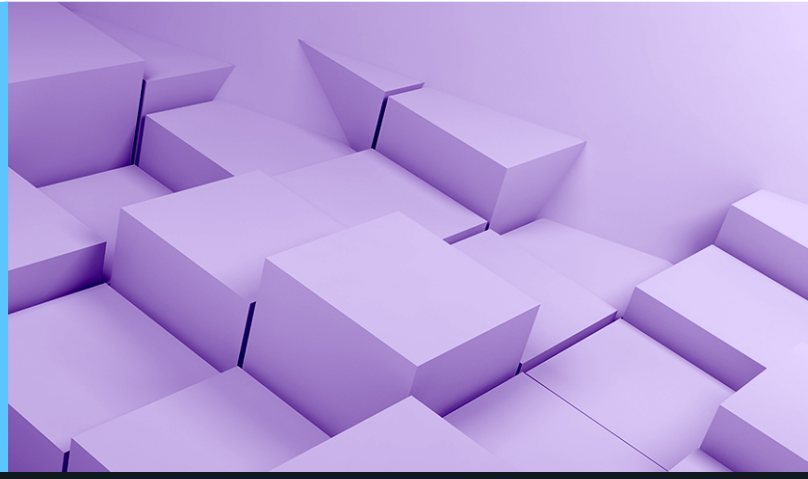
DIEZ RAZONES

NetApp para protección contra el ransomware



01 Espacio de aire lógico

Cree un espacio de aire lógico para bloquear archivos y objetos de forma segura. NetApp® SnapLock® Compliance y NetApp StorageGRID® S3 Object Lock ofrecen funcionalidades nativas de WORM (escritura única, lectura múltiple) para evitar que los datos se eliminen en el período de retención, incluso a manos de cuentas de administrador comprometidas.

02 Recuperación rápida

El mayor coste que supone un ataque de ransomware es el tiempo de inactividad. Haga que sus datos vuelvan a estar en línea rápidamente con copias de Snapshot inmutables de NetApp. Y descubra lo que supone restaurar terabytes de datos en segundos en lugar de horas.

03 Protección autónoma contra ransomware

Identifique y corrija rápidamente las ciberamenazas mediante la tecnología de aprendizaje automático. Esta tecnología, integrada en el software de NetApp ONTAP®, supervisa el sistema de archivos para detectar anomalías, que pueden ser un indicador de malware de actuación lenta. Use el bloqueo de extensiones de archivo antimalware incorporado para detectar e impedir desde un principio que se propague el malware conocido.

04 Detección de anomalías en el comportamiento del usuario

Detecte anomalías en tiempo real para identificar cuentas de usuario comprometidas o un posible comportamiento malicioso gracias a la función Cloud Secure de NetApp Cloud Insights. Si la usa en combinación con el componente NetApp FPolicy de ONTAP, podrá crear puntos de recuperación de datos automáticamente e incluso bloquear otros accesos a la cuenta para impedir el robo o la eliminación masiva de datos.

05 Compatible con la Confianza cero

Adopte un enfoque de seguridad basado en la Confianza cero, con controles como la autenticación multifactor, el acceso basado en roles, los registros completos y las auditorías para protegerse contra ataques secundarios.

06 Prevención de actividad maliciosa de administrador

Evite daños que provengan de cuentas de administrador comprometidas usando la verificación multiadministrador nativa de ONTAP. Esta función requiere que más de un administrador autorice acciones cruciales para el almacenamiento, como la eliminación de grandes volúmenes de copias de Snapshot.

07 Gestión avanzada de copias

Consiga una recuperación de desastres y un backup mejorados. Use NetApp SnapMirror® y el servicio de NetApp Cloud Backup para replicar sus copias de Snapshot de forma eficiente en otro sistema ONTAP o almacenamiento de objetos de su elección, ya sea en las instalaciones o en el cloud.

08 Mitigación de riesgos

Obtenga visibilidad sobre la postura de seguridad de sus datos. Identifique los datos confidenciales y su ubicación mediante NetApp Cloud Data Sense. Realice un seguimiento de los permisos de las carpetas y proporcione soluciones para mitigar riesgos potenciales, como el robo de datos.

09 Supervisión centralizada

Supervise su infraestructura de cloud híbrido mediante una interfaz sencilla. Identifique y corrija amenazas con la consola de protección contra ransomware, disponible en NetApp Cloud Manager.

10 Análisis forense

Use las soluciones demostradas de NetApp para realizar análisis forenses antes y después de eventos de ransomware. Consiga la información necesaria para detectar, gestionar y cerrar vías de ataque.

NetApp