



## Sentinel™ de Novell®

Sentinel™ de Novell® proporciona una visión integral y en tiempo real de las actividades de seguridad y conformidad con las directivas de su entorno de TI.

Logra una mayor efectividad en la administración de riesgos, ya que Sentinel supervisa y genera respuestas e informes para los eventos de seguridad y conformidad con las normas de virtualmente cualquier fuente de datos, incluidos los sistemas, dispositivos y las aplicaciones personalizados y de marca.

Seguridad automatizada y gestión de conformidad con las normas: En toda la empresa la gestión de un entorno de seguridad de TI distribuido y heterogéneo, mediante el uso de herramientas puntuales convencionales es una tarea mayor.

Todos los elementos del entorno, incluidos servidores, bases de datos, aplicaciones, cortafuegos, routers, conmutadores y sistemas de prevención y detección de intrusos, producen una multitud de datos que se deben agregar y analizar para tener una perspectiva clara de la seguridad de su organización y del estado de conformidad con las normas.

Sentinel de Novell reemplaza estos procesos manuales intensivos mediante una supervisión continua y automatizada de los controles de TI y de los eventos de seguridad y conformidad con las directivas. Sentinel correlaciona y analiza los eventos de conformidad con normativas y seguridad de todas las fuentes de datos en su entorno para que pueda identificar los eventos de seguridad en tiempo real y responder con rapidez.

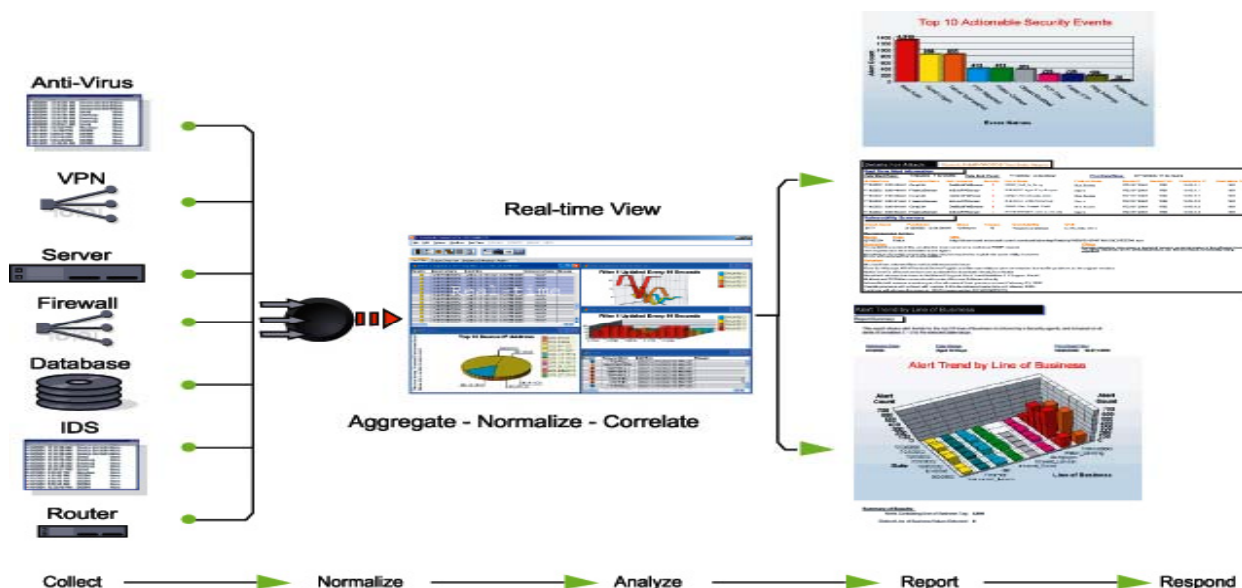
La gestión automatizada de respuesta a incidentes le permite documentar y formalizar el proceso de seguimiento, profundizando y respondiendo a los incidentes y violaciones de las directivas, y le brinda una integración en dos sentidos con sistemas de aviso de incidencias (troubleshooting). Sentinel le permite reaccionar con prontitud, resolver los incidentes con eficiencia y demostrar a los auditores que sus controles de TI funcionan correctamente.

Con Sentinel de Novell, obtiene:

- *Funciones de monitoreo de conformidad con las directivas y administración de seguridad en tiempo real, automatizadas e integradas en todos los sistemas y redes.*
- *Una infraestructura que permite a las directivas de la empresa impulsar las acciones y normativas de TI.*
- *Generación de documentos e informes de eventos de seguridad, sistemas y acceso en toda la empresa.*
- *Solución de problemas y gestión de incidentes incorporados.*
- *Capacidad para demostrar y monitorear la conformidad con las directivas internas y las regulaciones gubernamentales como Sarbanes-Oxley, HIPAA, GLBA y FISMA.*

## Descripción del producto

Novell Sentinel permite a las organizaciones recoger, monitorizar, relacionar y visualizar información sobre los millones de eventos que tienen lugar en su entorno TI todo ello en tiempo real. Con Novell Sentinel, los administradores, auditorías y responsables relacionados dispondrán en el momento de solicitarlo informes actualizados sobre la salud de la compañía en términos de seguridad y cumplimiento con la normativa vigente.



Con Novell Sentinel, el cliente disfruta de una solución que le permitirá reducir costes relacionados con la seguridad de infraestructuras y acceso y costes relacionados con el cumplimiento de legislaciones y normativas.

Los sistemas de prevención de intrusos, cortafuegos, aplicaciones de antivirus, conmutadores y routers generan grandes cantidades de datos todo el tiempo. ¿Pero qué ocurre si su cortafuegos indica un problema urgente mientras su Sistema de detección de intrusos permanece extrañamente silencioso? ¿Cuál de los dos está en lo correcto? ¿Cómo responde?

Sentinel correlaciona los datos pertinentes y aplica la taxonomía de eventos y relevancia comercial apropiadas para alertarle sobre los eventos de los que debe ocuparse. Reducirá las falsas alarmas y podrá concentrarse en los recursos que necesitan de su atención.

Mediante el uso de reglas empresariales incorporadas puede establecer una configuración que refleje las directivas y mejores prácticas de su empresa, así como monitorear y hacer un seguimiento del estado de las infracciones y de las acciones para la solución de problemas. Puede identificar rápidamente las nuevas tendencias o ataques, manipular e interactuar con información gráfica en tiempo real y desglosar los detalles del historial desde segundos a horas. Además, la arquitectura de mensajes basada en bus de Sentinel permite una integración fácil con el Gestor de identidades de Novell y otras soluciones de identidad, seguridad y gestión de acceso. Sentinel usa además una correlación incorporada a la memoria para reducir la carga en su base de datos y acelerar el envío de datos de eventos críticos.

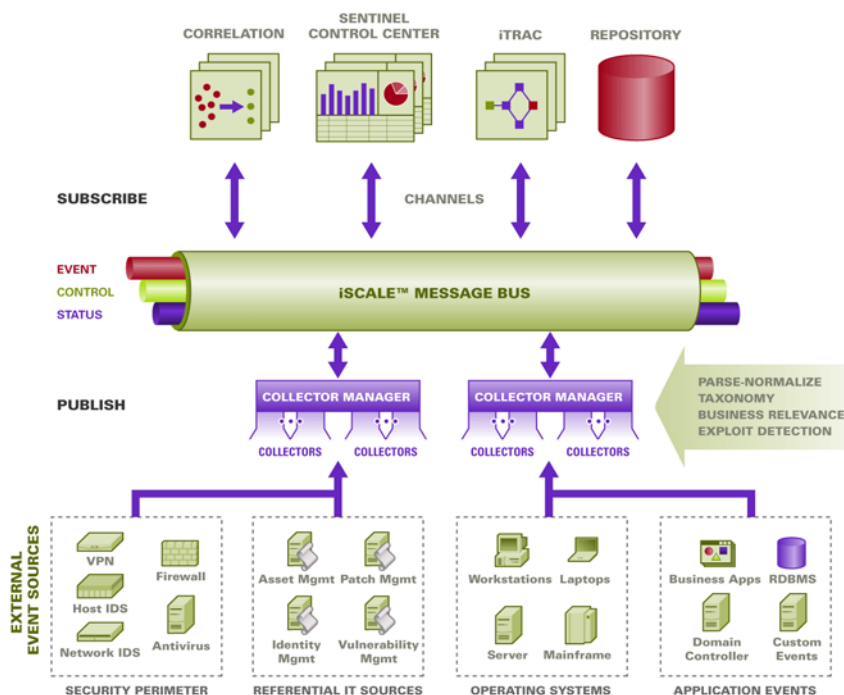
Sentinel es compatible con las plataformas Windows\*, UNIX\*, Solaris\* y Linux\*. Puede conectarse a cualquier dispositivo que se comunique a través de SNMP, ODBC y otros protocolos estándares.

## Componentes de Novell Sentinel

El servidor Novell Sentinel tiene como objetivo principal la generación de un centro unificado de información relacionada con eventos que se producen en los sistemas de la compañía. Dicha información, a la vez que es monitorizada, es también almacenada en una base de datos que puede ser Oracle o MS SQL Server con fines de histórico.

Más en detalle, el servidor Novell Sentinel se compone de los siguientes elementos:

- iSCALE message bus: Sistema de bus de mensajes patentado responsable de unir a todo el resto de componentes.
- Correlation engine: Es la parte responsable de ofrecer la posibilidad de relacionar datos tanto de los recibidos de los distintos sistemas conectados como con los existentes en la base de datos de histórico.
- Control Center: Herramienta gráfica de gestión y control.



- ActiveViews and Reporting: Herramienta de generación de vistas para la configuración del sistema de monitorización.
- iTRAC remediation work-flow: Sistema de gestión de flujos de aprobación con el objetivo de permitir la asociación de posibles remedios (avisar a un responsable, ejecutar un comando, apagar un servicio, etc..) en base a posibles incidentes. En este caso, un incidente es la obtención de un resultado concreto, que nosotros interpretamos como incidencia, procedente de una relación de datos (Correlation Engine).
- Collectors: Son los conectores que van a permitir acceder a los sistemas de eventos y registros de cada sistema para que, una vez la información traducida, poder gestionar la información en un formato común.



## Beneficios

- Obtener la visibilidad necesaria para gestionar de forma efectiva, tanto en tiempo como en coste, el entorno de seguridad de la compañía obteniendo así el mejor nivel de efectividad
- Detectar y resolver más rápidamente los posibles incidentes reduciendo así los costes de operación
- Disponer de los informes y métricas apropiados de forma rápida y actualizada satisfaciendo cualquier requerimiento por auditoría o cumplimiento de legislación.
- Con Sentinel Reports puede generar informes que demuestren cuando sea requerido el cumplimiento de políticas internas de seguridad y regulaciones gubernamentales (SOX, HIPAA, FISMA, etc.)
- Optimizar los ya reducidos recursos existentes mediante la eliminación de tediosos procesos manuales de recopilación de datos utilizando en su lugar sistemas automáticos de monitorización y análisis de procesos.

