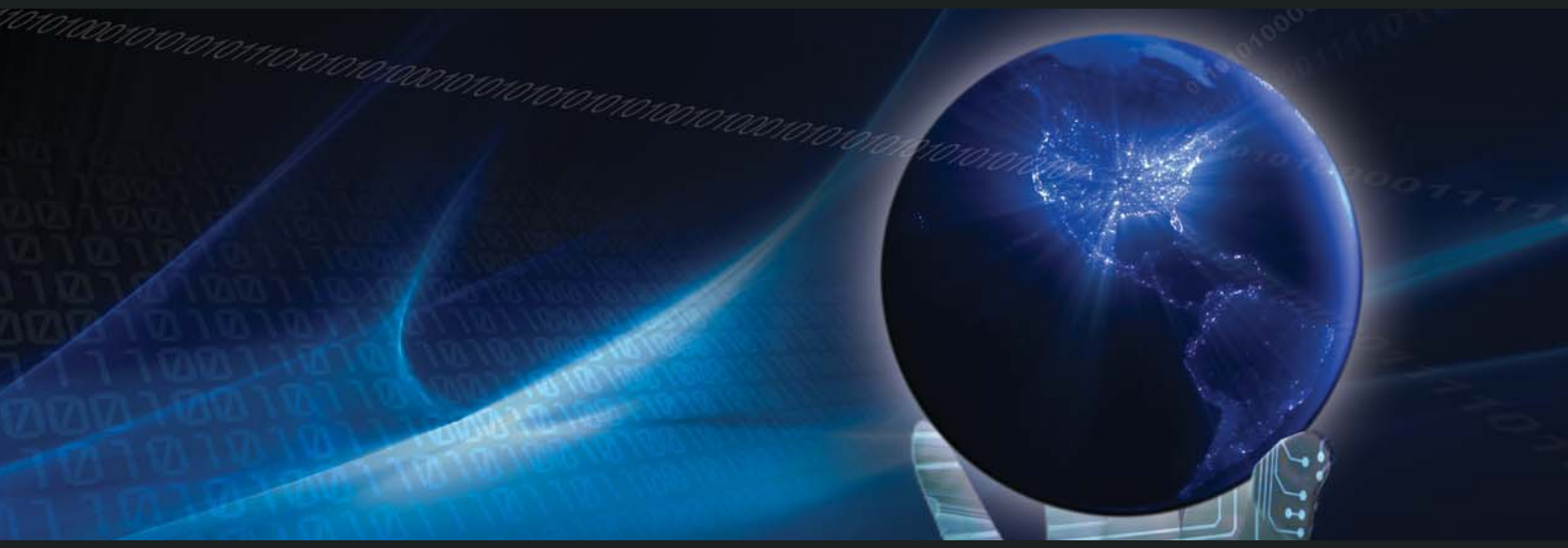
AccessData Enterprise



INVESTIGACIÓN Y RESPUESTA A INCIDENTES CON ALCANCE EN TODA LA ORGANIZACIÓN

AccessData®
A Pioneer in Digital Investigations Since 1987

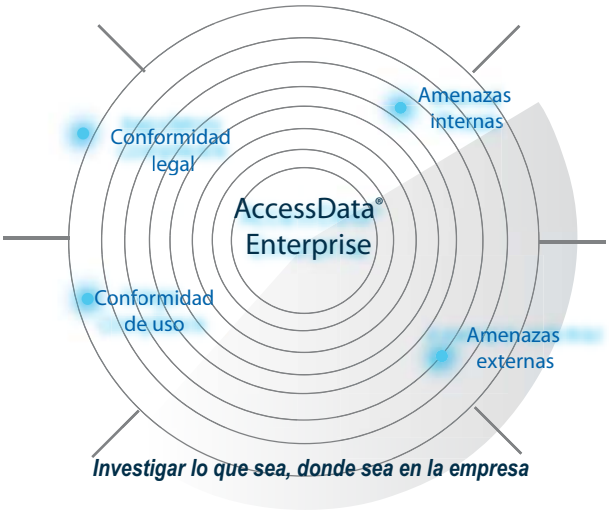
Defienda sus activos de información al conseguir visibilidad en toda su organización...

A pesar de todo el dinero invertido en tecnologías de prevención, seguirán surgiendo problemas. El método de detección es con frecuencia el accidental. Aunque la defensa perimetral y las tecnologías de alerta desempeñan una función esencial para la protección de activos de información, la capacidad de llevar a cabo investigaciones en toda la organización tiene la misma importancia. ¿Cómo identifica las violaciones de la seguridad que han conseguido traspasar sus defensas? ¿Cómo detecta el robo de propiedad intelectual cuando el delincuente es un empleado con un nivel de sofisticación tecnológica elevado? ¿Cómo verifica la actividad fraudulenta sin alertar a aquellos a los que está investigando? ¿Cómo se asegura de que se ha identificado adecuadamente el software malicioso y se han aislado todos los equipos en los que reside?

AccessData® Enterprise le permite conseguir una visibilidad de todos los datos de la organización para detectar, identificar, analizar, elaborar informes y preservar los datos, así como remediar problemas de seguridad. Es un nuevo tipo de producto de investigación desarrollado con criterios de ampliación, velocidad y funcionalidad. Esta solución empresarial fácil de utilizar permite tener la capacidad de investigar la red en todo momento y obligar al cumplimiento de políticas, proteger los datos y a los empleados y reducir costes.

Cumplimiento de las políticas y la normativa

AccessData Enterprise facilita el cumplimiento de la normativa y permite a las organizaciones responder rápidamente a las solicitudes legales e investigar con rapidez acusaciones o sospechas de mala conducta de los empleados, como fraude, robo de información personalmente identificable o robo de información de tarjetas de crédito. La visibilidad de los datos en equipos de escritorio y portátiles, dispositivos periféricos y unidades de red compartidas es esencial para cumplir la legislación y las políticas internas, y AD Enterprise permite disponer de ese nivel de visibilidad.



Investigar lo que sea, donde sea en la empresa

Conformidad de uso

Permite analizar miles de equipos para buscar procesos no autorizados y, si las políticas lo permiten, el personal de TI con las credenciales adecuadas sólo tendrá que hacer clic con el botón derecho para finalizar un proceso determinado. O si, por ejemplo, se detectan varios procesos no aprobados en varios equipos de la organización, el personal de TI puede iniciar una operación de corrección por lotes.

Amenazas internas

AccessData Enterprise le permite visualizar todos los de su organización independientemente del lugar en el que se encuentren. Puede investigar de manera proactiva los equipos de los usuarios de su red para identificar cualquier indicio de actos indebidos, como el robo de propiedad intelectual. Además, permite reaccionar inmediata y sigilosamente para determinar si un empleado es culpable de robo de IP, acoso u otro comportamiento indebido. Cuando se confirme una amenaza interna, se podrán conservar todas las pruebas forenses desde una ubicación centralizada, incluso si hay varios sospechosos distribuidos por el mundo. Por ejemplo, si uno de sus empleados es sospechoso de enviar información confidencial a un competidor, y esa persona se encuentra de viaje en el otro lado del mundo, su equipo portátil (si está instalado un agente) se comunicará con AD Enterprise cuando esté en línea. No es necesario que el empleado inicie la sesión en su red, sólo tiene que conectarse a Internet. (Por ejemplo, para consultar su correo electrónico en Starbucks.) No obstante, AD Enterprise le facilita el cumplimiento de la legislación de privacidad al permitirle “cortar” el acceso a equipos que se encuentren en la jurisdicción de países con una legislación de privacidad más estricta. Además, los permisos basados en funciones le permiten definir las operaciones que se pueden realizar en determinados nodos y quién puede realizarlas.

Amenazas externas

Las tecnologías de defensa perimetral y supervisión sólo pueden prevenir o alertar de amenazas que han sido definidas. Además, los hackers expertos disponen de multiples métodos avanzados para saltarse estas defensas. Por tanto, su solución de seguridad de la información no será completa si no dispone de visibilidad y alcance investigador en toda la organización, INCLUYENDO la capacidad de aplicar remedios inmediatamente desde una ubicación remota. El análisis proactivo y reactivo con AD Enterprise le permitirá identificar procesos delictivos y atributos maliciosos, incluso aquellos que hayan sido ocultados por rootkits. Le permite detectar amenazas externas, incluso amenazas avanzadas persistentes, analizar el peligro para comprender su funcionamiento, realizar una evaluación en toda la red para identificar todos los demás nodos afectados Y aplicar remedios en todos los nodos afectados desde una ubicación central. En muchas organizaciones, esta característica es la pieza faltante en su esquema de seguridad de la información. Sin esta capacidad de respuesta, las organizaciones no pueden prevenir eficazmente los daños generalizados en caso de que se produzca un incidente de seguridad, ni son capaces de asegurar la aplicación de un remedio eficaz.

Detectar, investigar y remediar...

ACCESSDATA® ENTERPRISE

AMENAZAS EXTERNAS

Hacking
Analizar detallada y rápidamente miles de equipos para determinar el alcance de la brecha y realizar el análisis de la causa raíz.

Software malicioso
Analizar rápidamente miles de equipos para detectar procesos y dll maliciosos, desconocidos y conocidos.

Amenazas avanzadas persistentes
Identificar elementos maliciosos que se estén ejecutando en la memoria.

Alertas de sistemas de detección de intrusos (IDS)
Ver la actividad actual en un determinado equipo para resolver alertas de IDS.

Evaluación del peligro
Crear un perfil de la amenaza e identificar todos los equipos contaminados.

INVESTIGACIONES INTERNAS

Alertas de supervisión del contenido
Relacionar rápidamente la actividad del usuario con una alerta de supervisión del contenido y conservar los datos forenses relevantes.

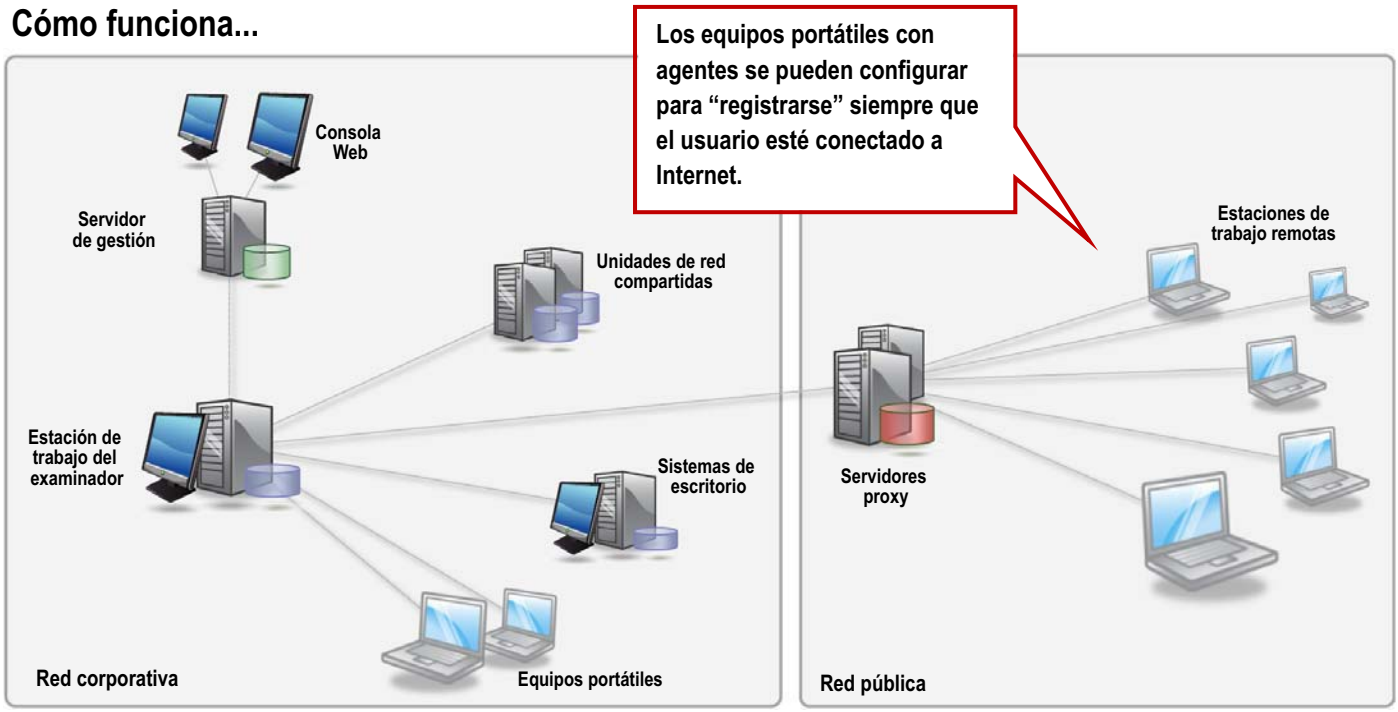
Mala conducta de los empleados
Realizar investigaciones forenses completas y sigilosas de las transmisiones para verificar si se ha producido alguna actividad maliciosa.

Robo de IP
Investigar rápida y exhaustivamente a varias personas centrándose en los archivos y el correo electrónico del usuario.

Infracciones de uso del equipo
Analizar rápidamente la red para detectar procesos no aprobados y realizar vistas previas de unidades para determinar si se han producido infracciones de uso del equipo.

Cuestiones legales
Realizar investigaciones forenses completas de las transmisiones para identificar, analizar y recopilar datos delicados relativos a cualquier cuestión.

Cómo funciona...



1. El examinador realiza la autenticación con el servicio de gestión, recibe autorización para determinadas operaciones de investigación y abre un caso.
2. Al realizar una investigación remota, el examinador solicita al servidor de gestión o a Active Directory una lista de los nodos y selecciona los equipos objetivo.
3. Si el examinador recibe autorización para los nodos de destino, las opciones de investigación pasan a estar disponibles y las solicitudes se envían a los agentes.
4. Los agentes verifican la autorización de la solicitud, aceptan comandos y devuelven información de estado del dispositivo, información de SO e información de la unidad.
5. El examinador elige realizar vistas previas de los dispositivos, adquirir unidades de disco duro o RAM o recopilar datos volátiles.
6. Los agentes responden con una visualización previa de las unidades conectadas y los datos volátiles.
7. FTK acepta los datos de los agentes y muestra la información solicitada en la interfaz gráfica del usuario.
8. El examinador realiza una visualización previa de los dispositivos, procesa los datos y analiza la información relevante para el caso.

Aspectos destacados de la solución:

Respuesta potente a los incidentes sin utilizar scripts...

- **Búsqueda de la memoria activa:** permite analizar miles de nodos para buscar una cadena o palabra clave en memoria, revisar los resultados en contexto y exportar archivos exe/dll de respuesta.
- **Consola de respuesta a incidentes integrada:** revisión rápida, análisis y correlación de procesos, sockets, controladores, usuarios, puertos, DLL, handles y mucho más, en una sola vista en distintos nodos, de RAM y API de Windows.
- Integración en la interfaz gráfica de una función para **detener un proceso y limpiarlo con sólo hacer clic con el botón derecho**.
- Visualizar datos estáticos y volátiles dentro de la misma interfaz.
- **Asistente para corrección por lotes:** definir operaciones de corrección automáticas y seguras para realizarlas en varios nodos.
- Analizar rápidamente miles de equipos, tanto de forma proactiva como reactiva.

Acceso seguro, análisis y conservación forense de diversos datos transmitidos...

- Análisis forense en varios equipos con funciones de **procesamiento, filtrado y elaboración de informes mediante asistentes**.
- **La integración con Active Directory** facilita la selección de nodos objetivo y la autenticación.
- **La integración con ePO** facilita enormemente la instalación del agente y la identificación de nodos objetivo.
- El primer sistema de la industria que permite adquirir con un solo clic **unidades de disco duro, RAM y datos volátiles**.
- **La capacidad de adquisición masiva** admite los trabajos más grandes.
- Sistema de **descifrado, recuperación y obtención de contraseñas** líder en el mercado.
- **Los equipos "se registran" automáticamente:** permite capturar y analizar datos de los equipos, independientemente del lugar en que se encuentren, ya sea en un café o en una oficina doméstica, sin necesidad de esperar a que el nodo se active en la red de la organización.

La única solución de investigación con capacidades de análisis automático y procesamiento avanzado...

- **El asistente para procesamiento de datos** procesa automáticamente correo electrónico, archivos comprimidos y espacio no asignado, elimina archivos binarios conocidos, verifica la identidad de los archivos y **categoriza e indexa automáticamente todos los datos**
- La base de datos de Oracle permite el tratamiento de enormes conjuntos de datos y permite la gestión de casos, el almacenamiento de metadatos y ofrece **potentes posibilidades de manipulación de datos**.
- **El procesamiento distribuido** permite procesar con facilidad enormes cantidades de datos.
- Funcionalidad de guardado y recuperación automáticos.