integrada en OXE Purple Communication Server o una infraestructura de clave pública (PKI) externa. La identidad de la pasarela Rainbow WebRTC es controlada por el servidor de comunicación OXE Purple durante el handshake TLS utilizando la lista de certificados de confianza (CTL) en su almacén de confianza.

Como se ilustra en el siguiente diagrama, los medios de voz se cifran en tránsito entre el usuario A en un teléfono de escritorio y el usuario B equipado con la aplicación del cliente de Rainbow, en PC/Mac/Web o smartphone. La pasarela Rainbow WebRTC realiza la retransmisión en tiempo real del flujo SRTP entre el usuario A y el usuario B.

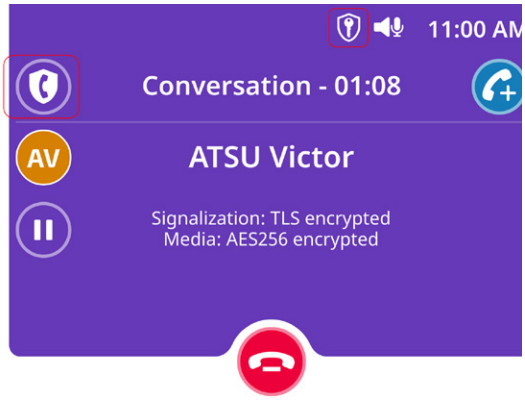
La pasarela Rainbow WebRTC es un componente de software completo que está virtualizado, admite la duplicación y el equilibrio de carga para una mayor escalabilidad.



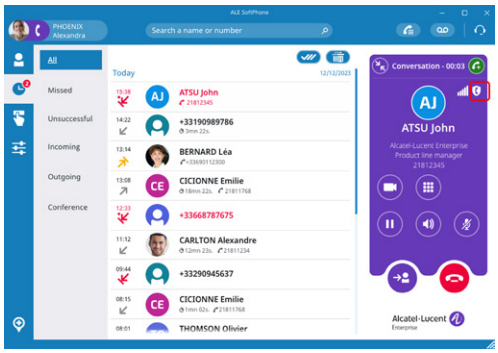
Icono de cifrado en las aplicaciones de softphone y teléfonos ALE

Cuando una comunicación está cifrada, aparece un icono de escudo o candado en la pantalla del teléfono o en la aplicación de softphone. Este mecanismo proporciona a los usuarios finales confianza en la confidencialidad de la conversación.

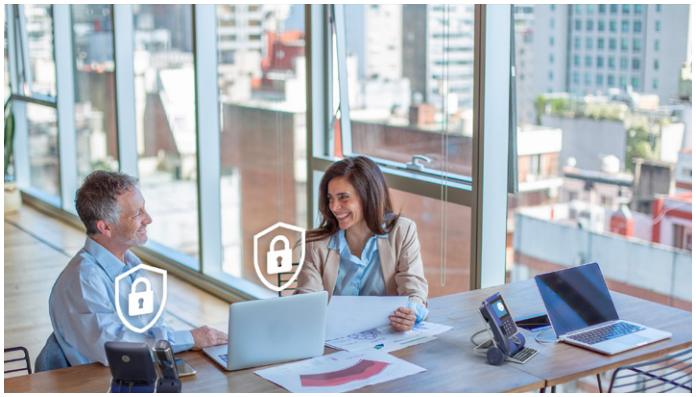
Teléfonos



Softphones



ALE SoftPhone



Hoja de soluciones
Cifrado nativo Alcatel-Lucent OmniPCX Enterprise Purple

Características y ventajas

Funciones	Ventajas
Confidencialidad cliente/dispositivo (protocolo y medios de señalización)	Prevención de ataques maliciosos, ataques de suplantación en teléfonos IP y escuchas no autorizadas de las comunicaciones
Autenticación mutua e integridad de la señalización de control de llamada (que garantiza que no se han modificado los mensajes) con la opción de personalización de certificados	Protección de las comunicaciones empresariales contra ataques de denegación de servicio
Compatible con DTLS 1.2 y SRTP con AES 256: • 100 % basado en software • Autenticación certificada SHA2 (4096 bits) • Teléfonos de escritorio ALE Enterprise y Essential (IP), IP Desktop Softphone, compatible con los teléfonos de escritorio ALE Premium de la serie S • GD4-XL/GD4/GD3/INTIP3/OMS y PCS • Cifrado DECT IP-XBS	Mecanismos de cifrado de última generación para garantizar el máximo nivel de protección y confidencialidad para todas las conversaciones, sea cual sea el dispositivo de hardware o la aplicación de software que utilice el empleado
Compatible con TLS 1.2 y SRTP con AES 256: • DeskPhones ALE Enterprise y Essential (ALE-30) en modo SIP, ALE-2 y ALE-3, ALE SoftPhone • Enlaces SIP • Cifrado de pasarela Rainbow WebRTC	Protección de las conversaciones dentro y fuera de la red corporativa, incluido el acceso a la red pública mediante enlaces SIP
Icono de cifrado en el teléfono y en la aplicación de softphone para indicar que la llamada está cifrada y es segura	Confianza del usuario final en la confidencialidad de la conversación
Cifrado de llamadas en tránsito con la aplicación Rainbow a través de la pasarela Rainbow WebRTC	Garantizar la confidencialidad de las conversaciones de los empleados que utilizan la aplicación del cliente de Rainbow en PC/Mac, Web, smartphone Android y iPhone
Grabación de llamadas cifrada con Alcatel-Lucent OmniPCX® RECORD Suite	Garantizar la confidencialidad de las conversaciones grabadas
Función de cifrado integrado basada en software para la solución OmniPCX Enterprise Purple	Implantación de procesos de seguridad de alto nivel sin entorpecer la administración del sistema de comunicación
Repercusión nula sobre las opciones de calidad de servicio (QoS) y la configuración de la red	Despliegue y configuración sencillos sin necesidad de cambios en la infraestructura de red
Apoyo a la redundancia geográfica y a la supervivencia de las sucursales locales	Continuidad del negocio en todas las situaciones sin comprometer la confidencialidad en caso de fallos de la red, del servidor o del centro de datos

Recomendaciones y buenas prácticas de ALE

Todas las empresas (públicas y privadas) son objetivos importantes de los ciberataques. Es esencial implementar el equipo más seguro disponible. Las herramientas de gestión integradas deben permitir la supervisión de la seguridad en todos los elementos.

Además, los dispositivos móviles están transformando el panorama de las comunicaciones y aumentando la necesidad de seguridad a medida que los ciberatacantes explotan los crecientes volúmenes de código contenidos en cada punto de acceso. El cifrado de nivel de defensa, la privacidad de los datos y los entornos de comunicación protegidos requieren una infraestructura segura y altamente disponible que sea eficiente y fácil de administrar.

ALE le recomienda:

Actualizar y supervisar su sistema de comunicación:

- Las actualizaciones del sistema son de vital importancia en términos de ciberseguridad. Esto mantiene su sistema de comunicación actualizado con protección contra la vulnerabilidad del software.
- Habilite la supervisión de su sistema de comunicación para rastrear actividades sospechosas mediante la configuración de umbrales de uso y alarmas en el sistema de gestión de la red

Autenticar y cifrar:

- Habilitar la autenticación mutua entre todos los dispositivos (teléfonos y pasarelas) y el servidor de comunicación con certificados personalizados en los entornos más sensibles
- La señalización debe estar cifrada para evitar los ataques de envenenamiento del protocolo y los ataques de intermediario
- Las comunicaciones IP deben estar cifradas para evitar las escuchas

Haga que su sistema de comunicación sea redundante y añada un componente de seguridad:

- El riesgo nunca puede ser igual a cero. Si una pasarela o el sistema de comunicación principal no funciona, un sistema de reserva puede tomar el relevo sin problemas cuando hay redundancia espacial
- Añada los componentes necesarios para proteger su sistema de comunicación, como un Session Border Controller (SBC) o un Reverse Proxy (RP), mientras que los servidores de notificación se utilizan para alertar a las personas necesarias

Educar:

- Eduque a los usuarios y administradores; aplique las mejores prácticas en sus equipos, incluyendo recordatorios para actualizar las contraseñas, forme a los usuarios sobre cómo luchar contra la ciberdelincuencia y cómo reconocer una llamada cifrada con el icono de escudo o candado en el teléfono

Para más información, consulte nuestros recursos adicionales:

Folleto OmniPCX Enterprise Purple

Ficha técnica OmniPCX Enterprise Purple

Protección de las soluciones de comunicaciones unificadas y colaboración

Alcatel·Lucent Enterprise