Acerca de la protección frente al ransomware de NetApp

ONTAP 9

NetApp
August 31, 2024

Tabla de contenidos

Acerca de la protección frente al ransomware de NetApp

La cartera de protección de NetApp y ransomware

El ransomware sigue siendo una de las amenazas más importantes que causan interrupciones en el negocio en 2024. Según los "Estado Sophos del ransomware 2024"datos, los ataques de ransomware afectaron al 72 % de su público encuestado. Los ataques de ransomware han evolucionado hasta ser más sofisticados y dirigidos, donde los actores encargados de amenazas emplean técnicas avanzadas como la inteligencia artificial para maximizar su impacto y sus beneficios.

Las organizaciones deben mirar por toda su postura de seguridad, desde el perímetro, la red, la identidad y la aplicación, y donde los datos se encuentran en el nivel de almacenamiento, para asegurar esas capas. Adoptar un enfoque de ciberprotección en la capa de almacenamiento centrado en los datos es crucial en el panorama actual de amenazas. Aunque ninguna solución individual puede frustrar todos los ataques, utilizar una cartera de soluciones que incluya colaboraciones y terceros ofrece una defensa en capas.

El Gama de productos de NetApp ofrece varias herramientas eficaces para la visibilidad, detección y corrección que ayudan a detectar el ransomware de manera temprana, prevenir la propagación y recuperarse rápidamente, si es necesario, para evitar costosos tiempos de inactividad. Las soluciones tradicionales de defensa en capas siguen siendo comunes, como las que utilizan las soluciones de terceros y de socios para la visibilidad y la detección. La corrección efectiva sigue siendo una parte crucial de la respuesta a cualquier amenaza. El enfoque único del sector que aprovecha la tecnología Snapshot de NetApp inmutable y la solución de aislamiento lógico de SnapLock son factores diferenciadores en el sector y una práctica recomendada en el ámbito de las capacidades de remediación del ransomware.

> A partir de julio de 2024, contenido del informe técnico *TR-4572: NetApp Ransomware Protection*, publicado anteriormente como PDF, se ha integrado con el resto de la documentación de producto de ONTAP.

Los datos son el destino principal

Los ciberdelincuentes atacan cada vez más los datos directamente, reconociendo su valor. Si bien la seguridad del perímetro, la red y las aplicaciones son importantes, se pueden omitir. Centrarse en la protección de los datos en su origen, la capa de almacenamiento, proporciona una última línea crucial de defensa. Obtener acceso a los datos de producción, cifrarlos o hacerlos inaccesibles es el objetivo de los ataques de ransomware. Para lograrlo, los atacantes deben haber traspasado ya las defensas existentes implementadas por las organizaciones en la actualidad, desde el perímetro hasta la seguridad de las aplicaciones.

[Capas de seguridad desde el perímetro hasta la seguridad de los datos]

Desafortunadamente, muchas organizaciones no aprovechan las funcionalidades de seguridad en la capa de datos. Aquí es donde entra en juego la cartera de productos de protección contra ransomware de NetApp, que te protege en la última línea de defensa.

El coste real del ransomware

El pago del rescate en sí no es el mayor efecto económico en una empresa. Aunque el pago no es insignificante, palidece en comparación con el coste de tiempo de inactividad de sufrir un incidente de ransomware.

Los pagos de rescates son solo un elemento de los costes de recuperación cuando se trata de eventos de ransomware. Salvo los rescates pagados, en 2024 organizaciones indicaron un coste medio de recuperación tras un ataque de ransomware de 2,73M 000 dólares, un aumento de casi 1M 000 dólares desde los 1,82M 000 millones registrados en 2023, según el "2024 Sophos State of Ransomware (Estado del ransomware de Sophos)" informe. Para las organizaciones que dependen en gran medida de la disponibilidad de TECNOLOGÍA, como el comercio electrónico, el comercio de acciones y el cuidado sanitario, los costes pueden aumentar hasta 10 veces o más.

Los costos de los seguros cibernéticos también continúan aumentando dada la probabilidad muy real de un ataque de ransomware en las compañías aseguradas.

Protección frente a ransomware en la capa de datos

NetApp entiende que su política de seguridad es amplia y profunda en toda su organización, desde el perímetro hasta el lugar donde residen los datos en la capa de almacenamiento. Su pila de seguridad es compleja y debe proporcionar seguridad en todos los niveles de su pila tecnológica.

La protección en tiempo real en la capa de datos es incluso más importante y tiene requisitos exclusivos. Para ser eficaces, las soluciones en esta capa deben ofrecer estos atributos críticos:

- **Seguridad por diseño** para minimizar la posibilidad de un ataque exitoso
- **Detección y respuesta en tiempo real** para minimizar el impacto de un ataque exitoso
- **Protección WORM con aire ACONDICIONADO** para aislar copias de seguridad de datos críticos
- **Un solo plano de control** para una defensa integral contra ransomware

NetApp puede proporcionar todo esto y mucho más.

[La cartera de productos de protección frente a ransomware de NetApp incluye los atributos críticos descritos]

La cartera de productos de protección frente a ransomware de NetApp

NetApp "protección contra ransomware incorporada"ofrece una defensa en tiempo real, sólida y con múltiples facetas para tus datos cruciales. Los algoritmos avanzados de detección impulsados por IA supervisan continuamente los patrones de datos, identificando rápidamente posibles amenazas de ransomware con una precisión del 99 %. Al reaccionar rápidamente a los ataques, nuestro almacenamiento puede realizar instantáneas rápidamente de los datos y proteger las copias, lo que garantiza una rápida recuperación.

Para reforzar aún más los datos, "copias cibernéticas"la funcionalidad de NetApp aísla los datos con una brecha lógica. Al proteger los datos cruciales, garantizamos una continuidad de negocio rápida.

NetApp "Protección contra ransomware de BlueXP"reduce las cargas operativas con un único plano de control para coordinar y ejecutar de forma inteligente una defensa contra el ransomware integral centrada en la carga de trabajo, de manera que puedas identificar y proteger datos de cargas de trabajo cruciales en riesgo con un solo clic, detectar y responder de forma precisa y automática para limitar el impacto de un ataque potencial y recuperar cargas de trabajo en minutos, no días, lo que protege tus valiosos datos de carga de trabajo y minimiza las costosas interrupciones.

Como solución de ONTAP nativa e integrada que protege el acceso no autorizado a los datos, "Verificación multi-admin (MAV)" cuenta con un sólido conjunto de funciones que garantizan que operaciones como la eliminación de volúmenes, la creación de usuarios administrativos adicionales o la eliminación de copias Snapshot solo se puedan ejecutar después de las aprobaciones de, al menos, un segundo administrador designado. De este modo, se evita que administradores comprometidos, malintencionados o inexpertos realicen cambios no deseados o eliminen datos. Puede configurar tantos aprobadores de administrador designados como desee antes de eliminar una copia de instantánea.

NetApp ONTAP aborda el requisito de "Autenticación multifactor (MFA)" la autenticación basada en web en System Manager y de la interfaz de línea de comandos de SSH.

La protección frente al ransomware de NetApp ofrece tranquilidad en un panorama de amenazas en constante evolución. Su enfoque integral no solo defiende las variantes actuales de ransomware, sino que también se adapta a las amenazas emergentes, proporcionando seguridad a largo plazo para su infraestructura de datos.

Obtenga información sobre otras opciones de protección

- "Protección frente a ransomware de Active IQ"
- "Seguridad de carga de trabajo de almacenamiento de Cloud Insights (CISWS)"
- "FPolicy"
- "SnapLock y copias Snapshot a prueba de manipulaciones"

Garantía de recuperación frente a ransomware

NetApp ofrece una garantía para restaurar los datos de SnapVault en caso de que se produzca un ataque de ransomware. Nuestra garantía: Si no podemos ayudarle a restaurar los datos de la snapshot, corregiremos. La garantía está disponible en las nuevas adquisiciones de sistemas AFF A-Series, AFF C-Series, ASA y FAS.

Leer más

- "Descripción del servicio de garantía de recuperación"
- "Blog de garantía de recuperación frente al ransomware".

Información relacionada

- Página de recursos del sitio de soporte de NetApp http://mysupport.netapp.com/ontap/resources
- Seguridad de los productos de NetApp https://security.netapp.com/resources/

SnapLock y copias Snapshot a prueba de manipulaciones para la protección contra el ransomware

Un arma vital en el arsenal de NetApp es SnapLock, que ha demostrado ser altamente eficaz para proteger contra las amenazas de ransomware. Al evitar la eliminación de datos no autorizados, SnapLock proporciona una capa adicional de seguridad, garantizando que los datos cruciales permanecen intactos y accesibles incluso en caso de ataques malintencionados.

Cumplimiento de normativas SnapLock

SnapLock Compliance (SLC) proporciona una protección indeleble para los datos. SLC prohíbe la eliminación de datos incluso cuando un administrador intenta reinicializar la cabina. A diferencia de otros productos de la

competencia, SnapLock Compliance no es vulnerable a los hacks de ingeniería social a través de los equipos de soporte de esos productos. Los datos protegidos por volúmenes de SnapLock Compliance se pueden recuperar hasta que los datos hayan alcanzado su fecha de vencimiento.

Para habilitar SnapLock, "ONTAP One"se necesita una licencia.

Leer más

- "Documentación de SnapLock"

Copias Snapshot a prueba de manipulaciones

Las copias Snapshot a prueba de manipulaciones (TPS) proporcionan un método rápido y cómodo de proteger los datos de actos malintencionados. A diferencia de SnapLock Compliance, TPS se utiliza normalmente en sistemas primarios en los que el usuario puede proteger los datos durante un tiempo determinado y dejarlos localmente para recuperaciones rápidas o donde no es necesario replicar datos fuera del sistema primario. TPS utiliza las tecnologías SnapLock para evitar que la copia snapshot primaria se elimine incluso por parte de un administrador de ONTAP utilizando el mismo período de retención de SnapLock. La eliminación de copias de snapshots se impide aunque el volumen no tenga la función SnapLock habilitada, aunque las snapshots no tengan la misma naturaleza indeleble de los volúmenes de SnapLock Compliance.

Para hacer copias snapshot a prueba de manipulaciones, "ONTAP One"se necesita una licencia.

Leer más

- "Bloquea una copia Snapshot para protegerte contra ataques de ransomware".

Bloqueo de archivos FPolicy

FPolicy bloquea los archivos no deseados para que no se almacenen en su dispositivo de almacenamiento de clase empresarial. FPolicy también le ofrece una forma de bloquear las extensiones de archivos de ransomware conocidas. Un usuario sigue teniendo permisos de acceso completo a la carpeta principal, pero FPolicy no permite que un usuario almacene los archivos que marca su administrador como bloqueados. No importa si esos archivos son archivos MP3 o extensiones de archivos ransomware conocidos.

Bloquea archivos maliciosos con el modo nativo de FPolicy

El modo nativo de FPolicy de NetApp (una evolución del nombre, Política de archivos) es un marco de bloqueo de extensiones de archivos que le permite bloquear las extensiones de archivos no deseadas para que entren en su entorno. Ha formado parte de ONTAP durante más de una década y es increíblemente útil para ayudarte a protegerte contra el ransomware. Este motor de confianza cero es valioso porque obtienes medidas de seguridad adicionales más allá de los permisos de la lista de control de acceso (ACL).

En el Administrador del sistema de ONTAP y BlueXP , hay una lista de más de 3000 extensiones de archivo disponibles para su referencia.

> Algunas extensiones pueden ser legítimas en su entorno y bloquearlas puede dar lugar a problemas inesperados. Cree su propia lista que sea adecuada para su entorno antes de configurar las FPolicy nativas.

El modo nativo de FPolicy se incluye en todas las licencias de ONTAP.

Leer más

- "Blog: Lucha contra el ransomware: Tercera parte: FPolicy de ONTAP, otra potente herramienta nativa (también gratuita)"

Habilite el análisis de comportamiento de usuarios y entidades (UEBA) con el modo externo de FPolicy

El modo externo de FPolicy es un marco de notificación y control de actividad de archivos que proporciona visibilidad de la actividad de archivos y usuarios. Una solución externa puede utilizar estas notificaciones para realizar análisis basados en IA con el fin de detectar comportamientos maliciosos.

El modo externo de FPolicy también se puede configurar para que espere a la aprobación del servidor FPolicy antes de permitir que pasen determinadas actividades. Se pueden configurar múltiples normativas de este tipo en un clúster, lo que le proporciona una gran flexibilidad.

> Los servidores FPolicy deben responder a las solicitudes de FPolicy si se configuran para proporcionar la aprobación; de lo contrario, el rendimiento del sistema de almacenamiento puede verse afectado de forma negativa.

El modo externo FPolicy se incluye en "Todas las licencias de ONTAP".

Leer más

- "Blog: Lucha contra el ransomware: Cuarta parte: UBA y ONTAP con el modo externo FPolicy."

Seguridad de carga de trabajo de almacenamiento de Cloud Insights (CISWS)

La seguridad de las cargas de trabajo de almacenamiento (SWS) es una función de NetApp Cloud Insights que mejora en gran medida la política de seguridad, la capacidad de recuperación y la responsabilidad de un entorno ONTAP. SWS adopta un enfoque centrado en el usuario, rastreando toda la actividad de archivos de cada usuario autenticado en el entorno. Utiliza análisis avanzados para establecer patrones de acceso normales y estacionales para cada usuario. Estos patrones se utilizan para identificar rápidamente comportamientos sospechosos sin la necesidad de firmas de ransomware.

Cuando SWS detecta un posible ransomware, eliminación de datos o ataque de exfiltración, puede tomar acciones automáticas como:

- Tome una copia Snapshot del volumen afectado.
- Bloquee la cuenta de usuario y la dirección IP sospechosa de actividad maliciosa.
- Enviar una alerta a los administradores.

Debido a que puede tomar acciones automatizadas para detener rápidamente una amenaza interna, así como rastrear cada actividad de archivos, SWS hace que la recuperación de un evento de ransomware sea mucho más simple y rápida. Con las herramientas avanzadas de auditoría y análisis forense integradas, los usuarios pueden ver inmediatamente qué volúmenes y archivos se vieron afectados por un ataque, de qué cuenta de usuario procede el ataque y qué acción maliciosa se realizó. Las snapshots automáticas mitigan los daños y aceleran la restauración de archivos.

[Resultados del ataque de seguridad de las cargas de trabajo de almacenamiento de Cloud Insights]

Las alertas de la protección autónoma contra ransomware (ARP) de ONTAP también se pueden ver en SWS, lo que proporciona una única interfaz para los clientes que usan ARP y SWS para protegerse de ataques de ransomware.

Leer más

- "Cloud Insights de NetApp"

Detección y respuesta integradas de NetApp ONTAP basadas en IA

A medida que las amenazas de ransomware se vuelven más y más sofisticadas, también lo deberían hacer tus mecanismos de defensa. La protección autónoma contra ransomware (ARP) de NetApp cuenta con la tecnología de la IA con la detección inteligente de anomalías integrada en ONTAP. Activa la acción para añadir otra capa de defensa a tu resiliencia cibernética.

ARP y ARP/AI se pueden configurar a través de la interfaz de gestión integrada de ONTAP, System Manager y se habilitan por volumen.

Protección de ransomware autónoma (ARP)

La protección autónoma contra ransomware (ARP), otra solución nativa integrada de ONTAP desde 9.10.1, analiza la actividad de archivos de cargas de trabajo de volúmenes de almacenamiento en NAS y la entropía de datos para detectar automáticamente potencial ransomware. ARP ofrece a los administradores detección en tiempo real, conocimientos y un punto de recuperación de datos para una detección potencial de ransomware sin precedentes on-box.

En el caso de ONTAP 9.15,1 y versiones anteriores que admiten ARP, ARP comienza en el modo de aprendizaje para aprender la actividad de datos de cargas de trabajo típicas. Esto puede tardar siete días en la mayoría de los entornos. Una vez completado el modo de aprendizaje, ARP cambiará automáticamente al modo activo y comenzará a buscar actividad de carga de trabajo anormal que podría ser ransomware.

Si se detecta alguna actividad anormal, se realiza inmediatamente una copia snapshot automática que proporciona un punto de restauración lo más cercano posible al momento del ataque con un mínimo de los datos infectados. Simultáneamente, se genera una alerta automática (configurable) que permite a los administradores ver la actividad anormal del archivo para que puedan determinar si la actividad es realmente maliciosa y tomar las medidas adecuadas.

Si la actividad es una carga de trabajo esperada, los administradores pueden marcarla fácilmente como un falso positivo. ARP aprende este cambio como actividad normal de la carga de trabajo y ya no lo marca como un ataque potencial en el futuro.

Para habilitar ARP, "ONTAP One"se requiere una licencia.

Leer más

- "Protección autónoma de ransomware"

Protección autónoma contra ransomware/IA (ARP/AI)

Con la introducción como versión preliminar tecnológica en ONTAP 9.15,1, ARP/AI lleva los sistemas de almacenamiento NAS a la detección en tiempo real integrada al siguiente nivel. La nueva tecnología de detección impulsada por la IA está entrenada en más de un millón de archivos y varios ataques de ransomware conocidos. Además de las señales utilizadas en ARP, ARP/AI también detecta el cifrado de encabezados. La potencia de la IA y las señales adicionales permiten que ARP/AI ofrezca una precisión de detección superior al 99%. Esto ha sido validado por SE Labs, un laboratorio de pruebas independiente que le dio a ARP/AI su calificación AAA más alta.

Dado que la formación de los modelos ocurre de forma continua en la nube, ARP/AI no requiere un modo de aprendizaje. Está activo en el momento en que se enciende. El entrenamiento continuo también implica que ARP/IA siempre se valida frente a nuevos tipos de ataques de ransomware a medida que se producen. ARP/AI también incluye funcionalidades de actualización automática que ofrecen nuevos parámetros a todos los clientes para mantener actualizada la detección de ransomware. Todas las demás funcionalidades de detección, información y punto de recuperación de datos de ARP se mantienen para ARP/AI.

Para habilitar ARP/AI, "ONTAP One"se requiere una licencia.

Leer más

- "Blog: La solución de detección de ransomware en tiempo real basada en IA de NetApp logra la calificación AAA"

Protección WORM aislada con copia digital vault

El enfoque de NetApp de un ciberalmacén es una arquitectura de referencia creada específicamente para un ciberalmacén con brecha lógica. Este enfoque aprovecha las tecnologías de refuerzo de la seguridad y cumplimiento de normativas, como SnapLock, para permitir copias Snapshot inalterables e indelebles.

Cyber vaulting con SnapLock Compliance y una red desconectada lógica

Una tendencia creciente es que los atacantes destruyan las copias de seguridad y, en algunos casos, incluso las cifren. Es por ello que muchos en el sector de la ciberseguridad recomiendan usar copias de seguridad aisladas como parte de una estrategia general de resiliencia cibernética.

El problema es que las brechas de aire tradicionales (cintas y soportes fuera de línea) pueden aumentar significativamente el tiempo de restauración, lo que aumenta el tiempo de inactividad y los costos generales asociados. Incluso un enfoque más moderno de una solución de brecha de aire puede resultar problemático. Por ejemplo, si el almacén de copia de seguridad se abre temporalmente para recibir nuevas copias de seguridad y, a continuación, desconecta y cierra su conexión de red a los datos primarios para que vuelvan a estar «fuera de juego», un atacante podría aprovechar la apertura temporal. Durante el tiempo en que la conexión está en línea, un atacante podría atacar para comprometer o destruir los datos. Este tipo de configuración también suele añadir complejidad no deseada. Un espacio de aire lógico es un excelente sustituto de un espacio de aire tradicional o moderno, ya que tiene los mismos principios de protección de la seguridad mientras se mantiene el backup online. Con NetApp, puede solucionar la complejidad del intercambio de aire en cinta o disco mediante el intercambio de aire lógico, lo que puede lograrse con copias Snapshot inmutables y NetApp SnapLock Compliance.

[Espacio aislado lógico con Cyber Vault de NetApp]

NetApp lanzó la función SnapLock hace más de 10 años para abordar los requisitos de cumplimiento de normativas relacionados con los datos, como la ley de portabilidad y responsabilidad del seguro médico

(HIPAA), Sarbanes-Oxley, y otras normas relativas a los datos normativos. También puede almacenar copias snapshot primarias en volúmenes de SnapLock para que las copias se puedan comprometer A WORM, lo que evita su eliminación. Hay dos versiones de licencia de SnapLock: SnapLock Compliance y SnapLock Enterprise. En cuanto a la protección frente a ransomware, NetApp recomienda SnapLock Compliance porque puede establecer un período de retención específico durante el cual se bloquean las copias de Snapshot y no se pueden eliminar, incluso para los administradores de ONTAP o el soporte de NetApp.

Leer más

- "Blog: Protección frente a ransomware en capas con la solución Cyber Vault de NetApp"

Copias Snapshot a prueba de manipulación

Mientras que aprovechar SnapLock Compliance como una barrera aérea lógica proporciona la máxima protección a la hora de evitar que los atacantes eliminen sus copias de backup, sí requiere que se muevan las copias snapshot mediante SnapVault a un volumen secundario habilitado para SnapLock. Por ello, muchos clientes ponen en marcha esta configuración en el almacenamiento secundario en la red. Esto puede provocar tiempos de restauración más largos en comparación con la restauración de una copia Snapshot de volumen primario en el almacenamiento primario.

A partir de ONTAP 9.12,1, las copias Snapshot a prueba de manipulación proporcionan una protección prácticamente de nivel de SnapLock Compliance para las copias snapshot en el almacenamiento primario y en los volúmenes primarios. No es necesario almacenar la copia snapshot mediante SnapVault en un volumen de SnapManager secundario. Las copias Snapshot a prueba de manipulaciones usan la tecnología SnapLock para evitar que se elimine la copia snapshot primaria, incluso por un administrador de ONTAP completo con el mismo período de retención de SnapLock. De este modo, se pueden acelerar los tiempos de restauración y se puede hacer backup de un volumen FlexClone mediante una copia Snapshot protegida a prueba de manipulaciones, algo que no puede hacerse con una copia Snapshot tradicional de SnapLock Compliance almacenadas en SnapVault.

La principal diferencia entre SnapLock Compliance y las copias Snapshot a prueba de manipulaciones es que SnapLock Compliance no permite que la cabina ONTAP se inicialice y se borre si existen volúmenes SnapLock Compliance con copias Snapshot almacenadas que todavía no han alcanzado su fecha de vencimiento. Para hacer que las copias de Snapshot sean a prueba de manipulaciones, se necesita una licencia de SnapLock Compliance.

Leer más

- "Bloquea una copia Snapshot para protegerte contra ataques de ransomware"

Protección frente a ransomware de Active IQ

NetApp Active IQ es un asesor digital que simplifica el cuidado y la optimización proactivos del almacenamiento de NetApp con inteligencia procesable para una gestión de datos óptima. Impulsado por los datos de telemetría de nuestra base instalada altamente diversa, Active IQ utiliza técnicas avanzadas de IA y ML para descubrir oportunidades que reduzcan el riesgo y mejorar el rendimiento y la eficiencia de su entorno de almacenamiento.

No solo puede "Active IQ de NetApp" ayudar "eliminar las vulnerabilidades de seguridad", sino que también proporciona información y orientación específicas para la protección contra el ransomware. Una tarjeta de bienestar dedicada muestra las acciones necesarias y los riesgos abordados, por lo que puede estar seguro de que sus sistemas cumplen con las recomendaciones de mejores prácticas.

[Supervisión de estado en la Consola de NetApp Active IQ]

Los riesgos y las acciones rastreadas en la página de bienestar de la defensa contra ransomware incluyen los siguientes (y muchos más):

- El recuento de copias de snapshots de volúmenes es bajo, lo que reduce la protección potencial frente a ransomware.
- FPolicy no está habilitado para todas las máquinas virtuales de almacenamiento (SVM) configuradas para protocolos NAS.

Para ver la protección frente al ransomware de Active IQ en acción, consulte "Active IQ de NetApp".

Resiliencia global con protección frente al ransomware de BlueXP

Es importante que la detección de ransomware se produzca lo antes posible, de modo que pueda prevenir la propagación y evitar costosos tiempos de inactividad. Sin embargo, una estrategia de detección de ransomware efectiva debería incluir más que una única capa de protección. La protección contra ransomware de NetApp adopta un enfoque integral que incluye funcionalidades integradas en tiempo real que se extienden a los servicios de datos mediante BlueXP y una solución aislada en capas para el almacenamiento cibernético.

Protección contra ransomware de BlueXP

BlueXP es un único plano de control para orquestar de forma inteligente una defensa completa frente al ransomware centrada en las cargas de trabajo. La protección frente a ransomware de BlueXP reúne las potentes funciones de ciberresiliencia de ONTAP, como ARP, FPolicy e copias Snapshot a prueba de manipulaciones y servicios de datos de BlueXP , como el backup y recuperación de datos de BlueXP . También agrega recomendaciones y directrices con flujos de trabajo automatizados para ofrecer una defensa integral a través de una única interfaz de usuario. Opera en el nivel de carga de trabajo para garantizar que las aplicaciones que ejecutan su empresa estén protegidas y se puedan recuperar lo más rápido posible en caso de ataque.

[La protección frente al ransomware de BlueXP es la inteligencia basada en IA y la ayuda necesarias para minimizar la pérdida de datos en las cargas de trabajo y recuperarse rápidamente. Esta imagen muestra la interfaz de usuario de BlueXP .]

Beneficios para el cliente:

- La preparación asistida contra el ransomware reduce la sobrecarga operativa y mejora la eficacia
- La detección de anomalías impulsada por IA/ML ofrece mayor precisión y una respuesta más rápida para contener el riesgo
- La restauración guiada coherente con las aplicaciones permite recuperar cargas de trabajo de forma más fácil y en unos minutos

"Protección contra ransomware de BlueXP" Hace que estas funciones del NIST sean más fáciles de lograr:

- Automáticamente **Descubra** y priorice los datos en el almacenamiento de NetApp **con un enfoque en las principales cargas de trabajo basadas en aplicaciones**.
- **Protección con un solo clic** de copia de seguridad de datos de carga de trabajo superior, configuración

inmutable, segura, bloqueo de archivos maliciosos y diferentes dominios de seguridad.

- * Detecte con precisión* ransomware de la forma más rápida posible utilizando **detección de anomalías basada en IA de próxima generación.**
- Respuesta automatizada y flujos de trabajo e integración con las principales soluciones **SIEM y XDR.**
- Restaure rápidamente los datos utilizando una **recuperación orquestada** simplificada para acelerar el tiempo de actividad de las aplicaciones.
- Implementa tu **estrategia** y **políticas** de protección contra ransomware, y **monitorea resultados**.