DISPOSITIVOS VXRAIL CON DISEÑO INTEGRAL DE SEGURIDAD DE DELL EMC

Resumen

El dispositivo VxRail™ es la plataforma ideal para la transformación de la infraestructura de TI y de la seguridad, y proporciona capas de protección para mantener la seguridad de sus datos y aplicaciones de negocio. Solo la familia de empresas de Dell Technologies puede brindar todas las soluciones integrales necesarias para mantenerse al día con el panorama actual de amenazas en constante evolución. Esta guía incluye las características de seguridad integradas y opcionales, las prácticas recomendadas y las técnicas comprobadas para asegurar su VxRail del núcleo al borde y a la nube.

Marzo de 2020

Tabla de contenido

INTRODUCCIÓN

En todas las industrias, las organizaciones están modernizando y transformando la forma en la que operan y ofrecen productos y servicios diferentes. Dónde se almacenan los datos, cómo se accede a ellos y la cantidad de dispositivos, del núcleo al borde y a la nube a un ritmo exponencial. La seguridad siempre será una parte de la TI; está centrada en la autenticación, los firewalls, el cumplimiento y los criminales cibernéticos. La seguridad ya no es un conjunto de proyectos, sino un ciclo de vida continuo que requiere una revisión y un análisis constantes. Dell Technologies cree que la seguridad nunca ralentiza sus procesos y, en cambio, acelera la innovación, lo que le permite pensar en formas nuevas y estratégicas, y aprovechar oportunidades.

VxRail de Dell EMC proporciona el camino más rápido y simple para esta transformación de seguridad, del núcleo al borde y a la nube. VxRail ofrece una infraestructura ágil con integridad de la pila completa y administración integral del ciclo de vida útil. De esta'manera, puede impulsar la eficiencia operativa, reducir los riesgos y permitir que los equipos se concentren en el negocio. La adopción de los sistemas de VxRail, que dejan de lado los silos operativos y permiten la innovación continua mediante el aprovisionamiento rápido y la implementación de cargas de trabajo, genera un importante ahorro de costos y eficiencia operativa. Esto les permite a las organizaciones de TI impulsar las oportunidades de negocio en lugar de simplemente brindar soporte a las operaciones empresariales. Creado para VMware, con VMware, para optimizar VMware, VxRail es el primer y único sistema de HCI diseñado junto con VMware para eliminar la complejidad operativa de la implementación, el aprovisionamiento, la administración, el monitoreo y la actualización de la infraestructura hiperconvergente de VxRail.

VxRail tiene seguridad incorporada en todos los niveles de la pila de tecnología integrada. Desde los procesadores y servidores PowerEdge, hasta el software del sistema de HCI de VxRail, con VMware software integrado. Protección del núcleo, el borde y la nube, lo que garantiza la disponibilidad, la integridad y la confianza en todas las cargas de trabajo: tradicionales y nativas de la nube.

LA TRANSFORMACIÓN DE LA SEGURIDAD COMIENZA CON DELL TECHNOLOGIES

La transformación de la seguridad dentro de Dell Technologies se trata de repensar la seguridad y de acelerar la innovación. Dell Technologies se centra en todos los niveles que cuentan con seguridad, desde las colaboraciones entre las empresas de Dell Technologies hasta el producto desarrollado y su ofrecimiento en el mercado. VxRail no es una excepción. Se creó con los más altos niveles de garantía de seguridad de los productos y proporciona funcionalidades de seguridad completamente integradas que su organización puede utilizar para optimizar la resiliencia de la ciberseguridad del borde al núcleo (vea la figura a continuación) y a la nube a fin de acelerar el proceso de innovación.

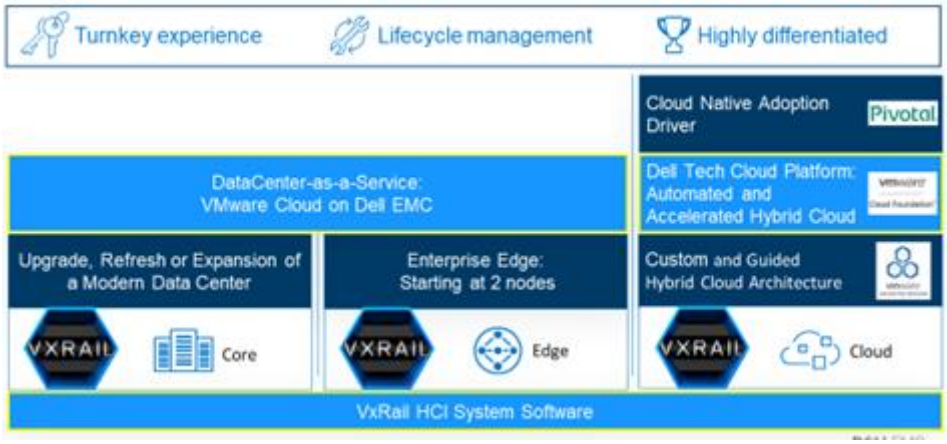

Figura 1: del núcleo al borde y a la nube

Forbes informó, según la investigación de seguridad basada en riesgos recientemente publicada en el Informe de vulneración de datos de mediados de año del 2019, que dentro de los primeros seis meses del 2019, hubo más de 3800 infracciones divulgadas públicamente, que alcanzaron un pico de 4100 millones de ataques. Acorde a estos números, las infracciones pueden superar los 6515 ataques divulgados públicamente que informó la misma empresa en 2018.

Dell Technologies puede garantizarle que sus estrategias de seguridad sigan el ritmo de sus iniciativas de modernización para reducir el riesgo de su negocio.

1. Unifique los programas de seguridad con el riesgo general de negocio para saber cuáles son los riesgos que vale la pena tomar.
2. Implemente operaciones de seguridad avanzadas que se adapten al panorama de amenazas en constante cambio, para que pueda responder de manera eficaz a las amenazas.
3. Construya una infraestructura moderna y resistente que proteja los terminales, la red, las aplicaciones y los datos.
4. Confíe en los servicios de asesoramiento de confianza para diseñar e implementar su programa de transformación de seguridad. Dell Technologies se encuentra en una posición única para ayudarlo a abordar todas estas áreas.

Si bien se requiere una defensa en capas con varios niveles de seguridad, estos elementos deben funcionar en conjunto. La transformación de la seguridad comienza con una resiliencia cibernética, una infraestructura moderna como VxRail que se diseñó y creó teniendo en cuenta la seguridad.

En la actualidad, el panorama de amenazas en constante evolución requiere un cambio del enfoque para prevenir o mitigar estas amenazas. La infraestructura obsoleta es difícil de defender y los productos específicos de múltiples vendedores añaden complejidad y aumentan el riesgo de tener vulnerabilidades que expongan la infraestructura a ataques. Ese nivel de complejidad facilita varios puntos de entrada para aquellos que quieren vulnerar los datos.

El estándar de seguridad y de cumplimiento también se debe tener en cuenta. Hay sanciones legales y financieras significativas por incumplimiento, y, si bien son costosas, esas sanciones pueden tener menos impacto en un negocio que la vulneración de datos. Es menos probable que las personas quieran establecer relaciones de negocios con una empresa que ha sufrido una vulneración de datos.

- Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS): protecciones para titulares de tarjetas de crédito
- Normativa general de la protección de datos (GDPR): normativa de la privacidad de los datos de la Unión Europea
- Ley alemana de protección de datos “Bundesdatenschutzgesetz” (BDSG): ley de protección de datos detallada
- Ley Sarbanes-Oxley (SOX): protección de la información confidencial relacionada con la generación de informes financieros de empresas públicas
- Ley Gramm-Leach-Bliley (GLBA): protección de información personal no pública (NPPI) en la industria de servicios financieros
- Ley de portabilidad y responsabilidad del seguro médico (HIPAA): protección de información y datos electrónicos de servicios de salud de los pacientes
- Ley de privacidad del consumidor de California (CCPA): mejora de los derechos de privacidad y de protección del consumidor para los residentes de California (ley firmada el 28/06/2018)

Dell Technologies cree que la transformación de la seguridad se trata de tener un partner de confianza: un partner que ayude a administrar su riesgo digital y a proporcionar servicios de seguridad administrados, y que aporte pericia, servicios, soluciones y productos que garanticen el funcionamiento de la pila completa, desde la infraestructura hasta las aplicaciones. Además, un partner debe optimizar las operaciones y convertir a la seguridad en una parte esencial de la estrategia empresarial.

Dell Technologies es un partner de seguridad de confianza para la transformación de la seguridad. Ya sea que se centre en los terminales, el centro de datos, los desarrolladores, las identidades, las operaciones de seguridad, la nube o la virtualización, la seguridad debe ser integral, y Dell Technologies puede ayudarlo. Podemos ayudarlo a abordar la seguridad y los riesgos empresariales, a solucionar las violaciones de seguridad, a recuperarse de un ataque de ransomware y a crear aplicaciones seguras. La seguridad tiene diferentes significados para la gente, algunos malos, algunos buenos. Pero, más allá de esto, en Dell Technologies queremos que las organizaciones nos adopten en el camino hacia la transformación de la seguridad.

Puente hacia el futuro digital

En la actualidad, la IT se está utilizando más que nunca para resolver los problemas empresariales. Las organizaciones lo están haciendo mediante la implementación de analítica de datos, inteligencia artificial, aplicaciones nuevas y dispositivos inteligentes para generar grandes cantidades de datos. Estos datos impulsan conocimientos procesables y ventajas competitivas únicas. A pesar de esto, muchas organizaciones todavía carecen de una visión y una estrategia digital claras; utilizan tecnología obsoleta. Esto impone limitaciones y crea una cultura resistente al cambio. Sin un buen plan, el riesgo y la seguridad no se consideran a tiempo o simplemente nunca forman parte de una discusión de estrategia más amplia. En este momento fundamental para la tecnología, esta forma reactiva de hacer negocios ya no es válida. Para acelerar la innovación y lograr el potencial de su futuro digital, las organizaciones deben reconsiderar la forma en la que entienden la seguridad.

En el mundo centrado en la TI, por lo general, la seguridad se ve más como un obstáculo que como un aporte para un cambio positivo. Día a día, es posible que el trabajo no se aprecie y que la administración no vea un rendimiento de la inversión. El personal de seguridad debe administrar las crecientes amenazas, los sistemas complejos y mantener un conocimiento práctico de un panorama en constante cambio. El conjunto diario de ataques cibernéticos en las noticias solo exacerba el estrés, al igual que el sentimiento de que todo lo relacionado a su organización puede perderse en un segundo. Pero la seguridad no tiene que estar asociada al miedo y a la frustración. La seguridad siempre está en búsqueda de la positividad y de la proactividad. Sin embargo, esto solo es posible con la actitud y la tecnología correctas. No podemos seguir pensando de esta manera sobre la seguridad y el riesgo. Para poner este cambio en perspectiva, piense en los frenos de un automóvil. En principio puede pensar que los frenos solo sirven para ralentizar la velocidad del automóvil, pero los frenos también son los que le permiten ir más rápido. Le dan la confianza para acelerar a la vez que lo preparan para los obstáculos y el camino que tiene por delante. La seguridad y el riesgo también deben ser vistos como aceleradores para las organizaciones y no como algo que ralentiza sus procesos.

LOS PROGRAMAS DE SEGURIDAD DE PRODUCTOS DE DELL EMC GENERAN CONFIANZA

Dell EMC comenzó a formular sus políticas de seguridad de productos en 2002 cuando el objetivo de la empresa pasó de ser principalmente un proveedor de hardware de almacenamiento a ser un proveedor de software de clase empresarial. La empresa implementó su programa de respuesta ante a las vulnerabilidades en 2004 y estableció una política de seguridad de productos para toda la empresa en 2005. La política implica estándares de seguridad amplios pero claros que abarcan la gama completa de productos de Dell EMC. Esta política se actualizó constantemente y, en 2007, se incorporó al nuevo ciclo de vida útil del desarrollo de seguridad (SDL) de la empresa. SDL incorporó una serie de prácticas de seguridad medibles y repetibles en cada paso del desarrollo y la implementación de los productos. En el 2012, la empresa también formalizó un programa de administración de riesgos de la cadena de suministro para extender las prácticas de seguridad a los proveedores de componentes de productos de Dell EMC. Dell EMC continúa actualizando sus programas de seguridad de productos a la vanguardia de los estándares y procesos de la industria.

Con VxRail, Dell EMC mantiene su compromiso con la seguridad. El ciclo de vida útil del desarrollo de VxRail sigue el proceso de desarrollo de Seguridad del producto de Dell EMC y el ciclo de vida útil del desarrollo de seguridad. El ciclo de vida útil del desarrollo de seguridad de Dell EMC sigue un riguroso enfoque para el desarrollo de productos seguros que implica la administración de riesgo a nivel ejecutivo antes de que se ofrezcan los productos en el mercado. Además, VMware vSphere es una parte importante de la infraestructura hiperconvergente de VxRail, que también se desarrolló mediante un ciclo de vida útil del desarrollo de seguridad similar.

Ciclo de vida útil de desarrollo seguro (SDL)

El ciclo de vida útil del desarrollo de seguridad de Dell EMC describe el conjunto de actividades requeridas durante todo el ciclo de vida útil del producto a fin de crear resiliencia de seguridad y funcionalidades de seguridad coherentes en los productos, y para responder rápidamente a las vulnerabilidades de seguridad informadas de manera externa. En línea con las prácticas recomendadas de la industria, Dell EMC se basa en un conjunto de controles implementados por las organizaciones de investigación y desarrollo (R&D) del producto. En la figura 2, se muestran algunas de las actividades típicas que se realizan como parte del SDL.

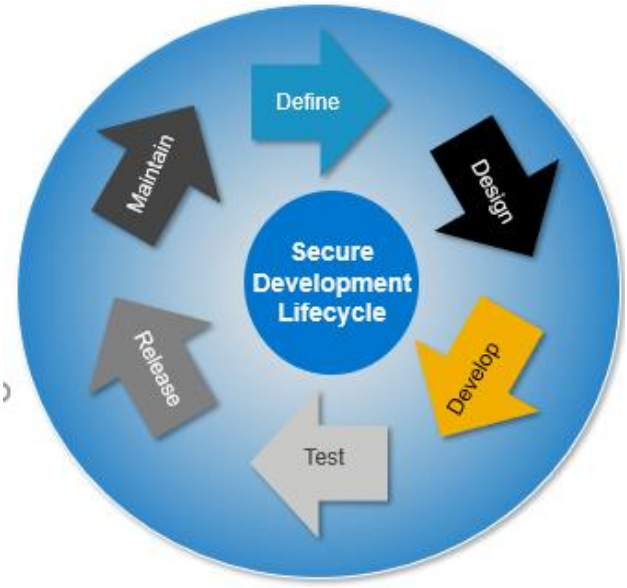

Figura 2: actividades del SDL de Dell EMC

La implementación y la validación de estos controles está impulsada por los líderes de seguridad dentro de las organizaciones de R&D del producto, que trabajan en estrecha colaboración con los asesores de seguridad de la oficina de seguridad de los productos (PSO). En la figura 3, se ilustra cómo este SDL se inscribe en un típico ciclo de vida útil ágil.

Agile Development Activity		SDL Activity
High Level Planning	Requirements	• Formalize security requirements in PRD/PCD • Product Security Training
	Architecture	• **Threat Modeling** • **Security Testing** (test planning)
Sprint 1..*n*	Design	• Update **threat model**
	Develop	• **Static Analysis**
	Test	• **Security Testing**
	Release	• **Security Scanning** • **Security Configuration Guide** • Inventory of Embedded Components
General Availability	Assure	• Perform Code Signing
	Assess	• Finalize and **submit scorecard** • Have a plan for mitigating any "critical" and/or "high" issues
Post-GA	Respond	• Respond to vulnerabilities following EMC's vulnerability response policy

Figura 3: SDL y un típico ciclo de vida útil ágil

La tarjeta de puntuación es un mecanismo que se utiliza en todo Dell EMC para comprender el estado de seguridad de un producto o solución cuando llega a su fecha de lanzamiento de Directed Availability/General Availability (DA/GA).

Desarrollo seguro

El enfoque integral de Dell EMC para asegurar el desarrollo seguro se centra en minimizar el riesgo de vulnerabilidades de software y los puntos débiles del diseño de los productos.

Este enfoque integral para el desarrollo seguro de software tiene en cuenta las políticas, las personas, los procesos y la tecnología, e incluye lo siguiente:

- La política de seguridad de productos de Dell EMC es un parámetro de referencia utilizado por las organizaciones de productos de Dell EMC para realizar un análisis comparativo de la seguridad de los productos con las expectativas del mercado y las prácticas recomendadas de la industria.
- Los equipos de ingeniería de Dell EMC son una comunidad de ingeniería conscientes de la seguridad. Todos los ingenieros asisten a un programa de seguridad de ingeniería basado en roles para capacitarse en las prácticas de seguridad recomendadas específicas de su trabajo y en cómo utilizar los recursos relevantes. Dell EMC se esfuerza por crear una cultura consciente de la importancia de la seguridad en toda su comunidad de ingenieros.
- El proceso de desarrollo de Dell EMC es seguro y reproducible. El SDL superpone los procesos de desarrollo estándar para lograr un alto grado de cumplimiento de la política de seguridad de productos de Dell EMC.
- Los equipos de desarrollo de Dell EMC utilizan las mejores tecnologías de seguridad de su clase. Dell EMC ha desarrollado una serie doble de software, estándares, especificaciones y diseños para elementos comunes de seguridad de software como autenticación, autorización, auditoría y responsabilidad, criptografía y administración de claves a partir del uso de tecnología de RSA de vanguardia. Cuando es necesario, se utilizan interfaces abiertas, lo que permite la integración con las arquitecturas de seguridad existentes de los clientes.
- El SDL de Dell EMC superpone la seguridad de los procesos de desarrollo estándar para lograr un alto grado de cumplimiento de la política de seguridad de productos de Dell EMC. El SDL de Dell EMC sigue un riguroso enfoque para el desarrollo de productos seguros que implica la administración de riesgo a nivel ejecutivo antes de que se ofrezcan los productos en el mercado.
- El SDL forma parte de un grupo más amplio de procesos que existen dentro del estándar de diseño seguro. El estándar de diseño seguro es un parámetro de referencia para la creación de seguridad en los productos de Dell EMC. El estándar se relaciona con la seguridad de toda la funcionalidad del producto y describe la funcionalidad de seguridad obligatoria. Esta se debe integrar en cualquier producto de Dell EMC ofrecido a los clientes. Este estándar permite lo siguiente a los productos de Dell EMC:
    - Cumplir con los requisitos de seguridad rigurosos de los clientes;
    - Ayudar a los clientes a cumplir con los requisitos normativos como PCI o HIPPA, entre otros;
    - Minimizar los riesgos para los productos y los entornos de los clientes de Dell EMC que pueden surgir a partir de las vulnerabilidades de seguridad.
    - La protección de código fuente indica cómo asegurar de manera adecuada los sistemas de ingeniería de Dell EMC que contienen código fuente en la propiedad intelectual relacionada con los productos, y cómo garantizar la integridad de los productos implementados en los entornos de los clientes.

Respuesta ante las vulnerabilidades de Dell EMC

Los atacantes pueden utilizar las vulnerabilidades de seguridad de cualquier componente del sistema para infiltrar y comprometer toda la infraestructura de TI. El tiempo entre el descubrimiento inicial de las vulnerabilidades y la disponibilidad de una corrección es una carrera entre los atacantes y los que buscan defender el sistema. La prioridad principal de Dell EMC es minimizar esta brecha de tiempo para reducir el riesgo.

El equipo de respuesta ante incidentes de seguridad de productos Dell (PSIRT) es responsable de coordinar la respuesta y la divulgación de todas las vulnerabilidades de productos de Dell EMC identificadas de forma externa. El PSIRT ofrece estrategias de información, orientación y mitigación oportunas a los clientes para abordar las amenazas que surgen a partir de las vulnerabilidades.

Cualquier persona puede notificar a Dell sobre posibles fallas de seguridad en sus productos a través del sitio web de la empresa o por correo electrónico. Se revisa, valida, corrige e informa cada aviso de acuerdo con las pautas de la industria.

Dell difunde información sobre las vulnerabilidades de los productos a todos los clientes de manera simultánea. Los asesores de la empresa identifican la gravedad de las vulnerabilidades y difunden la información mediante el uso de múltiples sistemas de generación de informes estandarizados. Al igual que el resto de nuestras prácticas de seguridad de productos, la política de divulgación de Dell se basa en las prácticas recomendadas de la industria.

Administración de riesgo de la cadena de suministro

Los programas exitosos de seguridad de productos son integrales e incluyen componentes y software subcontratados. Las pruebas de integridad dentro de la cadena de suministro son un componente fundamental para la creación y el cuidado de la confianza. Dell Technologies cuenta con un programa formal de administración de riesgos de la cadena de suministro que garantiza que los componentes de hardware utilizados en los productos de la empresa provengan de fuentes debidamente examinadas.

La seguridad de la cadena de suministro se define como la práctica y la aplicación de medidas preventivas y de control de detección que protegen los activos físicos, el inventario, la información, la propiedad intelectual y las personas. Abordar la seguridad física, de la información y del personal le brinda seguridad a la cadena de suministro mediante la reducción de las oportunidades de la introducción maliciosa de malware y de los componentes falsificados en la cadena de suministro.

El marco de trabajo de administración de riesgos de la cadena de suministro de Dell (a continuación) refleja el marco de trabajo integral de administración de riesgos del Plan nacional de protección de la infraestructura (NIPP). Este describe cómo el gobierno y el sector privado pueden trabajar en conjunto para mitigar los riesgos y cumplir con los objetivos de seguridad. La infraestructura de Dell incorpora un loop de retroalimentación abierto que permite una mejora continua. Los planes de moderación de riesgos se priorizan e implementan según corresponda durante todo el ciclo de vida de la solución. La figura 4 ilustra el proceso de administración de riesgos de la cadena de suministro.

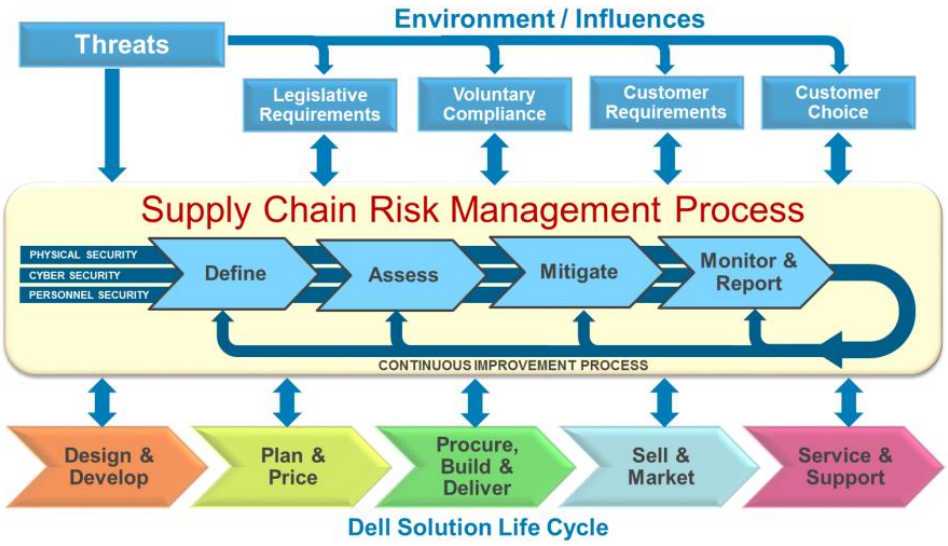

Figura 4: proceso de administración de riesgos de la cadena de suministro de Dell

Colaboración en la industria para mejorar la seguridad de los productos

Dell Technologies cree que un enfoque de colaboración es la manera más eficiente y eficaz de enfrentar las amenazas de seguridad que emergen constantemente y que se propagan rápidamente entre las organizaciones a través de los sistemas estrechamente interconectados de la actualidad.

Teniendo en cuenta los riesgos en aumento, los proveedores de tecnología deben dejar de lado sus objetivos de competencia en el mercado cuando se trata de la seguridad de los productos. Ningún proveedor puede resolver todos los problemas de seguridad de los productos de TI por sí mismo. La seguridad de TI es una tarea colectiva y colaborativa. Dell Technologies cree que colaborar con otras empresas es fundamental para garantizar que el mercado siga siendo un lugar en el que todos puedan prosperar.

Luego de décadas de haber invertido en la seguridad de los productos, Dell Technologies pudo establecer una amplia historia de mejoras y conocimientos exitosos, y la empresa comparte abiertamente lo que ha aprendido con sus clientes, colegas y socios. Dell Technologies comprende que el sistema de TI de un cliente no se ejecuta únicamente con los productos Dell Technologies, por lo que estamos comprometidos a mejorar la seguridad del ecosistema dondequiera que opere un producto. Eso significa ser un participante activo y un colaborador positivo de la industria.

El largo compromiso de Dell Technologies con el avance de la seguridad de los productos ha creado la necesidad de ayudar y fomentar a los miembros más nuevos de la industria. Los líderes de seguridad de los productos de la empresa facilitan el intercambio abierto de ideas en conferencias, a través de publicaciones de blogs y en otros eventos sociales y formales.

Participación en grupos de seguridad de productos de la industria

Dell Technologies participa de los grupos de seguridad de productos, en los que aprende y enseña prácticas progresivas recomendadas y cultiva un sentido de responsabilidad comunal para la seguridad de los productos. Las afiliaciones de la industria de Dell Technologies son las siguientes:

BSIMM: el Modelo de madurez para el desarrollo de software seguro (BSIMM) evalúa las iniciativas de seguridad de software de la industria, de modo que las organizaciones puedan ver el estado de sus iniciativas de seguridad y sepan cómo deben evolucionar.

Open Group: este consorcio de 400 miembros lleva a cabo programas de certificación respetados para el personal de TI, los productos y los servicios a fin de diseñar y mejorar los estándares de TI. Open Group trabaja para comprender los requisitos de TI actuales y emergentes, y para establecer o compartir las prácticas recomendadas a fin de cumplir con ellos

SAFECode: el foro de garantía de software para la excelencia en el código, cofundado por Dell EMC, es una iniciativa de la industria para identificar y promover las prácticas recomendadas a fin de ofrecer software, hardware y servicios más seguros y de confianza.

CSA: la Alianza de seguridad en la nube es la organización líder en el mundo que se dedica a definir y a concientizar sobre las prácticas recomendadas para ayudar a garantizar un entorno informático seguro en la nube.

FIRST: el Foro de equipos de respuesta a incidentes y seguridad es un líder mundial reconocido en respuesta ante incidentes. Dell PSIRT es miembro del equipo de FIRST de VxRail.

VxRail: la base para la modernización del centro de datos y la transformación de la TI

Para ganar la carrera contra el panorama de amenazas de seguridad en constante evolución, VxRail tiene la adaptabilidad necesaria a fin de defenderse contra las amenazas actuales y futuras. VxRail se basa en la generación actual de servidores PowerEdge de Dell y en las tecnologías de los procesadores de última generación, que proporcionan una plataforma segura y opciones de configuración flexibles. vSphere proporciona una virtualización del almacenamiento y de los servidores. A medida que aumentan los requisitos de carga de trabajo, VxRail se escala fácilmente. A medida que cambian las normativas, las opciones de configuración flexible de VxRail le permiten adaptarse rápidamente

VxRail puede ayudar a su organización a optimizar la resiliencia cibernética, a administrar el riesgo y a satisfacer los requisitos de cumplimiento de normas sin importar el sector de la industria en el que esté operando su organización. VxRail es el único dispositivo de infraestructura hiperconvergente totalmente integrado, preconfigurado y probado que cuenta con la tecnología de VMware vSAN. Ya sea que se implemente en el centro de datos, en el borde o como parte de una solución de nube híbrida, VxRail proporciona una distribución mejor, más simple y más segura de las aplicaciones cruciales del negocio, la infraestructura de escritorio virtual (VDI) y la infraestructura remota. VxRail permite que Dell EMC le proporcione al cliente las funcionalidades necesarias para optimizar la resiliencia cibernética en toda su implementación. En la figura 5, a continuación, se ilustra la seguridad incorporada de VxRail

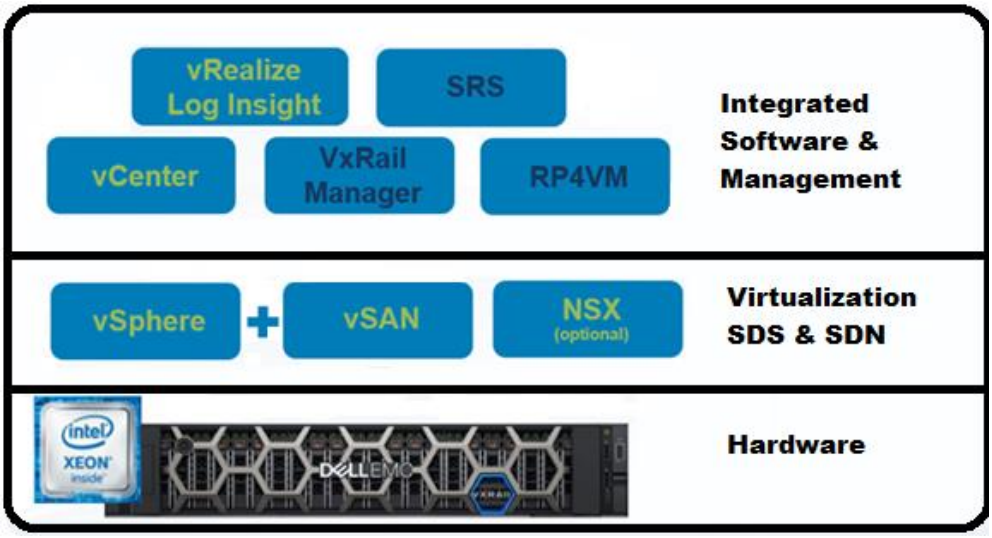

Figura 5: seguridad incorporada de VxRail

Servidores de almacenamiento de Dell EMC PowerEdge

VxRail se basa en la plataforma de servidores de Dell PowerEdge con características de seguridad integradas de hardware y de nivel del sistema para proteger la infraestructura con niveles de defensa. Las brechas se detectan rápidamente, lo que permite que el sistema se recupere y vuelva a una base de confianza. Las características de seguridad diferenciadas en los servidores PowerEdge son las siguientes:

- Bloqueo del sistema para evitar cambios no autorizados o inadvertidos. Es una nueva función del sector que impide los cambios no autorizados en la configuración, que crean vulnerabilidades de seguridad y ponen en riesgo la información confidencial.
- La arquitectura de resiliencia cibernética con características como el arranque seguro de UEFI, las funcionalidades de recuperación de BIOS y el firmware firmado proporcionan una protección mejorada contra los ataques.
- La característica de borrado del sistema de nivel del servidor garantiza la privacidad con su función de borrado rápido y seguro de todos los datos del usuario de la unidad y de toda la memoria no volátil cuando se retira un servidor.

Los servidores Dell EMC PowerEdge son el hardware fundamental que conforma los nodos en un clúster de VxRail. Los recursos de CPU, de memoria y de disco en cada nodo proporcionan los recursos agrupados del clúster, y las interfaces de red proporcionan conectividad. Por lo tanto, los servidores seguros Dell EMC PowerEdge son la base de la seguridad de VxRail.

Los servidores PowerEdge tienen un control de acceso remoto integrado al que se denomina iDRAC. iDRAC utiliza la comunicación segura, la autenticación y los controles de acceso basados en funciones para permitir la administración remota segura y la configuración del sistema físico. Con las alertas configurables, iDRAC puede enviar información de eventos a su sistema de administración de eventos y de incidentes de seguridad (SIEM) siempre que se acceda al hardware o se modifique la configuración. La detección y la generación de informes de cambios no autorizados protegen la integridad de VxRail. Obtenga más información sobre la Seguridad cibernética resiliente en los servidores de 14.ª generación Dell EMC PowerEdge.

Los servidores PowerEdge utilizan un firmware firmado y verificado criptográficamente para crear un sistema de confianza. Uso de las tecnologías de seguridad incorporadas directamente en el silicio. Funcionalidades como la tecnología de ejecución de confianza (TXT) de Intel verifican que el servidor ejecute solo la versión deseada del firmware, del BIOS y del hipervisor mientras evita la introducción no detectada del malware. En la figura 6, a continuación, se ilustra la raíz de confianza del hardware.

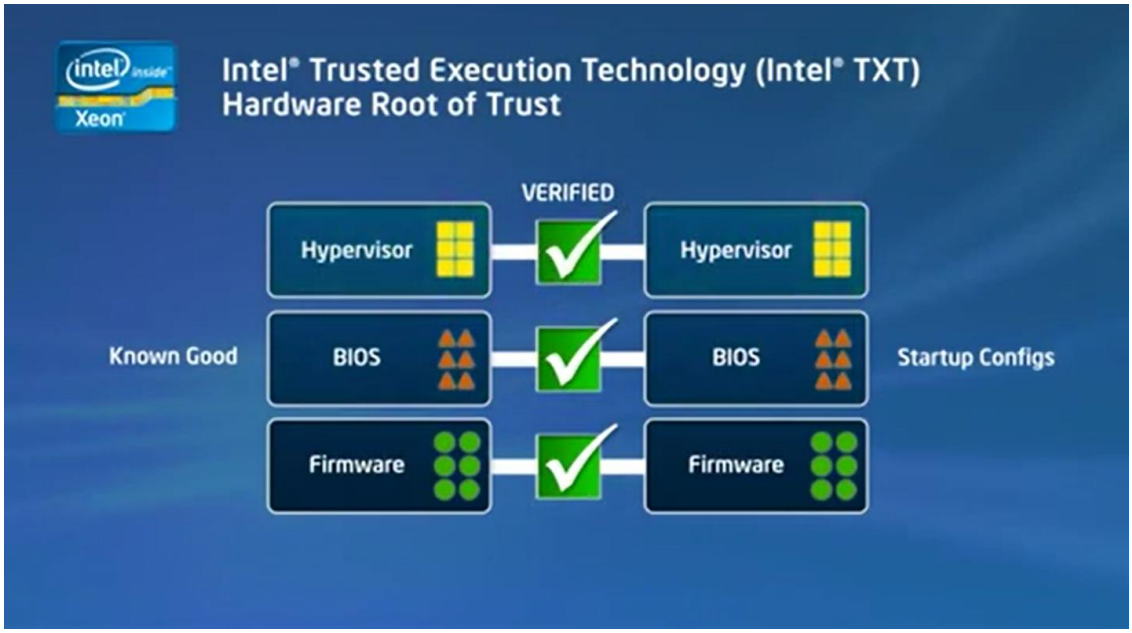

Figura 6: raíz de confianza del hardware

VxRail puede lograr niveles de protección aún mayores de la integridad de los servidores mediante la configuración de los nodos con un módulo de administración de la plataforma de confianza (TPM) (TPM v1.2 y v2.0). TPM es un estándar internacional para procesadores criptográficos seguros, una microcontroladora exclusiva que está diseñada a fin de proporcionar alta seguridad para claves de criptografía y una opción para todos los nodos de VxRail.

Software del sistema de HCI de Dell EMC VxRail

El software del sistema de HCI es la base para las funcionalidades de diferenciación de valor de VxRail. Desde el punto de vista de la pila de infraestructura, es el software de administración que se ejecuta con VMware software y el servidor PowerEdge para permitir que VxRail funcione como un sistema unificado único.

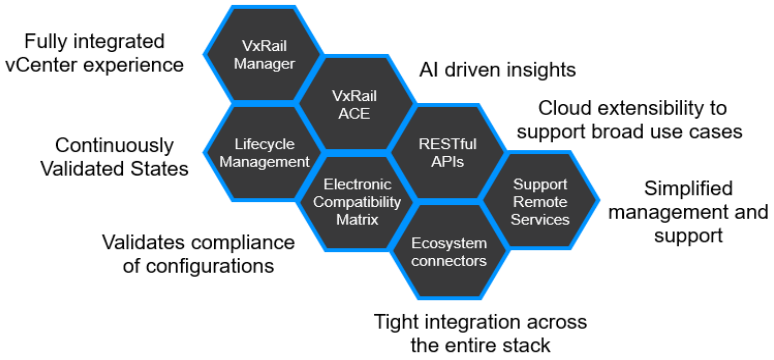

Figura 7: software del sistema de HCI de VxRail

Estados validados constantemente: VxRail se ejecuta con un software y un firmware previamente probados y validados para toda la pila de VxRail, entre ellos VMware software y los componentes del servidor PowerEdge. Las funcionalidades de administración del ciclo de vida útil de VxRail garantizan que los clústeres de VxRail se ejecuten en ese estado ya conocido durante todo su ciclo de vida útil, ya que el clúster cambia continuamente para aprovechar las últimas innovaciones de VMware software, correcciones de seguridad o correcciones de errores. El término “estados validados constantemente” incluye la estabilidad de configuración proporcionada por los clústeres de VxRail.

Matriz de compatibilidad electrónica: con todos estos diferentes componentes de software y de hardware en la pila, el equipo de VxRail está constantemente probando y validando toda la pila. De esta manera, cualquier estado que el usuario seleccione de la matriz de compatibilidad de VMware ya ha sido validado como un estado validado constantemente. Además, VxRail utiliza esta matriz para garantizar que la configuración del clúster cumpla con los requisitos normativos. Este beneficio reduce significativamente las inversiones en las iniciativas de pruebas y los recursos de los clientes, al mismo tiempo que le brinda al cliente la tranquilidad que necesita para desarrollar de manera predecible y segura sus clústeres de VxRail sin afectar las cargas de trabajo de las aplicaciones.

Conectores del ecosistema: para crear una matriz de compatibilidad electrónica exhaustiva, VxRail debe poder comunicarse con los miembros del ecosistema en la pila, lo cual incluye vSphere, vSAN, vCenter, el servidor PowerEdge y varios componentes de hardware internos. Los conectores permiten que VxRail conozca las versiones de software/firmware que se ejecutan en cada componente y administre el ciclo de vida útil de esos componentes. Las funcionalidades de automatización y orquestación permiten que VxRail se administre como un sistema unificado único.

VxRail Manager: la interfaz de usuario de administración principal de VxRail es el plug-in de vCenter llamado VxRail Manager. Los usuarios de VxRail pueden realizar cualquier actividad de VxRail a través de esta interfaz. Entre las actividades se encuentra la configuración inicial de clúster, el monitoreo de componentes de hardware, la realización de un cierre de clústeres, la expansión del clúster con la adición de nodos y la actualización del software del sistema de HCI de VxRail. Proporciona una experiencia de vCenter completamente integrada.

VxRail ACE (Motor de consultoría analítica): a medida que se realicen mejoras en la experiencia de administración del ciclo de vida de VxRail, gran parte de la TI pasará a depender de las funcionalidades analíticas de informática de VxRail ACE. ACE significa “Analytical Consulting Engine” (“Motor de consultoría analítica”). A través de la telemetría avanzada que el software del sistema de HCI recopila de los clústeres de VxRail, ACE se utiliza para obtener conocimientos impulsados por la inteligencia artificial que les permitirán a los usuarios administrar proactivamente sus clústeres. De esta manera puede mejorar el rendimiento y la disponibilidad. Los conocimientos obtenidos mediante inteligencia artificial están impulsando funcionalidades de administración más activas de múltiples clústeres de ACE, un área en la que los usuarios de HCI tendrán mayor interés a medida que amplíen su identificación de HCI y que la administración a escala se convierta en una tarea indispensable.

API de REST: los beneficios de VxRail en la administración del ciclo de vida se presentan idealmente como la plataforma de infraestructura preferida, ya que el enfoque en la simplificación de las operaciones de TI desempeña un rol fundamental que consiste en permitir que los equipos de TI se centren en los modelos de entrega de servicio de TI basados en la nube. La plataforma de VxRail ampliable a través de las API les permite a los clientes compilar sobre la base de soluciones de infraestructura como servicio. Las API también facilitan la administración a escala, lo que beneficia a los clientes que tienen una gran cantidad de clústeres de VxRail implementados en varias ubicaciones y que han elegido soluciones cifradas internas para administrar a escala.

Servicios de soporte remotos: la experiencia de soporte también puede ser un factor importante en la elección de la solución de HCI correcta. VxRail brinda compatibilidad con un solo proveedor para VMware software, el servidor PowerEdge y el software de VxRail mediante el soporte técnico de Dell. El soporte de VxRail incluye Secure Remote Services de Dell EMC, una conexión remota de dos vías proactiva para el monitoreo, el diagnóstico y la reparación remota que se realiza durante todo el proceso del ciclo de vida útil. De esta manera, se puede garantizar la máxima disponibilidad.

VMware vSphere

El conjunto de software VMware vSphere proporciona a VxRail una infraestructura virtualizada a petición altamente disponible y resiliente. ESXi, vSAN y vCenter Server son componentes principales de vSphere. ESXi es un hipervisor instalado en un nodo de servidor físico de VxRail para que este último pueda alojar varios servidores lógicos o máquinas virtuales. vSAN es el almacenamiento definido por software que utilizan las VM, y VMware vCenter Server es la aplicación de administración para los hosts ESXi, vSAN y las VM.

vSphere Platinum es una solución de seguridad creada especialmente para proteger las aplicaciones, la infraestructura, los datos y su acceso. Combina dos productos probados: vSphere para asegurar la infraestructura, los datos y el acceso; y AppDefense para asegurar las aplicaciones que se ejecutan en las VM. AppDefense protege la integridad de las aplicaciones que se ejecutan en vSphere mediante el aprendizaje automático para conocer el estado y el comportamiento de la aplicación y de la máquina. De esta manera, se pueden detectar y prevenir las amenazas. Los clientes de VxRail que hayan adquirido licencias Platinum (incluidas las suscripciones) de VMware tienen derecho a utilizar su licencia Platinum en VxRail para ejecutar vSphere Enterprise Plus. Es importante tener en cuenta que la administración del ciclo de vida (LCM) de AppDefense de vSphere Platinum es responsabilidad del cliente.

Al igual que Dell EMC, VMware tiene un riguroso proceso de ciclo de vida útil de desarrollo seguro de software y un centro de respuesta de seguridad. VxRail se desarrolla junto con VMware y es compatible con él, lo que garantiza que todos los componentes incluidos en la solución se diseñen, construyan, prueben e implementen en torno a la seguridad como prioridad principal. Para obtener más información sobre la Seguridad de los productos de VMware

VMware vCenter Server

vCenter Server es el punto de administración principal para la virtualización de servidores y el almacenamiento de vSAN. Una sola instancia de vCenter puede escalar a niveles empresariales y admitir cientos de nodos de VxRail y miles de máquinas virtuales. VxRail puede utilizar una instancia de vCenter que se implemente dentro del clúster de VxRail o utilice una instancia de vCenter ya existente.

vCenter proporciona una jerarquía lógica de centros de datos, clústeres y hosts. Esta jerarquía facilita la segmentación de los recursos por caso de uso o líneas de negocios, y permite que los recursos se muevan dinámicamente según sea necesario. Todo esto se realiza desde una única interfaz intuitiva.

vCenter Server proporciona las VM y los servicios de recursos, como el servicio de inventario, la programación de tareas, el registro de estadísticas, la alarma y la administración de eventos, y el aprovisionamiento y la configuración de las VM. vCenter Server también ofrece características de disponibilidad avanzadas. Estas son las siguientes:

- vSphere vMotion: permite la migración de cargas de trabajo de VM en directo sin tiempo de inactividad
- vSphere Distributed Resource Scheduler (DRS): equilibra y optimiza constantemente la asignación de recursos informáticos de VM entre los nodos del clúster
- vSphere High Availability (HA): ofrece funcionalidades de reinicio y de conmutación por error de las VM

Hipervisor VMware ESXI

En VxRail, el hipervisor ESXi aloja la VM en nodos del clúster. Las VM son seguras y portátiles, y cada una es un sistema completo con procesadores, memoria, redes, almacenamiento y BIOS. Las VM están separadas una de la otra, por lo que cuando un sistema operativo invitado que se ejecuta en una VM falla, las otras VM del mismo host físico no se ven afectadas y continúan ejecutándose. Las VM comparten el acceso a las CPU y ESXi es responsable de programar estas CPU. Además, ESXi asigna a las VM una región de memoria utilizable y administra el acceso compartido a las tarjetas de red físicas y a las controladoras de disco asociadas con el host físico. Todos los sistemas operativos basados en X86 son compatibles y las VM del mismo hardware de servidor físico pueden funcionar con diferentes sistemas operativos y aplicaciones.

Redes virtuales de VMware

Un requisito de seguridad fundamental es aislar el tráfico de la red. En VxRail, las funcionalidades de redes virtuales de vSphere proporcionan aislamiento y conectividad flexible. Las VM de VxRail se comunican entre sí mediante el switch distribuido virtual (VDS) de VMware, que funciona como un único switch lógico que abarca múltiples nodos en el mismo clúster. VDS utiliza protocolos de red estándar e implementaciones de VLAN, y reenvía cuadros en el nivel de enlace de datos.

VDS se configura en vCenter Server en el nivel del centro de datos y conserva una configuración de red segura y coherente a medida que las VM migran a través de varios hosts. El dispositivo VxRail utiliza el VDS para el tráfico del dispositivo y vSAN lo utiliza para el acceso a la red.

Además, VxRail puede configurarse con NSX para proporcionar seguridad de red definida por software y control de acceso más minucioso mediante la microsegmentación.

VMware vSAN

Los dispositivos VxRail cuentan con la tecnología de VMware vSAN para el almacenamiento definido por software de clase empresarial. vSAN incorpora los discos de hosts conectados de manera local a un clúster de vSphere para crear un pool de almacenamiento compartido distribuido. La capacidad se escala verticalmente mediante la incorporación de discos adicionales al clúster y se escala horizontalmente mediante la incorporación de nodos adicionales de VxRail. vSAN está completamente integrado con vSphere y funciona perfectamente con otras características de vSphere.

vSAN es reconocido por su eficiencia y su rendimiento. vSAN se optimiza automáticamente y equilibra la asignación en función de la carga de trabajo, la utilización y la disponibilidad de los recursos. vSAN ofrece una solución de alto rendimiento, optimizada para flash

y compatible con HCI para una variedad de cargas de trabajo. Las características de almacenamiento de clase empresarial incluyen las siguientes:

- Tecnología eficiente de reducción de datos que incluye la desduplicación y la compresión, así como la codificación de borrado
- Políticas de calidad de servicio (QoS) para controlar el consumo de la carga de trabajo en función de los límites definidos por el usuario
- Tecnologías de protección de los datos e integridad de los datos, entre ellas, las sumas de comprobación de software y los dominios de fallas
- Seguridad mejorada con cifrado de datos en reposo de vSAN

Con vSAN, los discos en cada nodo de VxRail se organizan automáticamente en grupos de discos con una sola unidad de memoria caché y una o más unidades de capacidad. Estos grupos de discos se utilizan para formar un único almacén de datos de vSAN, al que se puede acceder en todos los nodos de un clúster de VxRail.

VxRail ofrece dos opciones de configuración de almacenamiento de nodos de vSAN: una configuración híbrida que utiliza los SSD flash y los HDD mecánicos, y una configuración de SSD todo flash. La configuración híbrida utiliza los SSD flash para el almacenamiento en caché y los HDD mecánicos para el almacenamiento de datos persistente y de capacidad. La configuración todo flash utiliza los SSD flash para el almacenamiento en caché y para la capacidad. En la figura 8, se ilustran los conceptos básicos de vSAN.

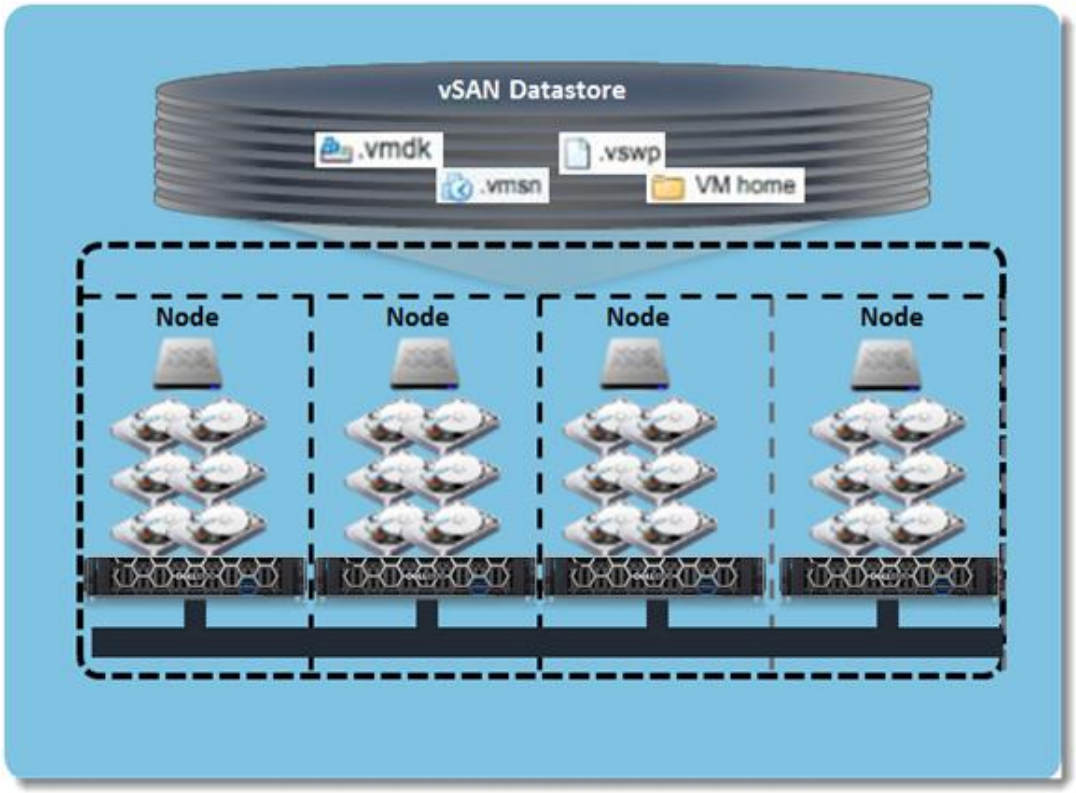

Figura 8: conceptos básicos de vSAN

vSAN se configura cuando el clúster de VxRail se inicializa por primera vez y se administra a través de vCenter. Durante el proceso de inicialización del dispositivo VxRail, vSAN crea un almacén de datos compartido distribuido a partir de los discos conectados localmente en cada nodo ESXi. La cantidad de almacenamiento en el almacén de datos es el total de todas las unidades de capacidad del clúster. La cantidad de almacenamiento utilizable dependerá del nivel de protección que se utilice. La configuración y la verificación organizadas de vSAN que se realizan como parte de la inicialización del sistema garantizan un rendimiento coherente y predecible, y hacen que el sistema se configure según las prácticas recomendadas.

Administración basada en políticas de almacenamiento (SPBM)

vSAN está dirigido por políticas y está diseñado para simplificar el aprovisionamiento y la administración del almacenamiento. Las políticas de almacenamiento de vSAN se basan en conjuntos de reglas que definen cuál es el requisito de almacenamiento que

necesitan las VM. Los administradores pueden cambiar dinámicamente las políticas de almacenamiento de las VM a medida que cambian los requisitos. Algunos ejemplos de posibles reglas de SPBM son la cantidad de fallas a tolerar, la técnica de protección de datos que se utilizará y la verificación de la habilitación de las sumas de comprobación de nivel de almacenamiento.

vRealize Log Insight de VMware

VMware vRealize Log Insight está integrado con VxRail, monitorea los eventos del sistema y proporciona notificaciones integrales continuas sobre el estado del entorno virtual y del hardware del dispositivo. vRealize Log Insight brinda una administración automatizada de registros en tiempo real para el dispositivo VxRail con monitoreo de registros, agrupamiento inteligente y análisis para simplificar la solución de problemas a escala en entornos físicos, virtuales y de nube de VxRail. El registro centralizado es un requisito fundamental para una infraestructura segura. Para los clientes que ya cuentan con una instalación de registro o una SIEM, VxRail se integra fácilmente con el protocolo estándar de registro del sistema de la industria.

VMware Cloud Foundation (VCF): con NSX

VMware Cloud Foundation en VxRail es una solución integrada diseñada de manera conjunta por Dell EMC y VMware con características que simplifican, optimizan y automatizan las operaciones de todo su centro de datos definido por software (SDDC) desde el día 0 hasta el día 2. La nueva plataforma ofrece un conjunto de servicios definidos por software de procesamiento (con vSphere y vCenter), almacenamiento (con vSAN), redes (con NSX), seguridad y administración de nube (con vRealize Suite) en entornos privados y públicos. Esto la convierte en el hub operativo de sus servicios de nube híbrida.

VMware Cloud Foundation en VxRail es el camino más simple hacia la nube híbrida a través de una plataforma de nube híbrida totalmente integrada que aprovecha las funcionalidades nativas de hardware y de software de VxRail y otras integraciones específicas de VxRail (como los plug-in de vCenter y las redes de Dell EMC). Estos componentes funcionan en conjunto para ofrecer una nueva experiencia de usuario en la nube híbrida lista para usar con una integración de pila completa. La integración de pila completa significa que usted dispone de la capa de infraestructura de HCI y la pila de software de nube en una experiencia completa, automatizada y lista para usar del ciclo de vida útil.

El centro de datos de VMware NSX es la plataforma de seguridad y de virtualización de red que habilita la red de nube virtual. Es un enfoque definido por software para las redes que se extiende a través de los centros de datos, las nubes, los terminales y las ubicaciones de borde. Con el centro de datos de NSX, las funciones de red se acercan a la aplicación y se distribuyen en todo el entorno, incluidos el enrutamiento, el firewall, el equilibrio de cargas y la conmutación. Al igual que el modelo operativo de las máquinas virtuales, las redes se pueden aprovisionar y administrar de forma independiente del hardware subyacente.

El centro de datos de NSX reproduce todo el modelo de red en software, lo que permite que cualquier topología de red, desde redes simples hasta redes complejas de múltiples niveles, se cree y se aprovisione en segundos. Los usuarios pueden crear múltiples redes virtuales con diversos requisitos y aprovechar una combinación de los servicios ofrecidos a través de NSX, como la microsegmentación, o a través de un amplio ecosistema de integraciones de otros fabricantes que van desde firewalls de última generación hasta soluciones de administración del rendimiento para construir entornos inherentemente más ágiles y seguros. Luego, estos servicios se pueden extender a una serie de terminales entre nubes y dentro de ellas. Para obtener información adicional, consulte la Guía de arquitectura de VMware Cloud Foundation en VxRail

Funcionalidades de seguridad de VxRail

Las funcionalidades de seguridad se dividen en 2 secciones: seguridad de datos y seguridad del sistema. En la siguiente configuración y administración segura del sistema de VxRail, se cumple con los principios de la tríada de confidencialidad-integridad-disponibilidad (CIA).

VxRail proporciona una pila completamente preconfigurada y probada para todas las funcionalidades de seguridad. Estas funcionalidades de seguridad se encuentran integradas y son parte del dispositivo.

SEGURIDAD DE DATOS

La seguridad de datos cumple con la tríada de CIA a fin de garantizar que los datos solo estén disponibles para cuentas autorizadas o específicas. Se cumplen los requisitos y las especificaciones. Esto incluye el acceso a los datos, ya sea físico o a nivel de usuario.

C (Confidentiality): confidencialidad

Evitar que la información confidencial llegue a las personas equivocadas y, al mismo tiempo, garantizar el acceso adecuado y autorizado a los datos de la empresa es un problema muy frecuente denominado confidencialidad o privacidad. VxRail aborda la confidencialidad de los datos en uso, los datos en movimiento y los datos en reposo de varias maneras diferentes.

Cifrado

El cifrado protege la confidencialidad de la información mediante su codificación de modo que sea ininteligible para los destinatarios no autorizados. Con VxRail, los almacenes de datos se pueden cifrar mediante el cifrado de datos en reposo de vSAN (D@RE), que proporciona protección validada de la norma FIPS 140-2 de nivel 1. Las VM individuales se pueden cifrar mediante el cifrado de vSphere y las VM en movimiento se pueden cifrar mediante el cifrado de vMotion. Se pueden configurar niveles adicionales de cifrado en función de los requisitos de las aplicaciones.

El cifrado de vSAN es la manera más fácil y flexible de cifrar los datos en reposo, ya que el almacén de datos completo de vSAN está cifrado con un único ajuste. Este cifrado se aplica a todo el clúster para todas las VM que utilizan el almacén de datos. Normalmente, los datos cifrados no se benefician de técnicas de reducción de espacio, como la desduplicación o la compresión. Sin embargo, con vSAN, el cifrado se realiza después de la desduplicación y la compresión, por lo que se mantienen los beneficios de estas técnicas de reducción de espacio.

El cifrado de VM proporciona la flexibilidad para habilitar el cifrado para VM individuales, lo que significa que un solo clúster puede tener VM cifradas y no cifradas. El cifrado de la VM se traslada con ella dondequiera que se aloje. Por lo tanto, incluso si la VM se trasladó a un almacén de datos fuera de VxRail, se mantendría cifrada.

Además, mientras que el cifrado de VM puede activarse y desactivarse, con las VM cifradas, la migración con vSphere vMotion siempre usará vSphere vMotion cifrado. Las VM que no están cifradas pueden seleccionar entre las opciones de cifrado desactivado, oportunista y requerido con vMotion. El oportunista se usaría de manera predeterminada en una VM sin cifrar con vMotion.
En la figura 9, a continuación, se resume la diferencia entre el cifrado de VM y el cifrado de vSAN

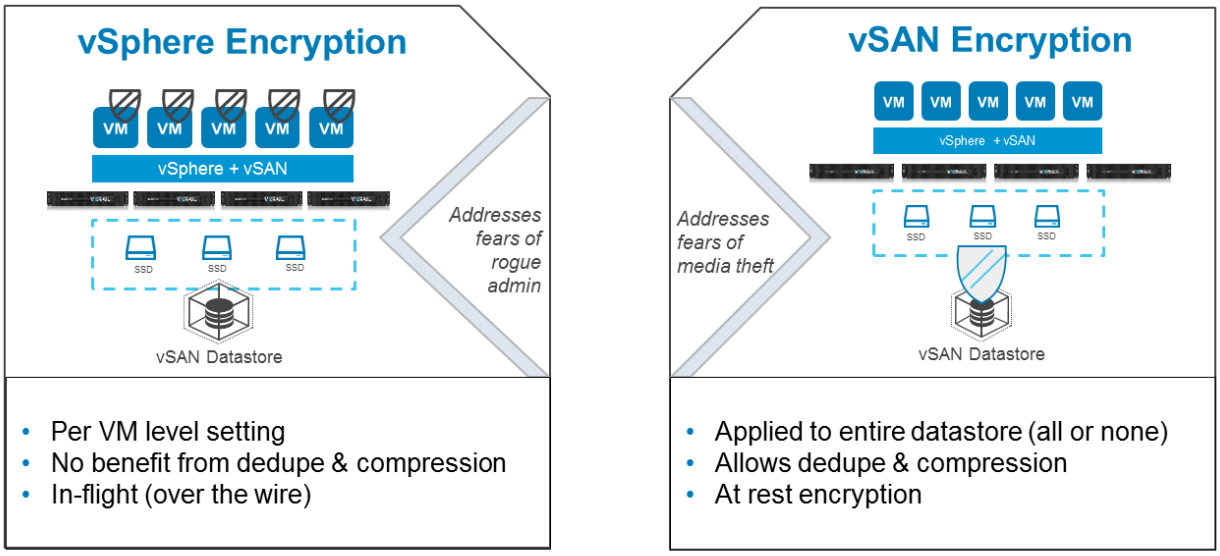

Figura 9: cifrado de VM vs. cifrado de vSAN

Además, VxRail es compatible con vMotion cifrado, en el que las VM se cifran cuando se mueven entre los hosts. Esto incluye las migraciones de vMotion dentro de VxRail, así como migraciones de vMotion desde o hacia un clúster de VxRail dentro de una instancia de vCenter. vMotion cifrada se puede utilizar con el cifrado de vSAN para tener el cifrado de datos en reposo y el cifrado de datos en transferencia. Se aplica el cifrado de vMotion para las VM con cifrado de vSphere habilitado.

A excepción del cifrado de vMotion, en el que vSphere proporciona las claves provisorias que se utilizan para cifrar los datos en movimiento, se requiere un servidor de administración de claves (KMS) para la generación, el almacenamiento y la distribución segura de las claves de cifrado. Cuando el cifrado está habilitado, vCenter establece una relación de confianza con el KMS y, luego, pasa la información de conexión del KMS a los hosts ESXi. Los hosts ESXi solicitan claves de cifrado directamente desde el KMS y realizan el cifrado y descifrado de datos. La conectividad de vCenter solo se requiere para la configuración inicial.

Debido a que el KMS es un componente fundamental de la infraestructura de seguridad, debe tener el mismo nivel de redundancia y de protección que generalmente se aplica a otros componentes fundamentales de la infraestructura, como DNS, NTP y Active Directory. Es importante recordar que el KMS se debe ejecutar separado físicamente de los elementos que cifra. Durante el inicio, los hosts ESXi solicitan las claves del KMS. Si el KMS no está disponible, el sistema no podrá completar el proceso de inicio.

VxRail y VMware admiten KMS que son compatibles con el protocolo de interoperabilidad de administración de claves (KMIP) v1.1 o superior, como Dell EMC CloudLink. VMware tiene una guía de compatibilidad de sistemas de gestión de claves validada con vSphere.

Dentro de vSphere, el cifrado se lleva a cabo por un conjunto de módulos comunes que están validados por la norma FIPS 140-2. Estos módulos comunes están diseñados, implementados y validados por el ciclo de vida útil de desarrollo seguro de VMware. Tener un conjunto de módulos comunes para el cifrado permite que VxRail facilite la implementación, la administración y el soporte de cifrado.

El cifrado está habilitado en VxRail a través de una configuración simple de vCenter. Los controles de acceso garantizan que solo las personas autorizadas puedan habilitar o deshabilitar el cifrado. Un rol denominado "administrador no asociado a criptografía" permite que un administrador realice tareas administrativas normales, pero que no tenga autoridad para alterar la configuración de cifrado.

Redes definidas por software VxRail mediante el NSX opcional

El entorno virtual dinámico, como VxRail, a menudo se beneficia de la flexibilidad que proporcionan los servicios de red definida por software (SDN). La forma más sencilla de proporcionar una SDN en VxRail es con VMware NSX, una licencia de software opcional que no está incluida en VxRail. NSX es una plataforma completa de seguridad y virtualización de red que les permite a los administradores crear redes virtuales completas, con enrutadores, firewalls y equilibradores de carga solo en software. Debido a que estas redes definidas por software son independientes de la infraestructura de red física subyacente, no dependen de que VxRail se conecte a un proveedor de switch en particular.

NSX con VxRail es una solución de seguridad integrada que reduce la necesidad de implementar componentes de software o de hardware de seguridad adicionales. Con NSX, los administradores de VxRail configuran la microsegmentación para asegurar y aislar las diferentes cargas de trabajo del grupo de usuarios, controlar el ingreso y el egreso, y proporcionar una seguridad mejorada para todas las cargas de trabajo, que incluyen las aplicaciones tradicionales de varios niveles y las VM de propósito general, así como los entornos de VDI. Algunos de los beneficios de usar NSX con VxRail son los siguientes:

- La capacidad de aplicar políticas de seguridad más próximas a las cargas de trabajo. Las políticas de seguridad se aplican en el software y los controles de seguridad se mueven con la carga de trabajo entre los hosts del clúster.
- La administración simplificada de seguridad se integra con la pila de vSphere y se administra en forma centralizada a través de vSphere HTML5 Web Client y del plug-in de NSX Manager.
- Controles de seguridad uniformes y automáticos mediante el uso de grupos y políticas. Las cargas de trabajo se identifican de forma automática y se colocan dinámicamente en el estado de seguridad correcto.
- La implementación eficiente de los controles de seguridad en el nivel de hipervisor reduce la latencia de las aplicaciones y el consumo de ancho de banda en comparación con los controles de seguridad externos o perimetrales.
- Aislamiento en el nivel de DMZ para controlar el ingreso y el egreso de los clientes internos y externos desde Internet mediante el uso de reglas adecuadas de permiso y denegación para controlar el tráfico.
- Detección y bloqueo de direcciones IP de VM falsificadas con la función SpoofGuard. Para obtener más información sobre esta funcionalidad, consulte la documentación de VMware sobre Cómo usar SpoofGuard.
- Firewall de identidad que le permite a un administrador de NSX crear reglas de DFW basadas en el usuario de Active Directory. Para obtener más información sobre esta funcionalidad, consulte la documentación de VMware NSX.

- Se integra con los servicios de seguridad de otros fabricantes, como la detección de intrusiones y la prevención de intrusiones (IDS/IDP).

NSX mejora el estado de seguridad de un entorno y cumple con las siguientes certificaciones y estándares:

- Certificación de Criterios Comunes: EAL 2+
- Firewall certificado por ICSA Labs
- FIPS 140-2
- Satisfacción de todas las recomendaciones de ciberseguridad de NIST para proteger las cargas de trabajo virtualizadas

Con la plataforma opcional de seguridad VMware NSX con VxRail, las políticas de seguridad y firewall están incorporadas. Esto brinda un dispositivo verdaderamente convergente, en lugar de seguridad que se encuentra de manera externa en el perímetro. La implementación de NSX con VxRail reduce aún más el tiempo que se necesita para implementar nuevas iniciativas de aplicaciones a medida que los controles de seguridad se vuelven parte del dispositivo, en lugar de estar en componentes de hardware o de software adicionales.

Modo de bloqueo

Para los entornos que necesitan una seguridad y flexibilidad aún mayores, el modo de bloqueo se puede configurar para hosts ESXi. En el modo de bloqueo, la capacidad de realizar operaciones de administración en hosts individuales es limitada, por lo que la tarea de administración se debe completar a través de vCenter.

El bloqueo en modo "normal" habilita a un grupo exclusivo de usuarios a formar parte de una lista que les permitirá administrar los servidores en forma local en lugar de tener que usar vCenter. Esta lista debe incluir ciertas cuentas de administración de VxRail.

En el modo estricto de bloqueo, no se permite que los usuarios administren los servidores en forma local. El bloqueo en el modo "estricto" no es compatible con VxRail.

Administración segura con HTTPS

El tráfico de administración inseguro representa un gran riesgo de seguridad. Es por eso que VxRail utiliza las interfaces de administración protegidas con la seguridad de capa de transporte “TLS 1.2” vCenter, iDRAC y el software del sistema de HCI, que deshabilitan la interfaz HTTP de texto claro y requieren el uso de HTTPS, el cual utiliza TLS 1.2. Además, el acceso a la línea de comandos de los servidores ESXi debe utilizar SSH. El uso de SSH y HTTPS es una parte vital del comando y el control seguros de VxRail.

Integridad

La integridad de los datos de una empresa es un requisito fundamental de las operaciones empresariales. VxRail garantiza la integridad de sus datos cuidando la coherencia, la precisión y la confiabilidad de los datos durante su ciclo de vida útil mediante el control el acceso de los usuarios y las características incorporadas de integridad, como las sumas de comprobación de datos

Segmentación de red

La segmentación de red se utiliza para separar el tráfico de red privado del tráfico público con el fin de reducir los espacios de ataque. También es un control de seguridad eficaz para limitar el movimiento de un atacante en las redes.

VxRail está diseñado con múltiples niveles de segmentación de red. Entre ellos se encuentra la segmentación física de la red de administración de hardware, la segmentación virtual de redes de aplicaciones y de infraestructura, y la microsegmentación de VM y de aplicaciones con el software opcional NSX de VMware. A través de la segmentación, la visibilidad de las herramientas administrativas fundamentales es limitada. Esto evita que los atacantes las usen para dañar el sistema. De manera predeterminada, la adecuada segmentación de red se configura automáticamente como parte de la inicialización del sistema, y el administrador tiene la flexibilidad para definir niveles adicionales de segmentación, tantos como sean necesarios en el entorno de la aplicación. Las prácticas recomendadas para la configuración de red se encuentran en la Guía de red de VxRail de Dell EMC.

VxRail utiliza switches distribuidos virtuales de VMware que segmentan el tráfico de manera predeterminada mediante VLAN independientes para administración, vSAN, vMotion y tráfico de aplicaciones. Las redes vSAN y vMotion son redes privadas no enrutables. Según las aplicaciones admitidas por una red de VxRail, el tráfico se puede segmentar aún más en base a diferentes aplicaciones, producción y tráfico no relacionado con la producción u otros requisitos.

El switch distribuido virtual de un VxRail se configura de manera predeterminada con Network I/O Control (NIOC) de vSphere. NIOC permite que el ancho de banda físico se asigne a diferentes redes virtuales de área local (VLAN). Algunos ataques cibernéticos, como la denegación de servicio y los gusanos, pueden generar un uso excesivo de los recursos. Esto puede causar una denegación de recursos a otros servicios que no se encuentran directamente en riesgo. NIOC puede garantizar que otros servicios tendrán el ancho de banda de red que necesitan para mantener su integridad en caso de que haya un ataque a algún servicio. Las configuraciones de NIOC se establecen automáticamente siguiendo las prácticas recomendadas cuando se inicia el sistema. La Guía de red de Dell EMC incluye detalles de la configuración de NIOC para las VLAN predeterminadas de VxRail.

Cada nodo de VxRail tiene un puerto físico Ethernet independiente para la interfaz de administración de hardware de iDRAC. La segmentación física de esta red les dificulta a los atacantes obtener acceso a la administración de hardware. En el caso de un ataque de denegación de servicio distribuido, la red segmentada físicamente no se verá afectada y el alcance de un posible ataque se verá limitado.

Arranque seguro de UEFI

El arranque seguro de UEFI protege al sistema operativo contra daños y ataques de rootkit. El arranque seguro de UEFI garantiza que el firmware, el cargador de arranque y el VMkernel presentan la firma digital de una autoridad de confianza. Además, el arranque seguro de UEFI para ESXi garantiza que los paquetes de instalación de VMware (VIB) estén firmados en forma criptográfica. Esto garantiza que la pila de arranque del servidor ejecute todo el software original y que no se haya modificado.

Suma de comprobación de software

Una parte clave de la integridad de datos es la validación de que los datos recuperados del almacenamiento no se han alterado desde que fueron creados. VxRail utiliza la suma de comprobación de integridad de datos de extremo a extremo en el nivel de bloque de manera predeterminada. La suma de comprobación se crea en el momento en que se escriben los datos. Luego, la suma de comprobación se verifica en la lectura y, si muestra que los datos han cambiado desde su escritura, se restauran desde otros miembros del grupo de RAID. vSAN también utiliza un mecanismo de corrección proactivo para detectar y corregir posibles daños en los datos, incluso en los datos a los que se accede con poca frecuencia.

Disponibilidad

Mantener su sistema de TI actualizado, asegurarse de que el hardware funcione correctamente y proporcionar un ancho de banda adecuado son claves para conservar la disponibilidad de los datos de una empresa para los usuarios autorizados. La administración del ciclo de vida del software VxRail, las características de disponibilidad de vSphere, el monitoreo proactivo y la recuperación integrada, así como la seguridad física del hardware y la configuración segura del sistema garantizan la máxima disponibilidad del sistema.

Administración del ciclo de vida del software VxRail

Una de las medidas más importantes que una organización puede tomar para mantener la seguridad de su infraestructura de TI es mantener las actualizaciones de software y los parches actualizados. Las actualizaciones y los parches no solo mejoran el rendimiento o corrigen problemas que podrían generar tiempo de inactividad: también corrigen los problemas de seguridad. Hay una enorme colaboración dentro de la comunidad de seguridad. Gracias a que VxRail se ha diseñado en forma conjunta con VMware, ya tenemos preparados los primeros planes de correcciones de seguridad, lo que permite que el equipo de VxRail valide y prepare rápidamente los parches de seguridad calificados. Sin embargo, no todos están del mismo lado, sino que es una carrera entre los defensores, que trabajan para mitigar y remediar las amenazas, y los atacantes, cuyo objetivo es utilizar las vulnerabilidades. Gracias a que VxRail se ha diseñado en forma conjunta con VMware, ya tenemos preparados los primeros planes de correcciones de seguridad, lo que permite que el equipo de VxRail valide y prepare rápidamente los parches de seguridad calificados.

La administración del ciclo de vida del software VxRail hace que las operaciones de actualización complejas y riesgosas sean fáciles de instalar y seguras de implementar. El sistema de HCI de VxRail es el único sistema en el que todos los componentes de software están diseñados, probados y ofrecidos como un paquete. Los paquetes de software de VxRail pueden incluir actualizaciones de BIOS, firmware, hipervisor, vSphere o cualquiera de los componentes de administración incluidos. Si se encuentran vulnerabilidades, las correcciones se implementan rápidamente para mitigar las amenazas, sin importar dónde se encuentren. Los paquetes de actualizaciones se prueban de manera minuciosa en la plataforma de hardware de VxRail y en toda la pila de software de VxRail antes de ofrecerse a los clientes.

Cuando hay actualizaciones disponibles, se notifica a los administradores a través del software del sistema de HCI. Luego, el administrador puede descargar directamente el paquete de actualización e iniciar o programar un proceso de actualización organizado. Las actualizaciones se realizan como procesos graduales mientras el sistema sigue funcionando al servicio de la empresa. Si se requiere un reinicio, las VM se migran de forma automática a otros nodos en el clúster antes de continuar.

La administración del ciclo de vida del software del sistema de HCI no solo reduce la complejidad, sino que hace que la infraestructura sea más segura, ya que reduce el tiempo y la dificultad para aplicar parches en los sistemas y eliminar el riesgo.

Características de disponibilidad de VxRail vSphere

VxRail utiliza las características incorporadas de disponibilidad de vSphere, que incluyen la alta disponibilidad de VMware (VMware HA), el programador de recursos distribuidos de VMware (DRS) y los clústeres expandidos de VMware. Estas funcionalidades son compatibles con el software automatizado de VxRail y proporcionan una disponibilidad continua de los servicios alojados en VxRail. Por lo tanto, se recomienda que los clientes utilicen versiones de vSphere que incluyan estas funcionalidades.

VMware HA supervisa el funcionamiento de las VM en un clúster de VxRail. Si una VM o un nodo falla, HA se reinicia en otro nodo en cualquier lugar del clúster. Una VM puede fallar por una serie de razones, como un ataque cibernético, una falla del hardware subyacente o un software dañado. A pesar de que VMware HA no previene las interrupciones, minimiza el tiempo que se necesita para restaurar el servicio.

VMware DRS distribuye la carga de trabajo de la VM en todos los hosts del clúster. A medida que las demandas de recursos de la VM cambian, DRS migra las cargas de trabajo de la VM mediante vSphere vMotion a otros hosts dentro del clúster. Los ataques cibernéticos pueden causar problemas de recursos en las VM que no se vieron afectadas por el ataque cibernético. Los ataques cibernéticos a menudo causan una utilización intensiva de los recursos por parte de la VM que fue atacada y, por lo tanto, una utilización intensiva de los recursos en el nivel del host, lo que afecta a los recursos disponibles para las otras VM en ese host. DRS protege las VM y las migra lejos de los hosts con restricciones de recursos. Esto permite que las VM continúen ofreciendo servicios.

El clúster extendido de VMware amplía el clúster de VxRail de un solo sitio a dos sitios para obtener más disponibilidad. Existe una sola instancia de la VM, pero las copias completas de sus datos se conservan en ambos sitios. En caso de que el sitio actual en el que se esté ejecutando la VM no esté disponible, la VM se reinicia en el otro sitio.

Protección de datos

Tener defensas de seguridad sólidas es indispensable, pero un plan de recuperación sólido y de confianza es igualmente importante. El respaldo y las replicaciones son los componentes fundamentales de la recuperación después de una violación. Para facilitar la recuperación, el software del sistema de HCI incluye respaldo y restauración basados en archivos. Todos los dispositivos de VxRail incorporan un paquete de inicio para Dell EMC RecoverPoint para VM (RP4VM), que proporciona la mejor replicación local y remota, y la mejor recuperación granular.

El respaldo y la restauración basados en archivos del software del sistema de HCI protegen los datos contra la eliminación accidental del dispositivo virtual o de daños internos del dispositivo. Los respaldos pueden configurarse para que ocurran de manera periódica o según sea necesario. Esta es una característica integral que respalda los archivos dentro del almacén de datos de vSAN. De esta manera, no se requieren hardware ni software adicionales.

Con RP4VM, si una VM se ve comprometida o si los datos están dañados, la VM y el conjunto de datos vuelven rápidamente al punto en el tiempo antes del ataque. De esta manera, el negocio se puede recuperar rápidamente. RP4VM se instala directamente desde VxRail Manager y se implementa rápidamente. El monitoreo diario se realiza a través del conocido plug-in de vCenter. La recuperación es fácil y se realiza a través de una interfaz conocida de vSphere.

Para las organizaciones que requieren funcionalidades mejoradas e integrales de protección de datos, VxRail admite opciones que incluyen Dell EMC Data Protection Suite for VMware, Dell EMC Power Protect y Dell EMC Data Domain Virtual Edition.

Los respaldos basados en archivos del software del sistema de HCI de VxRail garantizan la continuidad comercial en caso de que la VM de VxRail deba restaurarse.

SEGURIDAD DEL SISTEMA

Autenticación, Autorización y Contabilidad de VxRail

Infraestructura de autenticación, autorización y contabilidad (AAA) incorporada. La AAA está diseñada para controlar el acceso, lo que garantiza que las personas que utilicen el sistema sean las adecuadas. Además, establece sus niveles de acceso y registra la actividad para dar cuenta de lo que se ha hecho y quién lo ha hecho.

AUTENTICACIÓN

La autenticación del software del sistema de HCI se regula con el inicio de sesión único (SSO) a través del plug-in de vCenter. VxRail vCenter admite el sistema centralizado de administración de identidades de la organización, en conformidad con las políticas de seguridad de autenticación

A menudo, las organizaciones centralizan la administración de identidades mediante el uso de servicios de directorio como Microsoft Active Directory (AD) con LDAP. Si el VxRail es un entorno independiente y no forma parte de un dominio, los usuarios y las contraseñas se pueden administrar de forma local en vSphere e iDRAC. Desde el punto de vista de las prácticas recomendadas, se recomienda utilizar la autenticación centralizada.

Es posible que haya diferentes personas responsables de los servidores físicos, la administración del ciclo de vida de VxRail y la administración del servidor, el almacenamiento y el entorno de virtualización de red. Por lo tanto, VxRail utiliza controles detallados de acceso basados en funciones para iDRAC, el software del sistema de HCI y vSphere.

AUTORIZACIÓN

Mediante el uso del “principio de menos privilegio” (POLP), se le otorgan los derechos requeridos para desempeñar su rol a un usuario, pero solo los necesarios. vSphere incluye varios roles predefinidos que se utilizan para otorgar el privilegio adecuado. Por ejemplo, a un usuario se le puede otorgar el rol de administrador de vSphere, administración de HCIA, o ambos. El rol de administración de HCIA otorga a un usuario el privilegio de realizar las tareas de administración del ciclo de vida de VxRail desde el plug-in de administración de VxRail de vCenter. El administrador de vSphere otorga privilegios para realizar tareas de administrador en vCenter. Además, vSphere permite un nivel de control de acceso aún más minucioso mediante la creación de roles personalizados. Por ejemplo, se puede otorgar la capacidad de reconocer una alarma o crear un perfil de almacenamiento a un usuario con privilegios, pero no el de implementar las VM.

Los roles están asociados con diferentes usuarios y grupos, y con objetos específicos, en los que un objeto es una cosa o un grupo de cosas. Por ejemplo, un usuario o grupo puede tener permiso para reconocer alertas de una VM o un puerto en particular, pero no de otros objetos. Además, se pueden asignar roles restrictivos a los usuarios, como “sin acceso”, lo que les impide ver áreas específicas dentro de vCenter. A usuarios múltiples o grupos se les puede otorgar los mismos o diferentes niveles de acceso al mismo objeto. Los permisos concedidos a un objeto secundario se pueden utilizar para reemplazar los permisos heredados de un elemento primario.

El control de acceso basado en roles de vSphere admite los principios de seguridad granulares de “menores privilegios” y “separación de responsabilidad”, y permite que el administrador de seguridad mejore la seguridad por medio de la definición de permisos precisos basados en la estructura de administración de sistemas de una organización.

CONTABILIDAD

Comprender los cambios en la configuración y en el estado de los componentes es indispensable para conservar la seguridad y la disponibilidad de los sistemas. Los cambios pueden ser el resultado de una corrección temporal que causa una modificación de la configuración. Sin embargo, estos cambios también podrían ser un indicio de una intrusión. El monitoreo proactivo de la infraestructura es una actividad de seguridad importante.

La detección oportuna de una intrusión puede significar una diferencia entre una breve interrupción en la que el atacante no puede comprometer ningún sistema importante, y una intrusión que dura varios meses y pone en peligro muchos sistemas importantes. Si no se mantiene un sistema de registros de auditoría, es posible que no se pueda acceder a la información adecuada sobre el ataque para determinar su severidad. De acuerdo con el Informe global de seguridad de Trustwave de 2019 (registro necesario), el 57% de los incidentes que se analizaron comprendían redes corporativas e internas (hasta el 50 % en 2017).

La modificación de la configuración es una dificultad que afecta a todos los sistemas. En un comienzo, los sistemas pueden contar con una base de configuración segura, pero es posible que se vuelvan vulnerables con el tiempo. Estos cambios pueden suceder por una variedad de razones, entre ellas, un cambio temporal durante la solución de problemas o un cambio aprobado que debe formar parte de la configuración base. Sin monitoreo, esos cambios se vuelven muy difíciles de detectar.

El desafío de monitorear la información es que proviene de muchas fuentes diferentes: una VM independiente, un servidor físico, la infraestructura de virtualización, la red, los componentes de seguridad o las mismas aplicaciones. Para entender esta información se necesita de una vista consolidada de la actividad y de los cambios. VxRail incluye vRealize Log Insight. Log Insight reúne los registros de VMware, entre ellos los servidores, los dispositivos de red, el almacenamiento y las aplicaciones. Como se muestra en el gráfico que aparece a continuación, Log Insight crea un panel con gráficos basados en los datos de los registros. Esto ayuda al administrador a desglosar de manera rápida y sencilla la principal causa del problema. En la figura 10, a continuación, se muestra el panel de vRealize Log Insight.

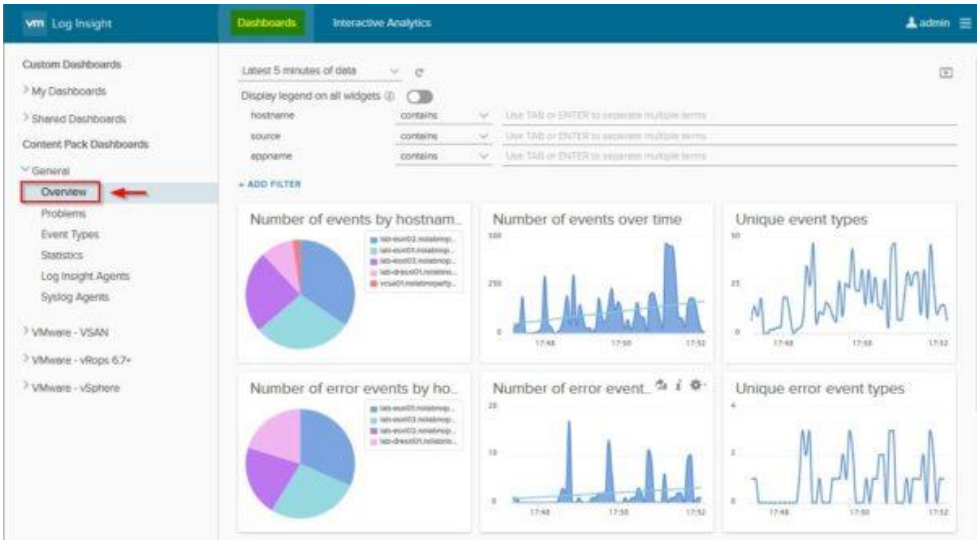

Figura 10: Realize Log Insight

La correlación de toda esta información es una de las muchas razones por las que VxRail utiliza el protocolo de tiempo de red (NTP) estándar de la industria para mantener todos los relojes de los componentes sincronizados.

Para las organizaciones que ya cuentan con un sistema de administración de registros o con un sistema de administración de eventos e incidentes de seguridad (SIEM), VxRail se integra fácilmente con el protocolo estándar de registro del sistema.

Seguridad de la ubicación física de VxRail

La seguridad física es una parte importante de cualquier solución de seguridad integral. Debido a que VxRail se puede implementar fuera de un centro de datos tradicional, la seguridad física puede tener una importancia aún mayor. Para evitar que el malware o el software infectado se introduzcan a través de una unidad USB, los puertos USB de VxRail se pueden deshabilitar y, luego, se pueden volver a habilitar solo cuando sea necesario.

Los nodos VxRail también se monitorean en otras situaciones como aberturas de chasis, falla o reemplazo de piezas, cambios de firmware y advertencias de temperatura. Esta información se guarda en el registro del ciclo de vida útil de iDRAC. En muchos casos, no es necesario abrir un chasis después de iniciada la producción, y el seguimiento de dicha actividad puede ser un indicador de un intento de comprometer el sistema.

Automatización

Una parte importante del mantenimiento de la seguridad es garantizar que todos los elementos relevantes de la configuración de seguridad se implementen en todos los objetos de un entorno. Un clúster individual de VxRail puede tener hasta 64 nodos físicos, y un vCenter puede administrar varios clústeres de VxRail, lo que brinda soporte a miles de VM. Incluso un cambio simple, si se debe configurar en todas las VM, puede demorar bastante en aplicarse. Además, cuando se realizan tareas repetitivas, las personas son propensas a cometer errores. Aquí es donde la automatización es indispensable.

La automatización permite que un entorno tenga menos errores de configuración y una configuración más coherente y, al mismo tiempo, aumenta la eficiencia y reduce el tiempo entre el momento en el que se toma una decisión y el momento en que se implementa, lo que aumenta el tiempo de creación de valor de esas decisiones.

Las herramientas compatibles, como vRealize Automation, permiten la automatización de vSphere y vSAN. Estas herramientas se pueden utilizar para automatizar las operaciones diarias estándar, como la creación de las VM o las políticas de almacenamiento. La automatización de vRealize también se puede utilizar para garantizar que la configuración de seguridad no se haya modificado de forma tal que ya no sea adecuada. Si la configuración cambia, la automatización de vRealize puede volver a configurar los servidores ESXi, vCenter o las VM individuales para que, una vez más, cumplan con la configuración de seguridad requerida. Además, debido a que la automatización de vRealize es una herramienta estándar de VMware, muchos equipos de virtualización de TI ya saben cómo trabajar con la automatización de vRealize y han creado perfiles que funcionan con un clúster de VxRail.

Paquete de endurecimiento de STIG de VxRail

La configuración de la seguridad puede ser un proceso complejo y propenso a errores, con muchos de los mismos riesgos que busca mitigar. Hay tres elementos diferentes que simplifican el proceso de seguridad de la infraestructura de VxRail. En primer lugar, vSphere tiene un enfoque "seguro por defecto" para la configuración. En segundo lugar, las guías de implementación técnica de seguridad de la Agencia de sistemas de información de defensa (DISA STIG) proporcionan un diseño para el endurecimiento de la seguridad y una variedad de herramientas de automatización que permiten que el monitoreo y la configuración de los parámetros de seguridad se verifiquen y se configuren según sea necesario. Esto permite que se configure el perfil de riesgo adecuado y que esté alineado con las necesidades del negocio. Por último, la capacidad de automatizar la reversión de la configuración a un estado seguro ya conocido cuando se producen cambios inesperados es una parte vital de la seguridad de VxRail.

A partir de vSphere 6.0, VMware comenzó una iniciativa para incorporar la seguridad a la configuración predeterminada de vSphere. Esto hace que VxRail sea más seguro desde el primer momento. Como parte de esta iniciativa, la mayoría de las configuraciones de seguridad recomendadas se clasificaron como específicas del sitio o se cambiaron a un valor predeterminado de la configuración de seguridad. Se actualizaron las configuraciones que antes tenían que cambiarse después de la instalación, de modo que la configuración de seguridad ahora es la predeterminada.

Los valores de configuración que se clasifican como específicos del sitio no pueden configurarse de manera predeterminada. Por ejemplo, el nombre de host de un servidor de registro del sistema remoto o NTP. Con VxRail, muchas de las configuraciones que VMware clasifica como específicas del sitio se configuran con el software del sistema de HCI como parte de la instalación.

Muchas organizaciones utilizan las STIG como base para endurecer sus sistemas. Estas STIG proporcionan una lista de comprobación en un PDF legible y un script automatizado. Esto permite que las herramientas de automatización lean la STIG y configuren el entorno para que coincida con la configuración recomendada con una mínima intervención manual. Mientras que las STIG de VMware existentes incluyen los componentes de VxRail (incluido vSphere), ESXi y vSAN facilitan mucho la implementación. El dispositivo VxRail de Dell que ejecuta el software del dispositivo VxRail v4.5.x o 4.7.x cumple con los requisitos de las guías de implementación técnica de seguridad (STIG) de DISA pertinentes.

Con el tiempo, las configuraciones pueden cambiar y estar en posiciones menos seguras. Debido a esto, es importante no solo monitorear la configuración, sino también automatizar la restauración del entorno al estado seguro inicial. VxRail admite múltiples opciones diferentes según el nivel de automatización requerido. VxRail cuenta con herramientas de endurecimiento automatizadas que comparan la configuración actual con las STIG y, si la configuración ha cambiado, la revierten al estado seguro ya conocido. Si se requiere una herramienta de automatización más amplia, VMware vRealize Suite trabaja con entornos de VxRail para automatizar la administración de la configuración y, al mismo tiempo, mantener la gestión y el control. Además, VMware ofrece AppDefense, una herramienta más centrada en las aplicaciones que utiliza el aprendizaje automático para reunir información sobre un estado bueno ya conocido para las VM y las aplicaciones que admiten. Con esta herramienta, cuando se detecta una variación del estado bueno ya conocido, se le notifica al administrador y se puede automatizar una respuesta a partir de una biblioteca de rutinas de respuesta ante incidentes.

Seguridad integrada en VxRail ACE

VxRail Analytical Consulting Engine (ACE) complementa la sencillez operacional integrada de VxRail de Dell EMC con la inteligencia operacional para los clústeres de VxRail. VxRail ACE ofrece una combinación de sencillez e inteligencia operativa con seguridad intrínseca, lo que permite que las empresas transformen la infraestructura de TI

VxRail ACE se ejecuta en una plataforma de servicios en la nube administrada por TI de Dell EMC. Como una solución SaaS basada en la nube, VxRail ACE tiene la flexibilidad para ofrecer una nueva funcionalidad a menudo y sin interrupciones, lo que proporciona una experiencia de cliente única. Su red neuronal para el aprendizaje profundo mejorará continuamente sus funcionalidades predictivas a medida que ingiera la gran cantidad de metadatos que VxRail puede recopilar de sus clústeres.

Los usuarios de VxRail pueden acceder a VxRail ACE en https://vxrailace.EMC.com con sus credenciales de soporte de Dell EMC.

Visión general de seguridad de VxRail ACE

VxRail ACE reúne datos de telemetría de nodos de VxRail en los clústeres de VxRail de la organización y transmite de forma segura esos datos a una solución de SaaS administrada por la TI de Dell EMC, como se puede observar en 01.

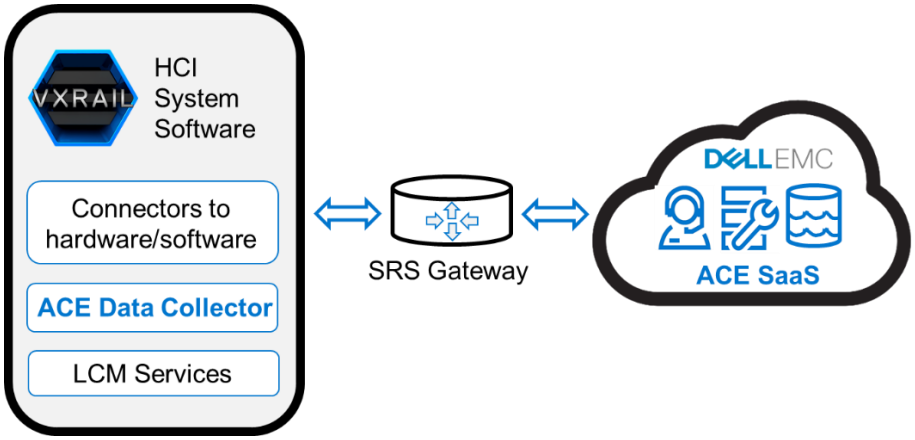

Figura 11: diagrama de arquitectura de alto nivel de VxRail ACE

Dell EMC comprende las preocupaciones de los clientes sobre el mantenimiento de la seguridad de sus datos. La seguridad es intrínseca a VxRail ACE, desde la recopilación de datos hasta los datos en tránsito y en reposo. Además, VxRail ACE se ha desarrollado de manera segura con el uso de controles de arquitectura como parte del ciclo de vida útil del desarrollo de seguridad estándar de Dell EMC. Este estándar define las actividades centradas en la seguridad que los equipos de productos de Dell EMC deben tener en cuenta para crear y ofrecer productos. De esta manera, los productos de Dell EMC minimizan los riesgos de nuestros productos y entornos de clientes causados por las vulnerabilidades de seguridad.

Recopilación de datos de VxRail ACE

En cada clúster de VxRail, se ejecuta un recopilador de datos adaptable (ADC) que recupera los datos de telemetría del software del sistema de HCI a partir de los conectores de hardware y de software de VxRail. El ADC no reúne información de identificación personal (PII). Los datos de telemetría recopilados por el ADC se visualizan en la tabla 1.

Telemetría básica (Topología de HW: dispositivos, unidad, firmware, PSU)	**Datos de rendimiento**	**Alarmas**	**Datos del sensor de hardware**
• Información del clúster • Información del dispositivo	• Clúster (CPU, memoria, disco) • VM (CPU, memoria, disco) • vSAN (disco, red)	• vCenter • VxRail	• Tipo de sensor • Estado • Nombre • Lectura actual

Table 1 Datos de telemetría de VxRail recopilados mediante ACE

Los datos de telemetría recopilados por el ADC no se almacenan localmente; los datos se transmiten en forma segura a través de la gateway de Secure Remote Support (SRS) de Dell EMC.

Datos en tránsito de VxRail ACE a Dell

Solo los datos que recopila el recopilador de datos adaptable (ADC) se envían al back-end de Dell EMC a través de la gateway de Secure Remote Service (SRS) de Dell EMC. VxRail ACE se suscribe para recibir notificaciones sobre la llegada de datos del sistema de HCI a través de la gateway de SRS. Los clientes de VxRail ACE controlan qué sistemas envían los datos del sistema de HCI a través de la gateway. Todos los datos que se transmiten a través de la gateway de SRS de Dell EMC están protegidos en tránsito por las prácticas estándar recomendadas de la industria. La gateway de SRS se autentica de forma bidireccional mediante los certificados digitales de RSA® junto con las políticas de acceso controladas por el cliente y un registro de auditoría detallado. La comunicación de punto a punto se establece a través del uso del estándar de cifrado avanzado (AES) de 256 bits, lo que garantiza que todos los datos se transporten en forma segura a la infraestructura administrada por TI de Dell EMC. Además, SRS proporciona una autenticación exclusiva de VPN y de múltiples factores. Una vez que los datos llegan a Dell, VxRail ACE cifra y almacena los datos del ACE en su propia infraestructura administrada por TI de Dell EMC.

Cifrado de datos en reposo de VxRail

Los datos del sistema de HCI recibidos desde los sistemas administrados de VxRail ACE se cifran y se almacenan en la infraestructura de Dell EMC administrada por TI de Dell.

Infraestructura de TI de Dell EMC:

- Proporciona una plataforma segura que garantiza que los datos de telemetría de cada cliente estén aislados.
- Proporciona alta disponibilidad, tolerancia a fallas y recuperación ante desastres.
- Ubica los datos de telemetría del cliente (incluidos los respaldos) en EE. UU.
- Conserva de manera indefinida los datos históricos para los sistemas que están siendo monitoreados activamente por ACE, incluso los conocimientos derivados de ACE.
- Brinda a cada cliente el acceso a un portal seguro e independiente desde el cual cada usuario solo puede ver aquellos sistemas en VxRail ACE que forman parte del acceso al sitio de ese usuario, tal como se describe en MyService360 de Dell EMC.

La oficina de seguridad y resiliencia de Dell Technologies (SRO), dirigida por el director de seguridad de Dell, es responsable de la seguridad y la protección de la infraestructura de tecnología de la información de Dell EMC que aloja la solución de SaaS de VxRail ACE. Esto se logra a través de políticas y procedimientos de seguridad regulatorios, y el cumplimiento de los controles de seguridad de la información, que incluyen medidas como firewalls en capas, sistemas de detección de intrusiones, antivirus líderes de la industria y protección contra malware. El equipo de ciberseguridad de Dell EMC participa en la realización de análisis de vulnerabilidad continuos en la aplicación y en el entorno subyacente. Cualquier corrección requerida se gestiona a través de un programa de corrección de vulnerabilidades en curso, como actualizaciones de software, parches o cambios en la configuración.

Todos los datos enviados a VxRail ACE se almacenan en la infraestructura alojada en el centro de datos de Dell EMC. La política de seguridad de la información garantiza que toda la información y los recursos de Dell EMC estén debidamente protegidos. Los propietarios de la información deben asegurarse de que todos los recursos sean contabilizados y de que cada recurso tenga un custodio designado. Todos los componentes de la infraestructura se encuentran en la red de enclaves protegidos por firewall de Dell EMC, que no admite el acceso externo. No se permite el inicio de sesión directo al servidor de base de datos y a la base de datos, excepto por parte los miembros del administrador del sistema y los equipos del administrador de la base de datos. Las cuentas de aplicaciones de la base de datos se administran con una autenticación estándar de la contraseña de la base de datos. Dell EMC implementó un proceso de administración de cambios en las prácticas recomendadas de la industria para garantizar que el hardware de la infraestructura de Dell EMC esté estable, controlado y protegido. La administración de cambios proporciona las políticas, los procedimientos y las herramientas necesarias para regir estos cambios, a fin de garantizar que se sometan a las revisiones y las aprobaciones adecuadas y que se comuniquen de manera efectiva a los usuarios.

Control de acceso a datos de VxRail ACE

El acceso a datos de VxRail ACE se puede dividir en dos categorías:

- Acceso de los clientes a VxRail ACE para ver los datos de su sistema y los conocimientos derivados de ACE.
- Acceso por parte del administrador interno del sistema de TI de Dell EMC y del administrador de la base de datos a la infraestructura de VxRail ACE que es administrada por Dell EMC.

En las subsecciones que se encuentran a continuación, se describe cómo el acceso a datos es controlado por estas dos categorías de usuarios.

Acceso del usuario final a VxRail ACE

Los clientes utilizan su cuenta de soporte existente para iniciar sesión en VxRail ACE. El acceso a los datos de VxRail ACE desde el portal de VxRail ACE requiere que cada usuario final tenga una cuenta de soporte válida de Dell EMC. La infraestructura de inicio de sesión único (SSO) de Dell EMC valida la autenticación. VxRail ACE utiliza el perfil de usuario del cliente de MyService360 de Dell EMC para el control de acceso. El perfil de usuario se crea y se asocia con un perfil del cliente válido cuando el usuario se registra en una cuenta con Dell EMC. VxRail ACE proporciona a cada cliente una vista segura e independiente de sus sistemas y garantiza que solo ellos puedan ver sus datos a través de VxRail ACE. Cada usuario solo puede ver aquellos sistemas en VxRail ACE que forman parte del acceso al sitio de ese usuario según su configuración en MyService360 de Dell EMC.

Acceso administrativo a la infraestructura de VxRail ACE administrada por la TI de Dell EMC

Dell EMC es consciente de la importancia de proteger la información confidencial y de propiedad de los clientes. Es por esto que todos los empleados de Dell EMC deben firmar un acuerdo que incluye disposiciones relacionadas con la información del cliente. Las obligaciones de este acuerdo incluyen todos los datos almacenados en máquina, de cualquier manera o en cualquier formato, mientras participan de los servicios de mantenimiento, y permanecen en vigencia incluso después de la finalización del empleo de Dell EMC.

Estándares y certificaciones compatibles

VxRail es una infraestructura hiperconvergente sólida y flexible que se puede configurar para permitir que las organizaciones satisfagan las normativas de cumplimiento. Si bien algunos proveedores de HCI aseguran tener compatibilidad, Dell EMC se dedica a buscar constantemente la certificación completa de los estándares de seguridad que son importantes para nuestros clientes. Comuníquese con su representante de Dell EMC para saber cómo VxRail cumple incluso con los requisitos normativos y empresariales más exigentes. A continuación se encuentra una lista de algunos de los estándares y las certificaciones de VxRail.

FIPS 140-2 para el cifrado de datos en reposo: la publicación del estándar federal de procesamiento de información 140-2 (FIPS PUB 140-2) establece los requisitos y los estándares para los componentes de hardware y de software de los módulos de criptografía. El FIPS 140-2 es requerido por el gobierno de EE. UU. y por otras industrias reguladas, como instituciones financieras y de servicios de salud que recopilan, almacenan, transfieren, comparten y distribuyen información confidencial pero no clasificada. Los servidores PowerEdge que utiliza VxRail están validados.

Criterios comunes EAL 2+: los Criterios comunes para la evaluación de la seguridad de la tecnología de la información es un estándar internacional (ISO/IEC 15408) para la certificación de seguridad de las computadoras. Las evaluaciones de Criterios comunes se realizan en los productos y los sistemas de seguridad de la computadora. Con ellos se analizan las características de seguridad del sistema y se proporciona un nivel de confianza para las características de seguridad del producto a través de los requisitos de garantía de seguridad (SAR) o de los niveles de seguridad de evaluación (EAL). La certificación de Criterios comunes no puede garantizar la seguridad, pero puede asegurarse de que las afirmaciones sobre los atributos de seguridad se verifiquen en forma independiente. Los servidores PowerEdge y los componentes de vSphere utilizados por VxRail cuentan con la certificación completa.

Marco de ciberseguridad de NIST: el marco de NIST para mejorar la infraestructura más importante es una pauta voluntaria desarrollada para mejorar la ciberseguridad, la administración de riesgos y la resiliencia de los sistemas de las organizaciones. NIST consultó a una amplia gama de partners del gobierno, de la industria y del entorno académico durante más de un año para crear un conjunto de pautas y prácticas sólidas basado en un consenso. La publicación especial 800-131A cuenta con recomendaciones para la longitud de las claves de cifrado.

NSA Suite B: Suite B es un conjunto de algoritmos criptográficos promulgados por la Agencia Nacional de Seguridad como parte de su programa de modernización criptográfica. Las versiones actuales de ESXi y de vCenter que se utilizan con VxRail admiten NSA Suite B.

Sección 508 VPAT: los estándares de la sección 508 de la Junta de acceso de los Estados Unidos se aplican a la tecnología electrónica y de la información adquirida por el gobierno federal, y define los requisitos de acceso para las personas con discapacidades físicas, sensoriales o cognitivas. Tanto el servidor PowerEdge como los componentes de software de vSphere que utiliza VxRail están en conformidad con la sección 508 VPAT.

Asistencia para el ajuste comercial (TAA): el programa de asistencia para el ajuste comercial es un programa federal que proporciona una posibilidad de crecimiento y de oportunidades de empleo a través de la ayuda a trabajadores de EE. UU. que han perdido sus trabajos como consecuencia del comercio exterior. Cuando se vende como un sistema, VxRail está en conformidad con TAA.

DISA-STIG: como parte del Departamento de defensa (DOD) de EE. UU., la Agencia de sistemas de la información de defensa (DISA) desarrolla estándares de configuración llamados Guías de implementación técnica de seguridad (STIG) como una de las formas para mantener la seguridad de la infraestructura de TI del DOD. Estas guías proporcionan orientación técnica sobre cómo bloquear los sistemas de información y el software que, de otra manera, correría riesgo de ser atacado. Dell EMC proporciona pasos manuales y automatizados para la configuración del dispositivo VxRail a fin de cumplir con los requisitos de STIG de la red de información del DoD (DISA).

IPv6: IPv6 es el protocolo de última generación que utiliza Internet. Además de resolver las limitaciones de direccionamiento de IPv4, IPv6 tiene muchos beneficios de seguridad, por eso muchos entornos están avanzando hacia la adopción de IPv6. VxRail aprobó las pruebas de interoperabilidad de USGv6 para IPv6 en el modo de doble pila además del estándar más alto para las pruebas de IPv6 Ready.

Módulo de plataforma segura: El grupo de informática de confianza define la especificación para el módulo de plataforma segura (TPM). TPM 1.2 y 2.0 están disponibles de manera opcional con VxRail. Ambas son certificaciones con los requisitos de seguridad de Criterios comunes y de FIPS 140-2 y TCG. vSphere es compatible con TPM 1.2 y TPM 2.0

Infraestructura de ciberseguridad de NIST y VxRail

La infraestructura de ciberseguridad de NIST (NIST CSF) proporciona una infraestructura de políticas de orientación de seguridad informática a fin de que las organizaciones del sector privado puedan evaluar y mejorar su capacidad para prevenir, detectar y defenderse contra los ataques cibernéticos. Esta infraestructura voluntaria consiste en estándares, pautas y prácticas recomendadas para administrar el riesgo relacionado con la ciberseguridad. El enfoque prioritario, flexible y rentable del marco de ciberseguridad promueve la protección y la resiliencia de la infraestructura más importante.

El material más importante del marco de ciberseguridad de NIST está organizado en cinco “funciones” que, a la vez, se subdividen en categorías, como se ve en la figura 12 que se encuentra a continuación.

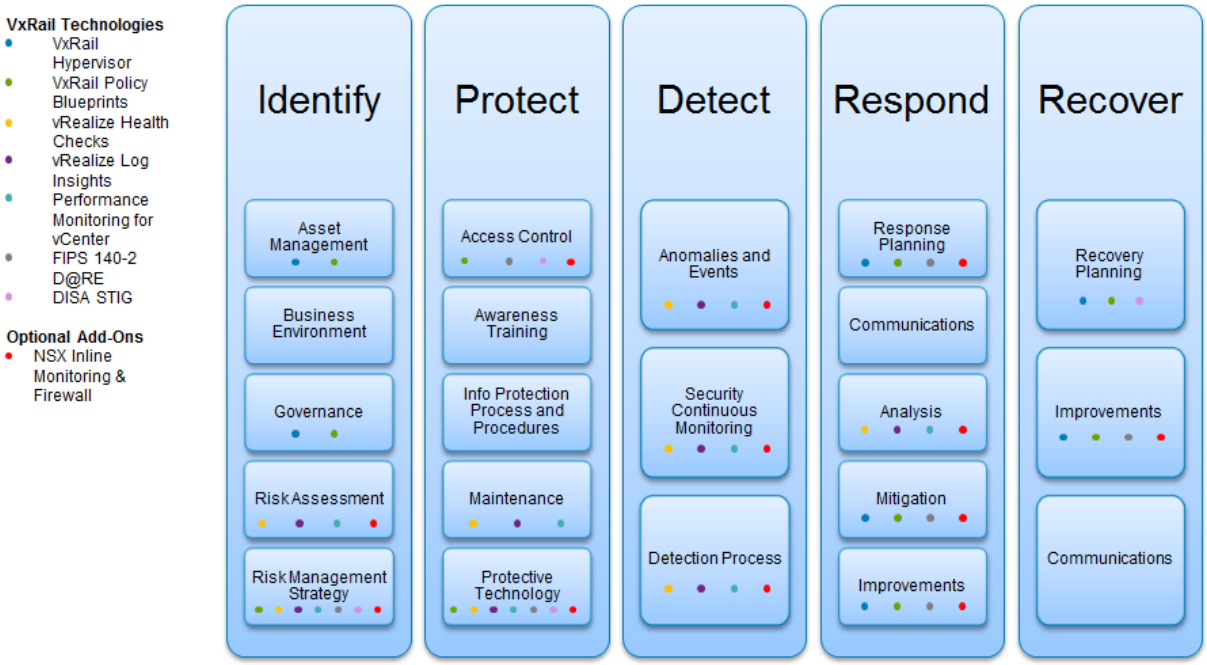

Figura 12: Instituto nacional de estándares y tecnología, infraestructura de ciberseguridad

Visite el sitio web de NIST para obtener más información sobre el marco de ciberseguridad de NIST. Para obtener más información sobre cómo VxRail se alinea con la infraestructura de ciberseguridad de NIST, vea el informe sobre las características de VxRail que admiten la infraestructura de ciberseguridad de NIST, disponible aquí infraestructura de seguridad.

Partners y soluciones de seguridad de VxRail

VxRail está diseñado con seguridad incorporada e implementada siguiendo las prácticas de seguridad recomendadas. Los usuarios están autenticados y autorizados con el nivel de acceso correspondiente. Los clústeres VxRail se configuran fácilmente con el cifrado de datos en reposo para proteger la confidencialidad de la información y el tráfico de segmentos de configuración de redes predeterminado. Además, cuentan con herramientas como RecoverPoint para VM, que garantiza que las aplicaciones y los servicios se puedan recuperar rápidamente si la integridad de los datos se ve comprometida. Estas características de seguridad son fundamentales e inherentes al dispositivo de VxRail.

Sin embargo, la protección de un entorno contra las amenazas actuales requiere una “defensa en profundidad” con varias capas de seguridad. Las redes que conectan las aplicaciones y los servicios que se ejecutan en el dispositivo VxRail con los usuarios que los consumen deben estar protegidas, y también deben protegerse las aplicaciones y los servicios. Los firewalls, los sistemas de detección y prevención de intrusiones, los antivirus y antimalware, la protección de terminales, la administración, y las operaciones de seguridad forman parte de una defensa multicapa. Solo Dell Technologies tiene todo el alcance de las tecnologías y de los servicios para ayudarlo a proteger la totalidad de su entorno.

El tamaño de su organización y el punto en el que se encuentra su organización a lo largo de su viaje de transformación de la TI definirán cuál es el mejor enfoque. Es posible que algunos entornos funcionen dentro de los marcos de seguridad existentes, mientras que otros pueden aprovechar la oportunidad de mejorar sus operaciones de seguridad a medida que transforman su infraestructura de TI. Las organizaciones a menudo utilizan a muchos proveedores diferentes como parte de su programa de seguridad, lo que agrega una complejidad que aumenta el riesgo. RSA y SecureWorks forman parte de la familia de Dell Technologies; ambos lo ayudan a administrar el riesgo y a proteger sus recursos digitales. Solo Dell Technologies puede brindar una relación de un solo proveedor con una gran pericia en seguridad en todo el mundo y un ecosistema de miles de partners. En la figura 13, a continuación, se ilustra el poder de Dell para ayudarlo a administrar los riesgos y a proteger sus datos.

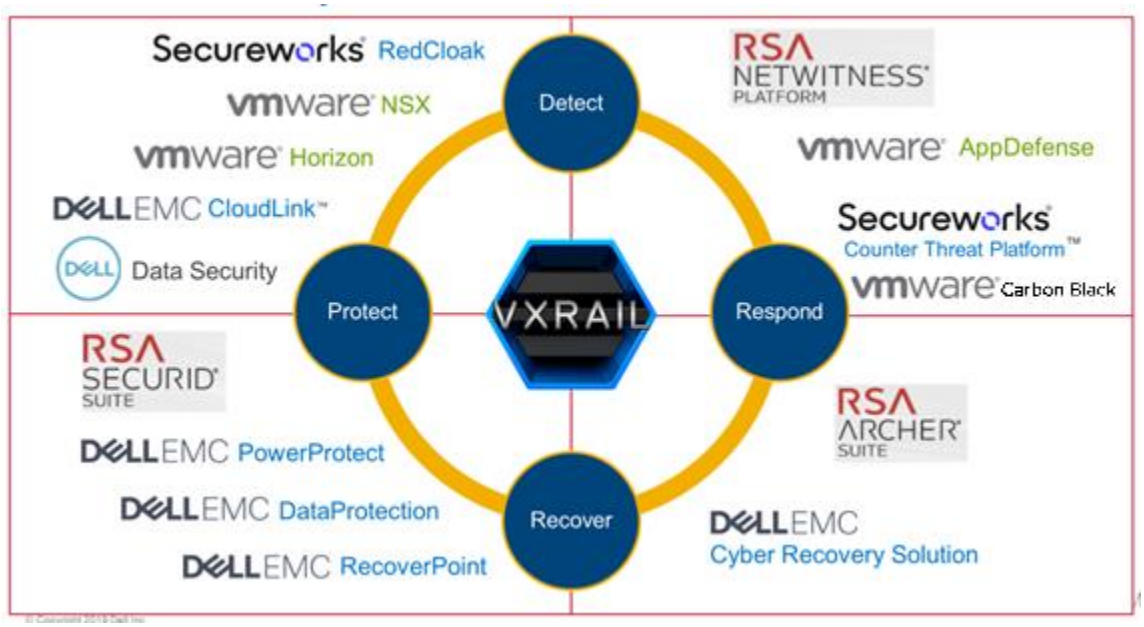

Figura 13: el poder de Dell para ayudarlo a administrar los riesgos y a proteger sus datos

Administración de identidades y de acceso

VxRail admite cuentas de usuario locales, integración de LDAP y un inicio de sesión único. A pesar de que es posible tener un VxRail independiente, la mayoría de los entornos se integrará con los sistemas de administración de identidades y de acceso (IAM) de la empresa que utilizan servicios de directorio como Microsoft Active Directory.

Administración de eventos y de incidentes de seguridad

El dispositivo VxRail incluye vRealize Log Insight para centralizar la administración de registros del sistema. Para las organizaciones que cuentan con una instalación centralizada de administración de registros, como Splunk o un sistema de administración de eventos y de incidentes de seguridad (SIEM), VxRail se puede integrar fácilmente con la interfaz de registro del sistema estándar de la industria. RSA NetWitness Suite proporciona una recopilación de registros, análisis y muchas otras características de seguridad que mejoran las funcionalidades de seguridad de VxRail.

Para los clientes que no desean administrar los eventos de seguridad por su cuenta, SecureWorks brinda servicios de administración de registros para VxRail y prácticamente cualquier activo de información importante o tecnología de seguridad. SecureWorks reúne y monitorea la información de seguridad que necesita para resguardar su empresa. Lo que es aún más importante, los expertos en seguridad altamente capacitados de SecureWorks, que trabajan desde sus centros de operaciones integradas contra amenazas, investigan y responden de inmediato ante cualquier actividad maliciosa las 24 horas del día, los 7 días de la semana.

Servidor de administración de claves

El cifrado es una herramienta poderosa para proteger la confidencialidad de la información, y VxRail ha incorporado funcionalidades de cifrado a fin de proteger los datos en uso, en movimiento y en reposo. Sin embargo, la seguridad de datos que proporciona el cifrado abarca únicamente la generación, la protección y la administración de las claves usadas en el proceso de cifrado.

Las claves de cifrado deben estar disponibles cuando se necesiten y el acceso a las claves durante las actividades de descifrado debe conservarse durante toda la vida útil de los datos. Por lo tanto, la administración adecuada de claves de cifrado es esencial para el uso eficaz de la criptografía. Muchas organizaciones centralizan la administración de claves en toda la empresa para simplificar la administración, aplicar políticas y proporcionar informes y auditorías de cumplimiento.

VxRail y vSphere admiten el protocolo de interoperabilidad de administración de claves (KMIP), lo que permite el funcionamiento con muchos sistemas empresariales de administración de claves. Dell EMC CloudLink proporciona una administración de claves que cumple con el KMIP, así como un cifrado para nubes públicas, privadas e híbridas. Para las organizaciones que ya cuentan con los servicios de administración de claves, VxRail y vSphere logran integrarse fácilmente y proporcionan un punto único de administración de claves en toda la empresa. VMware ofrece una lista de servidores de administración de claves compatibles.

Otros partners de seguridad

Asegurar la infraestructura de TI actual y los recursos digitales es un compromiso complejo. Una sola solución no puede ofrecer una defensa lo suficientemente sólida. Es por eso que Dell Technologies ofrece un ecosistema de partners que trabajan en conjunto para abordar los riesgos y las vulnerabilidades únicas de su entorno. Reconocemos que toda la industria debe trabajar en conjunto para ayudar a nuestros clientes a lograr sus objetivos de ciberseguridad.

El dispositivo VxRail de Dell EMC y VMware vSphere admiten estándares de seguridad abiertos, y los partners tienen un papel importante para ayudar a nuestros clientes a realizar la transición a un mundo de TI seguro, virtual y de múltiples nubes.

La documentación técnica de "Soluciones integrales para partners de VMware de redes y seguridad" asociadas en el apéndice A incluyen una lista de algunas soluciones de partners para redes, seguridad y cumplimiento que se integran con VMware vSphere®, vCenter™, vShield Endpoint™ y vCloud® Networking and Security™, y enumeran el conjunto completo de aplicaciones y de software compatibles con vSphere. Además de las API de EPSEC para la protección de antivirus y antimalware proporcionada por vShield Endpoint, la infraestructura del ecosistema de VMware vCloud facilita la inserción del servicio en el nivel de la tarjeta de interfaz de red virtual (vNIC) y del perímetro virtual. La guía de compatibilidad de VMware hace que encontrar el componente adecuado sea sencillo.

Conclusión

La transformación de la seguridad comienza con una infraestructura de TI segura. VxRail proporciona una infraestructura moderna y segura del núcleo al borde y a la nube y una infraestructura hiperconvergente. VxRail está diseñado, pensado, construido y administrado como un único producto para reducir el posible espacio de ataque mediante la disminución de la cantidad de componentes que están relacionados con la infraestructura. Los paquetes de administración del ciclo de vida del software de VxRail pueden incluir actualizaciones de BIOS, firmware, hipervisor, vSphere o cualquiera de los componentes de administración incluidos. Esto hace que la actualización de la pila completa de software sea mucho más simple y reduce la vulnerabilidad frente a los ataques.

La protección completa de un entorno contra las amenazas actuales requiere una “defensa en profundidad” con varias capas de seguridad. Las redes que conectan las aplicaciones y los servicios que se ejecutan en el dispositivo VxRail con los usuarios que los consumen deben estar protegidas, y también deben protegerse las aplicaciones y los servicios. Los firewalls, los sistemas de detección y prevención de intrusiones, los antivirus y antimalware, la protección de terminales, la administración, y las operaciones de seguridad forman parte de una defensa multicapa.

Dell Technologies sabe de seguridad y cuenta con expertos en todo el mundo que pueden ayudarlo a evaluar su entorno y a diseñar un plan de seguridad para cumplir con sus requisitos específicos. Para obtener más información, póngase en contacto con su representante de Dell Technologies.

Apéndice A: referencias

A continuación, se encuentran todos los enlaces y las referencias citadas en esta documentación técnica.

Recurso	URL
Seguridad basada en riesgos:	https://www.riskbasedsecurity.com/2019/02/13/over-6500-data-breaches-and-more-than-5-billion-records-exposed-in-2018/
Seguridad de productos de EMC:	https://www.dellemc.com/es-mx/products/security/index.htm
Ciclo de vida útil del desarrollo de seguridad de Dell EMC:	https://www.dellemc.com/es-mx/products/security/index.htm#tab0=2
Equipo de respuesta ante incidentes de seguridad de productos (PSIRT) de Dell:	https://www.dell.com/support/contents/mx/es/19/article/product-support/self-support-knowledgebase/security-antivirus/alerts-vulnerabilities/dell-vulnerability-response-policy
Ciberseguridad resiliente de los servidores de Dell EMC PowerEdge de 14.ª generación:	http://en.community.dell.com/techcenter/extras/m/white_papers/20444755/download
AppDefense:	https://www.vmware.com/products/appdefense.html
Guía de la arquitectura de VMware Cloud Foundation en VxRail:	https://www.dellemc.com/resources/es-mx/asset/technical-guides-support-information/products/converged-infrastructure/vmware_cloud_foundation_on_vxrail_architecture_guide.pdf
Seguridad de productos de VMware:	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/VMware-Product-Security.pdf
Guía de las redes de VxRail de Dell EMC:	https://www.dellemc.com/resources/en-us/asset/technical-guides-support-information/products/converged-infrastructure/h15300-VxRail-network-guide.pdf
Guía de uso de SpoofGuard de VMware:	https://docs.vmware.com/en/VMware-NSX-for-vSphere/6.4/com.vmware.nsx.admin.doc/GUID-06047822-8572-4711-8401-BE16C274EFD3.html
Documentación de VMware NSX:	https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/6.4/com.vmware.nsx.admin.doc/GUID-B5C70003-8194-4EC3-AB36-54C848508818.html
Seguridad para soluciones hiperconvergentes:	https://communities.vmware.com/servlet/JiveServlet/download/36084-3-183512/Security for Hyper-Converged Solutions_NSX.pdf
Informe de seguridad global de Trustwave de 2019:	https://www.trustwave.com/Resources/Library/Documents/2019-Trustwave-Global-Security-Report/
*1 Informe de investigación de vulneración de datos de 2017.	http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017
*2 "20.ª encuesta de CEOs" de PWC con 5351 miembros del público, en 22 países.	https://www.pwc.com/jg/en/publications/pwc-ceo-report-2017%20(2).pdf
Infraestructura de ciberseguridad de NIST:	https://www.nist.gov/cyberframework
Lista de servidores compatibles de administración de claves:	https://www.vmware.com/resources/compatibility/search.php?deviceCategory=kms&details=1&page=1&display_interval=10&sortColumn=Partner&sortOrder=Asc

Soluciones integrales de partners de VMware para redes y seguridad:	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vcns/vmware-integrated-partner-solutions-networking-security.pdf
Guía de compatibilidad de VMware:	https://www.vmware.com/resources/compatibility/search.php
Libro técnico sobre VxRail:	https://www.emc.com/collateral/technical-documentation/h15104-VxRail-appliance-techbook.pdf
Características de seguridad de Integrated Dell Remote Access Controller (iDRAC):	http://en.community.dell.com/techcenter/extras/m/white_papers/20441744/download
Documentación de vSAN:	https://docs.vmware.com/en/VMware-vSAN/index.html
Cuatro transformaciones comerciales:	https://www.youtube.com/watch?v=TcKJ39_4Rwc
Certificaciones de cifrado de VMware:	https://www.vmware.com/security/certifications/fips.html
vRealize Log Insight de VMware:	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vrealize-log-insight/vrealize-log-insight-datasheet.pdf
Certificaciones de NIST para la búsqueda por proveedor de FIPS 140-2 de Dell EMC y VMware:	https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search
Ciclo de vida útil de desarrollo seguro de VMware:	https://www.vmware.com/security/sdl.html
Administración de claves de VMware:	https://blogs.vmware.com/vsphere/2017/10/key-manager-concepts-toplogy-basics-vm-vsan-encryption.html
Guía de seguridad de vSphere 6.5:	https://docs.vmware.com/en/VMware-vSphere/6.5/vsphere-esxi-vcenter-server-65-security-guide.pdf
Los programas de seguridad de productos de Dell EMC generan confianza:	https://mexico.emc.com/products/security/index.htm
	Recursos de ACE
Demostración en video sobre la visión general de ACE	https://vxrail.is/acedemo
Demostración en video del paquete de Smart update	https://vxrail.is/aceupdates
Visión general de la solución	https://www.dellemc.com/resources/es-mx/asset/offering-overview-documents/products/converged-infrastructure/vxrail-ace-solution-brief.pdf
Visión general sobre MyService360 de Dell Technologies	https://www.delltechnologies.com/en-us/services/support-deployment-technologies/my-service-360.htm
Guía integral de seguridad mediante el diseño de VxRail (documentación técnica)	https://www.dellemc.com/resources/es-mx/asset/white-papers/products/converged-infrastructure/VxRail_Comprehensive_Security_by_Design.pdf
Prácticas de seguridad de productos de Dell Technologies	https://www.delltechnologies.com/es-mx/products/security/index.htm
	YouTube (Recursos de seguridad)
YouTube: visión general de la seguridad de VxRail	https://www.youtube.com/watch?v=ZTNmYBgJv4s
YouTube: endurecimiento y cumplimiento de la seguridad de VxRail	https://www.youtube.com/watch?v=ZjhfCE5nq6U