# Forescout eyeExtend Connect

## Integre fácilmente sus productos con la plataforma Forescout para obtener visibilidad de los dispositivos en su contexto y acelerar la respuesta ante amenazas en toda la empresa

Para aumentar el valor que se obtiene de la inversión en tecnologías de seguridad y de la información, los clientes de Forescout aprovechan las integraciones incluidas con productos de nueve tecnologías de seguridad conocidas. Dichas integraciones mejoran enormemente la eficiencia, gracias a la organización de los flujos de trabajo de seguridad. Además de estas ofertas prediseñadas, Forescout proporciona ahora a los clientes un método más rápido y sencillo para integrar más tecnologías en la plataforma Forescout. eyeExtend Connect, un nuevo producto de Forescout, permite ahora a nuestra comunidad de clientes y partners crear, consumir y compartir apps de eyeExtend que conectan la plataforma Forescout a otras tecnologías. De esta forma, los miembros de la comunidad aprovechan el valor de los productos de seguridad que ya poseen, junto al detallado contexto de los dispositivos que proporciona Forescout, automatizan los flujos de trabajo de seguridad y la implementación de directivas en soluciones distintas, y aceleran la respuesta en todos los sistemas con el fin de reducir los riesgos.

## La solución

Forescout eyeExtend Connect simplifica la creación de apps que son fáciles de utilizar y desplegar. Mediante las apps de Forescout eyeExtend, ahora es posible integrar la plataforma Forescout fácilmente con sus tecnologías de IT y de seguridad, y organizar flujos de trabajo de seguridad entre tecnologías de ciberseguridad dispares.

Con eyeExtend Connect, sus tecnologías de seguridad actuales aprovechan el detallado contexto de los dispositivos que ofrecen los datos de Forescout eyeSight, que incluyen, entre otra información, sus propiedades, el estado de la seguridad, el nivel de cumplimiento de las directivas de la empresa, la ubicación en la red o el contexto de los usuarios. Es posible extraer estos datos de dispositivos automáticamente mediante otros productos de IT o seguridad, o bien insertar los datos de dichos productos en la plataforma Forescout. eyeExtend Connect, además, ayuda a acelerar la respuesta a las amenazas, ya que permite automatizar acciones basadas en directivas aplicables a todos los sistemas, destinadas a reducir las amenazas, los incidentes y el incumplimiento de normativas.

eyeExtend Connect ofrece las siguientes herramientas para la organización de flujos de trabajo y el intercambio del contexto de los dispositivos.

eyeExtend connect

### Problemas

- La dependencia de productos de integración prediseñados de Forescout o de otros partners tecnológicos impide organizar el flujo de trabajo con otras tecnologías de seguridad internas de las empresas.
- Los largos ciclos de desarrollo de integraciones personalizadas aumentan el tiempo necesario para rentabilizar las inversiones actuales en seguridad.
- Las herramientas de seguridad que funcionan de forma aislada, sin compartir el contexto de los dispositivos y usuarios, requieren un gran esfuerzo manual para responder a los incidentes de seguridad, lo que incrementa el ciberriesgo y la pérdida de productividad.

### Ventajas

- Maximice la rentabilidad de su inversión actual en tecnología, gracias a la integración con todo tipo de herramientas de terceros.
- Consiga una rentabilización más rápida mediante la integración rápida y fácil con la plataforma de Forescout a través de las apps de eyeExtend.
- Mejore el estado de su seguridad gracias a la armonización de las herramientas de IT y de seguridad, la rápida obtención de información práctica sobre los dispositivos y la automatización de la resolución de riesgos y amenazas.

## Ventajas

- Cree y despliegue apps de eyeExtend fácilmente para integrarlas con la plataforma abierta Forescout.
- Comparta sus apps con la comunidad para colaborar y obtener aportaciones de otros miembros.
- Cree apps portátiles con scripts Python y configuración JSON.
- Se admite la integración con una amplia variedad de servicios web de terceros.
- Amplíe las funciones de visibilidad y control de Forescout con contexto de dispositivos y controles de otros distribuidores.
- Se admiten integraciones bidireccionales con interfaces API REST abiertas, basadas en estándares.
- Inserte y extraiga información de una base de datos SQL estándar.
- Genere consultas personalizadas para extraer e insertar información en un servidor LDAP estándar.
- Envíe y reciba información a través de syslog a un servidor seleccionado

## Apps de eyeExtend

Cree apps que aprovechen las funciones de la plataforma Forescout para conocer y compartir el contexto de los endpoints, aplicar acciones de control de la red e implementar directivas en todos los sistemas. eyeExtend Connect proporciona un esquema JSON fácil de utilizar, para definir parámetros, etiquetas y configuraciones controladas por el usuario para que sus apps de eyeExtend sean portátiles (se puedan migrar de entornos de prueba a producción, de la región A a la región B, de entornos de IT a OT, etc.). Además, las interacciones con API de terceros están definidas con scripts Python habituales, lo que ofrece bastante flexibilidad, ya que amplía los tipos de integraciones que se pueden generar. Los casos de uso e implementaciones esenciales, como la mitigación de amenazas, la respuesta ante incidentes y la gestión de cumplimiento, se pueden automatizar con plantillas de directivas que se integran en las apps.

Características principales de las apps de eyeExtend:

- Plug-and-play
- Descubrimiento de nuevos dispositivos y propiedades
- Acciones de control de terceros externos
- Plantillas de directivas personalizadas
- Interacciones con API a través de scripts
- Iconos de terceros personalizables

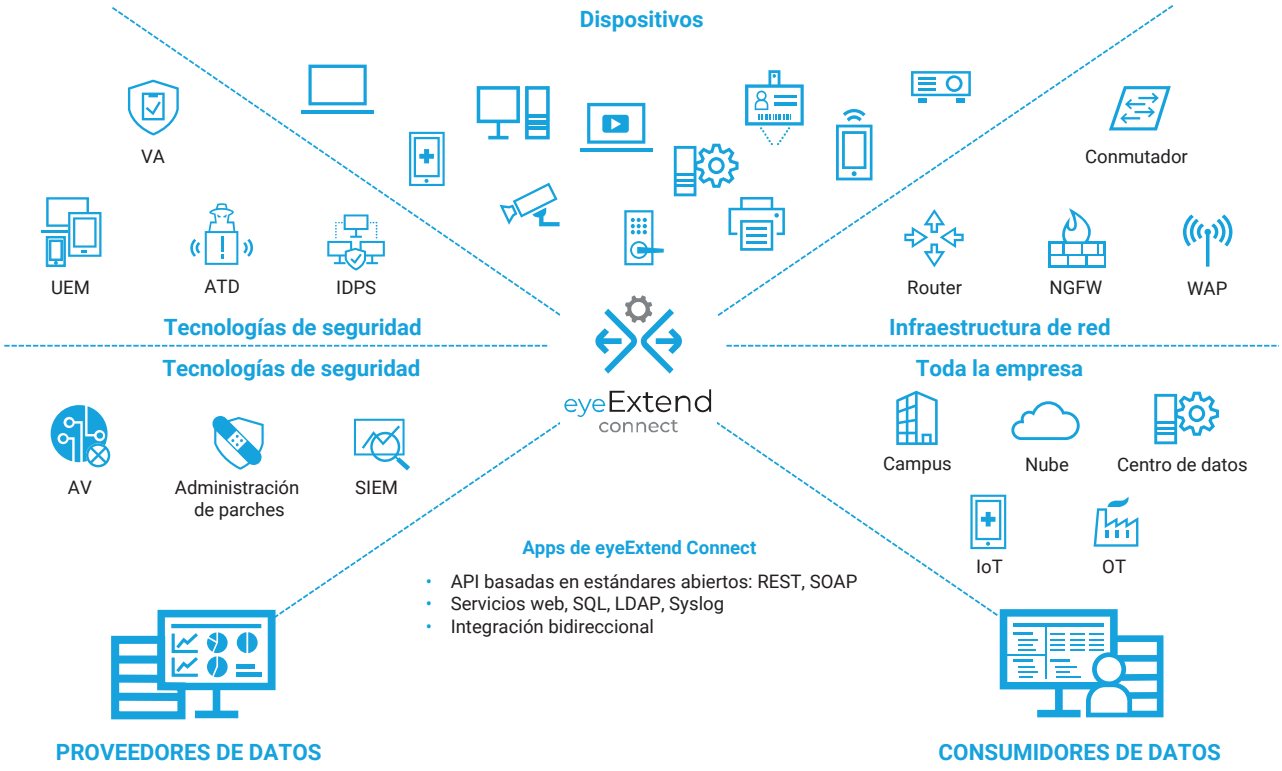
**API web e intercambio de datos (DEX)**
La plataforma Forescout proporciona un grupo de interfaces API RESTful que permiten a aplicaciones externas recuperar las propiedades y la información de directivas de Forescout. El plugin de intercambio de datos (DEX) facilita la comunicación bidireccional entre la plataforma Forescout y las API RESTful externas, para compartir el contexto de los dispositivos en tiempo real.

**SQL**
El plugin DEX puede insertar y extraer información de una base de datos SQL estándar. Este tipo de integración permite a las aplicaciones diseñadas internamente compartir información con productos de terceros que pueden interactuar a través de una base de datos interna o externa. Puede consultar bases de datos externas y crear propiedades de host para almacenar los datos que recupera la plataforma Forescout. Estas propiedades de host se pueden utilizar en las directivas de Forescout y se pueden consultar en vistas de dispositivos NAC y de inventario. Además, las bases de datos externas se pueden actualizar según la información que obtiene la plataforma Forescout, habitualmente para un producto de terceros.

**LDAP**
Genere consultas personalizadas a través del plugin DEX para extraer e insertar información en un servidor LDAP estándar. Por ejemplo, puede consultar el servidor LDAP para obtener información y crear las propiedades de host de Forescout para almacenar los datos que se han recuperado. Estas propiedades de host se pueden utilizar en las directivas de Forescout y se pueden consultar en vistas de dispositivos NAC y de inventario.

**Syslog**
El plugin DEX se puede configurar para enviar y recibir información a través de syslog a un servidor seleccionado. Este tipo de interfaz se utiliza para distintas integraciones con productos que incorporan registros y permite el análisis de los registros, como productos de administración de información y eventos de seguridad (SIEM), o con otras soluciones que envían y reciben alertas de esta manera. El formato del mensaje es personalizable.

### Figura 1: Organice los flujos de trabajo en distintos dispositivos, entornos y tecnologías de seguridad.




**VA:** Evaluación de vulnerabilidades, **ATD:** Detección de amenazas avanzadas, **IDPS:** Prevención de intrusiones en red, **UEM:** Administración de endpoints unificada, **AV:** Antivirus, **SIEM:** Administración de información y eventos de seguridad, **WAP:** Punto de acceso inalámbrico, **NGFW:** Firewall de próxima generación

## Casos de uso general

Forescout ofrece 25 soluciones listas para utilizar para resolver casos de uso concretos, en cambio, las apps de eyeExtend permiten resolver casos personalizados de los clientes. A continuación se incluyen algunos ejemplos:

**Descubra, clasifique y evalúe todos los dispositivos conectados a la red en el instante que se conectan**
Forescout eyeExtend Connect, basado en Forescout eyeSight, permite a un producto de IT o de seguridad integrado proporcionar contexto para identificar mejor los dispositivos en toda la empresa, incluidos los entornos de campus, centros de datos, OT y nube. Por ejemplo, la app eyeExtend para Ubiquiti ayuda a los clientes a incrementar la visibilidad de los dispositivos conectados a la Wi-Fi y usar los atributos de dispositivos que descubren, para tomar mejores decisiones sobre directivas en la plataforma Forescout. A continuación, esta app puede suministrar a otro producto ITSM (del inglés, Gestión de servicios de IT) o de administración de activos la información del dispositivo conectado a la Wi-Fi Ubiquiti, con el fin de ajustar su base de datos de administración de configuración (CMDB). Otra importante app, eyeExtend para Google Cloud, ayuda a los clientes a obtener visibilidad en tiempo real de sus instancias de computación en la nube y ver cómo evolucionan, mediante la integración con Google Cloud y la inserción del contexto de inventario de Google Cloud.

**Mejore la visibilidad y el control de los dispositivos conectados a VPN que acceden a la red**
eyeExtend Connect identifica todos los dispositivos que se conectan a la red corporativa a través de VPN. Gracias a la integración con la plataforma Forescout, los operadores de seguridad pueden determinar si el activo que se conecta a través de VPN es un recurso corporativo y controlar el acceso de los dispositivos que se conectan desde ubicaciones no autorizadas.

**Organice la seguridad o el flujo de trabajo de información de incumplimiento de directivas de IT**
Envíe alertas en tiempo real cuando se produce el incumplimiento de directivas, a través de plataformas de colaboración y mensajería. Al adoptar decisiones de directivas para automatizar las acciones de control de la red, puede configurar una directiva para obtener de la plataforma Forescout datos de incidentes de dispositivos, mediante plataformas de correo electrónico, mensajería o colaboración. Por ejemplo, la app eyeExtend para Slack se integra con la plataforma de colaboración para enviar alertas en tiempo real del incumplimiento de directivas a un canal que utiliza el equipo de IT o seguridad en Slack.

**Automatice la incorporación de dispositivos móviles, mejore la administración de la seguridad e implemente el cumplimiento continuo**
eyeExtend Connect organiza las acciones de intercambio y control de la información de los dispositivos con sistemas UEM para proporcionar una administración unificada de las directivas de seguridad para los dispositivos de su red, con independencia de su tipo (PC, Mac, Linux®, tablet, smartphone), conexión (por cable, inalámbrica, VPN), o el propietario (la empresa o un usuario individual). Esta administración de dispositivos global permite automatizar la incorporación de dispositivos, conseguir el cumplimiento de los dispositivos a través de acciones activadas por directivas, aplicar controles personalizados de acceso a la red y acelerar la respuesta y la corrección. Por ejemplo, con la app eyeExtend para Google Mobile Management, los clientes tienen ahora visibilidad del contexto de los dispositivos Chromebook. Estos datos ayudan a mejorar las directivas de acceso y seguridad de los dispositivos personales usados en la empresa (BYOD).

**Automatice las acciones y flujos de trabajo dentro del ecosistema de productos de IT y seguridad para mejorar las operaciones y reforzar la seguridad en toda la empresa**
eyeExtend Connect puede reenviar o recibir activadores de acciones que indican a la plataforma Forescout o a otro producto integrado que realice una acción específica. Estos activadores emplean automatización basada en directivas, en lugar de decisiones basadas en un guion, que requieren la intervención humana. Esto se traduce en un tiempo de respuesta más rápido y unas redes más seguras de forma generalizada.

**Aproveche los datos de contexto de los dispositivos para efectuar un análisis de correlación y acelerar la respuesta a incidentes**
eyeExtend Connect permite a la plataforma Forescout suministrar datos detallados de los dispositivos a un sistema SIEM para efectuar un análisis de correlación. De esta forma se obtiene una imagen completa de la superficie de ataque en toda la empresa, se reduce el tiempo para obtener información y se facilitan las investigaciones. Además, la plataforma Forescout simplifica las operaciones de seguridad, gracias a la automatización de acciones basadas en directivas, limitando el acceso del dispositivo a la red en función de la gravedad del incidente, que se obtiene del sistema SIEM en tiempo real.

En resumen, eyeExtend Connect le ayuda a conseguir rápidamente una mayor rentabilidad de la inversión en seguridad, ya que elimina el aislamiento de las herramientas de seguridad y las conecta a la inteligente plataforma Forescout, con el fin de automatizar de manera importante la mitigación de amenazas y el cumplimiento de normativas.

Nota: Algunas de las funciones de eyeExtend Connect formaban parte antes de producto OIM. Todas las funciones de OIM se han incorporado a eyeExtend Connect.

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San José, CA 95134, EE. UU.

C. e.: info-espana@forescout.com
Tel. (internacional) +1-408-213-3191
Soporte técnico 1-708-237-6591

Más información en Forescouttechnologies.es