



## Información sobre el producto: ArcSight Logger

# Combatir el delito informático, demostrar el cumplimiento normativo y agilizar las operaciones de TI

### Aspectos destacados:

- Agrupación integral de logs: datos de logs sin procesar y recopilación optimizada instantánea de más de 275 fuentes diferentes.
- Depósito de logs con calidad de auditoría: recopilación y almacenamiento seguro, controles de integridad, controles de acceso pormenorizados y políticas de retención automatizadas.
- Análisis potente: búsquedas interactivas de alto rendimiento en todos los formatos de datos (tanto estructurados como desestructurados), elaboración de informes integrales y motor de alertas en tiempo real con contenido de delitos informáticos, cumplimiento y operaciones de TI previamente empaquetados.
- Solución rentable: capture, almacene y realice búsquedas de hasta 42 TB de logs reales por dispositivo, suficiente para abarcar años de elaboración de informes.

ArcSight Logger ofrece una solución líder del mercado y rentable para realizar la gestión de todo tipo de logs con el fin de proteger a organizaciones públicas y privadas grandes, y pequeñas.

### Por qué es necesario contar con una solución integral de gestión de logs

Con todos los datos, transacciones y usuarios que hay en línea, los gobiernos y las empresas de todo el mundo son cada vez más vulnerables al fraude, robo y fugas de información por parte de hackers, software malicioso y empleados malintencionados. En un año, el robo y las fugas de información producidas por delitos informáticos han dado lugar a una pérdida mundial de un billón de dólares en concepto de propiedad intelectual y gastos. Por otra parte, el riesgo creciente del delito informático ha activado una tendencia a controlar el cumplimiento normativo. Hoy en día, incluso una empresa mediana puede estar sujeta al coste y esfuerzo del cumplimiento de numerosas normativas como, por ejemplo, Sarbanes-Oxley, HIPAA, FISMA, GLBA, PCI, BASEL II, NERC y las leyes internacionales de privacidad de datos, entre otras.

Los logs proporcionan un historial de auditorías que se puede analizar para detectar e investigar el delito informático, agilizar las auditorías reglamentarias y mejorar las operaciones de TI. Sin embargo, para hacer frente a las complejas amenazas de la seguridad informática en constante evolución, se necesitan soluciones comerciales de gestión de logs para permitir una recopilación completa, un almacenamiento eficaz y un análisis intuitivo y rápido de todos los datos de eventos, tanto estructurados como desestructurados.



## ArcSight Logger solución de primera clase para la gestión de logs

Las soluciones tradicionales de gestión de logs han fallado a la hora de satisfacer simultáneamente las necesidades de los equipos de operaciones de TI, cumplimiento y seguridad. Se centran solamente en datos estructurados para análisis de seguridad o en datos desestructurados para operaciones de TI. ArcSight Logger unifica la elaboración de informes, alertas, búsquedas y análisis de cualquier tipo de información de empresas, y esta característica lo hace único gracias a su capacidad de recopilar y analizar las ingentes cantidades de datos generados por las redes modernas.

ArcSight Logger contribuye a:

- **Combatir el delito informático**, ya que permite realizar análisis unificados de todo tipo de datos para que las investigaciones forenses sean más rápidas y simples.
- **Demostrar el cumplimiento normativo** a través de la recopilación y el almacenamiento de datos con calidad de auditoría, elaboración de informes previamente empaquetados y almacenamiento eficaz de datos regulados durante varios años.
- **Agilizar las operaciones de TI**, al permitir que las investigaciones de todo tipo de datos operativos necesarios para la gestión del cambio, la gestión de redes y la gestión de aplicaciones sean rápidas, mejores y más sencillas.

## Recopilación completa

ArcSight Logger admite la recopilación de logs sin procesar o desestructurados de cualquier sistema o fuente de log basada en un archivo, y también posee la gran biblioteca de ArcSight Connectors que recopila más de 275 fuentes diferentes de generación de logs. Además, el marco de ArcSight FlexConnector amplía las capacidades de recopilación de logs para personalizar las fuentes y las aplicaciones

internas que se necesitan para cumplir con la normativa y en las investigaciones forenses. ArcSight Connectors se pueden implementar como software o como dispositivos en los CPDs y en las oficinas regionales o sucursales para permitir una recopilación segura y fiable. ArcSight Connectors también ofrecen controles de ancho de banda, ordenamiento del tráfico de logs según la prioridad, almacenamiento en caché local y otras medidas para minimizar la pérdida de datos o su impacto en el tráfico de datos confidenciales de la empresa.

## Análisis forenses rápidos

ArcSight Logger proporciona cuadros de mando basados en la función o personalizados que combinan informes relevantes en una única consola. A partir de estos cuadros de mando de resumen, los usuarios pueden ahondar en los informes específicos y simular el flujo de trabajo de una auditoría. Los informes de ArcSight Logger impulsan un formato de evento común y no requieren el conocimiento previo de formatos de log de una fuente específica. Esto evita la necesidad de análisis específicos de dispositivo o proveedor. Los resultados interesantes de los informes se pueden analizar más profundamente a través de una sencilla interfaz de búsqueda similar a la de Google para investigar los datos de logs estructurados o desestructurados. A su vez, los patrones de búsqueda se pueden convertir en alertas en tiempo real para garantizar que los resultados posteriores generen una notificación inmediata dentro de la consola de ArcSight Logger o a través de SMTP, SNMP o un log del sistema.

Finalmente, los usuarios pueden pasar de una alerta a los eventos de base subyacentes que activaron dicha alerta para analizar las causas fundamentales. Aquí es donde la búsqueda desestructurada y el rápido rendimiento juegan un papel fundamental, ya que el análisis puede llevar a datos muy antiguos o que no sigan un formato concreto. Este flujo lógico en las diferentes formas de análisis elimina la necesidad de crear nuevo contenido en cada fase de una investigación.

## Rendimiento sin sacrificar ningún aspecto

La mayoría de las herramientas de gestión de logs admiten el análisis rápido de logs, pero en detrimento del ritmo de recopilación y la eficacia del almacenamiento, o exigen más hardware. ArcSight Logger posee una arquitectura única que minimiza estos efectos adversos y permite habilitar un único dispositivo ArcSight Logger para capturar logs sin procesar a velocidades de hasta 100 000 eventos por segundo, comprimir y almacenar hasta 42 TB de logs, o ejecutar búsquedas a más de millones de eventos por segundo, tanto para datos estructurados como desestructurados.

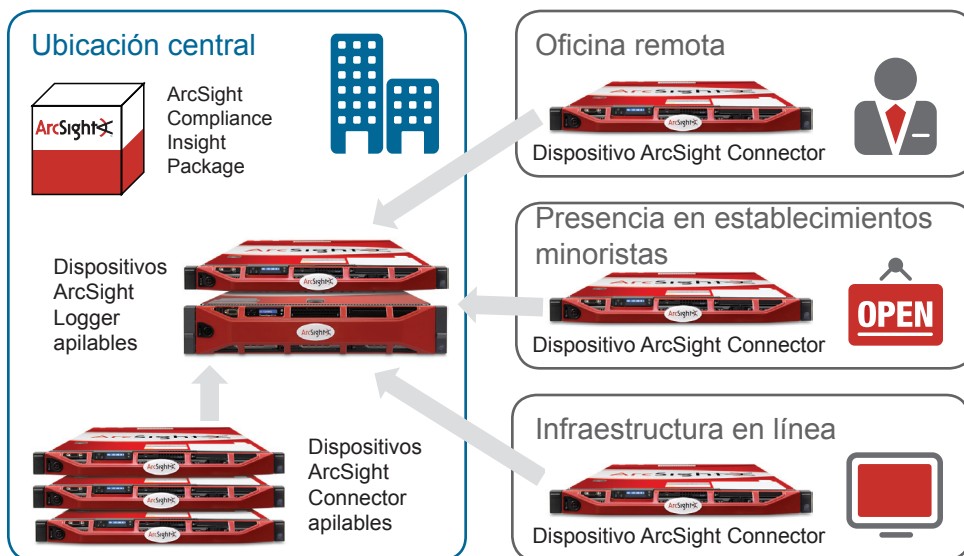
## Almacenamiento flexible

Además del almacenamiento integrado habilitado para RAID, ArcSight Logger también puede impulsar una inversión SAN existente como el almacenamiento de logs. Independientemente de que el almacenamiento esté integrado o no, los logs se comprimen de manera eficaz a una tasa de hasta 10:1. Los controles de acceso basados en la función protegen al sistema y a los datos de eventos. Además, se pueden crear políticas de retención múltiples basadas en las normativas, el tipo de fuente o la dirección IP. Una vez definidas, las políticas de retención se aplican automáticamente sin necesidad de realizar una limpieza manual.

## Contenido previamente empaquetado

ArcSight Logger se envía con contenido de sistema que se puede utilizar para el control de la seguridad cibernética, del cumplimiento y de las operaciones de TI. El contenido adicional específico de las normativas como PCI y SOX se encuentra disponible como paquetes de soluciones complementarias y se le asignan normas reconocidas tales como NIST 800-53, ISO-17799 y SANS.

Figura 1: ArcSight Logger admite diversas opciones de implementación optimizadas tanto para las pequeñas empresas como para los entornos más grandes, heterogéneos y de amplia distribución.



## Adaptación de pequeñas a grandes empresas

La incorporación de los dispositivos de ArcSight Logger a cualquier implementación aumentará notablemente el rendimiento de la recopilación y del análisis, además de la capacidad integrada. Como tales, las grandes organizaciones con diversos dominios administrativos o proveedores de servicio de seguridad gestionada (MSSP, por sus siglas en inglés) pueden optar por implementar varios dispositivos de ArcSight Logger de manera jerárquica u horizontal, para ampliar la capacidad y el rendimiento según fuera necesario. Debido a que los diversos dispositivos de ArcSight Logger funcionan como una matriz, la visualización general de los logs de toda la empresa permanece disponible en todo momento.

## Facilidad de implementación y gestión

La gestión de logs se realiza fácilmente con el dispositivo reforzado y de bajo consumo, y con la arquitectura de almacenamiento única de ArcSight Logger. No se requiere experiencia en administración de bases de datos ya que la GUI de administración 100% basada en la Web

simplifica la implementación y gestión continua sin necesidad de instalar un software cliente.

Las configuraciones especializadas, tal como ArcSight PCI Logger, ofrecen un dispositivo todo en uno para la recopilación, el almacenamiento y el análisis previamente empaquetado que resulta ideal para que los pequeños comerciantes reciban el impulso inicial para sus iniciativas de PCI con un mínimo de esfuerzo.

## Logs con calidad de auditoría

El uso de logs en auditorías de cumplimiento y litigios exige que las organizaciones demuestren la integridad y disponibilidad de los datos de logs en tránsito e inactivos. Se han incorporado varios controles con calidad de auditoría en ArcSight Logger. ArcSight Connectors proporcionan almacenamiento en caché local en ubicaciones remotas, lo que reduce el impacto de una pérdida de conectividad en el CPD. ArcSight Logger también admite la tolerancia automatizada a fallos de ArcSight Connectors en la ubicación remota a un destino secundario y centralizado de ArcSight Logger.

Los logs se transmiten y almacenan de manera fiable para garantizar que los eventos confidenciales no se eliminen o pierdan debido a enlaces de transmisión saturados, falta de memorias intermedias en la fuente o protocolos de transporte no fiables. Los controles de integridad se aplican conforme a la norma de gestión de logs NIST 800-92. La mayoría de las organizaciones gubernamentales necesitan normas muy específicas de seguridad e interoperabilidad. ArcSight Logger cumple todos los requisitos al ser compatible con los estándares FIPS y CAC.

## Complemente su inversión SIEM

La gestión de logs y las soluciones de gestión de eventos e información de seguridad (SIEM) utilizan los mismos datos subyacentes. Como tales, las organizaciones esperan una interacción entre estas inversiones. ArcSight Logger puede complementar cualquier inversión SIEM para ofrecer un depósito de logs rentable y duradero. En concreto, se integra bidireccionalmente con la oferta SIEM líder del mercado, ArcSight ESM, y está empaquetado con ArcSight Express.

La integración permite que ArcSight Logger envíe los eventos de seguridad a ArcSight ESM y a ArcSight Express de manera flexible para una comparación, visualización y detección de amenazas en tiempo real y en diferentes dispositivos. A su vez, ArcSight ESM y ArcSight Express pueden enviar alertas comparadas nuevamente a ArcSight Logger para realizar búsquedas y crear archivos con un simple clic del ratón. ArcSight es inigualable ya que ofrece una plataforma integrada de manera precisa, tanto para la gestión de registros como para las soluciones SIEM, lo cual impulsa una infraestructura de recopilación común para garantizar un bajo coste de propiedad y un alto rendimiento de la inversión.

## Especificaciones de la gama de dispositivos ArcSight Logger

Modelo	L3200 y L3200-PCI	L7200-SAN	L7200s	L7200x
<b>Gestión</b>	Explorador web, CLI			
<b>Fuentes compatibles</b>	Log de sistema sin procesar (TCP/UDP), logs basados en archivos sin procesar (FTP, SCP, SFTP) Recopilación optimizada para análisis de más de 275 productos comerciales Marco FlexConnector para fuentes de eventos heredados ArcSight Common Event Format (CEF), ArcSight ESM			
<b>SO</b>	Oracle Enterprise Linux 4, 64 bits			
<b>Compresión</b>	Hasta 10:1			
<b>Dispositivos</b>	200	Ilimitado	500	Ilimitado
<b>EPS máx</b>	2,000	75,000	5,000	100,000
<b>CPU</b>	1 x Intel Xeon E5504 Quad Core 2.0 GHz	2 x Intel Xeon E5504 Quad Core 2.0 GHz		
<b>RAM</b>	12 GB	24 GB		
<b>Almacenamiento</b>	2 x 1 TB - RAID 1	Externo - SAN	6 x 1 TB - RAID 5	
<b>Chasis</b>	1 U	2 U		
<b>Fuente de alimentación</b>	480 W - No redundante 100-240 V CA	2 x 870 W - Redundante 90-264 V CA		
<b>Interfaces Ethernet</b>	2 x 10/100/1000	4 x 10/100/1000		
<b>Adaptador de bus de host</b>	N/C	Emulex LPe 11002	N/C	
<b>Dimensiones (profundidad x ancho x alto)</b>	62,7cm x 43,4cm x 4,3cm	68,1cm x 44,2cm x 8,6cm		

El rendimiento real dependerá de factores específicos del entorno del usuario.

### Acerca de ArcSight:

ArcSight (NASDAQ: ARST) es un proveedor líder a nivel mundial de soluciones de gestión de cumplimiento y seguridad que brinda protección a empresas y organismos gubernamentales. ArcSight identifica, evalúa y reduce las amenazas cibernéticas y los riesgos de la organización internos y externos para las actividades asociadas con activos y procesos confidenciales. Con la plataforma SIEM de ArcSight líder del mercado, las organizaciones podrán proteger de manera proactiva sus activos, cumplir con las políticas reglamentarias y corporativas, y controlar los riesgos asociados con el robo, el fraude, las guerras electrónicas y el espionaje informático. Para obtener más información, visite [www.arcsight.com](http://www.arcsight.com).



#### ArcSight, Inc.

5 Results Way, Cupertino, CA 95014, EE. UU.  
[www.arcsight.com](http://www.arcsight.com) [info@arcsight.com](mailto:info@arcsight.com)

Oficina corporativa: 1-888-415-ARST  
Oficina central EMEA: +44 870 351 6510  
Oficina central del Pacífico Asiático: 852 2166 8302

© 2009 ArcSight, Inc. Todos los derechos reservados.  
ArcSight y el logotipo de ArcSight son marcas comerciales de ArcSight, Inc. Todos los demás nombres de productos y empresas pueden ser marcas comerciales o marcas comerciales registradas de sus respectivos propietarios.  
ARST-PB001-102509-12