Recuperación acelerada ante ransomware con Dell PowerProtect Backup Services

Recupérese del ransomware en horas, no días

Características clave

Los ataques de ransomware son cada vez más frecuentes, avanzados y caros

- Incapacidad de identificar y restaurar rápidamente las copias de seguridad o los archivos no infectados
- Propagación de la contaminación y reinfección debido a los datos de recuperación
- Pérdida de datos, incapacidad para recuperar un conjunto de datos completo
- Dificultades para coordinar la respuesta ante incidentes
- Exigencias de tiempos de RPO/RTO más rápidos
- El costoso tiempo de inactividad empresarial provoca una pérdida de ingresos y daños a la reputación de la marca
- Multas legales y normativas por una protección de datos inadecuada

El reto

El ransomware es una amenaza seria para todas las empresas. Los ciberataques se producen con frecuencia y pueden causar daños catastróficos. Al 79 % de las organizaciones les preocupa experimentar un evento disruptivo en los próximos 12 meses.1 Las empresas que pierden sus datos corren el riesgo de declararse en quiebra después de un desastre. Los ataques de ransomware no solo son cada vez más frecuentes, sino también más avanzados tecnológicamente y más costosos.

La solución

La recuperación rápida y fiable elimina cualquier razón para pensar incluso en pagar un rescate. Sin embargo, cuando se produce un incidente de seguridad o un ciberataque, las organizaciones deben conocer el radio de impacto y la causa raíz antes de la recuperación. Gracias a la instantánea perfecta y con cámara de aire de las cargas de trabajo y las máquinas virtuales disponible de forma ininterrumpida, la supervisión continua de las anomalías de datos y usuarios, la integración con herramientas de seguridad y la recuperación automatizada de datos limpios, puede mejorar su estado de seguridad y transformar una experiencia devastadora en un incidente del que podrá sobrevivir.

Capacidades

Para todas las cargas de trabajo:

• Asegúrese de que tiene copias de seguridad inmutables y con cámara de aire disponibles de forma ininterrumpida

• Recupere datos limpios en las instalaciones o en la cloud con RPO/RTO de horas, no días ni semanas

• El servicio Managed Data Detection and Response (MDDR) proporciona supervisión en tiempo real de forma ininterrumpida de los entornos de copia de seguridad

• Restaure cargas de trabajo y máquinas virtuales en cualquier región/cuenta de AWS. Si utiliza datos de su organización de producción y crea muchas copias de ellos almacenándolos en varios lugares, está poniendo en un gran riesgo a su organización.

Recuperación acelerada ante ransomware para cargas de trabajo clave:

• Supervise y detecte proactivamente anomalías con algoritmos basados en ML

• Coordine las actividades de respuesta y recuperación a través de integraciones de SIEM y SOAR

• Analice las instantáneas en busca de malware antes de la recuperación y elimine instantáneas y archivos infectados de las copias de seguridad

• Recupere automáticamente la versión limpia más reciente de cada archivo en un marco de tiempo especificado a partir de una instantánea de referencia

Protección

El primer paso para evitar daños causados por el ransomware es garantizar que tenga una copia inmutable y con cámara de aire. Dell PowerProtect Backup Services, que se basa en una infraestructura de cloud muy resiliente, hace imposible que el ransomware cifre los datos de las copias de seguridad. La arquitectura de confianza cero, que incluye autenticación multifactor, cifrado de envoltorio y acceso a cuentas independientes, garantiza que el ransomware no pueda utilizar credenciales del entorno principal comprometido para manipular el entorno de copia de seguridad o los datos. Por último, las funciones de prevención de eliminación excesiva y eliminación suave (papelera de reciclaje) proporcionan una capa adicional de seguridad para proteger las copias de seguridad contra la eliminación.

Detección

Detectar un ataque de ransomware lo antes posible puede ayudar a los equipos de respuesta ante incidentes y evitar la propagación de la contaminación. El módulo de recuperación acelerada ante ransomware de Dell PowerProtect Backup Services proporciona un centro de mando de seguridad para supervisar el estado de su entorno de copia de seguridad. Con información de acceso y detección de anomalías, puede identificar rápidamente actividades inusuales en todo su entorno y sus datos. Consulte la ubicación, la identidad y la información de actividad de todos los intentos de acceso de los usuarios y las API. Detecte anomalías con algoritmos de ML patentados que proporcionan alertas de actividad de datos inusual (por ejemplo, eliminación, cifrado, etc.). El algoritmo aprende los patrones de su entorno de copia de seguridad específico, por lo que no requiere ninguna configuración o ajuste de reglas. También utiliza información basada en entropía para reducir los falsos positivos.

in situ en 4 horas

Cuando un analista de seguridad o TI detecta un evento sospechoso o, peor aún, confirma que se ha producido un incidente de ransomware, la velocidad de respuesta se vuelve crítica. Aunque hay muchas herramientas de seguridad del entorno principal valiosas que se pueden utilizar para la coordinación de detección y respuesta, los análisis y los datos de registro de cambios de datos secundarios (sistemas de copia de seguridad) mejoran las actividades de investigación, respuesta y análisis forense. El módulo de recuperación acelerada ante ransomware de Dell PowerProtect Backup Services ofrece sólidas integraciones de API listas para usar que facilitan la integración de la solución en su ecosistema de seguridad general. La coordinación de las actividades de respuesta mediante soluciones SIEM y SOAR puede reducir drásticamente el tiempo medio de respuesta (MTTR) al completar automáticamente acciones como poner en cuarentena sistemas y las instantáneas infectados o analizar las copias de seguridad de IOC en función de un cuaderno de estrategias de ransomware predeterminado.

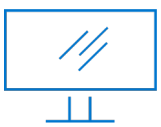
Recuperación

Después de la fase de respuesta inicial viene el duro trabajo de recuperación. Para muchas empresas, este es un proceso manual y que consume mucho tiempo. El tiempo de permanencia de los actores maliciosos y el ransomware puede variar de semanas a meses,

lo que dificulta saber hasta qué punto hay que llegar para encontrar datos limpios. Incluso después de identificar la mejor instantánea, el malware oculto puede provocar una reinfección. Sin embargo, un punto de recuperación de hace 2 semanas no es aceptable para la mayoría de los usuarios empresariales. Sin embargo, encontrar y validar datos más recientes después de un incidente de ransomware es un proceso manual, tedioso y, a menudo, inasumible.

Dell PowerProtect Backup Services alivia esta carga con una arquitectura de copia de seguridad eficaz y herramientas automatizadas para acelerar la recuperación. La plataforma de cloud de Dell PowerProtect Backup Services realiza copias de seguridad de las cargas de trabajo directamente en la cloud, listas para su recuperación inmediata en caso de ataque de ransomware.

El módulo de recuperación acelerada ante ransomware le permite recuperarse con confianza, ya que garantiza la higiene de los datos de recuperación. Puedes analizar instantáneas en busca de malware e IOC utilizando la detección antivirus integrada o utilizando inteligencia de amenazas de sus propias investigaciones forenses o canales de inteligencia de amenazas. El análisis de instantáneas antes de la recuperación elimina la reinfección.



Más información acerca de PowerProtect Backup Services

Comunicación un experto de Dell Technologies