



# Forcepoint DLP

**TERMINE CON EL ROBO Y LA PÉRDIDA DE DATOS, DEMUESTRE QUE CUMPLE CON LOS REQUISITOS REGLAMENTARIOS Y PROTEJA SU MARCA, SU REPUTACIÓN Y SU PROPIEDAD INTELECTUAL**



# Forcepoint DLP

**TERMINE CON EL ROBO Y LA PÉRDIDA DE DATOS, DEMUESTRE QUE CUMPLE CON LOS REQUISITOS REGLAMENTARIOS Y PROTEJA SU MARCA, SU REPUTACIÓN Y SU PROPIEDAD INTELECTUAL**

La fuga de datos puede tener consecuencias devastadoras, desde una reputación dañada hasta multas y sanciones reguladoras. Forcepoint DLP le permite descubrir y proteger la información confidencial donde quiera que ésta se encuentre: en las terminales, en la nube o en las instalaciones. Adopte servicios de colaboración en la nube, como Microsoft Office 365 y Box, para promover la innovación y fomentar el crecimiento de su empresa. Proteja la información de importancia crítica en computadoras portátiles con Mac OS X y Microsoft Windows. Proteja información personal y de propiedad intelectual, cumpla rápidamente con los requisitos reglamentarios mediante una extensa biblioteca de políticas predeterminadas y haciendo uso de las capacidades únicas que Forcepoint pone a su alcance para la prevención de la pérdida de datos (DLP, Data Loss Prevention) y detener el robo de datos.

## Forcepoint DLP enriquece su negocio

- Reduzca el riesgo de robo de datos al adoptar servicios en la nube como Microsoft Office 365 y Box ya que ofrecen mayor visibilidad de la información.
- Implemente controles efectivos de seguridad que fácilmente puede auditar para cumplir con los requisitos reglamentarios.
- Identifique información confidencial contenida en imágenes y capturas de pantalla.
- Identifique y prevenga amenazas internas mediante el análisis de comportamientos.
- Encuentre y proteja fácilmente los archivos almacenados en dispositivos de usuarios finales con Mac, Microsoft Windows y Linux.
- Unifique sus soluciones de seguridad, coordine las políticas de defensa, comparta la inteligencia entre distintos puntos y aproveche las ventajas de centralizar la administración de la seguridad de sus datos.
- El centro de gestión de incidentes y el flujo de correo electrónico le permiten que las personas adecuadas revisen los incidentes y respondan frente a la pérdida de datos cuando se produzcan.

## Principales características

- Reconoce la información confidencial oculta en imágenes, documentos escaneados y capturas de pantalla.
- Implementa con seguridad servicios en la nube, como Microsoft Office 365 y Box, y conserva la visibilidad y el control de la información confidencial.
- Drip DLP evalúa la actividad de transmisión acumulativa de datos en el transcurso del tiempo, descubriendo las pequeñas fugas de de datos.
- Identifica a los empleados de alto riesgo al detectar las actividades que indican el robo
- Detecta datos de marcas digitales en los dispositivos finales dentro o fuera de la red corporativa.
- Acepta dispositivos finales de Mac OS X y Microsoft Windows.
- Detecta la información confidencial enviada fuera de la organización por correo electrónico, descargas en la web, IM y servicios en la nube para clientes. Incluye decodificación de SSL cuando se usa con Forcepoint Web Security.

# “La seguridad de datos TRITON Architecture fue la solución más sólida que encontramos para estar protegidos y prevenir las fugas de datos.”

– Amir Shahar, Gerente de Seguridad de la Información, Cellcom Israel Ltd.

## Capacidades de Forcepoint DLP

### ▶ ADOpte LA INNOVACIÓN CON CONFIANZA

Para satisfacer las necesidades de sus clientes y seguir siendo competitivo necesita innovar y dejar que sus empleados adopten nuevas tecnologías. Con Forcepoint DLP de Forcepoint usted puede aprovechar poderosos servicios en la nube tales como Microsoft Office 365, Box y Salesforce.com, los cuales permiten que su organización siga creciendo e innovando. Forcepoint DLP potencia las capacidades de sus empleados móviles, protegiendo la información confidencial y la propiedad intelectual dentro y fuera de su red.

### ▶ CUMPLA CON LOS REQUISITOS REGLAMENTARIOS Y DEMUÉSTRELO

Una extensa biblioteca de políticas predeterminadas hace que sea más fácil para su personal de IT implementar rápidamente los controles necesarios para cumplir con los requisitos reglamentarios y proteger la propiedad intelectual. Usted puede elegir las políticas adecuadas para cumplir con sus requisitos reglamentarios, así como las políticas necesarias para proteger su propiedad intelectual. Forcepoint le ofrece un conjunto de capacidades avanzadas de detección de IP cuya flexibilidad le permite satisfacer las necesidades de protección de datos, mediante una interfaz GUI fácil de usar y con la que podrá seleccionar políticas adecuadas para la protección de su propiedad intelectual y su información confidencial en una única plantilla. Forcepoint también lo ayuda a satisfacer las expectativas de los auditores, brindándoles informes estandarizados que pueden personalizar de acuerdo a sus necesidades.

### ▶ ENCUENTRE Y PROTEJA LA INFORMACIÓN CONFIDENCIAL DENTRO DE UNA IMAGEN

En una captura de pantalla malintencionada o en los registros de legales escaneados y almacenados como imágenes, los que presentan puntos ciegos para soluciones de DLP tradicionales, pero no para Forcepoint DLP. Con el reconocimiento óptico de caracteres (OCR: Optical Character Recognition) de Forcepoint, usted puede identificar y proteger de forma confiable los datos sensibles que aparecen dentro de una imagen. Esta capacidad única le permite controlar el flujo de información confidencial en capturas de pantallas, páginas de fax, teléfonos inteligentes y fotos, así como en documentos de cheques, recibos y archivos legales escaneados, protegiéndolo de ataques avanzados y de la amenaza interna del robo de datos. Otras de nuestras capacidades únicas le permiten identificar encriptado personalizado y métodos de “Drip DLP” (DLP “por goteo”) que se emplean a menudo para evitar la detección.

### ▶ IDENTIFIQUE COMPORTAMIENTOS DE “ALTO RIESGO” DE LOS USUARIOS Y CAPACÍTELOS PARA MEJORAR SU HABILIDAD DE RECONOCER AMENAZAS

Ya sea por errores del usuario o de malas intenciones, los usuarios finales se encuentran a menudo en el centro de los incidentes de pérdida de datos. Forcepoint DLP de Forcepoint utiliza análisis de comportamientos para identificar proactivamente a los usuarios de alto riesgo:

- Los usuarios ingeniosos a menudo implican un riesgo debido a sus malos hábitos, los cuales deben ser enfatizados y corregidos antes de que produzcan pérdida de datos.
- Los empleados disgustados pueden ser identificados rápidamente de acuerdo a sus actividades malintencionadas.

Forcepoint DLP de Forcepoint brinda a los usuarios acceso seguro a los datos que necesitan para hacer que funcione la organización, mitigando al mismo tiempo las amenazas internas.



# Componentes de Forcepoint DLP

Existen dos opciones centrales dentro de Forcepoint DLP que se pueden implementar juntas o de forma independiente, lo que le permite cumplir con sus objetivos de seguridad. Además de que esto le brinda la flexibilidad suficiente para satisfacer necesidades actuales y la capacidad de crecer con su organización.

## FORCEPOINT DLP DISCOVERY

Para proteger sus datos, debe encontrarlos donde quiera que se ubiquen. Forcepoint DLP Discovery le permite encontrar y proteger sus datos confidenciales en toda su red, así como datos confidenciales almacenados en la nube, tales como Microsoft Office 365 y Box. Al agregar Forcepoint DLP Endpoint, el poder de Forcepoint DLP Discovery se puede extender a dispositivos finales de Mac OS X y Microsoft Windows, dentro y fuera de la red.

## FORCEPOINT DLP NETWORK

La última oportunidad para detener el robo de datos se presenta cuando ya está circulando a través de los canales del correo electrónico y la web. Forcepoint DLP Network lo ayuda a identificar e impedir la pérdida accidental y malintencionada de datos a partir de ataques externos o de ataques producidos de la creciente amenaza interna. Responda a las técnicas de evasión de las amenazas avanzadas con un poderoso OCR que le permite reconocer datos dentro de una imagen. Use Drip DLP para detener el robo de datos con un registro a la vez y monitoree el comportamiento y las anomalías a fin de identificar usuarios de alto riesgo.

## FORCEPOINT DLP ENDPOINT

Forcepoint DLP Endpoint extiende las capacidades de OCR, Drip DLP y otras capacidades de control de robo de datos a dispositivos finales de Mac OS X y Microsoft Windows, tanto dentro como fuera de su red. Forcepoint le permite compartir de forma segura los datos almacenados en dispositivos extraíbles usando encriptado de archivos basados en su política. Monitoree las descargas en la web, incluidos los HTTP, así como las descargas en la nube como Microsoft Office 365 y Box. Integración total con Outlook, Notes y clientes por correo electrónico, usando la misma interfaz que emplea para las soluciones de Forcepoint para datos, Web, correo electrónico y dispositivos finales.

## MÓDULO DE ANÁLISIS DE IMÁGENES

Para cumplir con los requisitos reglamentarios en muchas partes del mundo, o simplemente para asegurar un entorno sin acoso, el Módulo de Análisis de Imágenes ofrece la capacidad de identificar imágenes explícitas, como las que contienen pornografía, que se encuentran almacenadas en la red de la organización o circulando por los canales del correo electrónico o la web

**“Duermo mejor de noche  
sabiendo que nuestros  
datos están seguros con  
Forcepoint.”**

—Ahmet Taskeser, Senior SIMM Leader, Finansbank



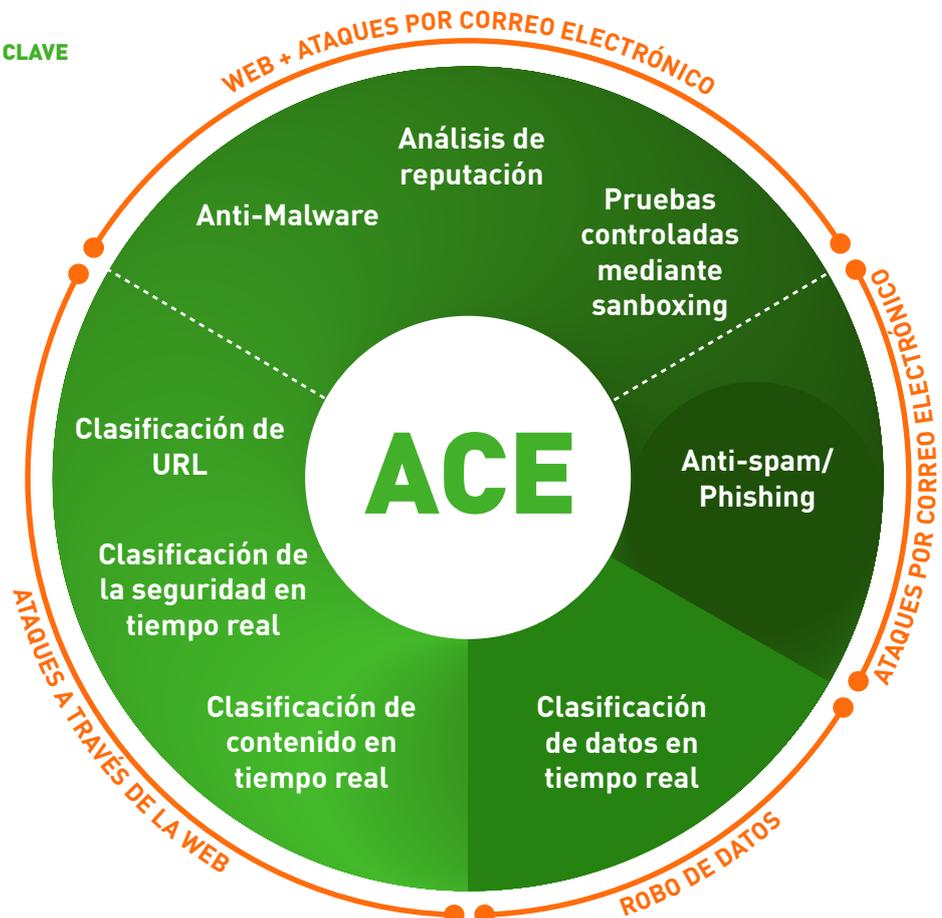
# El poder que respalda las soluciones TRITON Architecture

## Motor avanzado de clasificación ACE (Advanced Classification Engine)

Forcepoint ACE proporciona defensas contextuales en línea, en tiempo real para la seguridad de la web, correo electrónico y los datos, utilizando la calificación de riesgos compuesta y el análisis predictivo, para así proporcionar seguridad más eficaz a la que se puede tener acceso actualmente. Brinda también contención a través del análisis del tráfico entrante y saliente con defensas atentas a los datos, proporcionando protección líder en la industria contra el robo de datos. Los clasificadores de seguridad en tiempo real y análisis de contenido y de datos, son el resultado de muchos años de investigación y desarrollo, los cuales permiten que ACE detecte todos los días más amenazas que los motores de antivirus tradicionales (la prueba se actualiza todos los días en <http://securitylabs.forcepoint.com>). ACE es la principal defensa detrás de todas las soluciones Forcepoint TRITON Architecture y cuenta con el respaldo de Forcepoint ThreatSeeker Intelligence.

### SET INTEGRADO DE CAPACIDADES DE EVALUACIÓN DE DEFENSA EN 8 ÁREAS CLAVE

- 10,000 análisis disponibles para respaldar inspecciones profundas.
- Motores de seguridad predictivos que anticipan muchos movimientos.
- La operación en línea no solo monitorea, sino que además **bloquea** las amenazas.



## Forcepoint ThreatSeeker Intelligence

Forcepoint ThreatSeeker Intelligence, administrada por Forcepoint Security Labs, proporciona la inteligencia central de seguridad colectiva para todos los productos de seguridad Forcepoint. Une más de 900 millones de dispositivos finales, incluyendo información de Facebook y; junto con las defensas de seguridad de Forcepoint ACE, analiza más de 5 mil millones de solicitudes por día. Este extenso reconocimiento de amenazas de seguridad permite a Forcepoint ThreatSeeker Intelligence ofrecer actualizaciones de seguridad en tiempo real que bloquean amenazas avanzadas, malware, ataques de phishing, señuelos y estafas, además de proporcionar las últimas calificaciones web. No hay nada que pueda igualar a Forcepoint ThreatSeeker Intelligence en cuanto a su tamaño y al uso de las defensas en tiempo real de ACE para analizar ingresos colectivos de datos. Cuando se actualiza a Web Security, Forcepoint ThreatSeeker Intelligence lo ayuda a reducir el grado de exposición a las amenazas a través de la web y al robo de datos.

## TRITON Architecture

Con la mejor seguridad en su clase, la arquitectura unificada de Forcepoint TRITON Architecture ofrece protección a solo un clic de distancia, con defensas en línea en tiempo real de Forcepoint ACE. Las inigualables defensas en tiempo real de ACE cuentan con el respaldo de Forcepoint ThreatSeeker Intelligence y con la experiencia de los investigadores de Forcepoint Security Labs. El poderoso resultado es una arquitectura unificada y simple, con una sola interfaz para el usuario e inteligencia de seguridad unificada.

## **CONTACT**

[www.forcepoint.com/contact](http://www.forcepoint.com/contact)

© 2017 Forcepoint. Todos los derechos reservados. Forcepoint y el logo de FORCEPOINT son marcas registradas de Forcepoint. Raytheon es una marca registrada de Raytheon Company. Todas las demás marcas usadas en este documento son propiedad de sus respectivas empresas.

[BROCHURE\_FORCEPOINT\_DLP\_ES] 400004ES.030117

