



PROTECCIÓN CONTRA RIESGOS DIGITALES

Descubra información comprometida, evite ataques dirigidos y mejore su seguridad

Los ciberdelincuentes están permanentemente tratando de comprometer credenciales y datos confidenciales de las empresas para obtener acceso a una red de información muy valiosa.

Esta información luego la utilizan para realizar ataques altamente sofisticados con fines de lucro.

La información comprometida es la causa principal de la mayoría de filtraciones de datos y ataques dirigidos. Dado este alto volumen que está a la venta en la Dark Web, nuestra Protección contra Riesgos Digitales (DRP por sus siglas en inglés) brinda tranquilidad e informa la exposición al riesgo en detalle. DRP reduce los ataques a través de su amplio espectro de visibilidad y mitigación proactiva de amenazas.

Obtenga control sobre los datos comprometidos antes de que afecten a su organización con visibilidad e informes detallados.

La Protección Contra Riesgos Digitales Defiende Contra Las Amenazas Dirigidas Mediante:

- La identificación exacta de qué credenciales de sus empleados se han violado y están circulando por la Dark Web
- La mitigación de sus efectos informando el tipo de exposición al riesgo para garantizar una acción rápida contra los datos comprometidos
- El descubrimiento proactivo de cómo la presencia digital de su organización está siendo atacada por phishing, violación de marca y mucho más

LAS CARACTERÍSTICAS INCLUYEN:

Monitoreo de credenciales comprometidas

Descubra las credenciales de los empleados existentes en las bases de datos de la Dark Web con informes detallados.

Detección y eliminación de amenazas

Detecte y elimine sitios de phishing, cuentas de redes sociales falsas y violaciones de marcas comerciales.

Informes de nombres de dominio ocupados

Descubra dominios que han sido apropiados cibernéticamente o con errores tipográficos que involucren el nombre o la marca de su empresa.

Detección de documentación expuesta y código fuente filtrado

Encuentre documentos filtrados o robados relacionados con su empresa en los mercados de la Dark Web y foros de piratería. Descubra código fuente expuesto accidental o maliciosamente en repositorios de código público como Github.

Descubrimiento de sistemas informáticos vulnerados

Encuentre menciones de sus sistemas en los mercados de la Dark Web y los foros de piratería, monitoreando las fuentes de inteligencia de amenazas y las listas de Incidentes de seguridad (IoC).

BENEFICIOS

Reduce los procesos manuales al informar continuamente sobre las amenazas recién descubiertas.

Mitiga los efectos de una violación de datos.

Proporciona una visibilidad incomparable en la Dark Web.

Monitoreo las 24 horas para reportar rápidamente datos comprometidos.

Minimiza la exposición al riesgo, manteniendo a las organizaciones bien informadas.

Ha habido un aumento del 450% en las violaciones que contienen nombres de usuario y contraseñas a nivel mundial en los últimos dos años.¹

Sobre Appgate

Appgate es la empresa de acceso seguro. Potenciamos la forma en que las personas trabajan y se conectan proporcionando soluciones diseñadas específicamente sobre los principios de seguridad Zero Trust. Este enfoque de seguridad definido por las personas permite conexiones rápidas, simples y seguras desde cualquier dispositivo y ubicación a las cargas de trabajo en cualquier infraestructura de TI en entornos híbridos, locales y en la nube. Obtenga más información en appgate.com

¹ <https://betanews.com/2021/06/07/username-password-breaches-increase/>

