El DLP que funciona

La nueva generación de protección de datos está aquí.

La plataforma patentada de Nueva Generación de Protección de Datos y Prevención de Pérdida de Datos de GTB, mantienen los datos seguros en instalaciones On-premise como en off-premise y cloud, incluidos los puestos de usuarios basados en Windows, Linux y Mac y en aquellos que estén en la Nube, realizando escaneo local y monitorizando en tiempo real con detección de huella digital del documento.

GTB aparece en los últimos cuadrantes de Gartner como visionario, siendo una clara apuesta por la sencillez de uso y la eficiencia de funcionamiento.

Las empresas están luchando para identificar y proteger la información sensible. Los datos confidenciales de los clientes, propiedad intelectual, secretos comerciales y los documentos legales se comparten sin la debida autorización, lo que cuesta a las organizaciones miles o millones de Euros, dependiendo del tamaño, en la restitución de los mismos. Debido a que esta información sensible es fácilmente accesible, en los entornos de hoy en día, la necesidad de seguridad de los datos se ha ampliado. Con el aumento de los ataques de phishing, APTs y brechas de información privilegiada, los datos, en todas sus formas, están en riesgo: Datos en reposo, Ubicados en la red o unidades compartidas, datos en movimiento, los datos se envían por correo electrónico, Etc. y datos en uso - datos guardados en dispositivos de medios extraíbles, tales como: unidades USB, CD, disquetes, iPods, cámaras, etc.

Recientemente, la ley de protección de datos y sobre todo, las amenazas internas ha aumentado significativamente la criticidad de los mismos. La información que se está almacenando en la red y dispositivos de medios extraíbles está entrando en manos de terceros, violando así las leyes locales y estatales, y las regulaciones diseñadas para proteger tales datos: Sarbanes Oxley, GLBA, HIPAA, CA SB1386, CA AB1950, Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI), Patric Act, FISMA, FERC / NERC, GDPR, ITAR y otros.

Si Sólo se soportan los protocolos SMTP, HTTP, FTP E IM a nivel de red, y el agente no es capaz de ver otros protocolos, ES UNA LIMITACIÓN REAL Y NO ES DLP.

Funcionalidades:

- Detección por patrón en los EndPoint, estando conectado o desconectado de la red, sin necesidad de "llamar a casa".
- Capacidades de DLP completas en la inspección de datos en uso en los EndPoint.
- Protección / Prevención en tiempo de exfiltración e Infiltración de Datos.
- Identificar datos sensibles en imágenes con el OCR, en más de 74 idiomas, tanto a nivel de Red, puesto de usuario, descubrimiento y clasificación de datos.
- Descifrado SSL.
- Control de aplicaciones.
- Native Cloud.
- Control Shadow IT.
- Implementación fácil, fácil de usar y controles de seguridad efectivos, con políticas que ayudan a cumplir los requerimientos de cumplimiento y normativa.
- Descubrimiento, clasificación y seguridad de datos en Linux, Mac y Windows..
- Gestión centralizada de la seguridad de los datos.
- Políticas de flujo a nivel corporativo, para la gestión de incidentes e informes Forenses para responder a los primeros análisis y responder ante posibles incidentes.
- Enterprise workflow, policy, incident management and forensic reports enable first responders to analyse and respond to possible incidents..
- URL Filtering.
- Identificar a los usuarios internos con alto riesgo.
- Tiempo Real, Gestión de Derechos de Automático dependiendo del contenido