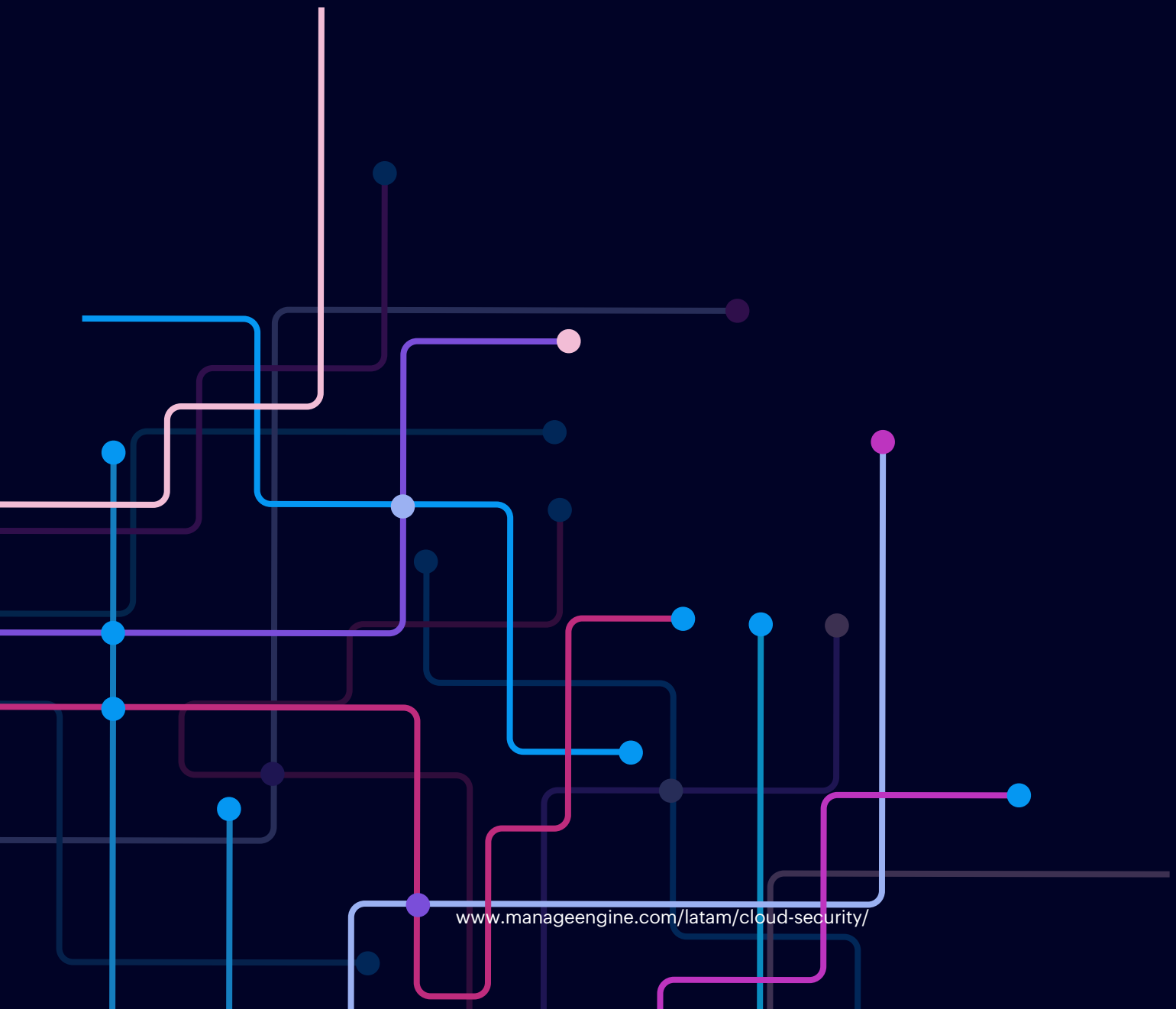
ManageEngine
Cloud Security Plus

Técnicas de integridad de datos y medidas de seguridad adoptadas por Cloud Security Plus



www.manageengine.com/latam/cloud-security/

Cloud Security Plus tiene varios mecanismos para garantizar que la seguridad e integridad de los datos de los logs se mantiene en cada etapa del proceso de gestión de los logs. Este documento profundiza en los métodos de integridad de datos adoptados por Cloud Security Plus al proteger los datos de logs que se recopilan, monitorean y analizan.

Recopilación de logs

- **Seguridad de logs en tránsito:**
  Diferentes técnicas de seguridad y encriptación como **TLS**, **AES-256** y más se emplean para proteger los logs que están en tránsito. Con base en el tipo de datos de logs, las técnicas varían.

  1. **Codificación:**
     a. **En tránsito:** Cualquier transferencia de datos al servidor sucede usando HTTPS. Además, durante la transferencia de datos se emplea TLS y códigos robustos para mejorar la seguridad.

     b. **En reposo:** Los usuarios pueden establecer HTTPS como el protocolo predeterminado para toda comunicación desde la consola web.

     c. **Protección de la base de datos:** Se puede acceder a la base de datos del producto solo al proporcionar credenciales específicas de la instancia y se limita al acceso del host local. La contraseña almacenada en una base de datos en el entorno del cliente se dividen unidireccionalmente usando bcrypt y se filtran de todos nuestros logs. Ya que se usa el algoritmo de división bcrypt con per-user-salt, sería exorbitante y muy tedioso hacer ingeniería inversa a las contraseñas.

- **Seguridad de los logs en reposo:**
  Los logs en reposo se refieren a los datos de logs que se almacenan en Elasticsearch (ES), bases de datos y archivos temporales. Para garantizar la integridad de los logs almacenados, se usa la encriptación **AES-256.**

- **Datos de ES en tránsito:**
  La integridad de los datos de ES mientras se transfieren usando TLS se protegen usando el plugin Search Guard ES.

Otras medidas de seguridad

- **Proteger la comunicación web:**
  Cloud Security Plus es una solución web con un cliente web al que se puede acceder desde cualquier lugar de la red. Habilitar el protocolo HTTPS garantiza que toda la comunicación web está protegida.

- **Control de acceso basado en roles (RBAC):**
  Cloud Security Plus le permite compartimentalizar sus datos entre los técnicos del producto. Se dan dos niveles de acceso: administrador y operario, con el fin de limitar el acceso de los usuarios y controlar funciones específicas e información de dispositivos. De esta forma, puede garantizar que solo personal autorizado accede a los datos. El administrador tendrá acceso a todas las pestañas. Los administradores pueden permitir y restringir el acceso a las pestañas de informes, búsqueda y alertas al operario.

- **Acciones del técnico:**
  Cloud Security Plus proporciona una opción integrada para generar la pista de auditoría de las acciones de todos los usuarios realizadas en el producto. Esto le permite garantizar la aprobación dentro de la solución misma.

- **Terminar la sesión después del tiempo de inactividad:**
  Con Cloud Security Plus, usted puede establecer un tiempo de vencimiento de la sesión y si la sesión está inactiva por más de 10 minutos (que es el tiempo mínimo), la sesión se terminará. Los usuarios pueden cambiar el parámetro predeterminado de 30 minutos para el vencimiento de la sesión a 10 minutos al realizar estos pasos:

1. Inicie sesión en la consola web de Cloud Security Plus como Administrador.
2. Vaya a **Ajustes** > **Ajustes del sistema** > **Ajustes de conexión.**
3. En el campo **Tiempo de vencimiento de la sesión** dé el valor **10.**

Almacenamiento de datos

- **Archivo de índice de ES:**
  Cloud Security Plus permite archivar el índice de ES luego del número específico de días.
  Puede almacenar el índice de ES al seguir estos pasos:

  1. Inicie sesión en Cloud Security Plus como Administrador.
  2. Vaya a **Ajustes** > **Ajustes de administrador** > **Alertas/Logs.**
  3. En el campo **Almacenar índice de ES** dé el número específico de días.

Contacte a servicio al cliente para más detalles

Para más detalles, contacte a servicio al cliente support@cloudsecurityplus.com.