

# Proofpoint Targeted Attack Protection URL Isolation for Very Attacked People

## Aplicación de controles de acceso adaptables con sus VAP

### VENTAJAS PRINCIPALES

- Aísla las URL maliciosas del correo electrónico corporativo mediante un control adaptable según el riesgo.
- La integración con TAP aporta visibilidad y controles adaptables dinámicos para sus VAP.
- Impide el robo y la captación de credenciales.
- Facilita a los usuarios una navegación sin contratiempos, al mismo tiempo que conserva una privacidad absoluta de los datos.
- Permite que los usuarios naveguen con seguridad por sitios web desconocidos, con la tranquilidad de saber que la organización está segura.

Proofpoint Targeted Attack Protection (TAP) URL Isolation for Very Attacked People (VAP) protege a las organizaciones al permitir que sus personas muy atacadas puedan navegar con seguridad por sitios web desconocidos. Evita que sufran ataques basados en URL y web. Y utiliza tecnología de aislamiento basada en la nube para reducir su superficie de ataque y evitar que su organización sufra ataques de phishing y dirigidos.

Detener una amenaza antes del primer punto de la infección resulta fundamental para evitar que los agresores pongan en peligro los activos más importantes de una organización: su personal. Para defenderse como es debido de los ataques de *phishing* y de los ataques dirigidos se necesita una solución multicapa, que permita a los usuarios continuar con su trabajo diario y evite que la seguridad de la organización se vea afectada.

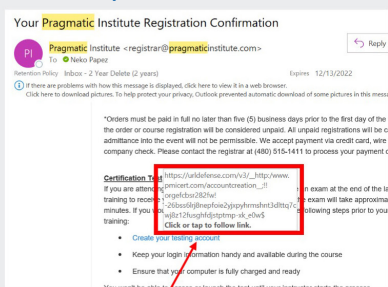
Gracias a TAP URL Isolation for VAP, los usuarios podrán navegar con seguridad por sitios web desconocidos, mientras siguen protegidos de los ataques basados en URL y la web. Con esta integración, cada vez que un usuario VAP haga clic en una URL de un mensaje del correo electrónico corporativo, esta se analizará y aislará según la política configurada. Los empleados acceden con seguridad a estos sitios web desde su correo electrónico corporativo, con la tranquilidad de que la organización no corre peligro.

### Aplicación de controles de aislamiento adaptables para usuarios muy atacados

Gracias a su integración con TAP, TAP URL Isolation for VAP puede aislar también las URL de los mensajes que se envían a sus usuarios expuestos a un riesgo mayor, que se conocen como VAP. La lista de personas muy atacadas (VAP) se genera dinámicamente dentro de la solución Proofpoint Targeted Attack Protection, en función de la amenaza del nivel de riesgo. La integración ofrece también funciones de detección y análisis de phishing en tiempo real.

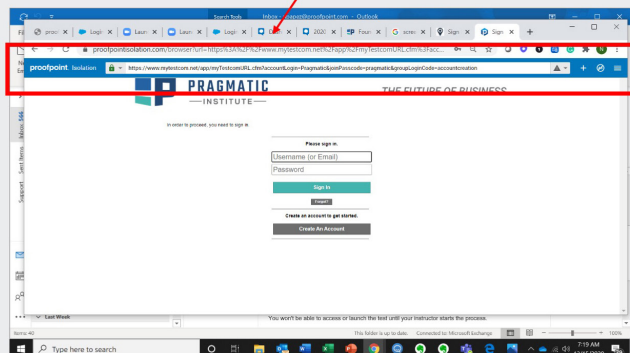
Cuando se activa una sesión del navegador aislada, se comunica al panel de TAP correspondiente para descubrir nuevas amenazas y controlar el riesgo. La integración entre los controles de aislamiento adaptable con TAP sirve para disminuir el riesgo de forma eficaz.

### Aplicación de los controles de aislamiento adaptables con sus VAP



Los enlaces que incluyen los mensajes de correo electrónico corporativo se reescribirán automáticamente con el sistema de protección de URL de Proofpoint y estas URL se abrirán en un entorno aislado.

Una vez aisladas las URL, los usuarios están protegidos frente al robo de credenciales y los ataques dirigidos. En esta fase se desactivarán las funciones de carga y descarga.



TAP URL Isolation for VAP

### Mayor visibilidad para los clics aislados

Para proteger su organización, resulta fundamental saber quiénes son sus VAP, cómo están siendo atacados y cuándo interactúan con posibles URL maliciosas. Ahora, en la página de detalles de amenazas TAP de Proofpoint podrá comprobar cuántos clics se han aislado. Si en su organización se ha activado TAP URL Isolation for VAP, puede saber cuántos clics se han protegido con la integración de la tecnología de aislamiento Proofpoint TAP y actualizar sus políticas en la consola de aislamiento para proteger todavía más clics de las categorías de alto riesgo.

### Reducción de la superficie de ataque con inteligencia avanzada sobre amenazas

Aislamos automáticamente las URL sospechosas de acuerdo con dos métodos de análisis predictivo. El primero es una comprobación de la reputación en la que el gráfico de amenazas Nexus de Proofpoint sirve para saber si una URL específica se incluye o no en nuestra lista de sitios maliciosos. Para ello se combina nuestra plataforma de aprendizaje automático NexusAI, técnicas de detección avanzadas y conocimientos humanos especializados.

El segundo es nuestro análisis de amenazas, que envía el código HTML a nuestro motor estático para comprobar y resolver si la página es maliciosa o no. En una sesión aislada, los archivos y los adjuntos de correo electrónico con payloads o macros maliciosas no se descargan nunca. Los datos que introduce el usuario se limitan de forma dinámica para reducir el robo de credenciales a través del navegador. Y las descargas se bloquean, con el fin de evitar ataques de malware por descargas desapercibidas. Además, se mantienen alejados de sus endpoints todos los tipos de contenidos web maliciosos. La solución incluso aísla el contenido de sitios de confianza que han sido comprometidos.

Nuestra solución también garantiza el cumplimiento de las normativas. Las sesiones de navegación aisladas están completamente ocultas para su personal de TI y su entorno. De esta forma evita cualquier problema relacionado con la privacidad de los empleados o el incumplimiento de normativas.

El despliegue de Proofpoint TAP URL Isolation es sencillo porque la solución está completamente alojada en la nube y se integra fácilmente con Proofpoint Targeted Attack Protection para usar estos controles de aislamiento adaptable con sus VAP. Todo esto contribuirá a reducir costes, incrementará la productividad del personal de TI y generará un clima de confianza entre los empleados.

## MÁS INFORMACIÓN

Para obtener más información, visite [proofpoint.com/es](https://proofpoint.com/es).

#### ACERCA DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFFT) es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentran más de la mitad del Fortune 1000, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en [www.proofpoint.com/es](https://www.proofpoint.com/es).

©Proofpoint, Inc. Proofpoint es una marca comercial de Proofpoint, Inc. en Estados Unidos y en otros países. Todas las marcas comerciales mencionadas en este documento son propiedad exclusiva de sus respectivos propietarios.