proofpoint.

Controles de acceso y de la privacidad para Proofpoint Information Protection

Satisfaga los requisitos de cumplimiento mientras protege los derechos de los empleados y elimina los sesgos

Ventajas principales

- Mantenga la confianza de los empleados.
- Proteja la información empresarial crítica.
- Garantice el cumplimiento de las leyes de privacidad.
- Prevenga el sesgo en las investigaciones.

Proteger la privacidad de los datos es cada vez más importante y complejo. La aceleración de la transformación digital, la adopción del trabajo híbrido y la proliferación de aplicaciones en la nube han dificultado aún más la protección de los datos sensibles. A medida que las empresas siguen acumulando volúmenes cada vez mayores de datos, su valor percibido aumenta. Desgraciadamente, con este aumento de valor también aumenta el riesgo de pérdida y robo de datos, incluso por parte de usuarios internos.

A pesar de las crecientes dificultades, las empresas no pueden permitirse cometer errores. Las empresas de todo el mundo están sometidas a una presión cada vez mayor para cumplir las estrictas leyes de privacidad de datos que exigen medidas sólidas de seguridad y privacidad de los datos. El incumplimiento puede resultar costoso; las fuertes multas y la pérdida de negocio son habituales. Más de un tercio de los profesionales de la seguridad afirman que las multas y los incumplimientos normativos son consecuencia de las filtraciones de datos[1].

Proofpoint ofrece una completa gama de productos diseñados para reforzar la seguridad de los datos y gestionar las amenazas internas, garantizando al mismo tiempo el cumplimiento de las normativas relativas a la privacidad de datos. La gama de soluciones Proofpoint Information Protection aplica sólidos controles de acceso y de privacidad. Limita la visibilidad solo a quienes realmente la necesitan y preserva el anonimato de los usuarios garantizando la privacidad de los datos de identificación personal. Como resultado, Proofpoint mejora la seguridad de los datos y ayuda a eliminar los sesgos en sus investigaciones. Se beneficia de un enfoque equilibrado de la seguridad de la información.

Enfoque centrado en la privacidad

Proofpoint Information Protection se basa en principios de privacidad por diseño. Esta metodología adopta una estrategia de protección de datos proactiva. Sitúa la privacidad en la vanguardia del diseño de sistemas para garantizar que los sistemas de TI, la infraestructura y los procesos empresariales incorporen la privacidad como elemento central desde el principio. Este enfoque sitúa la visibilidad, la transparencia y la orientación al usuario en el centro de su diseño.

Este conjunto de soluciones forma parte de la plataforma Human-Centric Security, que mitiga las cuatro principales áreas de riesgo asociado a las personas.

1 Informe Data Loss Landscape 2024 de Proofpoint.

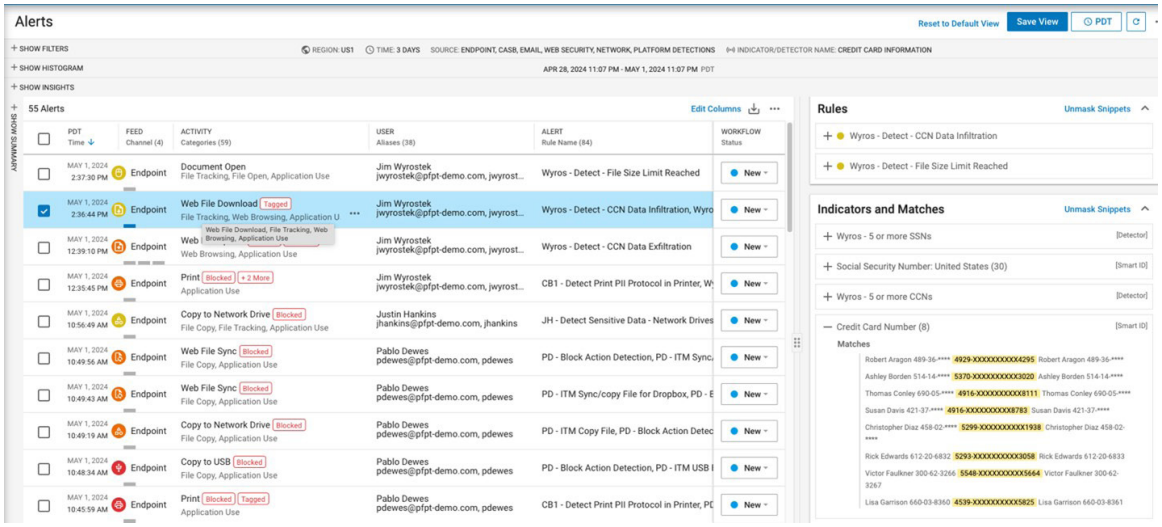

Figura 1: Enmascaramiento de números de tarjetas de crédito en Proofpoint Information Protection.

Administre la residencia y el almacenamiento de los datos

Proofpoint establece data centers (centros de datos) regionales estratégicamente en Estados Unidos, Canadá, Europa, Australia y Japón para cumplir los requisitos de privacidad y localización de los datos. Disfrute de control total sobre dónde se almacenan sus datos en todos estos data centers.

Para administrar el almacenamiento de datos de los endpoints, Proofpoint le permite crear grupos de endpoints. Cada agrupación puede asociarse a un data center específico, por lo que puede separar fácilmente los datos geográficamente. Por ejemplo, un grupo en EE. UU. puede administrar los datos de los endpoints de EE. UU., que se envían al data center de ese país.

Garantice la privacidad con controles de acceso basados en atributos

Los controles de acceso basados en atributos de Proofpoint Information Protection ofrecen una forma flexible y eficaz de administrar el acceso a los datos. Garantizan que los analistas de seguridad solo tengan visibilidad de los datos cuando sea absolutamente necesarios.

Por ejemplo, puede definir reglas granulares y asignar accesos para que un analista de seguridad que esté en EE. UU. solo pueda ver datos de EE. UU., y no datos de Europa o de la región Asia-Pacífico. Este nivel específico de control de acceso reduce considerablemente el riesgo de exposición innecesaria de los datos. Y cuando un analista necesite acceder a los datos de un usuario específico como parte de una investigación, el administrador del sistema también puede limitar este acceso en el tiempo, es decir, definir el tiempo que el analista puede acceder a estos datos.

Garantice la privacidad de los datos con enmascaramiento de fragmentos

Proofpoint Information Protection ofrece una función de enmascaramiento de datos para garantizar la privacidad. El enmascaramiento de datos oculta los datos forenses digitales sensibles, como los datos médicos protegidos y los datos personales de la consola, para que esta información no pueda ser identificada. Este enfoque garantiza que solo aquellos que necesiten acceder a los datos puedan verlos en su forma completa y sin enmascarar.

Los administradores del sistema pueden definir qué identificadores de datos desean ocultar. Pueden decidir mostrar solo los cuatro últimos dígitos del número de una tarjeta de crédito y ocultar todo lo demás. También pueden decidir el tipo y la cantidad de datos a los que pueden acceder los usuarios, en función de su responsabilidad. Por ejemplo, pueden especificar que solo los analistas autorizados puedan ver extractos de datos sensibles.

Proteja los datos de los usuarios con anonimización

Proofpoint Information Protection también protege los datos de los usuarios mediante la anonimización, que le permite ocultar la identidad de un usuario. Puede anonimizar el nombre de usuario, el nombre de host, la dirección IP, la información de ubicación y los nombres de archivo.

La anonimización garantiza que solo los analistas de seguridad autorizados puedan ver los datos de identificación de los usuarios supervisados. Este proceso también ayuda a eliminar los sesgos durante las investigaciones. Considere el siguiente escenario: un directivo acaba de incumplir una norma de la empresa. Si se conociera su identidad, el incidente podría tratarse de forma diferente o un analista de seguridad podría hacer la vista gorda.

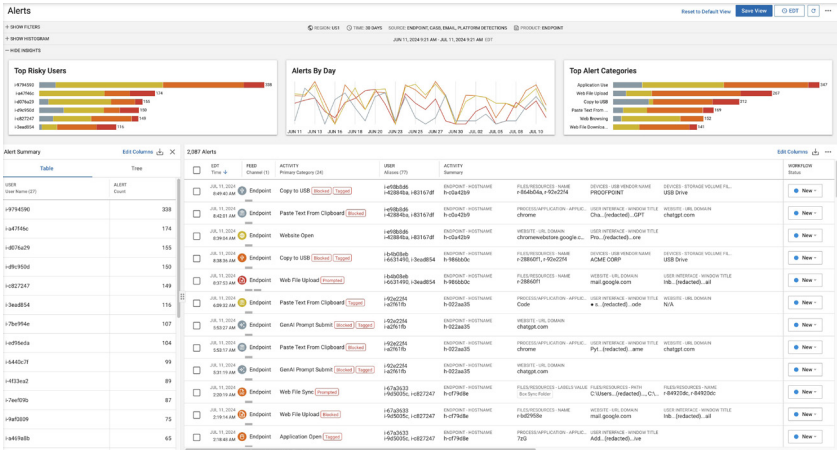

Figura 2: Vista de datos de usuario anonimizados en Proofpoint Information Protection.

Cuando sea necesario conocer la identidad de un usuario más adelante durante las investigaciones, el analista de seguridad puede solicitar la desanonimización de los datos, que puede ser concedida por un administrador.

Encuentre el equilibrio entre privacidad y seguridad de los datos

En cualquier empresa, es importante encontrar el equilibrio adecuado entre la seguridad y la privacidad de los datos. Para conseguirlo, tenga en cuenta estos principios:

- **Supervise los principales canales de pérdida de datos.** Concentre sus esfuerzos de protección de datos en los métodos de trabajo. La mayoría de las fugas y exposiciones de datos se producen a través del correo electrónico, las aplicaciones en la nube y las memorias USB.
- **Sea claro y transparente.** Asegúrese de que su personal conoce las normas de la empresa en materia de seguridad y confidencialidad de los datos. Explique claramente lo que está supervisando. Esto le ayudará a crear un clima de confianza.
- **Forme a los usuarios con notificaciones automáticas.** Cuando un usuario infringe las normas de la empresa, se puede generar automáticamente una notificación para informarle. El envío de una notificación automática alerta al usuario de un comportamiento de riesgo, al tiempo que elimina la vergüenza y la emoción asociadas a una reunión con su jefe o con RR. HH.
- **Sea selectivo.** No necesita recopilar datos sobre todo y sobre todos. Determine qué datos son importantes y qué necesita saber realmente sobre las actividades de los empleados.
- **Controle el acceso a los datos.** Aunque los administradores de seguridad, los analistas, el departamento jurídico y de RR. HH. puedan tener acceso ilimitado a los datos de los empleados, esto no siempre va en pro de la privacidad. Por lo tanto, asegúrese de utilizar los controles de acceso que proporcionan las herramientas DLP e ITM.

Garantice la privacidad de los datos con Proofpoint

Las soluciones Proofpoint Information Protection, como Data Loss Prevention e Insider Threat Management permiten garantizar el nivel máximo de protección de los datos, garantizando el cumplimiento de las normativas en materia de privacidad de los datos. Esto también contribuye a eliminar los sesgos durante sus investigaciones. Proofpoint Information Protection tiene en cuenta el contenido y el comportamiento, para que pueda identificar los datos sensibles o regulados e identificar las actividades de riesgo y las intenciones maliciosas, todo ello desde una consola centralizada que proporciona visibilidad en todos los canales, incluidos los endpoints, el correo electrónico, la nube y la web.

Proofpoint Managed Information Protection reúne a las personas, los procesos y la tecnología apropiadas. Así podrá diseñar, aplicar y desarrollar su programa para optimizar la protección de datos y garantizar la privacidad.

MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.