CONTROL DE CANALES DE DATOS

Channel/protocol		Searchinform	McAfee	ForcePoint	Symantec
Correos (POP3, IMAP, SMTP, MAPI, web mail)		+	+	+ (excepto correo web entrante)	+ (excepto correo web entrante)
Mensajería Instantánea regulares (icq, msn, mmp, xmpp, etc.)		+	+	+	+
Mensajería Instantánea con cifrado de extremo a extremo (Telegram, Viber, etc.)		+	-	-	-
Telefonia corporativa (VOIP-SIP)		+	-	+	-
Internet	Correo web	+	+	+	+
	Mensajería Instantánea Web	+	+	+	+
	Redes Sociales	+	+	+	+
	Foros, Chats	+	+	+	+
	Almacenamiento en la nube	+	+	+	+
	Peticiones Obtenidas	+	-	+	-
	SSL	+	+	+	+
Skype\Skype Corporativo\Web Skype		+	+	+	+
Texto de mensaje de intercepción enviado a través de canales de Internet compatibles		+	+	+	+
Archivos de intercepción enviados a través de canales de Internet soportados		+	+	+	+
FTP(S)		+	+	+	+
Contenido del portapapeles		+	+	+	+
Impresión		+	+	+	+
Capturas de pantalla con referencia a aplicaciones activas		+	+ +	Sin referencia a las aplicaciones.	+
Grabación de video con referencia a aplicaciones activas		+	-	-	-
Grabación de cámara web - capturas de pantalla, video		+	-	-	-
Micrófono de grabación con más discurso en conversión de texto		+	-	-	-
Conexión en vivo a monitor y micrófono.		+	-	-	-
Cifrado de archivos de usuario		+	A través de la integración con Mcafee Encryption	-	-
Auditoría de operaciones del sistema de archivos		+	-	-	-
Tecleos		+	Limitado a ciertas operaciones	+	-
Control del contenido de archivos en almacenamiento en red.		+	+	+	+
Control del contenido de archivos en recursos locales (no públicos) de PC		+	-	-	-
Auditoría de software y hardware instalados.		+	-	-	-
Capturar contactos de usuario		+	-	-	-
Autocompletar el perfil de seguridad del usuario.		+	Información de LDAP solamente	Información de LDAP solamente	Información de LDAP solamente
Auditoría del tiempo de trabajo - aplicaciones activas y actividades web		+	-	-	-
Medios removibles		+	+	+	+
Identificación de usuario		Microsoft AD, Novel eDirectory	Microsoft AD, Novel eDirectory	Microsoft AD, Novel eDirectory	Microsoft AD, Novel eDirectory
Posibilidad de utilizar un servidor de transporte especializado para oficinas regionales		+	-	-	-
Interceptar todos los datos en todos los canales y mantener un archivo de los datos para investigaciones y análisis		+	-	-	-
Búsqueda de texto completo con la ayuda de la tecnología de indexación de datos		**Solución propia de alto rendimiento, desarrollada a lo largo de 20 años**	Solo datos en reposo	La búsqueda de texto completo no está disponible	La búsqueda de texto completo no está disponible

SearchInform DLP controla muchos más canales de datos que sus rivales más cercanos. Muchos canales se controlan en un nivel superior, como la captura de datos cifrados, anonimizados y los datos enviados con la ayuda de los protocolos de tunelización. En el caso de SearchInform DLP, el control de todos los canales está sujeto a su funcionalidad completa, proporcionar captura de mensajes de texto, llamadas, archivos transferidos, credenciales de usuario y lista de contactos, software instalado y eliminado, etc.

Otro beneficio clave es la capacidad de controlar los servicios de telefonía sin la necesidad de instalar agentes en estaciones de trabajo. El control exhaustivo de las acciones de los usuarios permite realizar investigaciones efectivas y detectar las causas raíz y las fuentes de incumplimiento de las políticas de seguridad. La grabación de video de las acciones del usuario es primordial en las investigaciones de violaciones de seguridad y otros incidentes. El registrador de claves ayuda a controlar el acceso a los recursos restringidos, incluso aquellos con la mayor protección, así como el cifrado de datos destinado a bloquearlo desde el departamento de seguridad inútil.

El control detallado de las acciones de los usuarios hace posible llevar a cabo investigaciones de manera efectiva y recopilar evidencia sustancial. Las acciones rutinarias son automatizadas al máximo. Control de entrada de teclado, monitoreo de la actividad del archivo, grabación de audio, con posterior conversión de sonido a texto, grabación de video, que usted podría navegar por supuesto, no necesitas verlo todo, puedes seleccionar solo una pieza en el software de interés, todo esto proporciona una ayuda inestimable en la investigación detallada de violaciones, cuando el veredicto del sistema debe estar respaldado por evidencia irrefutable.

ANALISIS DE DATOS CAPTURADOS

Para identificar información crítica en los datos transferidos por los usuarios, se utilizan las siguientes tecnologías

Detección de información sensible	Searchinform	McAfee	ForcePoint	Symantec
Búsqueda por palabra clave	+	+	+	+
Busque el texto disfrazado - translit, typos, números en lugar de letras	+	-	-	-
Búsqueda de frases	+	+	+	+
Utilizando un texto completo como consulta de búsqueda	+	-	-	-
Morfología	+	+	+	+
Sinónimos	+	+	+	+
Búsqueda de atributos de archivo	+	+	+	+
Buscar documentos protegidos por contraseña	+	+	-	+
Consultas complejas utilizando varias consultas de búsqueda simultáneamente	+	Solo datos en reposo	-	-
Búsqueda simple de expresiones regulares	+	+	+	+
Búsqueda compleja de expresiones regulares	+	-	-	-
Búsqueda digital de huellas digitales de texto	+	+	+	+
Búsqueda de huella digital binaria	+	+	+	+
Búsqueda de imágenes similares - pasaportes, tarjetas de crédito, etc.	+	-	-	-
Búsqueda de sellos corporativos.	+	-	-	-
Detección de tipo de imagen - foto \ escaneo	+	-	-	-
Reconocimiento de texto en archivos gráficos (OCR) y búsqueda de contenido.	+	+	+	+
Búsqueda de texto en audio	+	-	-	-

La tecnología de análisis de contenido es un sello distintivo de SearhInform DLP, lo que nos diferencia de la competencia. Hemos desarrollado una amplia variedad de algoritmos de búsqueda únicos, que no están disponibles en ningún otro sistema DLP, Ejemplo: búsqueda de contenido similar, lo que ayuda a encontrar contenido con un alto grado de relevancia en el significado para consultar texto, otra herramienta importante son las políticas de seguridad inteligente personalizables de cualquier complejidad, que puede incluir lingüística, atributivo, cuantitativo, matemáticas y otros tipos de análisis simultáneamente. Esto produce una gran relevancia en los resultados de búsqueda y ahorra a los oficiales de seguridad de la información mucho tiempo al detectar e investigar violaciones de seguridad y otros incidentes.

Una ventaja más de SearchInform DLP es un modelo híbrido único de almacenamiento y procesamiento de datos. Te permite trabajar con series de resultados analíticos de cualquier longitud, sin ningún límite en los resultados mostrados. A eso, las consultas de búsqueda de datos indexados no llevan mucho tiempo en absoluto, son decenas de veces más rápido que las consultas similares de cualquier base de datos existente en hardware equivalente. Esto permite a los oficiales de seguridad de la información trabajar con un almacén de datos completo, sin dividir los datos en partes archivadas y operativas.

Informes

Tipo de información	SearchInform	McAfee	ForcePoint	Symantec
Software instalado / eliminado	+	-	-	-
Hardware instalado / eliminado	+	-	-	-
Empleado de eficiencia laboral y productividad	+	-	-	-
Actividades durante el tiempo de trabajo	+	-	-	-
Perforaciones tardías, puñaladas tempranas, empleados ausentes	+	-	-	-
Tiempo dedicado a varios sitios web	+	-	-	-
Tiempo empleado en diversas aplicaciones	+	-	-	-
Auto categorización de la URL visitada	+	+	+	+
Comportamiento anormal	+	-	+	+

La mayor amplitud de informes es una ventaja considerable de SearchInform DLP. El sistema viene con informes comunes preestablecidos, así como el creador de informes, lo que significa que junto con las comunicaciones del usuario, usted puede mantener un ojo en la ética de trabajo, productividad y eficacia de los procesos de negocio.

También existe la capacidad de generar informes sobre el inventario de equipos y hardware. El inventario se somete periódicamente a conciliación, por lo que le da una imagen completa de los componentes instalados / eliminados.

CONCLUSION

El control más completo de los flujos de información

SearchInform DLP controla más canales que sus rivales más cercanos. Los canales son controlados en un nivel más profundo (intercepción de conexiones encriptadas, impersonales o de túnel). Todos los canales son monitoreados con total consideración de su funcionalidad (monitoreo de mensajes, llamadas, archivos transferidos, datos de usuario y contactos)

La tecnología de vigilancia estrecha

SearchInform DLP no solo le permite activar el monitoreo cercano del usuario, como actividad de archivos, keylogger, grabación de audio, capturas de pantalla, grabación de video de acciones), pero también hace que sea conveniente trabajar con la información recibida. Por ejemplo, búsqueda de video: no es necesario ver todo el día laboral, simplemente desplácese hasta la aplicación seleccionada. No es necesario escuchar el audio manualmente, puede convertir la voz en texto y analizarlo como tal.

Control de eficiencia de trabajo y productividad

SearchInform DLP incluye un componente para monitorear la productividad de los trabajadores- en este momento, es la solución más funcional del mercado con aproximadamente 50 informes, con la más alta calidad - Se monitorizan unos 20 tipos de navegadores, incluyendo modo privado. Además, CUALQUIER sitio visitado se refiere automáticamente a una de las 80 categorías: juegos, noticias, compras, etc.

Herramientas analíticas únicas

Por encima de los medios convencionales de análisis de textos- expresiones regulares, diccionarios, búsquedas de frases- SearchInform DLP ofrece herramientas como la búsqueda de texto con un significado o contenido similar,
buscando imágenes similares(pasaportes, tarjetas de crédito) buscando documentos con sellos corporativos. También está disponible cualquier combinación de las búsquedas anteriores como parte de una única política. Una característica única del producto es la capacidad de proteger los datos de cualquier forma – texto, imágenes e incluso audio- Para cualquier fuente de audio, incluida la negociación, puede aplicar políticas de protección de texto.

Conveniencia de la administración

SearchInform DLP tiene su propio conjunto de herramientas para administrar servicios, componentes, bases de datos e índices. Y también, herramientas propias para notificar al administrador sobre mal funcionamiento.
No es necesario monitorear el estado de la solución con la ayuda de sistemas externos o usar shells de SO o DBMS para resolver tareas típicas. Con todo lo anterior, la implementación del Circuito de Seguridad de la Información es un procedimiento muy rápido y simple.