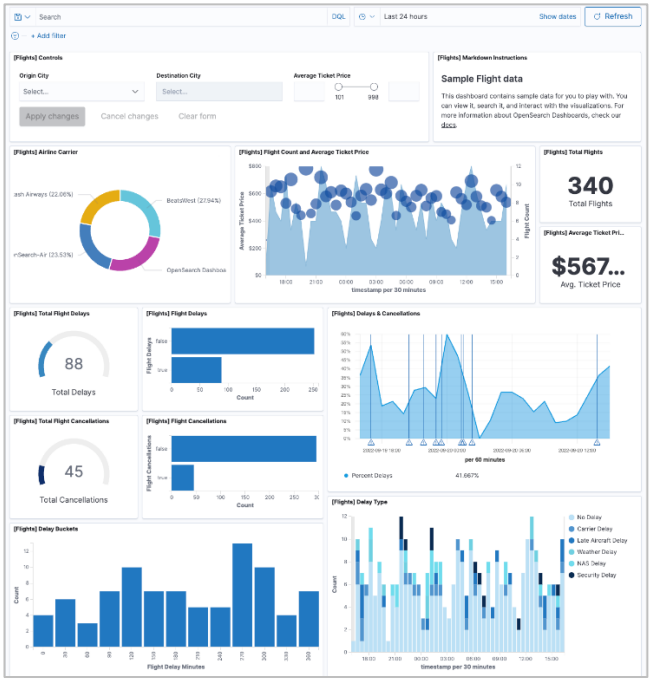
AppVisors Log365

Appvisor Log 365 es el motor para los datos de las maquinas. Colecta, indexa, correlaciona, almacena y aprovecha los datos de las maquinas generados por sus sistemas e infraestructura de TI, puede ser física, virtual o en la nube. Utilice Appvisor Log 365 y los datos de las máquinas para ofrecer nuevos niveles de visibilidad y conocimiento para TI y la empresa haciendo uso de una poderosa consola de administración.



La oportunidad de los datos de las máquinas

Todas sus aplicaciones de TI, sistemas e infraestructura generan datos cada milésima de segundo cada día. Estos datos de las máquinas contienen un registro definitivo de todas las transacciones de los usuarios, el comportamiento del cliente, el comportamiento de la máquina, las amenazas de seguridad, las actividades fraudulentas y mucho más. También son dinámicos, no estructurados y no estándar, y constituyen la mayor parte de los datos de su organización.

Los datos de las máquinas son un recurso muy valioso, pero las organizaciones rara vez obtienen el valor que necesitan de ellos.

Las soluciones de análisis, gestión y monitoreo de datos existentes simplemente no están diseñados para este tipo de datos.

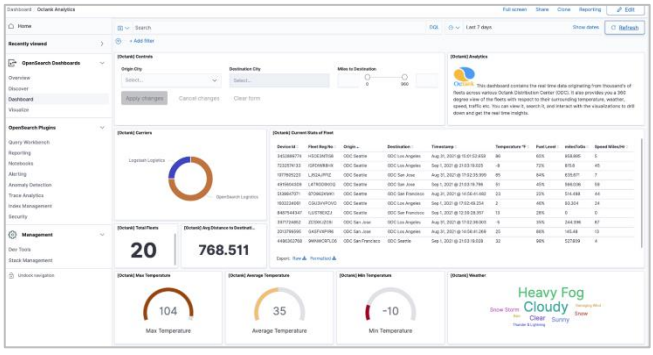
Tome la gestión de la información. Los sistemas de gestión de almacenes de datos y base de datos relacionales se basan en esquemas rígidos, y están diseñados para datos estructurados y uniformes. Estos proporcionan análisis históricos, pero no visibilidad en tiempo real. La búsqueda Enterprise está diseñada para los datos generados por las personas, tales como documentos y páginas web. Estos datos son muy diferentes de los datos de las máquinas. Los datos de las máquinas tienen un orden de mayor magnitud, y poseen gran volumen y diversidad en comparación con los datos tradicionales y estructurados.

Cree péneles personalizados para los usuarios de TI y la empresa en tan solo unos cuantos clics.

Las herramientas de gestión de TI, las de seguridad de la información y las de gestión de eventos funcionan en silos y están diseñadas para manejar un solo nivel de la organización.

Estos proporcionan una visión estrecha de los datos subyacentes y están estructurados para tipos específicos de datos y fuentes. O bien monitorean los sistemas, con graves lagunas en los datos que recogen. Tampoco proporcionan contexto histórico.

Lo cierto es que buscar una mejor manera de clasificar, separar y comprender las enormes cantidades de datos de las maquinas puede transformar la manera en la que las organizaciones de TI gestionan, protegen y auditan la información. También puede proporcionar información valiosa para el negocio acerca de las tendencias y comportamientos de sus clientes y servicios.



Desbloquee la búsqueda, el monitoreo y el análisis en tiempo real de datos comerciales y operativos.

El enfoque de Appvisor Log 365

Appvisor Log 365 es el motor para los datos de las maquinas. Fue desarrollado para superar completamente los desafíos que comprenden los datos de las maquinas; colecta, indexa, almacena y aprovecha los datos no estructurados de las maquinas.

Además, colecta, indexa y aprovecha sus series de datos temporales y no estructurados de las máquinas. Appvisor Log 365 puede leer los datos desde casi cualquier fuente imaginable, como por ejemplo el tráfico de red, servidores web, aplicaciones personalizadas, servidores de aplicaciones, hipervisores, sistemas GPS, comentarios del mercado de valores, medios sociales y bases de datos estructuradas preexistentes. Ofrece una comprensión de lo que está sucediendo en tiempo real y un análisis profundo de lo que ha sucedido en sus sistemas e infraestructura de TI. Convierte los datos de las máquinas en el conocimiento que necesita para tomar decisiones informadas.

Los datos de las máquinas tienen muchos usos para TI y la empresa:

- **Administración de aplicaciones**: soluciona problemas en entornos de aplicaciones, monitorea la degradación del rendimiento.
- **Seguridad y cumplimiento normativo**: proporciona una respuesta rápida para los incidentes, correlación y monitoreo en profundidad de todas las fuentes de datos.
- **Gestión de infraestructura y operaciones**: monitorea de manera proactiva para garantizar el tiempo de actividad, rápidamente identifica y resuelve los problemas.
- **Análisis web y empresarial:** obtiene visibilidad e inteligencia de clientes, servicios y transacciones, y detecta tendencias y patrones de comportamiento en tiempo real.
- **Análisis predictivo:** aprovecha las tendencias de datos históricos y de crecimiento para ayudar a predecir el futuro y alerta cuestiones claves.

Visualice los datos de registro y rastreo con análisis de registros interactivos.

Encontrar y corregir problemas, seguir el rastro de un atacante, presentar informes para el cumplimiento normativo y analizar el comportamiento de los clientes requiere de una visión completa.

Resolver problemas a menudo significa correlacionar los registros del servidor web, los mensajes SOA, las transacciones de base de datos, el rendimiento virtual y los cambios de la configuración.

Investigar los incidentes de seguridad exige tanto el análisis de los eventos de los registros del servidor, firewall y los sistemas de IDS, además de los eventos, las configuraciones y scripts de las aplicaciones para entender lo que ha sucedido.

Cumplir con las normativas requiere de revisiones sistemáticas y retención de datos a largo plazo de toda la infraestructura, y colocar más barreras para acceder a estos datos a fin de satisfacer las necesidades operativas de todos los días.

Cuando la empresa busca una mejor inteligencia, esto puede requerir una correlación en tiempo real y un análisis de las transacciones y eventos de muchas fuentes de TI, potencialmente combinadas con los datos de la empresa.

Appvisor Log 365 provee a ingenieros de redes, administradores de sistemas, analistas de seguridad y cumplimiento normativo, desarrolladores, personal de soporte o mesa de ayuda y usuarios de negocios por igual nuevos niveles de visibilidad, todo desde una sola solución. A esto llamamos ofrecer inteligencia operativa.

¿Cómo se diferencia Appvisor Log 365?

Appvisor Log 365 es diferente de los enfoques anteriores en cuanto a gestión, auditoría, seguridad y acumulación de informes de inteligencia de los sistemas de TI. Veamos cómo lo hace:

Resultados inmediatos sin riesgo. Appvisor Log 365 es un software empresarial sencillo. Los usuario pueden instalarlo en minutos, alimentarlo con cualquier dato de las maquinas e inmediatamente obtener productividad. No se necesitan más ejércitos de consultores o DBA (administradores de bases de datos) para hacer que funcione.

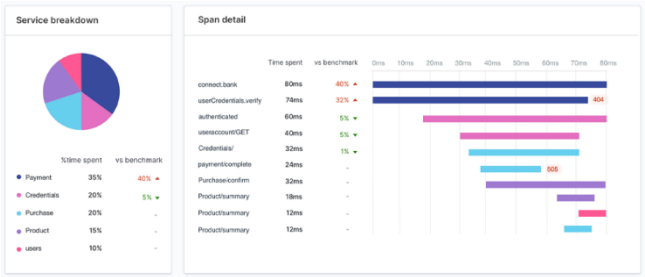
Detecte y mitigue los problemas más rápido con la detección de anomalías.

Appvisor Log 365 se basa en una tecnología de indexación y búsqueda de alto rendimiento. Cada día, millones de personas buscan y navegan por miles de millones de páginas web servidas por computadoras de todo el mundo. La búsqueda es flexible, intuitiva y ofrece resultados inmediatos.

Appvisor Log 365 posee fundamentalmente una tecnología de indexación y búsqueda que aporta un nuevo significado a la velocidad y capacidad de respuesta. Con ella usted puede buscar miles de millones de eventos en cuestión de segundos y empezar a ver resultados de inmediato.

Diseñado para datos no estructurados basados en el tiempo

Los datos de las maquinas son datos no estructurados con marcas de tiempo, son dinámicos y no estándares. Estos capturan todas las interacciones entre máquina y máquina y máquina y usuario generando volúmenes que superan con creces los datos estructurados de la empresa. También están creciendo a un ritmo exponencial. Appvisor Log 365 no utiliza ningún esquema predefinido, por lo que puede leer datos en cualquier formato y desde cualquier fuente imaginable.



Diagnostique problemas de rendimiento y reduzca el tiempo de inactividad de la aplicación.

Indexa datos desde cualquier fuente

Los sistemas de gestión, SIEM, CEP/ECA y los productos de administración de eventos requieren semanas o meses para desarrollar o configurar conectores personalizados para cada fuente de datos. Appvisor Log 365 recoge directamente los datos de decenas de miles de fuentes y los trae de manera segura a una ubicación central en tiempo real.

Permite el análisis de datos en tiempo real e históricos.

Los sistemas de TI tradicionales fuerzan una decisión entre el monitoreo en tiempo real o el análisis histórico. Con Appvisor Log 365, puede buscar y analizar la transmisión de datos en tiempo real y datos históricos desde una solución. Esto significa que puede identificar y responder a los patrones de comportamiento o actividad de interés antes de que sea demasiado tarde.

El software que los usuarios desean utilizar

Se utiliza para dar sentido a la gestión de su infraestructura de TI en silos.

Pero con los ambientes actuales distribuidos y de escalabilidad horizontal y la proliferación de aplicaciones de aplicaciones y de virtualización complejas basadas en la Web, esto simplemente ya no funciona. Appvisor Log 365 rompe las barreras entre los silos de TI. Busque, informe, monitoree y analice todos los datos de cualquier aplicación, servidor y dispositivos; todo desde un solo lugar y en tiempo real. Se integra fácilmente con herramientas existentes de gestión, seguridad y cumplimiento normativo de la empresa. Encontrar y corregir problemas, seguir el rastro de un atacante, rastrear transacciones y obtener nuevos conocimientos a partir de los datos operativos es de repente mucho más rápido y fácil.

Cree vistas y paneles personalizados

Appvisor Log 365 ayuda a dar sentido a grandes volúmenes de datos de la máquina para satisfacer las necesidades de los diferentes usuarios y grupos en la organización. Cree rápidamente paneles personalizados que integren varios gráficos y vistas de sus datos en tiempo real y véalos desde su computadora de escritorio o dispositivo móvil.

Appvisor Log 365 escala desde una computadora portátil hasta un centro de datos

Durante una época en que cada gasto es analizado profundamente, las organizaciones no siempre cuentan con los recursos necesarios. Es por eso que Appvisor Log 365 está diseñado para adaptarse a cualquier ambiente y precio.

Proporcionar las capacidades clave para la inteligencia operativa

- Colecta e indexa universalmente los datos de las máquinas desde prácticamente cualquier fuente
- Permite la búsqueda e investigación de incidentes de forma libre desde un solo lugar
- Automáticamente, descubre conocimientos a partir de los datos y permite a los usuarios añadir sus propios
- Monitorea sus datos y proporciona alertas en tiempo real cuando se cumplen condiciones específicas.
- Proporciona información y análisis muy eficaces
- Proporciona la capacidad de crear vistas y paneles personalizados para diferentes roles
- Se escala eficazmente con el uso de hardware no especializado
- Proporcionar seguridad y controles de acceso basados en roles granulares
- Es compatible con esquemas multi empresa y se implementa de manera flexible.

Tablero de Administración (Dashboard)

Appvisor Log 365 Dashboards le brinda variedad de visualizaciones de datos para representar gráficamente tendencias, valores atípicos y patrones en sus datos. Estos tableros son personalizables y permite mostrar la información que a su organización le sea más relevante.

- Permite añadir fuentes externas
- Puede generar informes desde el Dashboard, Visualizar, Descubrir (búsqueda guardada).
- Puede generar reportes basados en búsquedas.

Gestión de reportes

Proporciona reportes que permiten medir las siguientes capacidades de inteligencia:

- Tendencias y análisis de DNS y DHCP
- Gestión de direcciones IP
- Seguridad y cumplimiento.
- Reportes personalizables y a demanda
- Permite adicionar nuevos tipos de reportes.
- Crear reportes en formato PNG, PDF y CSV.
- Búsquedas flexibles de información o eventos por: palabra clave, expresiones booleanas, expresiones de comparación y campos.

Alertas

Appvisor Log 365 proporciona alertas configurables y permite la gestión de alertas mediante:

- Traps SNMP y SYSLOG
- Enviar correos electrónicos

Puede usar el complemento Alerting en Appvisor Log 365 Dashboards para monitorear sus datos y crear notificaciones de alerta que se activan cuando ocurren condiciones en uno o más índices, y separar los datos críticos de datos irrelevantes (ruido de fondo).

¿Por qué utilizar Appvisor Log365?

Búsqueda de texto completo rápida y escalable
Ayude a los usuarios a encontrar la información correcta dentro de su aplicación, sitio web o catálogo de lago de datos.

Supervisión de aplicaciones e infraestructura
Almacene y analice fácilmente los datos de registro y establezca alertas automáticas para el bajo rendimiento.

Gestión de información de eventos y seguridad
Centralice los registros para habilitar el monitoreo de seguridad en tiempo real y el análisis forense.

Seguimiento de la salud operativa
Utilice registros de observabilidad, métricas y seguimientos para monitorear sus aplicaciones y negocios en tiempo real.

Especificaciones del Sistema

Appvisor Log365 Virtual Appliance es compatible con VMware ESXi 6.5, 6.0 y 5.5. Los usuarios deben asegurarse de que su hardware cumpla con los requisitos de VMware para esta solución a fin de obtener un rendimiento y una confiabilidad óptima.

Las soluciones de administración de registros consumen muchos recursos y la selección del hardware adecuado juega un papel importante para garantizar un rendimiento óptimo.

La siguiente tabla indica los requisitos de hardware sugeridos según el tipo de flujo:

ESPECIFICACIONES APPLIANCE VIRTUAL		
vCPU: 6	vCPU: 12	vCPU: 24
vRAM: 12 GB	vRAM: 32 GB	vRAM: 64 GB
vDisk: 1 TB	vDisk: 6 TB	vDisk: 14 TB
vNIC: 1 Gbps	vNIC: 1 Gbps	vNIC: 10 Gbps
FLOW		
Low Flow	Normal Flow	High Flow
2GB/d	10GB/d	30GB/d

Utilice la siguiente tabla para determinar el tipo de flujo para su instancia.

Log type	Size (in Bytes)	Category	Log Units		
			Low Flow (EPS)	Normal Flow (EPS)	High Flow (EPS)
Linux, HP, pfSense, Juniper, Infoblox	150	Type 1 Syslogs	2000	10000	20000
Cisco. Sonicwall, Huaweii, Netscreen, Meraki, H3C	300	Type 2 Syslogs	1500	6000	12000
Barracuda, Fortinet, Checkpoint	450	Type 3 Syslogs	1200	4000	7000
Palo Alto, Sophos, F5, Firepower, and other syslogs	600	Type 4 Syslogs	800	2500	5000