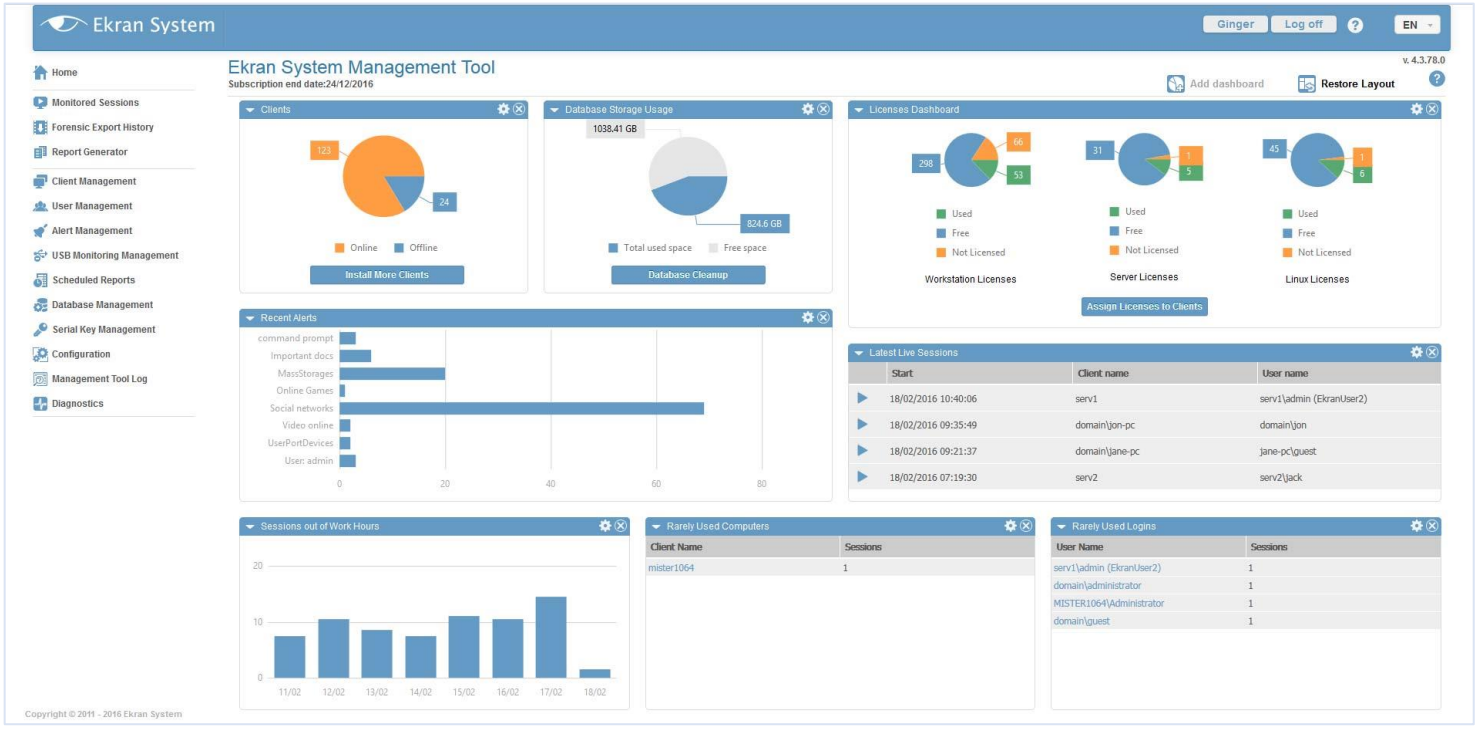
MONITORIZA, DETECTA & ANALIZA
las amenazas de los usuarios

SOFTWARE DE MONITORIZACIÓN DE LA ACTIVIDAD DE LOS USUARIOS
para sus servidores y puestos de trabajo

Ekran ayuda a controlar la seguridad mediante el registro de las actividades del usuario en ordenadores de sobremesa y servidores Virtuales, Citrix, Windows, Linux**,** tanto para las sesiones locales, como para las remotas. Todas las acciones de los usuarios se registran, incluyendo el cambio de ventanas activas, teclado y el ratón. Los datos monitoreados se envían al servidor de Ekran, de auditoría y análisis de seguridad o, si no hay una conexión de red, se almacena en la memoria caché del cliente hasta que se restablezca la conexión.



SUPERVISIÓN DE LA ACTIVIDAD DEL USUARIO

Ekran es una solución mediante la que se obtiene una trazabilidad de la actividad del usuario.

Se lleva a cabo mediante la grabación de la sesión de usuario capturando toda la actividad realizada en pantalla, en un formato de vídeo, así como acompañamiento de meta-datos, como el nombre de la aplicación activa, el título de la ventana activa, si visitó una URL, las pulsaciones del teclado, y los comandos escritos.

Ekran realiza seguimiento de la actividad del usuario en servidores y estaciones de trabajo- locales, RDP y grabación de la sesión de terminal para plataformas Windows y Citrix, también realiza grabaciones de sesiones Telnet SSH para servidores Linux.

A diferencia del software enfocado al seguimiento de la actividad del usuario, es decir, soluciones para grabar sesiones de Terminal Server o actividad PC mediante herramientas de monitoreo, Ekran es una solución universal, que proporciona los registros de auditoría de actividad de usuario detallada para cualquier punto de la red corporativa a través de una única Web.

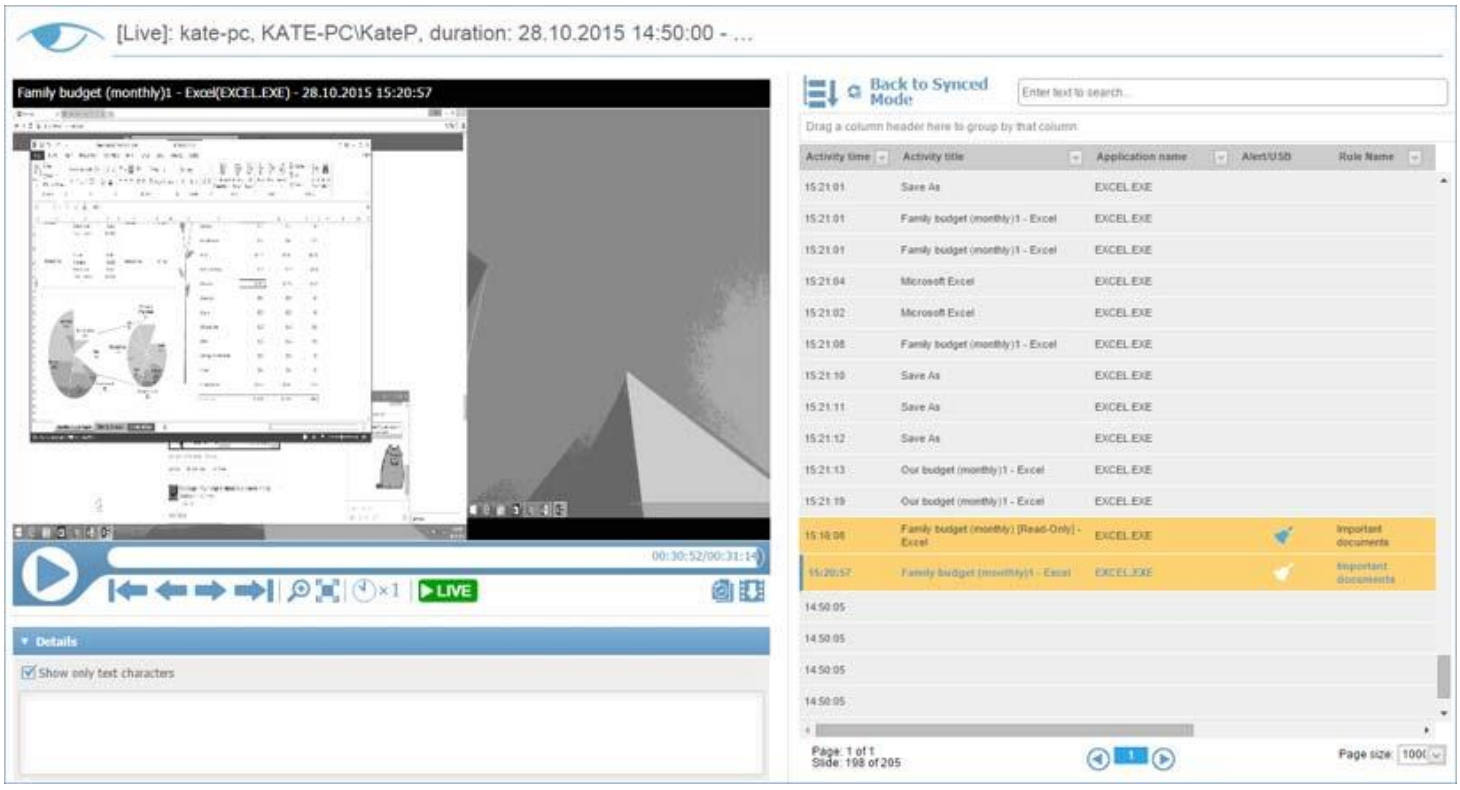
FORMATO DE VÍDEO AVANZADO

La solución se basa en los principios de la actividad del ordenador, mediante la vigilancia pasiva con la captura de cualquier acción realizada por el usuario. Un formato de vídeo indexado avanzado se utiliza para el registro: se puede ver todo lo que sus usuarios han hecho, mediante el uso de la reproducción de vídeo, con opciones de búsqueda de texto.

Se puede navegar rápidamente a los episodios clave en busca de:

- El nombre de la aplicación lanzada
- El título de la ventana activa
- La dirección URL especificada en un navegador web
- El texto introducido desde el teclado del usuario
- Los comandos ejecutados en Linux (tanto de entrada del usuario y ejecutando los scripts)
- La información sobre los dispositivos USB conectados

Además de la búsqueda a la carta, puede configurar alertas en tiempo real, que le notificará acerca de eventos sospechosos y proporcionar enlaces de video relacionados con ellos.

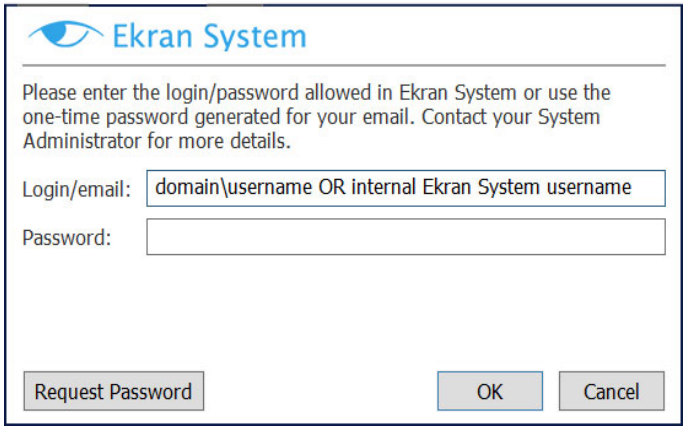


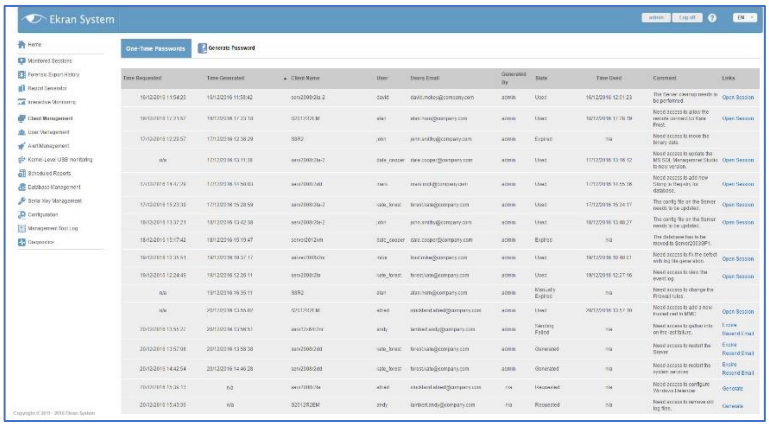
La grabación de vídeo como herramienta para registrar y supervisar la actividad del usuario proporciona una serie de beneficios: incluye cualquier acción iniciada por el usuario, está integrado y no necesita correlación de datos de seguridad adicional, y permite comprender rápidamente, reconstruir y responder un incidente de seguridad, reduciendo así los costos de largos análisis de seguridad

ASIGNAR ACTIVIDAD PRIVILEGIADA A UN USUARIO EN PARTICULAR

El problema típico de gestión de acceso de usuarios privilegiados, es que se comparten cuentas de administrador "despersonalizados". Muchos sistemas de TI tienen credenciales de usuarios privilegiados como "admin" o "root" generalmente compartidas entre varios administradores. Se hace difícil asignar un conjunto específico de acciones para una persona en particular, que tiene acceso a credenciales compartidas, y por lo tanto complica la gestión de identidades.

Para realizar dicho control en las cuentas administrativas más transparentes, Ekran proporciona la segunda capa de autentificación para las conexiones privilegiadas compartidas. Después de habilitar esta opción, los usuarios al iniciar sesión con un nombre de usuario privilegiado genérico, tendrán que introducir además sus credenciales de cuenta personales. Por lo tanto, cualquier grabación de la actividad del usuario está inequívocamente asignada a una persona específica y el seguimiento de usuarios privilegiados es más preciso.





MONITORIZACIÓN DE USUARIOS PRIVILEGIADOS

Ekran permite monitorizar usuarios, independientemente del nivel de privilegios que posean. Usando reglas de política de vigilancia avanzada, puede configurar los clientes Ekran para que supervisen sólo los usuarios que inician sesión en cuentas privilegiadas, si fuera necesario.

Otras actividades de amenazas de seguridad y de riesgo típicas asociadas a usuarios con privilegios son:

- Fraude interno,
- Creación de una cuenta de Backdoor o mediante la instalación de software Backdoor,
- Cambios críticos de configuración de infraestructura y de software,
- Escalada no autorizada de privilegios o los cambios de contraseña de usuario,
- La instalación de malware, la instalación de software de proveedores no confiables,
- La fuga de datos sensibles.

Los usuarios privilegiados, con frecuencia son los administradores de sistemas o administradores de bases de datos, son una parte esencial de cualquier configuración de la infraestructura informática y el apoyo a sistemas de TI y de negocio. La monitorización de un usuario privilegiado y su auditoría, es una parte esencial de cualquier seguridad corporativa. Ekran permite monitorizar usuarios, independientemente del nivel de privilegios que posean. Usando reglas de política de vigilancia avanzada, puede configurar los clientes Ekran para que supervisen sólo los usuarios que inician sesión en cuentas privilegiadas, si fuera necesario.

REQUISITOS DE CUMPLIMIENTO NORMATIVO

Lograr el cumplimiento normativo, es una tarea compleja, que requiere la capacidad de monitorizar cientos e incluso miles de aplicaciones en funcionamiento. No menos importante es que la solución de cumplimiento no debe imponer restricciones que impidan que su negocio crezca de forma natural.

En la lista de los requisitos de cumplimiento normativo, es necesario poder visualizar y grabar las acciones que afecten a datos sensibles o datos determinados por la ley. Una solución es tener un registro que enumera todas las consultas de bases de datos de la aplicación de usuario principal.

SOLUCIÓN DE CUMPLIMIENTO EFICIENTE

Ekran ofrece una cobertura completa de toda la actividad del usuario en servidores y estaciones de trabajo. Al localizar una aplicación ejecutada, una página web abierta en un navegador, o cualquier área visible de la pantalla, proporciona a los auditores de cumplimiento una evidencia innegable. Ekran permite crear rápidamente informes de auditoría, en los que se pueden realizar búsquedas fáciles por palabras clave.

- *Monitorizar todas las aplicaciones de principio a fin*

Ekran permite ahorrar tiempo a los responsables de cumplimiento, que pasan decenas de horas recogiendo información sobre cada aplicación que se utiliza en la red de la empresa, con la esperanza de asegurarse de tener un registro de auditoría completo. Independientemente del tipo de aplicación, se registra toda la actividad realizada en la misma. Así, Ekran elimina la necesidad de supervisar cada aplicación por separado.

- *Asegurar la credibilidad*

Ekran ofrece infraestructura de seguridad fiable y la reproducción completa de las sesiones de usuario, lo que demuestra la credibilidad de la fuente de la actividad del usuario. Además, al almacenar datos en bases de datos MS SQL seguras, puede asegurarse de que Ekran cumple con el protocolo de seguridad de base de datos.

- *Revelando la verdadera identidad de "administrador"*

No se puede proporcionar a un auditor externo pruebas convincentes de si a los datos ha accedido uno u otro "administrador". Para cumplir con ello se debe proporcionar la verdadera identidad de la persona que accede a los datos como administrador. Ekran permite superar este obstáculo con su sistema de autenticación avanzada.