SEGURANÇA ABRANGENTE POR PADRÃO DOS EQUIPAMENTOS DELL EMC VXRAIL

Resumo

VxRail™ Appliance, a plataforma ideal para a transformação da infraestrutura de TI e da segurança, oferece camadas de proteção para manter seus dados e aplicativos empresariais seguros. Somente a família de empresas da Dell Technologies pode fornecer todas as soluções completas necessárias para acompanhar o ritmo do atual ambiente de ameaças em evolução. Este guia abrange os recursos de segurança integrados e opcionais, as melhores práticas e as técnicas comprovadas para proteger seu VxRail do núcleo à borda e à nuvem.

Março de 2020

Sumário

INTRODUÇÃO

Em todos os setores, as organizações estão modernizando e transformando a maneira como operam e oferecem produtos e serviços diferenciados. Onde os dados residem, como são acessados e o número de dispositivos do núcleo à borda e à nuvem a uma taxa exponencial. A segurança sempre será parte da TI, com foco em autenticação, firewalls, conformidade e criminosos cibernéticos. A segurança não é mais um conjunto de projetos, mas um ciclo de vida contínuo que exige revisão e análise constantes. A Dell Technologies acredita que a segurança nunca poderá atrasar você. Em vez disso, ela acelera a inovação, permitindo que você pense de maneira inédita e estratégica e aproveite as oportunidades.

O Dell EMC VxRail oferece o caminho mais rápido e mais simples para essa transformação da segurança do núcleo à borda e à nuvem. O VxRail oferece uma infraestrutura ágil com integridade da pilha total e gerenciamento do ciclo de vida completo para impulsionar a eficiência operacional, reduzir os riscos e permitir que as equipes se concentrem nos negócios. A adoção dos sistemas VxRail, que rompem com os silos operacionais e possibilitam inovações contínuas por meio do provisionamento rápido e da implementação de cargas de trabalho, resulta em economia significativa e eficiência operacional, permitindo que as organizações de TI gerem oportunidades de negócios em vez de simplesmente dar suporte às operações de negócios. Desenvolvido para a VMware, com a VMware e para aprimorar a VMware, o VxRail é o primeiro e único sistema de HCI projetado para eliminar a complexidade operacional da implementação, do provisionamento, do gerenciamento, do monitoramento e da atualização da infraestrutura hiperconvergente do VxRail.

O VxRail tem segurança incorporada a todos os níveis dos conjuntos de tecnologia integrados. Começando com cada processador e servidor PowerEdge e indo até o software do sistema de HCI do VxRail, inclusive o software VMware integrado. Protegendo o núcleo, a borda e a nuvem, garantindo disponibilidade, integridade e confiança para todas as cargas de trabalho — tradicionais e nativas da nuvem.

A TRANSFORMAÇÃO DA SEGURANÇA COMEÇA COM A DELL TECHNOLOGIES

A transformação da segurança na Dell Technologies se resume a reformular a segurança e acelerar a inovação. A Dell Technologies se concentra em todos os níveis de segurança, desde as colaborações entre as empresas da Dell Technologies até o produto desenvolvido e lançado. O VxRail não é uma exceção, pois é criado com os mais altos níveis de garantia de segurança do produto e oferece recursos de segurança totalmente integrados, que podem ser utilizados pela organização para otimizar a resiliência da segurança cibernética da borda ao núcleo e à nuvem para acelerar a inovação (veja a figura abaixo).

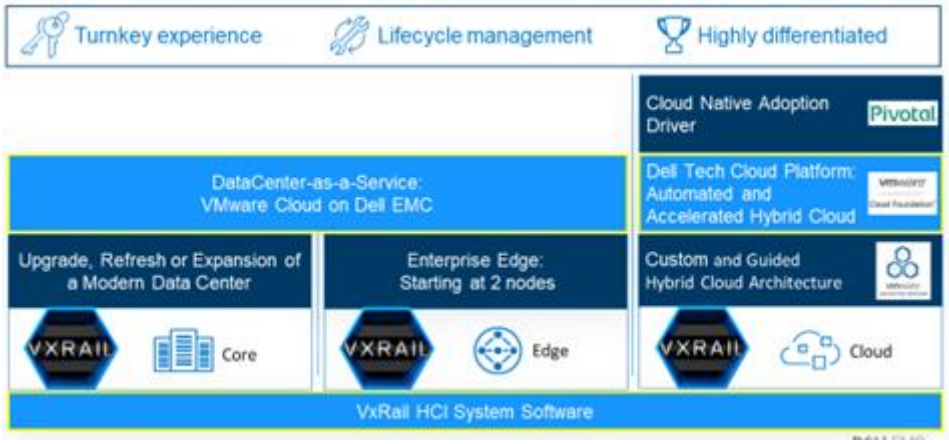

Figura 1: Do núcleo à borda e à nuvem

Relatado pela Forbes; com base em uma pesquisa RiskBased Security publicada recentemente no 2019 MidYear QuickView Data Breach Report, que revela que, nos primeiros seis meses de 2019, o número de violações divulgadas publicamente é superior a 3.800, expondo a incrível quantidade de 4,1 bilhões de registros comprometidos. Com base nesses números, as violações podem superar os 6.515 eventos de comprometimento de dados publicamente divulgados e relatados em 2018 pela mesma empresa.

A Dell Technologies pode garantir que suas estratégias de segurança acompanhem suas iniciativas de modernização para reduzir os riscos aos negócios.

1. Unifique os programas de segurança com o risco geral aos negócios para saber quais riscos valem a pena.
2. Implemente operações avançadas de segurança que se adaptam ao ambiente de ameaças em constante transformação para responder de modo eficaz às ameaças.
3. Construa uma infraestrutura moderna e resiliente que proteja endpoints, rede, aplicativos e dados.
4. Conte com os serviços confiáveis de consultoria para projetar e implementar seu programa de transformação da segurança. A Dell Technologies está exclusivamente posicionada para ajudar você a lidar com todas essas áreas.

Embora seja necessário estabelecer uma defesa em camadas com vários níveis de segurança, todos esses elementos devem funcionar em conjunto. A transformação da segurança começa com uma infraestrutura moderna com resiliência cibernética, como o VxRail, que foi projetado e desenvolvido com foco na segurança.

O atual ambiente de ameaças em evolução exige uma mudança de abordagem para evitar ou reduzir essas ameaças. A infraestrutura ultrapassada é difícil de proteger, e os produtos pontuais de vários fornecedores trazem mais complexidade e aumentam o risco de vulnerabilidades a serem exploradas. Esse nível de complexidade oferece vários pontos de entrada para os agentes mal-intencionados.

O padrão de segurança e a conformidade também precisam ser considerados. Geralmente, há significativas sanções legais e financeiras pela falta de conformidade. E embora sejam dispendiosas, elas podem causar menos impacto sobre as empresas do que uma violação pode causar na reputação da empresa. É menos provável que as pessoas façam negócios com uma empresa que tenha sofrido uma violação.

- Padrão de segurança de dados do setor de cartões de pagamento (PCI DSS) — proteções para titulares de cartão de crédito
- Regulamento geral de proteção de dados (GDPR) — norma de privacidade de dados da União Europeia
- Bundesdatenschutzgesetz alemã (BDSG) — lei de proteção de dados em detalhes
- Lei Sarbanes-Oxley (SOX) — proteção de dados confidenciais relacionados a relatórios financeiros de empresas públicas
- Lei Gramm-Leach-Bliley (GLBA) — proteção de informações pessoais não públicas (NPPI) no setor de serviços financeiros
- Lei de responsabilidade e portabilidade de seguros de saúde (HIPAA) — proteção de informações e dados eletrônicos de pacientes na área de saúde
- Lei de privacidade do consumidor da Califórnia (CCPA) — aprimoramento dos direitos de privacidade e da proteção dos consumidores residentes na Califórnia (em vigor a partir de 28/06/2018)

A Dell Technologies acredita que a transformação da segurança exige trabalhar com um parceiro de confiança, que ajude a gerenciar o risco digital, prestar serviços gerenciados de segurança e disponibilizar especialização, serviços, soluções e produtos que protejam a pilha completa, desde a infraestrutura até os aplicativos, e otimizem as operações, tornando a segurança uma parte essencial da estratégia da empresa.

A Dell Technologies é uma parceira de segurança confiável para a transformação da segurança. Não importa se o foco está em endpoints, data center, desenvolvedores, identidades, operações de segurança, nuvem ou virtualização — a segurança precisa ser completa, e a Dell Technologies pode ajudar. Podemos ajudar a controlar os riscos de segurança e negócios, lidar com violações de segurança, recuperar-se de um ataque de ransomware e criar aplicativos seguros. A segurança significa muitas coisas para muitas pessoas — algumas ruins, outras boas. Independente de qualquer coisa, a Dell Technologies quer acompanhar as organizações na respectiva jornada.

Ponte para o futuro digital

Vivemos em um momento no qual precisamos mais do que nunca da TI para resolver os problemas de negócios. As organizações fazem isso implementando lógica analítica de dados, inteligência artificial, novos aplicativos e dispositivos inteligentes, o que gera enormes volumes de dados. Esses dados geram percepções acionáveis e vantagens competitivas exclusivas. Apesar disso, muitas organizações ainda não têm uma visão e uma estratégia digitais claras. Elas usam tecnologias desatualizadas, o que resulta em restrições e uma cultura resistente à mudança. Sem um plano adequado, o risco e a segurança frequentemente se tornam uma consideração posterior ou simplesmente nunca fazem parte da discussão sobre a estratégia mais ampla. Nesse ponto crucial das tecnologias, essa forma reativa de conduzir os negócios não é mais sustentável. Para acelerar a inovação e concretizar o potencial do futuro digital, as organizações devem repensar como elas entendem a segurança

No universo de TI, a segurança é geralmente vista mais como um obstáculo do que um acelerador de mudanças positivas. No dia a dia, o trabalho pode ser ingrato e os gerentes podem ter dificuldades em ver o retorno sobre o investimento. A equipe de segurança deve gerenciar o acúmulo de ameaças e sistemas complexos e manter um conhecimento prático de um ambiente em constante transformação. O bombardeio aparentemente diário de ataques cibernéticos na imprensa só agrava essa tensão, assim como o sentimento opressor de que tudo o que a organização possui pode ser perdido em um segundo. Mas a segurança não precisa ser forjada por receios e frustrações. A segurança sempre buscou ser mais positiva e proativa, mas isso só é possível com a mentalidade e as tecnologias adequadas. Não podemos mais continuar abordando a segurança e os riscos como fazíamos no passado. Para colocar essa mudança em perspectiva, pense nos freios de um carro. Inicialmente, você pode pensar que os freios só servem para reduzir a velocidade, mas eles também permitem que você vá mais rápido. Eles dão confiança para você acelerar e, ao mesmo tempo, o preparam para os obstáculos e para a estrada à sua frente. A segurança e o risco também precisam ser vistos como aceleradores para as organizações, e não algo que as atrase.

COMO CONQUISTAR A CONFIANÇA COM OS PROGRAMAS DE SEGURANÇA DE PRODUTO DA DELL EMC

A Dell EMC começou a formular suas políticas de segurança de produtos em 2002, quando a empresa deixou de ser basicamente uma fornecedora de hardware para armazenamento e passou a atuar como fornecedora de software de classe empresarial. A empresa lançou seu programa de resposta a vulnerabilidades em 2004 e estabeleceu uma política de segurança de produto em toda a empresa em 2005. A política decreta padrões de segurança amplos, porém claros, que englobam a gama completa de produtos da Dell EMC. Essa política foi continuamente atualizada e, em 2007, foi integrada ao novo ciclo de vida de desenvolvimento da segurança (SDL) da empresa. O SDL introduziu uma série de práticas de segurança mensuráveis e reproduzíveis em todas as etapas do desenvolvimento e da implementação de produtos. Em 2012, a empresa também formalizou um programa de gerenciamento de riscos da cadeia de suprimentos para estender as práticas de segurança aos fornecedores de componentes dos produtos da Dell EMC. A Dell EMC continua a desenvolver seus programas de segurança de produto e está sempre na vanguarda dos processos e padrões do setor.

Com o VxRail, a Dell EMC continua seu compromisso com a segurança. O ciclo de vida do desenvolvimento do VxRail segue o processo de desenvolvimento da segurança de produto da Dell EMC integrado ao ciclo de vida de desenvolvimento da segurança. O ciclo de vida de desenvolvimento da segurança da Dell EMC segue uma abordagem rigorosa para proteger o desenvolvimento de produtos e envolve o gerenciamento de riscos em nível executivo antes que os produtos sejam enviados ao mercado. Além disso, o VMware vSphere é uma parte significativa da infraestrutura hiperconvergente do VxRail, que também foi desenvolvida com o uso de um ciclo de vida semelhante de desenvolvimento da segurança.

Ciclo de vida de desenvolvimento seguro (SDL)

O ciclo de vida de desenvolvimento da segurança da Dell EMC descreve o conjunto de atividades necessárias durante todo o ciclo de vida do produto para incorporar resiliência e recursos de segurança consistentes aos produtos e responder prontamente às vulnerabilidades de segurança relatadas externamente. Alinhada às melhores práticas do setor, a Dell EMC se baseia em um conjunto de controles que são implementados pelas organizações de pesquisa e desenvolvimento de produtos. A Figura 2 mostra algumas das atividades típicas executadas como parte do SDL.

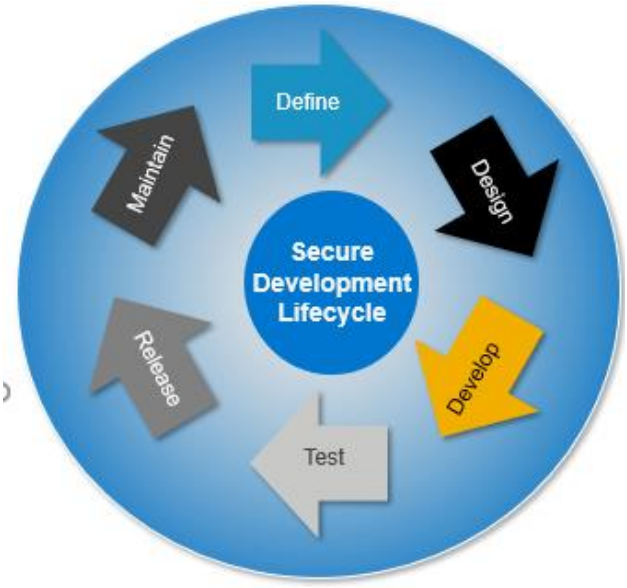

Figura 2: Atividades do SDL da Dell EMC

A implementação e validação desses controles são orientadas pelos líderes de segurança das organizações de pesquisa e desenvolvimento de produtos, que trabalham em estreita colaboração com os consultores de segurança do escritório de segurança de produto (PSO). A Figura 3 ilustra a associação desse SDL a um típico ciclo de vida 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 e um típico ciclo de vida ágil

A pontuação é um mecanismo usado em todos os negócios da Dell EMC para capturar a postura de segurança de um produto/solução quando ele atinge a data de disponibilidade direcionada/disponibilidade geral (DA/GA).

Desenvolvimento seguro

A abrangente abordagem da Dell EMC para o desenvolvimento seguro se concentra em minimizar os riscos de vulnerabilidades de software e as fragilidades de design nos produtos.

Essa abordagem abrangente para o desenvolvimento de software seguro atravessa políticas, pessoas, processos e tecnologias e inclui o seguinte:

- A política de segurança de produto da Dell EMC é uma referência comum às organizações de produtos da Dell EMC para avaliar a segurança do produto em relação às expectativas do mercado e às melhores práticas do setor.
- As equipes de engenharia da Dell EMC são uma comunidade de engenharia consciente da segurança. Todos os engenheiros participam de um programa de engenharia de segurança baseado em função para receber treinamento sobre as melhores práticas de segurança específicas ao trabalho e sobre como usar os recursos relevantes. A Dell EMC se esforça para criar uma cultura que reconheça a segurança em toda a sua comunidade de engenharia.
- O processo de desenvolvimento da Dell EMC é seguro e reproduzível. O SDL sobrepõe os processos de desenvolvimento padrão para obter um alto grau de conformidade com a política de segurança de produto da Dell EMC.
- As equipes de desenvolvimento da Dell EMC se baseiam nas melhores tecnologias de segurança da categoria. A Dell EMC desenvolveu um conjunto de software, padrões, especificações e designs para os elementos comuns de segurança de software, como autenticação, autorização, auditoria, responsabilidade, criptografia e gerenciamento de chaves, usando a tecnologia RSA de última geração. Quando apropriado, interfaces abertas são usadas, o que permite a integração com as arquiteturas de segurança existentes dos clientes.
- O SDL da Dell EMC sobrepõe a segurança em processos de desenvolvimento padrão para obter um alto grau de conformidade com a política de segurança de produto da Dell EMC. O SDL da Dell EMC segue uma abordagem rigorosa para proteger o desenvolvimento de produtos, que envolve o gerenciamento de riscos em nível executivo antes de os produtos serem enviados ao mercado.
- O SDL faz parte de um conjunto mais amplo de processos que existem dentro do padrão de design seguro. O padrão de design seguro é a referência de desempenho para incorporar a segurança aos produtos da Dell EMC. O padrão está relacionado à segurança dos recursos de todos os produtos e descreve a funcionalidade de segurança obrigatória, que deve ser integrada a qualquer produto fornecido pela Dell EMC aos clientes. Este padrão permite aos produtos da Dell EMC:
    - Atender aos rigorosos requisitos de segurança dos clientes,
    - Ajudar os clientes a cumprir requisitos regulamentares, como PCI, HIPPA etc.,
    - Minimizar os riscos para os produtos da Dell EMC e os ambientes dos clientes oriundos de vulnerabilidades de segurança.
    - A proteção do código-fonte identifica como proteger adequadamente os sistemas de engenharia da Dell EMC que contêm o código-fonte da propriedade intelectual relacionada ao produto e como garantir a integridade dos produtos implementados nos ambientes dos clientes.

Resposta a vulnerabilidades da Dell EMC

As vulnerabilidades de segurança em qualquer componente do sistema podem ser usadas por invasores, que podem se infiltrar e comprometer toda a infraestrutura de TI. O tempo entre a detecção inicial das vulnerabilidades e a disponibilidade de uma correção se transforma em uma corrida entre os invasores e os defensores. A maior prioridade da Dell EMC é minimizar essa lacuna de tempo para reduzir os riscos.

A equipe de resposta a incidentes de segurança de produtos (PSIRT) da Dell é responsável por coordenar a resposta e a divulgação de todas as vulnerabilidades de produtos da Dell EMC identificadas externamente. A PSIRT oferece aos clientes informações em tempo hábil, orientação e estratégias de redução para lidar com as ameaças das vulnerabilidades.

Qualquer pessoa pode notificar a Dell — por meio do site da empresa ou por e-mail — sobre possíveis falhas de segurança em seus produtos. Todos os avisos são investigados, validados, corrigidos e relatados de acordo com as diretrizes do setor.

A Dell divulga informações sobre vulnerabilidades de produtos simultaneamente a todos os clientes. Os assessores da empresa identificam a gravidade das vulnerabilidades e distribuem as informações usando vários sistemas padronizados de geração de relatórios. Como o restante de nossas práticas de segurança de produtos, a política de divulgação da Dell é baseada nas melhores práticas do setor.

Gerenciamento de riscos da cadeia de fornecimento

Programas bem-sucedidos de segurança de produtos são abrangentes e se estendem a componentes e produtos de software terceirizados. Os testes de integridade na cadeia de suprimentos são um componente essencial do fortalecimento e da preservação da confiança. A Dell Technologies tem um programa formal de gerenciamento de riscos da cadeia de suprimentos que garante que os componentes de hardware utilizados nos produtos da empresa sejam originários de fontes adequadamente verificadas.

A segurança da cadeia de suprimentos é definida como a prática e aplicação de medidas preventivas e detectoras de controle que protegem ativos físicos, inventário, informações, propriedade intelectual e pessoas. Lidar com a segurança física, de informações e de pessoas ajuda a proporcionar garantia da cadeia de suprimentos reduzindo as oportunidades de introdução mal-intencionada de malware e componentes desconhecidos.

A estrutura de gerenciamento de riscos da cadeia de suprimentos Dell (abaixo) espelha a abrangente estrutura de gerenciamento de riscos do plano nacional de proteção de infraestrutura (NIPP), que descreve como o governo e o setor privado podem trabalhar juntos para reduzir riscos e cumprir os objetivos de segurança. A estrutura da Dell incorpora um circuito de feedback aberto que permite fazer melhorias contínuas. Os planos de diminuição de risco são priorizados e implementados conforme apropriado durante todo o ciclo de vida das soluções. A Figura 4 ilustra o processo de gerenciamento de riscos da cadeia de suprimentos.

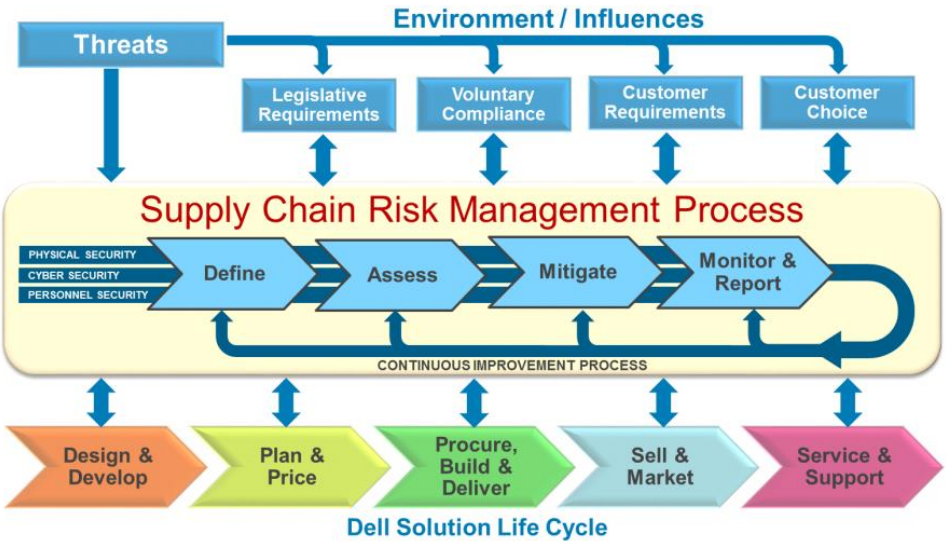

Figura 4: Processo de gerenciamento de riscos da cadeia de suprimentos da Dell

Colaboração do setor para aprimorar a segurança dos produtos

A Dell Technologies acredita que uma abordagem colaborativa é a maneira mais eficiente e eficaz de lidar com as ameaças de segurança que surgem constantemente e podem se espalhar rapidamente entre as organizações por meio dos atuais sistemas densamente interconectados.

Considerando os riscos mais altos, os provedores de tecnologia devem deixar de lado seus objetivos de competição no mercado quando se trata da segurança dos produtos. Nenhum fornecedor individual pode solucionar todos os problemas de segurança dos produtos de TI. A segurança de TI é uma iniciativa coletiva e colaborativa. A Dell Technologies acredita que a colaboração com outras empresas é essencial para garantir que o mercado continue sendo um local onde todos possam prosperar.

As décadas dedicadas à segurança dos produtos ajudaram a Dell Technologies a estabelecer um rico histórico de melhorias bem-sucedidas e percepções, e a empresa compartilha abertamente o que aprendeu com seus clientes, colegas e parceiros. A Dell Technologies entende que os sistemas de TI dos clientes não são executados exclusivamente em produtos da Dell Technologies e, portanto, ela assume o compromisso de aprimorar a segurança do ecossistema onde o produto opera. Isso significa ser um participante ativo e um colaborador positivo em todo o setor.

O longo compromisso da Dell Technologies com o avanço da segurança dos produtos resultou no dever de auxiliar e promover os membros mais novos do setor. Os líderes de segurança de produtos da empresa facilitam a troca aberta de ideias em conferências, por meio de postagens do blog e em outros locais sociais e formais.

Participação em grupos de segurança de produtos do setor

A Dell Technologies participa ativamente de grupos de segurança de produtos, onde aprende e ensina sobre as melhores práticas progressivas e cultiva um senso de responsabilidade comunitária pela segurança dos produtos. As afiliações da Dell Technologies no setor incluem:

BSIMM — o Building Security in Maturity Model avalia as iniciativas de segurança de software do setor para que as organizações possam enxergar onde seus esforços de segurança se encontram e como elas devem desenvolvê-los.

The Open Group — este consórcio de 400 membros executa programas respeitados de certificação para a equipe de TI, os produtos e os serviços a fim de projetar e aprimorar os padrões de TI. O consórcio The Open Group trabalha para entender os requisitos de TI atuais e emergentes e estabelecer ou compartilhar as melhores práticas para cumpri-los

SAFECode — o Software Assurance Forum for Excellence in Code, cofundado pela Dell EMC, é um esforço liderado pelo setor a fim de identificar e promover melhores práticas para fornecer software, hardware e serviços mais seguros e confiáveis.

CSA — a Cloud Security Alliance é uma organização líder mundial dedicada a definir e gerar conscientização sobre melhores práticas para ajudar a garantir um ambiente computacional de nuvem seguro.

FIRST — o Forum of Incident Response and Security Teams é um reconhecido líder global em resposta a incidentes. A PSIRT da Dell faz parte do FIRSTVxRailteam.

VxRail: a base para a modernização do data center e a transformação da TI

Para vencer a corrida contra o ambiente de ameaças à segurança em constante evolução, o VxRail tem adaptabilidade para oferecer proteção contra ameaças atuais e futuras. O VxRail foi desenvolvido com base na geração atual de servidores Dell PowerEdge e nas mais recentes tecnologias de processadores, o que oferece uma plataforma segura e opções flexíveis de configuração. O vSphere oferece virtualização de servidores e do armazenamento. À medida que aumentam os requisitos das cargas de trabalho, o VxRail é facilmente dimensionado. Conforme as normas se transformam, as opções flexíveis de configuração do VxRail permitem que ele se adapte

O VxRail pode ajudar sua organização a otimizar a resiliência cibernética, gerenciar riscos e cumprir os requisitos de conformidade, independentemente do setor em que sua organização opera. O VxRail é o único equipamento de infraestrutura hiperconvergente totalmente integrado, pré-configurado, testado e habilitado pelo VMware vSAN. Independentemente de ser implementado no data center, na borda ou como parte de uma solução de nuvem híbrida, o VxRail oferece aplicativos essenciais aos negócios, VDI e infraestrutura remota com mais qualidade, simplicidade e segurança. O VxRail permite que a Dell EMC forneça aos clientes os recursos necessários para otimizar a resiliência cibernética em toda a implementação. A Figura 5 abaixo ilustra a segurança integrada ao VxRail

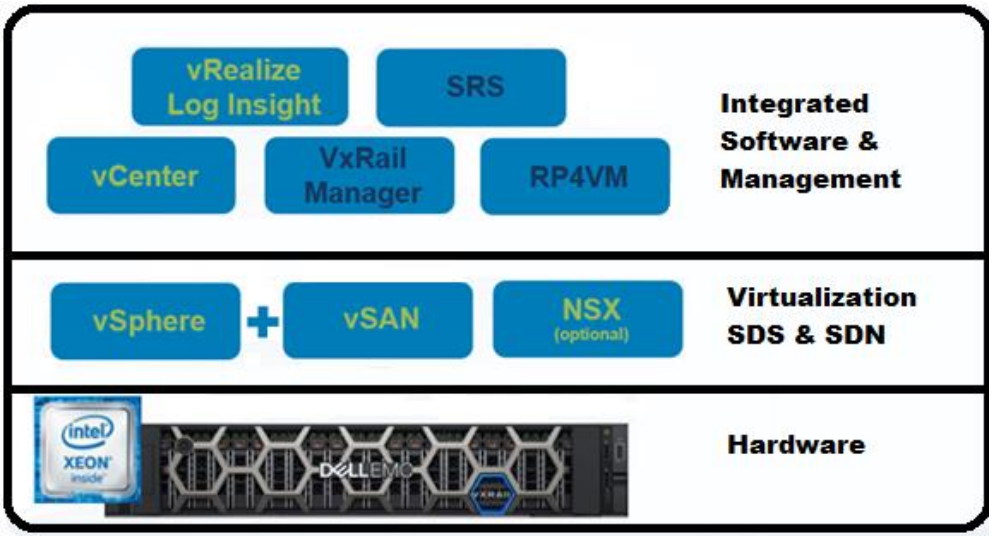

Figura 5: Segurança integrada ao VxRail

Servidores Dell EMC PowerEdge

O VxRail se baseia na plataforma de servidor Dell PowerEdge com hardware incorporado e recursos de segurança no nível do sistema para proteger a infraestrutura com camadas de defesa. As violações são rapidamente detectadas, o que permite que o sistema se recupere para uma linha de base confiável. Os recursos de segurança diferenciados dos servidores PowerEdge incluem:

- Bloqueio do sistema para impedir alterações inadvertidas ou não autorizadas. Esse recurso pioneiro no setor impede as alterações de configuração que criam vulnerabilidades de segurança e expõem dados confidenciais.
- A arquitetura com resiliência cibernética e recursos, como inicialização segura de UEFI, recuperação de BIOS e firmware assinado, oferece proteção aprimorada contra ataques.
- O recurso de apagamento do sistema no nível do servidor garante a privacidade ao apagar com rapidez e segurança todos os dados do usuário da unidade e toda a memória não volátil quando um servidor é desativado.

Os servidores Dell EMC PowerEdge são o hardware essencial que compõe os nós de um cluster do VxRail. A CPU, a memória e os discos em cada nó oferecem os recursos agrupados para o cluster, e as interfaces de rede oferecem a conectividade. Portanto, os servidores seguros Dell EMC PowerEdge são a base da segurança do VxRail.

Os servidores PowerEdge têm um controlador de acesso remoto integrado conhecido como iDRAC. O iDRAC usa comunicação segura, autenticação e controles de acesso baseado em função para permitir a configuração e o gerenciamento remotos e seguros do sistema físico. Com alertas configuráveis, o iDRAC pode enviar informações de eventos para o sistema de gerenciamento de eventos e incidentes de segurança (SIEM) sempre que o hardware é acessado ou a configuração é alterada. A detecção e a geração de relatórios de alterações não autorizadas protegem a integridade do VxRail. Para obter mais informações, consulte Cyber Resilient Security in 14th Generation of Dell EMC PowerEdge.

Os servidores PowerEdge usam firmware com assinatura e verificação criptográficas para criar um sistema de confiança. Aproveitando as tecnologias de segurança incorporadas ao silício. Recursos como a Trusted Execution Technology (TXT) da Intel verificam se o servidor executa apenas a versão pretendida do firmware, BIOS e hypervisor, evitando a introdução de malware não detectado. A Figura 6 abaixo ilustra a raiz de confiança do hardware.

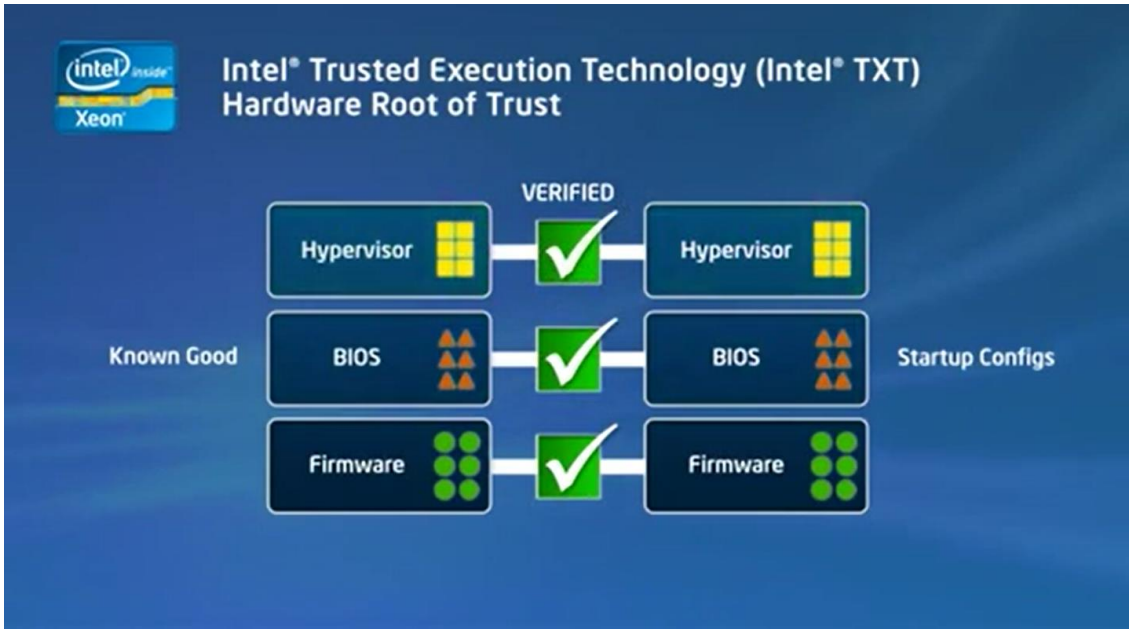

Figura 6: Raiz de confiança do hardware

O VxRail pode obter níveis ainda mais altos de proteção da integridade dos servidores, configurando os nós com um módulo Trusted Platform Management (TPM) opcional (TPM 1.2 e 2.0). O TPM é um padrão internacional para criptoprocessadores seguros, um microcontrolador dedicado que foi projetado para oferecer alta segurança para chaves de criptografia e uma opção para todos os nós do VxRail.

Software do sistema de HCI do Dell EMC VxRail

O software do sistema de HCI do VxRail é a base dos recursos com diferenciação de valor do VxRail. Sob a perspectiva da pilha da infraestrutura, é o software de gerenciamento que é executado em conjunto com o software da VMware e o servidor PowerEdge para permitir que o VxRail atue como um sistema unificado singular.

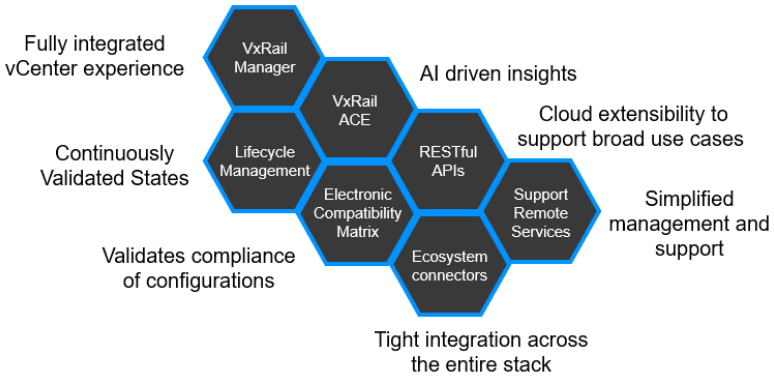

Figura 7: Software do sistema de HCI do VxRail

Estados validados continuamente — o VxRail é executado em software e firmware testados previamente e validados para toda a pilha do VxRail, inclusive os componentes do software da VMware e do servidor PowerEdge. Os recursos de gerenciamento do ciclo de vida do VxRail garantem que os clusters do VxRail sejam executados nesse estado bom e conhecido durante todo o ciclo de vida, à medida que o cluster passa por mudanças contínuas para aproveitar as mais recentes inovações de software da VMware, reparos de segurança ou correções de bugs. O termo “estados validados continuamente” abrange a estabilidade de configuração oferecida pelos clusters do VxRail.

Matriz de compatibilidade eletrônica — com todos esses diferentes componentes de software e hardware na pilha, a equipe do VxRail faz testes e validações constantes em toda a pilha para que o estado desejado que o usuário determina a partir da matriz de compatibilidade da VMware seja confirmado como um estado validado continuamente. Além disso, o VxRail consulta essa matriz para garantir que a configuração em cluster continue em conformidade. Esses benefícios reduzem drasticamente o esforço de teste e os recursos que um cliente precisaria investir, oferecendo também ao cliente a tranquilidade de que ele precisa para evoluir seus clusters do VxRail de modo previsível e seguro, sem afetar as cargas de trabalho dos aplicativos.

Conectores de ecossistema — para criar uma extensa matriz de compatibilidade eletrônica, o VxRail precisa conseguir se comunicar com os membros do ecossistema na pilha, o que inclui o vSphere, vSAN, vCenter e o servidor PowerEdge, além de vários componentes de hardware. Os conectores permitem que o VxRail saiba as versões de software/firmware executadas em cada componente e gerencie o ciclo de vida desses componentes. Os recursos de automação e orquestração permitem que o VxRail seja gerenciado como um sistema singular e unificado.

VxRail Manager — a principal interface do usuário de gerenciamento do VxRail é o plug-in do vCenter chamado VxRail Manager. Os usuários do VxRail podem executar qualquer atividade do VxRail por meio dessa interface, inclusive a configuração inicial do cluster, o monitoramento dos componentes de hardware, a execução do desligamento uniforme de clusters, a expansão do cluster pela adição de nós e a atualização do software do sistema de HCI do VxRail. Ele proporciona uma experiência no vCenter totalmente integrada.

VxRail ACE (Analytical Consulting Engine) — à medida que aprimoramentos são feitos para melhorar a experiência de gerenciamento do ciclo de vida do VxRail, uma grande parte disso dependerá dos recursos de computação analítica do VxRail ACE. ACE significa mecanismo de consultoria analítica. Por meio da telemetria avançada que o software do sistema de HCI reúne sobre os clusters do VxRail, o ACE é usado para apresentar percepções orientadas por IA que permitirão aos usuários gerenciar proativamente seus clusters para melhorar o desempenho e a disponibilidade. As percepções orientadas por IA também estão gerando recursos mais ativos de gerenciamento de vários clusters no ACE, que é uma área na qual os usuários da HCI terão um interesse cada vez maior à medida que expandirem o respectivo espaço ocupado pela HCI e o gerenciamento em escala se tornar uma necessidade.

APIs REST — os benefícios do VxRail para o gerenciamento do ciclo de vida se posicionam de maneira ideal como a plataforma de infraestrutura preferida, já que o foco na simplificação das operações de TI desempenha um papel fundamental para permitir que as equipes de TI se concentrem em modelos de prestação de serviços de TI. Tornar a plataforma VxRail extensível por meio de APIs permite que os clientes façam a integração de soluções de infraestrutura como serviço. As APIs também permitem o gerenciamento em escala, que pode beneficiar os clientes com um grande número de clusters do VxRail implementados em várias localizações, que escolheram soluções de script internas para o gerenciamento em escala.

Serviços de suporte remoto — a experiência de suporte também pode ser um fator essencial na escolha da solução de HCI adequada. O VxRail dá suporte de fornecedor único para o software da VMware, o servidor PowerEdge e o software do VxRail, tudo por meio do suporte técnico da Dell. O suporte do VxRail inclui o Dell EMC Secure Remote Services para call home e conexão remota proativa e bidirecional para fins de monitoramento, diagnóstico e reparo remotos durante todo o processo do ciclo de vida a fim de garantir a disponibilidade máxima.

VMware vSphere

A suíte de software VMware vSphere oferece ao VxRail uma infraestrutura virtualizada, resiliente, sob demanda e altamente disponível. ESXi, vSAN e vCenter Server são componentes essenciais do vSphere. O ESXi é um hypervisor instalado em um nó de servidor físico do VxRail na fábrica, que permite que um único servidor físico hospede vários servidores lógicos ou VMs. O vSAN é o armazenamento definido por software usado pelas VMs, e o VMware vCenter Server é o aplicativo de gerenciamento de hosts do ESXi, vSAN e VMs.

O vSphere Platinum é uma solução de segurança de uso específico projetada para proteger aplicativos, infraestrutura, dados e o acesso a eles. Ele combina dois produtos comprovados: o vSphere, para proteger a infraestrutura, os dados e o acesso, e o AppDefense, para proteger os aplicativos em execução nas VMs. O AppDefense protege a integridade dos aplicativos em execução no vSphere usando aprendizagem automática para compreender o estado e o comportamento pretendidos do aplicativo e da máquina a fim de detectar e evitar ameaças. Os clientes do VxRail que compraram licenças Platinum (inclusive assinaturas) da VMware têm o direito de usar a licença Platinum no VxRail executando o vSphere Enterprise Plus. É importante observar que o LCM do AppDefense do vSphere Platinum é de responsabilidade do cliente

Como a Dell EMC, a VMware segue um rigoroso processo de ciclo de vida de desenvolvimento de software seguro e um centro de resposta de segurança. O VxRail é desenvolvido em conjunto e é compatível com a VMware, garantindo que todos os componentes incluídos na solução sejam projetados, criados, testados e implementados tendo a segurança como prioridade máxima. Para obter mais informações, consulte VMware Product Security

VMware vCenter Server

O vCenter Server é o principal ponto de gerenciamento da virtualização de servidores e do armazenamento do vSAN. Uma única instância do vCenter pode ser dimensionada para níveis empresariais, comportando centenas de nós do VxRail e milhares de VMs. O VxRail pode usar uma instância do vCenter implementada no cluster do VxRail ou usar uma instância existente do vCenter.

O vCenter fornece uma hierarquia lógica de data centers, clusters e hosts. Essa hierarquia facilita a segmentação de recursos por caso de uso ou linhas de negócios, além de permitir que os recursos sejam movidos dinamicamente, conforme necessário. Isso tudo é feito a partir de uma única interface intuitiva.

O vCenter Server oferece serviços de VM e recursos, como serviço de inventário, programação de tarefas, log de estatísticas, alarmes e gerenciamento de eventos, além de provisionamento e configuração de VMs. O vCenter Server também oferece recursos avançados de disponibilidade, inclusive:

- vSphere vMotion — permite a migração de cargas de trabalho de VMs em tempo real sem tempo de inatividade
- vSphere Distributed Resource Scheduler (DRS) — equilibra e otimiza continuamente a alocação de recursos de computação das VMs em todos os nós do cluster
- vSphere High Availability (HA) — oferece recursos de failover e reinicialização de VMs

Hypervisor VMware ESXI

No VxRail, o hypervisor ESXi hospeda a VM nos nós do cluster. As VMs são seguras e portáteis, e cada VM é um sistema completo com processadores, memória, sistema de rede, armazenamento e BIOS. As VMs são isoladas umas das outras. Portanto, quando um sistema operacional convidado em execução em uma VM falhar, outras VMs no mesmo host físico não serão afetadas e continuarão sendo executadas. As VMs compartilham o acesso às CPUs, e o ESXi é responsável pela programação da CPU. Além disso, o ESXi atribui uma região de memória utilizável às VMs e gerencia o acesso compartilhado às placas de rede física e aos controladores de disco associados ao host físico. Todos os sistemas operacionais baseados em x86 são aceitos, e as VMs no mesmo hardware de servidor físico podem executar diferentes sistemas operacionais e aplicativos.

Sistema de rede virtual da VMware

Um requisito de segurança fundamental é isolar o tráfego de rede. No VxRail, os recursos de sistema de rede virtual do vSphere oferecem conectividade e isolamentos flexíveis. As VMs do VxRail se comunicam entre si usando o VMware Virtual Distributed Switch (VDS), que funciona como um único switch lógico que abrange vários nós no mesmo cluster. O VDS usa protocolos de rede padrão e implementações de VLAN, além de encaminhar quadros na camada do link de dados.

O VDS é configurado no nível do data center no vCenter Server, mantendo a configuração de rede segura e consistente à medida que as VMs migram entre vários hosts. O equipamento VxRail conta com o VDS para seu tráfego, e o vSAN conta com o VDS para seu acesso à rede.

Além disso, o VxRail pode ser configurado com o NSX para oferecer segurança de rede definida por software e controle de acesso de nível mais alto usando a microssegmentação.

VMware vSAN

Os equipamentos VxRail são habilitados pelo VMware vSAN para o armazenamento definido por software de classe empresarial. O vSAN agrega os discos dos hosts anexados localmente em um cluster do vSphere para criar um pool de armazenamento compartilhado distribuído. O scale-up da capacidade é feito com a adição de discos extras ao cluster. Já o scale-out é feito com a adição de nós do VxRail extras. O vSAN é totalmente integrado ao vSphere e funciona perfeitamente com outros recursos do vSphere.

O vSAN é notável por seu desempenho e eficiência. O vSAN é otimizado automaticamente e equilibra a alocação com base na carga de trabalho, na utilização e na disponibilidade de recursos. O vSAN oferece uma HCI de alto desempenho e otimizada para flash, que é adequada para uma variedade de cargas de trabalho. Os recursos de armazenamento de classe empresarial incluem:

- Tecnologia eficiente de redução de dados, inclusive desduplicação e compactação, bem como codificação de eliminação
- Políticas de QoS para controlar o consumo das cargas de trabalho com base em limites definidos pelo usuário
- Tecnologia de integridade e proteção de dados, inclusive somas de verificação de software e domínios de falha
- Segurança avançada com criptografia de dados em repouso do vSAN

Com o vSAN, os discos em cada nó do VxRail são organizados automaticamente em grupos de discos com uma única unidade de cache e uma ou mais unidades de capacidade. Esses grupos de discos são utilizados para formar um único datastore do vSAN, que pode ser acessado em todos os nós de um cluster do VxRail.

O VxRail oferece duas opções diferentes de configuração de armazenamento de nós do vSAN: uma configuração híbrida, que usa SSDs flash e discos rígidos mecânicos, e uma configuração de SSD All-Flash. A configuração híbrida usa SSDs flash para o armazenamento em cache e discos rígidos mecânicos para a capacidade e o armazenamento persistente de dados. A configuração All-Flash usa SSDs flash para o armazenamento em cache e a capacidade. A Figura 8 ilustra os conceitos básicos do vSAN.

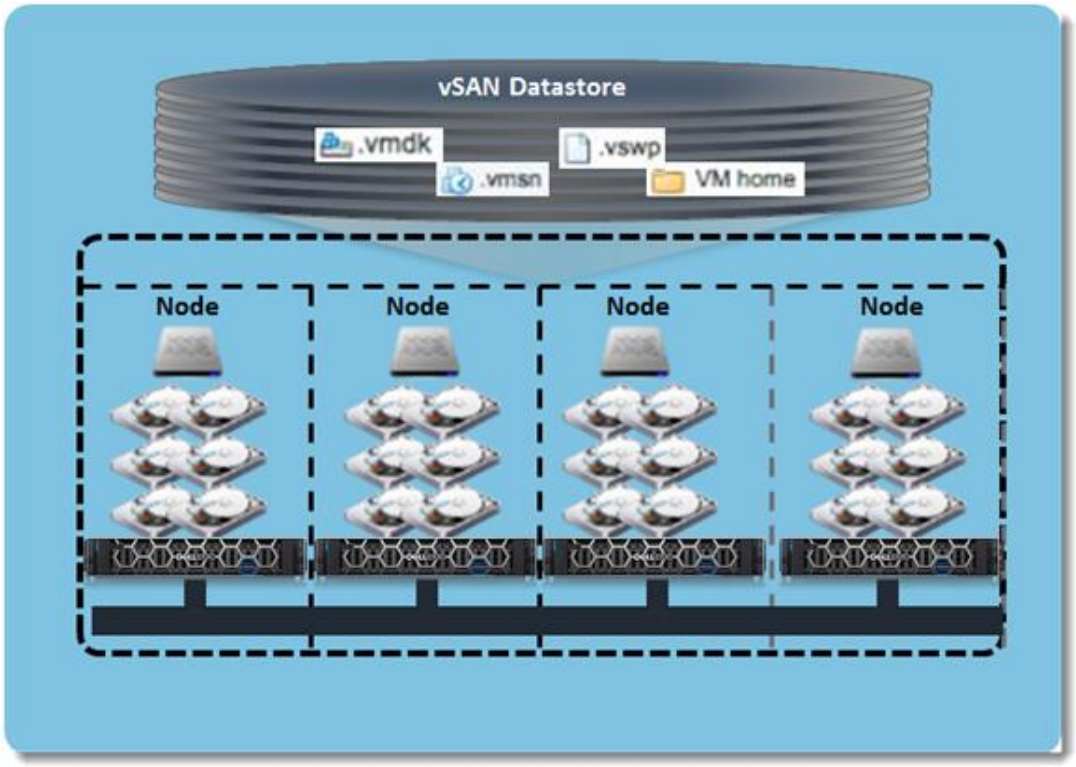

Figura 8: Conceitos básicos do vSAN

O vSAN é configurado quando o cluster do VxRail é inicializado pela primeira vez e gerenciado pelo vCenter. Durante o processo de inicialização do equipamento VxRail, o vSAN cria um datastore compartilhado e distribuído dos discos localmente conectados em cada nó do ESXi. O volume de armazenamento no datastore é uma agregação de todas as unidades de capacidade no cluster. O volume de armazenamento utilizável dependerá do nível de proteção usado. A configuração e a verificação do vSAN orquestradas e executadas como parte da inicialização do sistema garantem o desempenho consistente e previsível e uma configuração de sistema que segue as melhores práticas.

Gerenciamento baseado em política de armazenamento (SPBM)

O vSAN é orientado por políticas e projetado para simplificar o provisionamento e o gerenciamento do armazenamento. As políticas de armazenamento do vSAN são baseadas em conjuntos de regras que definem o requisito de armazenamento para VMs. Os administradores podem alterar dinamicamente a política de armazenamento de uma VM à medida que os requisitos mudam. Exemplos de regras de SPBM são o número de falhas a serem toleradas, a técnica de proteção de dados a ser usada e se as somas de verificação no nível do armazenamento estão ativadas.

VMware vRealize Log Insight

Incluído com o VxRail, o VMware vRealize Log Insight monitora os eventos do sistema e oferece notificações contínuas e abrangentes sobre o estado do ambiente virtual e do hardware do equipamento. O vRealize Log Insight oferece gerenciamento de eventos automatizado e em tempo real para o equipamento VxRail com monitoramento de log, agrupamento inteligente e lógica analítica para simplificar a solução de problemas em escala nos ambientes físico, virtual e de nuvem do VxRail. O log centralizado é um requisito fundamental de uma infraestrutura segura. Para os clientes que já têm uma instalação de log ou SIEM, o VxRail se integra facilmente usando o protocolo de syslog padrão do setor.

VMware Cloud Foundation (VCF) — inclusive NSX

O VMware Cloud Foundation on VxRail é uma solução integrada e projetada em conjunto pela Dell EMC e VMware com recursos que simplificam, otimizam e automatizam as operações de todo o data center definido por software (SDDC) do dia zero ao segundo dia. A nova plataforma oferece um conjunto de serviços definidos por software para computação (com vSphere e vCenter), armazenamento (com vSAN), sistema de rede (com NSX), segurança e gerenciamento da nuvem (com vRealize Suite) em ambientes privados e públicos, o que o torna o hub operacional de sua nuvem híbrida.

O VMware Cloud Foundation on VxRail oferece o caminho mais simples para a nuvem híbrida por meio de uma Hybrid Cloud Platform totalmente integrada que utiliza recursos de hardware e software nativos do VxRail e outras integrações exclusivas do VxRail (como plug-ins do vCenter e sistema de rede da Dell EMC). Esses componentes trabalham juntos para proporcionar uma nova experiência turnkey de nuvem híbrida aos usuários com integração da pilha total. A integração da pilha total significa que você obtém a camada de infraestrutura de HCI e a pilha de software de nuvem em uma única experiência de ciclo de vida turnkey, completa e automatizada.

O VMware NSX Data Center é a plataforma de segurança e virtualização de rede que habilita a rede virtual da nuvem. Trata-se de uma abordagem definida por software para o sistema de rede, que se estende por data centers, nuvens, endpoints e localizações de borda. Com o NSX Data Center, as funções de rede, inclusive comutação, roteamento, firewall e balanceamento de carga, ficam mais próximas ao aplicativo e são distribuídas por todo o ambiente. Semelhante ao modelo operacional das VMs, as redes podem ser provisionadas e gerenciadas de modo independente do hardware subjacente.

O NSX Data Center reproduz o modelo de rede completo no software, permitindo que qualquer topologia de rede, desde redes simples até redes complexas de várias camadas, seja criada e provisionada em segundos. Os usuários podem criar várias redes virtuais com requisitos diversos, aproveitando uma combinação dos serviços oferecidos pelo NSX, inclusive microssegmentação, ou de um amplo ecossistema de integrações de terceiros, que variam desde firewalls de última geração até soluções de gerenciamento de desempenho, para criar ambientes inerentemente mais ágeis e seguros. Esses serviços podem ser estendidos a uma série de endpoints dentro da nuvem e entre nuvens. Para obter mais informações, consulte o VMware Cloud Foundation on VxRail Architecture Guide

Recursos de segurança do VxRail

Os recursos de segurança são divididos em duas seções: Segurança de dados e Segurança do sistema. A configuração e o gerenciamento seguros do sistema do VxRail seguem os princípios da tríade de confidencialidade/integridade/disponibilidade (CIA).

O VxRail oferece uma pilha totalmente pré-configurada e testada para todos os recursos de segurança. Esses recursos de segurança são integrados e incluídos no equipamento.

SEGURANÇA DE DADOS

A segurança de dados segue a tríade CIA para garantir que os dados estejam disponíveis apenas às contas autorizadas e/ou específicas. Que a conformidade e as especificações sejam atendidas. Isso inclui o acesso físico e em nível de usuário aos dados.

Confidencialidade

Impedir que as informações confidenciais cheguem às pessoas erradas e, ao mesmo tempo, garantir o acesso autorizado e adequado aos dados de uma empresa é um problema fundamental resumido como confidencialidade ou privacidade. O VxRail aborda de várias maneiras diferentes a confidencialidade dos dados em uso, dos dados em movimento e dos dados em repouso.

Criptografia

A criptografia protege a confidencialidade das informações por meio da codificação para torná-las ininteligíveis aos destinatários não autorizados. Com o VxRail, os datastores podem ser criptografados usando a criptografia de dados em repouso (D@RE) do vSAN, que oferece proteção validada por FIPS 140-2 de nível 1. As VMs individuais podem ser criptografadas usando a criptografia do vSphere, e as VMs em movimento podem ser criptografadas usando a criptografia do vMotion. Níveis adicionais de criptografia podem ser configurados com base nos requisitos dos aplicativos.

A criptografia do vSAN é a maneira mais fácil e flexível de criptografar os dados em repouso, pois todo o datastore do vSAN é criptografado com uma única configuração. Essa criptografia abrange todo o cluster para todas as VMs que usam o datastore. Normalmente, os dados criptografados não se beneficiam das técnicas de redução de espaço, como desduplicação ou compactação. No entanto, com o vSAN, a criptografia é executada após a desduplicação e a compactação e, portanto, a vantagem completa dessas técnicas de redução de espaço é mantida.

A criptografia de VMs oferece a flexibilidade para ativar a criptografia por VM, o que significa que um único cluster pode ter VMs criptografadas e não criptografadas. A criptografia de VMs segue a VM onde quer que ela esteja hospedada. Portanto, mesmo que a VM seja movida para um datastore fora do VxRail, ela permanecerá criptografada.

Além disso, embora a criptografia de VMs possa ser ativada e desativada, para as VMs que são criptografadas, a migração com o vSphere vMotion sempre usa o vSphere vMotion criptografado. As VMs não criptografadas podem ter a opção de criptografia Desativada, Oportunista e Obrigatória com o uso do vMotion. A opção Oportunista seria utilizada por padrão em VMs não criptografadas durante o vMotion. A Figura 9 abaixo resume a diferença entre a criptografia de VMs e a criptografia do vSAN

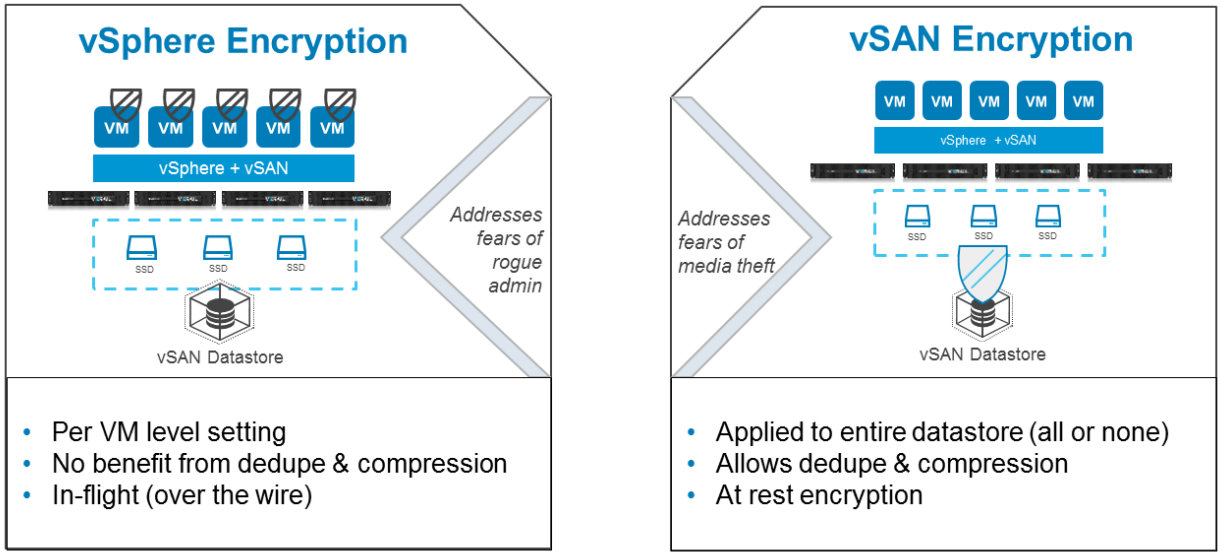

Figura 9: Criptografia de VMs versus Criptografia do vSAN

Além disso, o VxRail aceita o vMotion criptografado, no qual as VMs são criptografadas quando são movidas entre hosts. Isso inclui migrações do vMotion no VxRail, bem como migrações do vMotion para ou a partir de um cluster do VxRail em uma instância do vCenter. O vMotion criptografado pode ser usado com a criptografia do vSAN para ter a criptografia dos dados em repouso e dos dados em trânsito. O vMotion criptografado é imposto para as VMs com a criptografia do vSphere ativada.

À exceção da criptografia do vMotion, na qual o vSphere fornece as chaves temporárias usadas para criptografar os dados em trânsito, um servidor de gerenciamento de chaves (KMS) é necessário para a geração segura, o armazenamento e a distribuição das chaves de criptografia. Quando a criptografia é ativada, o vCenter estabelece uma relação de confiança com o KMS e, em seguida, transmite as informações de conexão do KMS para os hosts do ESXi. Os hosts do ESXi solicitam as chaves de criptografia diretamente do KMS e fazem a criptografia e a descriptografia dos dados. A conectividade do vCenter só é necessária para a instalação inicial.

Como o KMS é um componente essencial da infraestrutura de segurança, ele deve ter o mesmo nível de redundância e proteção normalmente aplicado a outros componentes essenciais da infraestrutura, como DNS, NTP e Active Directory. É importante lembrar que o KMS deve ser executado fisicamente separado dos elementos que ele criptografa. Durante a inicialização, os hosts do ESXi solicitarão as chaves do KMS. Se o KMS estiver indisponível, o sistema não conseguirá concluir a inicialização.

O VxRail e a VMware aceitam KMSs que são compatíveis com o protocolo de interoperabilidade de gerenciamento de chaves (KMIP) versão 1.1 ou superior, como o Dell EMC CloudLink. A VMware mantém um guia de compatibilidade de KMSs, que foi validado em relação ao vSphere.

No vSphere, a criptografia é tratada por um conjunto comum de módulos que são validados por FIPS 140-2. Esses módulos comuns são projetados, implementados e validados pelo ciclo de vida de desenvolvimento seguro da VMware. Ter um conjunto de módulos comuns de criptografia permite que o VxRail torne a criptografia mais fácil de implementar, gerenciar e dar suporte.

A criptografia é ativada no VxRail por meio de uma configuração simples no vCenter. Os controles de acesso garantem que somente as pessoas autorizadas tenham permissão para ativar ou desativar a criptografia. Uma função denominada “Sem administrador de criptografia” permite que um administrador execute tarefas administrativas normais, mas sem autoridade para alterar as configurações de criptografia.

SDN (Software-Defined Networking) do VxRail usando o NSX opcional

Um ambiente virtual dinâmico como o do VxRail geralmente se beneficia com a flexibilidade que o SDN (Software-Defined Networking) oferece. As maneiras mais fáceis de fornecer o SDN no VxRail são com o VMware NSX, que é uma licença de software opcional que não está incluída no VxRail. O NSX é uma plataforma completa de virtualização de rede e segurança que permite que os administradores criem redes virtuais inteiras, inclusive roteadores, firewalls e balanceadores de carga, puramente no software. Como esse Software-Defined Networking é dissociado da infraestrutura de rede física subjacente, ele não depende de o VxRail ser associado a determinado fornecedor de switch.

O NSX com VxRail é uma solução de segurança integrada que reduz a necessidade de implementar componentes adicionais de hardware ou software de segurança. Com o NSX, os administradores do VxRail configuram a microssegmentação para proteger e isolar as cargas de trabalho de diferentes grupos de usuários, controlar a entrada e a saída e oferecer segurança aprimorada para todas as cargas de trabalho, inclusive aplicativos tradicionais de vários níveis e VMs de uso geral, bem como ambientes de VDI. Alguns dos benefícios do uso do NSX com o VxRail incluem:

- A capacidade de aplicar políticas de segurança mais próximas à carga de trabalho. As políticas de segurança são aplicadas no software, e os controles de segurança são movidos com a carga de trabalho entre os hosts do cluster.
- O gerenciamento simplificado com segurança é integrado à pilha do vSphere e gerenciado centralmente por meio do Web Client em HTML5 do vSphere e do plug-in NSX Manager.
- Controles de segurança consistentes e automáticos usando grupos e políticas. As cargas de trabalho são automaticamente identificadas e dinamicamente definidas com a postura de segurança correta.
- A implementação eficiente de controles de segurança no nível do hypervisor reduz a latência e o consumo de largura de banda dos aplicativos em comparação com os controles de segurança externos ou baseados em perímetro.
- Isolamento no nível da DMZ para controlar a entrada e a saída de clients internos e externos a partir da Internet usando regras apropriadas de autorização e recusa a fim de controlar o tráfego.
- Detecção e bloqueio de endereços IP de VMs falsificados usando o recurso SpoofGuard. (Para obter mais informações sobre esse recurso, consulte a documentação Using SpoofGuard da VMware.)
- Firewall de identidade que permite que um administrador do NSX crie regras de DFW baseadas no usuário do Active Directory. (Para obter mais informações sobre esse recurso, consulte a documentação do VMware NSX.)
- Integra-se a serviços de segurança de terceiros, como detecção de invasão e prevenção contra invasões (IDS/IDP).

O NSX aprimora a postura de segurança de um ambiente e é compatível com os seguintes padrões e certificações:

- Certificação Common Criteria — EAL 2+
- Firewall certificado pelo ICSA Labs
- Validação
- Satisfação de todas as recomendações de segurança cibernética do NIST para a proteção de cargas de trabalho virtualizadas

Com a utilização da plataforma de segurança VMware NSX opcional com o VxRail, o firewall e as políticas de segurança são integrados. Isso oferece um equipamento realmente convergente, em vez de uma segurança situada externamente no perímetro. A implementação do NSX com o VxRail reduz ainda mais o tempo necessário para implementar novas iniciativas de aplicativos, já que os controles de segurança se tornam parte do equipamento, em vez de componentes adicionais de hardware ou software que são acoplados.

Modo de bloqueio

Para ambientes que precisam de ainda mais segurança com flexibilidade, o modo de bloqueio pode ser configurado para o ESXi. No modo de bloqueio, a habilidade de executar operações de gerenciamento em hosts individuais é limitada, forçando a conclusão da tarefa de gerenciamento por meio do vCenter.

O bloqueio no modo “Normal” permite que um grupo seleto de usuários seja adicionado à lista de permissões, possibilitando que eles gerenciem os servidores localmente, em vez de usar o vCenter. Essa lista de permissões deve incluir determinadas contas de gerenciamento do VxRail.

No modo de bloqueio estrito, nenhum usuário pode gerenciar os servidores localmente. O bloqueio no modo “Estrito” não é aceito pelo VxRail.

Gerenciamento seguro com HTTPS

O tráfego de gerenciamento não seguro é um risco de segurança significativo. Por isso, o VxRail usa interfaces de gerenciamento protegidas com a segurança de camada de transporte “TLS 1.2”. O vCenter, o iDRAC e o software do sistema de HCI desativam a interface HTTP de texto sem criptografia e exigem o uso de HTTPS, que utiliza TLS 1.2. Além disso, o acesso à linha de comando dos servidores do ESXi deve usar SSH. O uso de SSH e HTTPS é uma parte vital do controle e comando seguros do VxRail.

Integridade

A integridade dos dados das empresas é um requisito fundamental das operações de negócios. O VxRail garante a integridade de seus dados ao manter a consistência, a precisão e a confiabilidade dos dados durante seu ciclo de vida, controlando o acesso dos usuários e os recursos de integridade incorporados, tais como somas de verificação de dados

Segmentação de rede

A segmentação de rede é utilizada para isolar o tráfego da rede privada do tráfego público a fim de reduzir a superfície de ataque. Ela também é um controle de segurança eficaz para limitar a movimentação de um invasor em todas as redes.

O VxRail foi projetado com vários níveis de segmentação de rede, inclusive a segmentação física da rede de gerenciamento de hardware, a segmentação virtual de redes de aplicativo e infraestrutura e a microssegmentação no nível da VM e do aplicativo com o software NSX opcional da VMware. Por meio da segmentação, a visibilidade das ferramentas administrativas essenciais é limitada, evitando que os invasores as usem contra o sistema. Por padrão, a segmentação de rede apropriada é automaticamente configurada como parte da inicialização do sistema, e o administrador tem a flexibilidade de definir níveis adicionais de segmentação para o ambiente de aplicativos, conforme necessário. As melhores práticas de configuração de rede são apresentadas no Guia de rede do Dell EMC VxRail.

O VxRail usa switches virtuais distribuídos da VMware que segmentam o tráfego por padrão usando VLANs separadas para gerenciamento, vSAN, vMotion e tráfego de aplicativos. As redes do vSAN e do vMotion são redes privadas e não roteáveis. Dependendo dos aplicativos aceitos pela rede do VxRail, o tráfego pode ser segmentado ainda mais com base no tráfego de aplicativos, de produção e de não produção, além de outros requisitos.

O switch virtual distribuído no VxRail é configurado por padrão com o controle de E/S de rede (NIOC) do vSphere. O NIOC permite que a largura de banda física seja alocada para diferentes VLANs. Alguns ataques cibernéticos, como worms e negação de serviço, podem levar ao uso excessivo de recursos. Isso pode causar uma negação de recursos a outros serviços que não estão sendo diretamente atacados. O NIOC pode garantir que outros serviços tenham a largura de banda de rede de que precisam para manter a integridade em caso de ataque a outros serviços. As configurações do NIOC são definidas automaticamente seguindo melhores práticas recomendadas quando o sistema é inicializado. O Guia de rede da Dell EMC inclui detalhes das configurações do NIOC para as VLANs padrão do VxRail.

Cada nó do VxRail tem uma porta Ethernet física separada para a interface de gerenciamento de hardware do iDRAC. A segmentação física dessa rede dificulta o acesso dos invasores ao gerenciamento de hardware. Em caso de ataque de negação de serviço distribuída, a rede segmentada fisicamente não é afetada, o que limita o escopo de um possível ataque.

Boot seguro UEFI

A inicialização segura de UEFI protege o sistema operacional contra corrupção e ataques de rootkit. A inicialização segura de UEFI confirma se o firmware, o carregador de inicialização e o VMkernel foram todos assinados digitalmente por uma autoridade confiável. Além disso, a inicialização segura de UEFI para ESXi confirma se os pacotes de instalação da VMware (VIBs) foram criptograficamente assinados. Isso garante que a pilha de inicialização do servidor esteja executando todos os produtos de software genuínos e que ela não tenha sido alterada.

Soma de verificação (checksum) de software

Uma parte essencial da integridade dos dados é a confirmação de que os dados recuperados do armazenamento não foram alterados desde que foram gravados. O VxRail usa, por padrão, a soma de verificação da integridade dos dados completa e em nível de block. A soma de verificação é criada quando os dados são gravados. Em seguida, a soma de verificação é verificada na leitura e, se ela mostrar que os dados foram alterados desde quando foram gravados, eles serão reconstruídos a partir de outros membros do grupo de RAID. O vSAN também usa um mecanismo proativo de depuração para detectar e corrigir uma possível corrupção dos dados, mesmo em dados acessados com pouca frequência.

Disponibilidade

Manter seu sistema de TI atualizado, certificar-se de que o hardware está funcionando corretamente e oferecer largura de banda adequada são fundamentais para manter a disponibilidade dos dados das empresas para os usuários autorizados. O gerenciamento do ciclo de vida do software do VxRail, os recursos de disponibilidade do vSphere, o monitoramento proativo e a recuperação integrada, além da segurança física do hardware e a configuração segura do sistema garantem a máxima disponibilidade do sistema.

Gerenciamento do ciclo de vida do software do VxRail

Uma das medidas mais essenciais que uma organização pode adotar para manter sua infraestrutura de TI segura é manter em dia as atualizações e os patches de software. As atualizações e os patches não apenas resolvem problemas que podem resultar em tempo de inatividade ou melhorar o desempenho, mas também corrigem frequentemente as vulnerabilidades de segurança. Há muita colaboração na comunidade de segurança. Como o VxRail foi projetado em conjunto com a VMware, somos referência prévia nos planos de correções de segurança, o que permite que a equipe do VxRail valide e prepare rapidamente patches de segurança pré-qualificados. Mas nem todos estão do mesmo lado, o que resulta em uma corrida entre os defensores, que trabalham para reduzir e corrigir as ameaças, e os invasores, cujo objetivo é explorar as vulnerabilidades. Como o VxRail foi projetado em conjunto com a VMware, somos referência prévia nos planos de correções de segurança, o que permite que a equipe do VxRail valide e prepare rapidamente patches de segurança pré-qualificados

O gerenciamento do ciclo de vida do software do VxRail faz com que as operações de atualização, que poderiam ser complexas e arriscadas, sejam fáceis de instalar e seguras de implementar. O sistema de HCI do VxRail é o único em que todos os componentes de software são projetados, testados e lançados como um pacote. Os pacotes de software do VxRail podem incluir atualizações de BIOS, firmware, hypervisor, vSphere ou qualquer um dos componentes de gerenciamento incluídos. Se e quando vulnerabilidades forem detectadas, as correções serão rapidamente desenvolvidas para reduzir as ameaças, independentemente de onde elas estejam. Os pacotes de atualização são amplamente testados na plataforma de hardware do VxRail e em toda a pilha de software do VxRail antes de serem lançados aos clientes.

Os administradores são notificados pelo software do sistema de HCI quando as atualizações estão disponíveis. Em seguida, o administrador pode fazer download do pacote de atualizações diretamente e iniciar ou agendar um processo de atualização orquestrado. As atualizações são executadas como processos contínuos enquanto o sistema permanece on-line servindo os negócios. Se uma reinicialização for necessária, as VMs serão migradas automaticamente para outros nós do cluster antes de continuar.

O gerenciamento do ciclo de vida do software do sistema de HCI reduz a complexidade, o que torna a infraestrutura mais segura, reduzindo o tempo e a dificuldade necessários para corrigir os sistemas e eliminar os riscos.

Recursos de disponibilidade do vSphere para VxRail

O VxRail utiliza os recursos de disponibilidade integrados do vSphere, inclusive VMware High Availability (HA), VMware Distributed Resource Scheduler (DRS) e clusters estendidos da VMware. Esses recursos dão suporte ao software automatizado do VxRail e garantem a disponibilidade contínua dos serviços hospedados no VxRail. Portanto, é recomendável que os clientes usem versões do vSphere que contenham esses recursos.

O VMware HA monitora a execução de VMs em um cluster do VxRail. Se uma VM ou um nó falhar, o HA será reiniciado em outro nó, em outro lugar do cluster. As VMs podem falhar por vários motivos, inclusive ataque cibernético, falha do hardware subjacente ou software corrompido. Embora o VMware HA não impeça interrupções, ele minimiza o tempo necessário para restaurar os serviços.

O VMware DRS distribui a carga de trabalho da VM a todos os hosts do cluster. Conforme mudam as demandas por recursos da VM, o DRS usa o vSphere vMotion para migrar as cargas de trabalho da VM para outros hosts no cluster. Os ataques cibernéticos podem causar problemas com os recursos de VMs que não foram visadas pelo ataque. Geralmente, os ataques cibernéticos resultam na intensa utilização de recursos pela VM atacada e, portanto, na intensa utilização de recursos no nível do host, o que afeta os recursos disponíveis para as outras VMs nesse host. O DRS protege as VMs, migrando-as para fora dos hosts com restrição de recursos e permitindo que as VMs continuem oferecendo os serviços.

O cluster estendido da VMware amplia o cluster do VxRail de um único local para dois locais, o que resulta em um nível mais alto de disponibilidade. No entanto, se houver apenas uma instância da VM, as cópias completas de seus dados serão mantidas nos dois locais. Se o local em que a VM é executada no momento ficar indisponível, a VM será reiniciada no outro local.

Proteção de dados

Sólidas defesas de segurança são essenciais, mas ter um plano de recuperação robusto e confiável também é importante. O backup e as replicações formam a base da recuperação após uma violação. Para ajudar na recuperação, o software do sistema de HCI inclui backup e restauração baseados em arquivo. Todos os equipamentos VxRail incorporam um pacote inicial do Dell EMC RecoverPoint for VMs (RP4VM), que oferece o que há de melhor em replicação local e remota e recuperação granular.

O backup e a restauração baseados em arquivo do software do sistema de HCI protegem contra a exclusão acidental do equipamento virtual ou a corrupção interna do equipamento. Os backups podem ser configurados para ocorrer regularmente ou conforme a necessidade. Este é um recurso completo que faz backup dos arquivos dentro do datastore do vSAN, de modo que produtos de hardware e software adicionais não são necessários.

Com o RP4VM, se uma VM for comprometida ou os dados forem danificados ou retidos, por exemplo, a VM e o conjunto de dados serão rapidamente revertidos ao point-in-time antes do ataque, permitindo que a empresa se recupere rapidamente. Instalado diretamente a partir do VxRail Manager, o RP4VM é rapidamente implementado, e o monitoramento diário ocorre através do plug-in familiar do vCenter. A recuperação é fácil e ocorre por meio de uma interface familiar do vSphere.

Para as organizações que precisam de recursos aprimorados e abrangentes de proteção de dados, o VxRail oferece opções que incluem o Dell EMC Data Protection Suite for VMware, o Dell EMC PowerProtect e o Dell EMC Data Domain Virtual Edition.

Os backups baseados em arquivo do software do sistema de HCI do VxRail ajudam a garantir a continuidade dos negócios no raro evento de uma VM do VxRail precisar ser reconstruída.

SEGURANÇA DO SISTEMA

Autenticação, autorização e responsabilidade do VxRail

Estrutura de autenticação, autorização e responsabilidade (AAA) integrada. A estrutura AAA foi projetada para controlar o acesso, garantindo que a pessoa certa esteja usando o sistema, fornecer o nível de acesso que essa pessoa tem e registrar as atividades para contabilizar seus objetivos e quem as executou.

AUTENTICAÇÃO

A autenticação no software do sistema de HCI é feita por SSO via plug-in do vCenter. O VxRail vCenter é compatível com o sistema de gerenciamento de identidade centralizado da organização de acordo com as políticas de segurança da autenticação

Geralmente, as organizações centralizam o gerenciamento de identidades utilizando serviços de diretório, como o Microsoft Active Directory (AD), usando o LDAP. Se o VxRail for um ambiente independente que não faz parte de um domínio, os usuários e as senhas poderão ser gerenciados localmente no vSphere e no iDRAC. De acordo com a melhor prática, é recomendável usar a autenticação centralizada.

Muitas vezes, pode haver indivíduos diferentes responsáveis pelos servidores físicos, pelo gerenciamento do ciclo de vida do VxRail e pelo gerenciamento do ambiente de virtualização de servidor, armazenamento e rede. Portanto, o VxRail usa controles de acesso refinados e baseados em função para o iDRAC, o software do sistema de HCI e o vSphere.

Autorização

Usando o “princípio de privilégio mínimo” (POLP), um usuário recebe os direitos exigidos para desempenhar sua função, mas não mais do que o necessário. O vSphere inclui várias funções predefinidas que são usadas para conceder o privilégio apropriado. Por exemplo, um usuário pode receber a função de administrador do vSphere, gerenciamento de HCIA ou ambas. A função de gerenciamento de HCIA concede ao usuário um privilégio para executar tarefas de gerenciamento do ciclo de vida do VxRail a partir do plug-in de gerenciamento do VxRail no vCenter. O administrador do vSphere concede o privilégio de executar tarefas de administrador no vCenter. Além disso, o vSphere permite um nível ainda mais detalhado de controle de acesso pela criação de funções personalizadas. Por exemplo, um usuário privilegiado pode ter permissão para confirmar um alarme ou criar um perfil de armazenamento, mas não para implementar VMs.

As funções são associadas a usuários e grupos e com objetos específicos, sendo que um objeto é uma coisa ou um grupo de coisas. Por exemplo, um usuário ou grupo pode ter permissão para confirmar alertas de uma VM ou porta específica, mas não de outros objetos. Além disso, funções restritivas, como “Sem acesso”, podem ser atribuídas aos usuários, impedindo que eles vejam áreas específicas no vCenter. Vários usuários ou grupos podem receber níveis de acesso iguais ou diferentes para o mesmo objeto. As permissões concedidas a um objeto secundário podem ser usadas para substituir as permissões herdadas de um objeto principal.

O controle de acesso baseado em função do vSphere aceita princípios de segurança granular de “privilégio mínimo” e “separação de responsabilidade” e permite que o administrador de segurança aumente a segurança ao definir permissões precisas com base na estrutura de gerenciamento de sistemas da organização.

RESPONSABILIDADE

Compreender as alterações na configuração e no status do componente é fundamental para manter os sistemas seguros e disponíveis. As alterações podem resultar de uma correção temporária que causa um desvio de configuração. Alternativamente, essas alterações podem indicar uma possível invasão. Monitorar proativamente a infraestrutura é uma importante atividade de segurança.

A detecção em tempo hábil de uma invasão pode significar a diferença entre uma breve interrupção, na qual o invasor não consegue comprometer nenhum sistema essencial, e uma invasão que persiste por meses, resultando no comprometimento de vários sistemas essenciais. Deixar de manter um sistema de logs de auditoria pode não apresentar informações adequadas sobre o ataque para determinar sua gravidade. De acordo com o 2019 Trustwave Global Security Report (registro obrigatório), 57% dos incidentes investigados envolveram redes corporativas e internas (um aumento de 50% em comparação a 2017).

O desvio de configuração é um desafio que afeta todos os sistemas. Os sistemas podem começar com uma linha de base de configuração segura, mas, ao longo do tempo, alterações ocorridas podem deixar o sistema vulnerável. Essas alterações podem ocorrer por vários motivos, inclusive uma alteração temporária durante a solução de problemas ou uma alteração aprovada que deve se tornar parte da configuração de linha de base. Sem o monitoramento, essas alterações se tornam muito difíceis de detectar.

O desafio de monitorar as informações é que elas vêm de muitas fontes diferentes: uma VM individual, um servidor físico, a infraestrutura de virtualização, a rede, os componentes de segurança ou os próprios aplicativos. Interpretar essas informações exige uma visão consolidada das atividades e das alterações. O VxRail inclui o vRealize Log Insight. O Log Insight compila logs da VMware, inclusive servidores, dispositivos de rede, armazenamento e aplicativos. Como mostra o gráfico abaixo, o Log Insight cria um painel de indicadores com gráficos baseados nos dados dos logs. Isso ajuda o administrador a se aprofundar com rapidez e facilidade até a causa raiz do problema. A Figura 10 abaixo mostra o painel de indicadores do vRealize Log Insight.

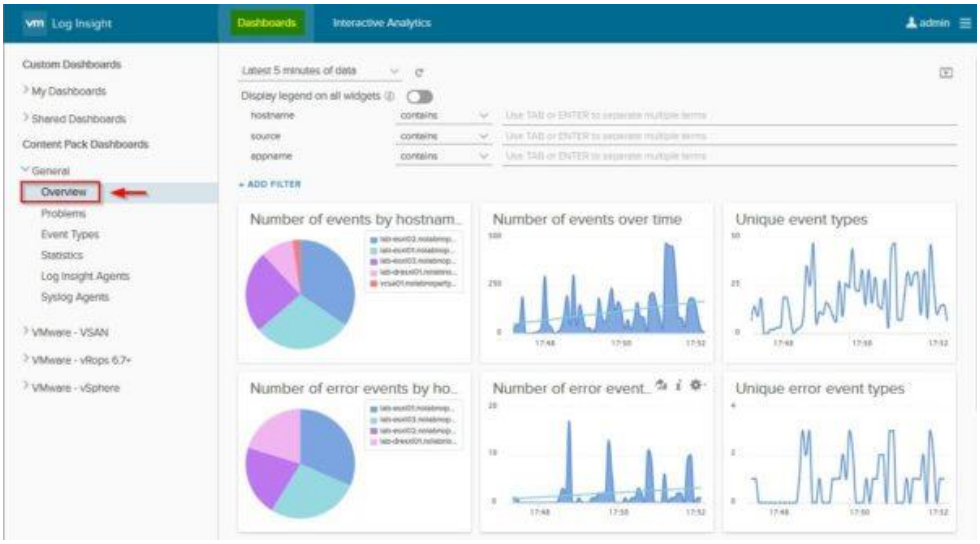

Figura 10: vRealize Log Insight

Correlacionar todas essas informações é um dos vários motivos pelos quais o VxRail usa o Network Time Protocol (NTP) padrão do setor para manter todos os relógios dos componentes em sincronia.

Para as organizações que já têm um sistema de gerenciamento de logs ou sistema de gerenciamento de eventos e incidentes de segurança (SIEM), o VxRail se integra facilmente com o uso do protocolo syslog padrão.

Segurança da localização física do VxRail

A segurança física é uma parte importante de qualquer solução de segurança abrangente. Como o VxRail pode ser implementado fora de um data center tradicional, a segurança física pode assumir uma importância ainda maior. Para impedir que um malware ou software infectado seja introduzido por meio de uma unidade USB, as portas USB no VxRail podem ser desativadas — e ativadas somente quando necessário.

Os nós do VxRail também monitoram outros eventos, como aberturas de chassi, falhas ou substituições de peças, alterações de firmware e avisos de temperatura. Essas informações são registradas no log de ciclo de vida do iDRAC. Em muitos casos, um chassi não precisa ser aberto depois de colocado em produção, e rastrear essa atividade pode indicar uma tentativa de comprometer o sistema.

Automação

Uma parte importante da manutenção da segurança é garantir que todos os elementos relevantes de configuração da segurança sejam implementados em todos os objetos de um ambiente. Um cluster individual do VxRail pode ter até 64 nós físicos, e vários clusters do VxRail podem ser gerenciados por um vCenter, comportando assim milhares de VMs. Mesmo uma simples alteração — caso ela precise ser configurada em todas as VMs — poderá levar um tempo significativo para entrar em efeito. Além disso, ao executar tarefas repetitivas, as pessoas ficam propensas a cometer erros. É aqui que a automação se torna essencial.

A automação permite que um ambiente tenha menos erros de configuração e uma configuração mais consistente. Além disso, ela aumenta a eficiência e reduz o tempo entre a decisão ser tomada e implementada, aumentando o tempo de retorno das decisões.

Ferramentas compatíveis, como o vRealize Automation, permitem a automação do vSphere e do vSAN. Essas ferramentas podem ser usadas para automatizar as operações diárias padrão, como a criação de VMs ou as políticas de armazenamento. O vRealize Automation também pode ser usado para confirmar se a configuração de segurança não se desviou das configurações apropriadas. Se a configuração tiver sido alterada, o vRealize Automation poderá reconfigurar os servidores do ESXi, o vCenter ou VMs individuais para que eles atendam novamente à configuração de segurança requerida. Além disso, como o vRealize Automation é uma ferramenta padrão da VMware, muitas equipes de virtualização de TI já sabem como trabalhar com o vRealize Automation e criaram perfis que funcionarão com um cluster do VxRail.

Pacote de fortalecimento de STIG do VxRail

A configuração da segurança pode ser um processo complexo e propenso a erros, que apresenta muitos dos riscos que ela pretende reduzir. Três elementos diferentes simplificam o processo de proteção da infraestrutura do VxRail. Primeiro, o vSphere tem uma abordagem “segura por padrão” para a configuração. Em segundo lugar, os Guias de implementação técnica de segurança da Agência de Sistemas de Informação de Defesa (DISA STIGs) oferecem um modelo para o fortalecimento da segurança, e uma variedade de ferramentas de automação permitem que o monitoramento e a configuração de parâmetros de segurança sejam verificados e definidos conforme necessário. Isso permite que o perfil de risco apropriado seja configurado para corresponder às necessidades dos negócios. Por último, a capacidade de automatizar a reversão da configuração para um estado seguro e conhecido quando ocorrem alterações inesperadas é uma parte vital da segurança do VxRail.

A partir do vSphere 6.0, a VMware adotou uma iniciativa para incorporar a segurança à configuração padrão do vSphere. Isso torna o VxRail mais seguro de modo integrado. Como parte dessa iniciativa, as configurações de segurança mais recomendadas foram classificadas como específicas ao local ou alteradas para um padrão de configuração segura. As configurações que, anteriormente, precisavam ser alteradas após a instalação foram atualizadas, o que significa que a configuração segura se tornou o padrão.

As definições de configuração que são classificadas como específicas ao local não podem ser configuradas por padrão. Por exemplo, o nome do host de um servidor NTP ou syslog remoto. Com o VxRail, muitas das configurações que a VMware classifica como específicas ao local são definidas pelo software do sistema de HCI como parte da instalação.

Muitas organizações usam STIGs como uma linha de base para fortalecer seus sistemas. Esses STIGs oferecem uma checklist em um PDF legível e um script automatizado. Isso permite que as ferramentas de automação leiam o STIG e configurem o ambiente para fazer a correspondência com a configuração recomendada com o mínimo de intervenção manual. Embora os STIGs existentes da VMware abranjam os componentes do VxRail, inclusive o vSphere, o ESXi e o vSAN tornam a implementação o mais simples possível. O equipamento Dell VxRail que executa o software do equipamento VxRail versão 4.5.x ou 4.7.x cumpre com os requisitos relevantes dos Guias de implementação técnica de segurança (STIG) da DISA.

Ao longo do tempo, as configurações podem se desviar para posições menos seguras. Por isso, é importante não apenas monitorar a configuração, mas também automatizar a restauração do ambiente para o estado seguro inicial. O VxRail oferece várias opções diferentes, dependendo do nível de automação requerido. O VxRail tem ferramentas automatizadas de fortalecimento, que verificam a configuração atual em relação a um STIG e, se a configuração tiver sido alterada, revertem a configuração para o estado seguro conhecido. Se uma ferramenta de automação mais abrangente é necessária, o VMware vRealize Suite funciona com ambientes VxRail para automatizar o gerenciamento da configuração e, ao mesmo tempo, manter a governança e o controle. Além disso, a VMware oferece o AppDefense, uma ferramenta mais focada em aplicativos, que usa aprendizagem automática para coletar informações sobre um estado bom e conhecido das VMs e dos aplicativos aos quais elas dão suporte. Com essa ferramenta, quando for detectada uma variação do estado bom e conhecido, o administrador será notificado e uma resposta poderá ser automatizada a partir de uma biblioteca de rotinas de resposta a incidentes.

Segurança integrada ao VxRail ACE

O VxRail Analytical Consulting Engine (ACE) complementa a simplicidade operacional integrada do Dell EMC VxRail com inteligência operacional para os clusters do VxRail. O VxRail ACE oferece uma combinação de simplicidade operacional e inteligência operacional com segurança intrínseca, possibilitando que as empresas se dediquem à transformação da infraestrutura de TI

O VxRail ACE é executado em uma plataforma de nuvem gerenciada pela TI da Dell EMC. Como uma solução de SaaS baseada em nuvem, a VxRail ACE tem a flexibilidade para oferecer novas funcionalidades com frequência e sem disrupções, proporcionando uma experiência excepcional para os clientes. Sua rede neural de aprendizagem profunda aprimorará continuamente seus recursos preditivos, incluindo diversos metadados que o VxRail pode coletar sobre seus clusters.

Os usuários do VxRail podem acessar o VxRail ACE em https://vxrailace.emc.com usando suas credenciais de suporte da Dell EMC.

Visão geral da segurança do VxRail ACE

O VxRail ACE coleta dados de telemetria dos nós do VxRail em todos os clusters do VxRail da organização e transmite com segurança esses dados para uma solução de SaaS gerenciada pela TI da Dell EMC, conforme mostrado na Figura 011.

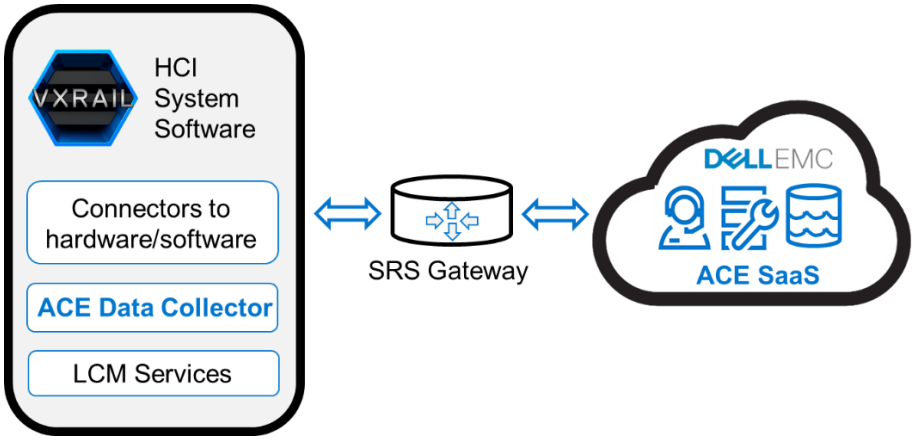

Figura 11: Diagrama da arquitetura de alto nível do VxRail ACE

A Dell EMC entende as preocupações dos clientes em manter a segurança de seus dados. A segurança é intrínseca ao VxRail ACE desde a coleta de dados até o trânsito e os dados em repouso. Além disso, o VxRail ACE foi desenvolvido de maneira segura com o uso de controles arquitetônicos como parte do ciclo de vida de desenvolvimento de segurança padrão da Dell EMC. Esse padrão define as atividades focadas na segurança que as equipes de produtos da Dell EMC devem seguir ao criar e lançar produtos para permitir que os produtos da Dell EMC minimizem os riscos aos produtos e ambientes dos clientes em virtude de vulnerabilidades de segurança.

Coleta de dados do VxRail ACE

Em cada cluster do VxRail, um coletor de dados adaptável (ADC) é executado e obtém dados de telemetria do software do sistema de HCI por meio de conectores de hardware e software do VxRail. O ADC não coleta informações de identificação pessoal (PII). Os dados de telemetria coletados pelo ADC são mostrados na Tabela 1.

Telemetria básica (Topologia de hardware: equipamentos, unidade, firmware, PSU)	**Dados de desempenho**	**Alarmes**	**Dados do sensor de hardware**
• Informações do cluster • Informações do dispositivo	• Cluster (CPU, memória, disco) • VM (CPU, memória, disco) • vSAN (disco, rede)	• vCenter • VxRail	• Tipo do sensor • Status • Nome • Leitura atual

Table 1 Dados de telemetria do VxRail coletados pelo ACE

Os dados de telemetria coletados pelo ADC não são armazenados localmente. Eles são transmitidos com segurança pelo gateway do suporte remoto seguro (SRS) da Dell EMC.

Dados do VxRail ACE em trânsito para a Dell

Somente os dados coletados pelo coletor de dados adaptável (ADC) são enviados ao back-end da Dell EMC pelo gateway do suporte remoto seguro (SRS) da Dell EMC. O VxRail ACE recebe notificações de entrada de dados do sistema de HCI pelo gateway do SRS. Os clientes do VxRail ACE controlam quais sistemas enviam dados do sistema de HCI pelo gateway. Todos os dados transmitidos pelo gateway do SRS da Dell EMC são protegidos em trânsito pelas melhores práticas padrão do setor. O gateway do SRS é autenticado de modo bidirecional por meio de certificados digitais da RSA® em conjunto com políticas de acesso controladas pelo cliente e um log de auditoria detalhado. A comunicação ponto a ponto é estabelecida por meio do padrão de criptografia avançada (AES) de 256 bits, que garante que todos os dados sejam transportados com segurança para a infraestrutura gerenciada pela TI da Dell EMC. Além disso, o SRS oferece autenticação baseada em vários fatores e VPN dedicada. Depois que os dados chegam à Dell, o VxRail ACE criptografa e armazena os dados do ACE em sua própria infraestrutura gerenciada pela TI da Dell EMC.

Dados em repouso do VxRail ACE

Os dados do sistema de HCI recebidos dos sistemas gerenciados pelo VxRail ACE são criptografados e armazenados na infraestrutura da Dell gerenciada pela TI da Dell EMC.

A infraestrutura de TI da Dell EMC:

- Oferece uma plataforma segura que garante que os dados de telemetria de cada cliente sejam isolados.
- Oferece alta disponibilidade, tolerância a falhas e recuperação de desastres.
- Localiza os dados de telemetria do cliente (inclusive backups) nos Estados Unidos.
- Retém indefinidamente os dados históricos dos sistemas que estão sendo ativamente monitorados pelo ACE, inclusive informações oriundas do ACE.
- Dá a cada cliente acesso a um portal seguro e independente, no qual cada usuário pode ver apenas os sistemas no VxRail ACE que fazem parte do acesso do usuário ao site, conforme definido no Dell EMC MyService360.

O Escritório de segurança e resiliência (SRO) da Dell Technologies, liderado pelo diretor de segurança da Dell, é responsável pela segurança e proteção da infraestrutura de tecnologia da informação da Dell EMC que hospeda a solução de SaaS VxRail ACE. Isso é feito por meio de políticas e procedimentos regentes de segurança estabelecidos e da aplicação de controles de segurança das informações, que incluem medidas como firewalls de várias camadas, sistemas de detecção de invasão, antivírus líder do setor e proteção contra malware. A equipe de segurança cibernética da Dell EMC está envolvida na execução de verificações de vulnerabilidade contínuas nos aplicativos e no ambiente subjacente. Qualquer correção necessária é tratada por meio de um programa contínuo de correção de vulnerabilidades, como atualizações de software, patches ou alterações de configuração.

Todos os dados enviados ao VxRail ACE são armazenados na infraestrutura hospedada no data center da Dell EMC. A política de segurança das informações garante que todas as informações e os recursos da Dell EMC sejam protegidos adequadamente, e os proprietários das informações devem garantir que todos os recursos sejam contabilizados e que cada recurso tenha um custodiante designado. Todos os componentes da infraestrutura estão localizados na rede de enclave dedicada e protegida por firewall da Dell EMC, que não está exposta ao acesso externo. Nenhum log-in direto individual no banco de dados e no servidor de banco de dados é permitido, exceto pelos membros das equipes de administradores do sistema e administradores do banco de dados. As contas dos aplicativos de banco de dados são gerenciadas por meio da autenticação por senha de banco de dados padrão. A Dell EMC implementou um processo de gerenciamento de mudanças com melhores práticas do setor para garantir que o hardware da infraestrutura da Dell EMC seja estável, controlado e protegido. O gerenciamento de mudanças oferece as políticas, os procedimentos e as ferramentas para governar essas mudanças a fim de garantir que elas sejam submetidas a análises e aprovações e sejam comunicadas de maneira eficaz aos usuários.

Controle de acesso aos dados do VxRail ACE

O acesso aos dados do VxRail ACE pode ser dividido em duas categorias:

- Acesso ao VxRail ACE pelos clientes para visualizar os dados do sistema e as percepções oriundas do ACE.
- Acesso à infraestrutura do VxRail ACE gerenciada pela Dell EMC pelo administrador do sistema de TI interno da Dell EMC e pelo administrador do banco de dados.

As subseções abaixo descrevem como o acesso aos dados é controlado por essas duas categorias de usuários.

Acesso do usuário final ao VxRail ACE

Os clientes usam a conta de suporte existente para fazer log-in no VxRail ACE. O acesso aos dados do VxRail ACE a partir do portal do VxRail ACE exige que cada usuário final tenha uma conta de suporte válida da Dell EMC. A autenticação é tratada pela infraestrutura de logon único (SSO) da Dell EMC. O VxRail ACE usa o perfil de usuário do cliente do Dell EMC MyService360 para o controle de acesso. O perfil do usuário é criado e associado a um perfil do cliente válido quando o usuário registra uma conta na Dell EMC. O VxRail ACE oferece a cada cliente uma visualização segura e independente de seus sistemas e garante que ele só consiga ver seus próprios dados por meio do VxRail ACE. Cada usuário pode ver apenas os sistemas no VxRail ACE que fazem parte do acesso do usuário ao site de acordo com a configuração desse usuário no Dell EMC MyService360.

Acesso administrativo à infraestrutura do VxRail ACE gerenciada pela TI da Dell EMC

A Dell EMC é muito sensível à importância de proteger as informações confidenciais e exclusivas dos clientes. Para isso, todos os funcionários da Dell EMC devem assinar um contrato, que inclui disposições que abordam todas as informações do cliente. As obrigações desse contrato se estendem a todos os dados percebidos armazenados em qualquer máquina de qualquer modo ou formato, enquanto os funcionários estão envolvidos nos serviços de manutenção, e permanecem em vigor mesmo após a rescisão do vínculo empregatício com a Dell EMC.

Padrões e certificações compatíveis

O VxRail é uma infraestrutura hiperconvergente robusta e flexível que pode ser configurada para permitir que as organizações cumpram as normas de conformidade. Embora alguns fornecedores de HCI possam alegar compatibilidade, a Dell EMC está buscando ativamente a certificação completa quanto aos padrões de segurança que são importantes para os clientes. Entre em contato com um representante da Dell EMC para discutir como o VxRail cumpre até mesmo os mais rigorosos requisitos regulamentares e de negócios. Veja abaixo uma lista com alguns dos padrões e certificações que se aplicam ao VxRail.

Criptografia de dados em repouso do FIPS 140-2 — a publicação 140-2 do Federal Information Processing Standard (FIPS 140-2) estabelece requisitos e padrões para os componentes de hardware e software dos módulos de criptografia. O FIPS 140-2 é obrigatório pelo governo dos EUA e outros setores regulamentados, como instituições financeiras e da área de saúde, que coletam, armazenam, transferem, compartilham e disseminam informações confidenciais, mas não classificadas. Os servidores PowerEdge usados pelo VxRail foram validados.

Common Criteria EAL 2+ — Common Criteria for Information Technology Security Evaluation é um padrão internacional (ISO/IEC 15408) para a certificação da segurança de computadores. As avaliações Common Criteria são executadas em sistemas e produtos de segurança de computadores para avaliar os recursos de segurança dos sistemas e fornecer um nível de confiança para os recursos de segurança dos produtos por meio de requisitos de garantia de segurança (SARs) ou níveis de garantia de avaliação (EALs). A certificação Common Criteria não pode garantir a segurança, mas pode garantir que as afirmações sobre atributos de segurança foram verificadas de maneira independente. Os servidores PowerEdge e os componentes do vSphere usados pelo VxRail detêm a certificação completa.

Estrutura de Segurança Cibernética do NIST — a estrutura do NIST para melhorar a infraestrutura essencial é uma diretriz voluntária desenvolvida para ajudar as organizações a melhorar a segurança cibernética, o gerenciamento de riscos e a resiliência de seus sistemas. O NIST consultou uma ampla variedade de parceiros do governo, do setor e de instituições acadêmicas por mais de um ano para criar um conjunto consensual de diretrizes e práticas sólidas. A publicação especial 800-131A apresenta recomendações para o comprimento das chaves de criptografia.

NSA Suite B — o Suite B é um conjunto de algoritmos criptográficos promulgados pela Agência de Segurança Nacional como parte de seu programa de modernização criptográfica. As versões atuais do ESXi e do vCenter usadas com o VxRail aceitam o NSA Suite B.

Section 508 VPAT — os padrões Section 508 do United States Access Board se aplicam às tecnologias eletrônicas e da informação adquiridas pelo governo federal e definem os requisitos de acesso para pessoas com deficiências físicas, sensoriais ou cognitivas. O servidor PowerEdge e os componentes do software do vSphere usados pelo VxRail cumprem o Section 508 VPAT.

Trade Adjustment Assistance (TAA) — o Trade Adjustment Assistance é um programa federal que oferece um caminho para o crescimento dos empregos e das oportunidades por meio de auxílio aos funcionários dos EUA que perderam seus trabalhos como resultado do comércio exterior. Quando vendido como um sistema, o VxRail é compatível com o TAA.

DISA-STIG — a Agência de Sistemas de Informação de Defesa (DESA) do Departamento de Defesa (DOD) dos Estados Unidos desenvolve padrões de configuração conhecidos como Guias de implementação técnica de segurança (STIGs) como uma das formas de manter a segurança da infraestrutura de TI do DOD. Esses guias oferecem orientação técnica para bloquear sistemas de informações e/ou software que, de outra forma, poderiam estar vulneráveis a um ataque. A Dell EMC oferece etapas manuais e automatizadas para a configuração do equipamento VxRail a fim de garantir a conformidade com os requisitos do STIG de redes de informação (DISA) do DOD.

IPv6 — o IPv6 é o protocolo de última geração usado pela Internet. Além de resolver as limitações de endereçamento do IPv4, o IPv6 tem uma série de benefícios de segurança, e muitos ambientes estão começando a adotar o IPv6. O VxRail foi aprovado no teste de interoperabilidade para IPv6 do USGv6 no modo de pilha dupla, bem como o padrão mais alto no teste de preparo para IPv6.

Trusted Platform Module — o Trusted Computing Group define a especificação Trusted Platform Module (TPM). O TPM 1.2 e 2.0 estão opcionalmente disponíveis com o VxRail. Ambos são certificações com requisitos de segurança do FIPS 140-2, TCG e Common Criteria. O vSphere aceita o TPM 1.2 e o TPM 2.0

Estrutura de Segurança Cibernética do NIST e VxRail

A Estrutura de Segurança Cibernética do NIST (NIST CSF) oferece uma estrutura de políticas de orientação sobre a segurança de computadores, que define como as organizações do setor privado podem avaliar e aprimorar a respectiva habilidade de impedir, detectar e responder a ataques cibernéticos. Essa estrutura voluntária consiste em padrões, diretrizes e melhores práticas para gerenciar os riscos relacionados à segurança cibernética. A abordagem priorizada, flexível e econômica da estrutura de segurança cibernética ajuda a promover a proteção e a resiliência das infraestruturas essenciais.

O material “central” da NIST CSF é organizado em cinco “funções”, que são subdivididas em categorias, como visto na Figura 12 abaixo.

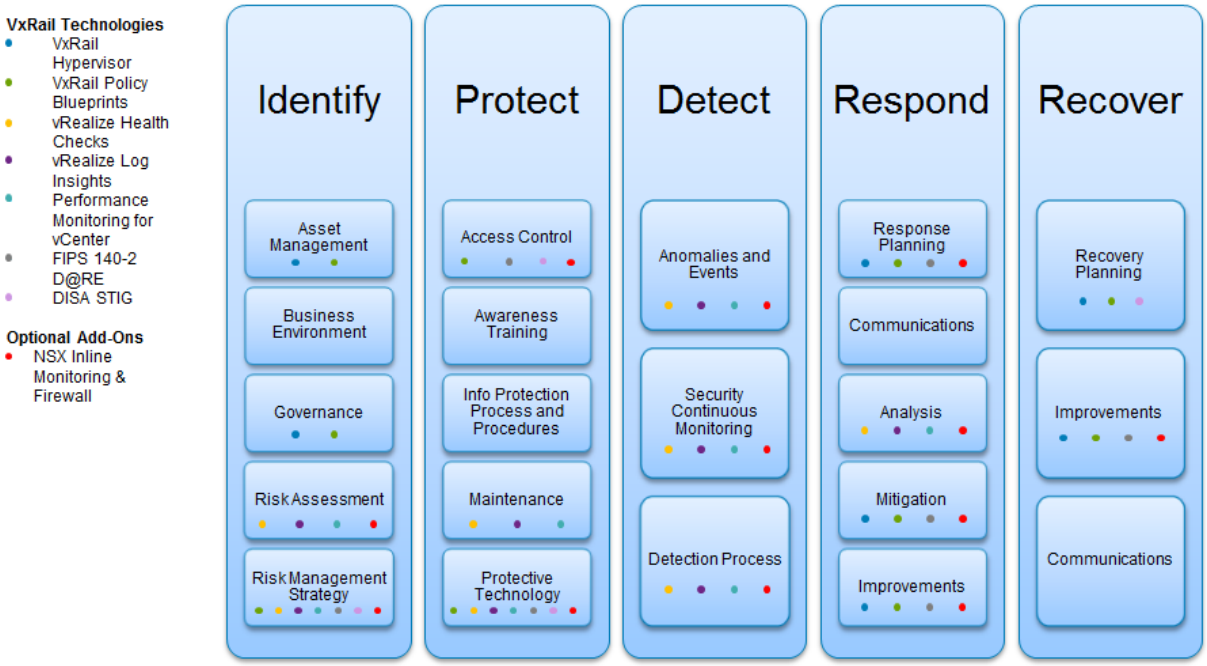

Figura 12: Instituto Nacional de Padrões e Tecnologia, Estrutura de Segurança Cibernética

Acesse o site do NIST para obter mais informações sobre a NIST CSF. Para obter mais informações sobre como o VxRail se alinha à NIST CSF, consulte o documento VxRail Features Supporting NIST Cyber Security Framework, disponível aqui: Estrutura de Segurança.

Parceiros e soluções de segurança do VxRail

O VxRail foi projetado com segurança integrada e implementada seguindo melhores práticas de segurança. Os usuários são autenticados e autorizados com o nível de acesso adequado. Os clusters do VxRail são facilmente configurados com a criptografia de dados em repouso para proteger a confidencialidade das informações contidas, o tráfego de segmentos de configuração de rede padrão e com ferramentas como o RecoverPoint for VMs, garantindo que os aplicativos e serviços possam ser rapidamente recuperados se a integridade dos dados for comprometida. Esses recursos de segurança são fundamentais e inerentes ao equipamento VxRail.

No entanto, proteger um ambiente contra as ameaças atuais exige “defesa profunda” com várias camadas de segurança. As redes que conectam os aplicativos e serviços executados no equipamento VxRail para os usuários que os consomem devem ser protegidas, e os próprios aplicativos e serviços também devem ser protegidos. Firewalls, sistemas de prevenção e detecção de invasão, antivírus/antimalware, proteção de endpoints, além de operações de segurança e gerenciamento fazem parte de uma defesa multicamada. Somente a Dell Technologies têm a amplitude completa de tecnologias e serviços para ajudar você a proteger totalmente seu ambiente.

O porte de sua organização e onde ela está na jornada de transformação da TI determinarão a abordagem adequada. Alguns ambientes podem estar funcionando nas estruturas de segurança existentes, enquanto outros podem aproveitar a oportunidade de transformar as operações de segurança à medida que transformam a infraestrutura de TI. Geralmente, as organizações utilizam muitos fornecedores diferentes como parte do respectivo programa de segurança, o que aumenta a complexidade e, consequentemente, os riscos. A RSA e a Secureworks fazem parte da família Dell Technologies e ambas ajudam a gerenciar riscos e a proteger seus ativos digitais. Somente a Dell Technologies pode oferecer um relacionamento de fornecedor único com conhecimento especializado em segurança em todo o mundo e um ecossistema de milhares de parceiros. A Figura 13 abaixo ilustra o poder da Dell para ajudar você a gerenciar riscos e proteger seus dados.

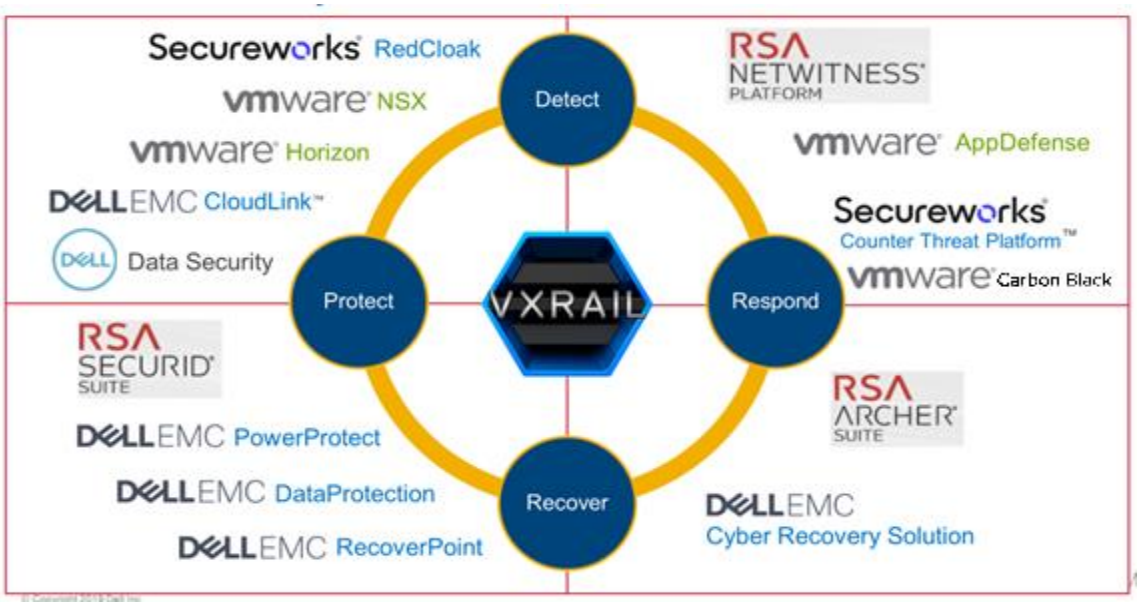

Figura 13: O poder da Dell para ajudar você a gerenciar riscos e proteger seus dados

Gerenciamento de identidade e acesso

O VxRail aceita contas de usuário locais, integração ao LDAP e logon único. Embora seja possível ter um VxRail independente, a maioria dos ambientes se integrará aos sistemas empresariais de gerenciamento de identidade e acesso (IAM) que usam serviços de diretório, como o Microsoft Active Directory.

Gerenciamento de eventos e incidentes de segurança

O equipamento VxRail inclui o vRealize Log Insight para centralizar o gerenciamento de eventos do sistema. Para organizações que têm uma instalação existente de gerenciamento de eventos centralizado, como Splunk ou um sistema de gerenciamento de eventos e incidentes de segurança (SIEM), o VxRail pode ser facilmente integrado usando a interface syslog padrão do setor. O RSA NetWitness Suite oferece coleta de logs, análise e muitos outros recursos de segurança que aprimoram as funcionalidades de segurança do VxRail.

Para os clientes que não desejam gerenciar eventos de segurança por conta própria, a Secureworks oferece serviços de gerenciamento de eventos para o VxRail e praticamente qualquer ativo de informação ou tecnologia de segurança essencial. A Secureworks coleta e monitora as informações de segurança de que você precisa para manter sua empresa protegida. O mais importante é que os especialistas em segurança da Secureworks, que trabalham em Centros de operações contra ameaças integrados, investigam e respondem imediatamente e 24x7 a qualquer atividade mal-intencionada.

Servidor de gerenciamento de chaves

A criptografia é uma ferramenta avançada para proteger a confidencialidade das informações, e o VxRail tem recursos de criptografia incorporados para proteger os dados em uso, em trânsito e em repouso. Entretanto, a segurança de dados fornecida pela criptografia só é tão boa quanto a geração, a proteção e o gerenciamento das chaves usadas no processo de criptografia.

As chaves de criptografia devem estar disponíveis quando forem necessárias, e o acesso às chaves durante as atividades de descriptografia deve ser preservado durante a vida útil dos dados. Portanto, o gerenciamento adequado das chaves de criptografia é essencial para o uso efetivo da criptografia. Muitas organizações centralizam o gerenciamento de chaves em toda a empresa para simplificá-lo, além de impor políticas e fornecer relatórios e auditorias de conformidade.

O VxRail e o vSphere aceitam o protocolo de interoperabilidade de gerenciamento de chaves (KMIP), permitindo que ele funcione com muitos sistemas empresariais de gerenciamento de chaves. O Dell EMC CloudLink oferece gerenciamento de chaves compatível com KMIP, bem como criptografia para as nuvens pública, privada e híbrida. Para organizações com serviços existentes de gerenciamento de chaves, o VxRail e o vSphere se integram facilmente, fornecendo um ponto único de gerenciamento de chaves em toda a empresa. A VMware oferece uma lista de servidores de gerenciamento de chaves compatíveis.

Outros parceiros de segurança

Proteger a infraestrutura de TI e os ativos digitais atuais é uma tarefa complexa. Uma única solução não pode oferecer uma defesa suficientemente robusta. É por isso que a Dell Technologies oferece um ecossistema de parceiros que trabalham em conjunto para lidar com as vulnerabilidades e os riscos exclusivos de seu ambiente. Reconhecemos que todo o setor deve trabalhar em conjunto para ajudar nossos clientes a cumprir suas respectivas metas de segurança cibernética.

O equipamento Dell EMC VxRail e o VMware vSphere aceitam padrões de segurança abertos, e os parceiros desempenham um papel importante para ajudar nossos clientes na transição para um universo de TI seguro, virtual e em várias nuvens.

O white paper “VMware Integrated Partner Solutions for Networking and Security” vinculado ao Apêndice A inclui uma lista com algumas soluções de parceiros de sistema de rede, segurança e conformidade, que são integradas ao VMware vSphere®, vCenter™, vShield Endpoint™ e vCloud® Networking and Security™, além de apresentar o conjunto completo de aplicativos e produtos de software compatíveis com o vSphere. Além das APIs EPSEC para a proteção antivírus/antimalware fornecidas pelo vShield Endpoint, a estrutura de ecossistema do VMware vCloud oferece inserção de serviços no nível da vNIC e da borda virtual. O Guia de compatibilidade da VMware torna fácil encontrar o componente certo.

Conclusão

A transformação da segurança começa com uma infraestrutura de TI segura. O VxRail oferece uma infraestrutura moderna e segura do núcleo à borda e à nuvem. Uma infraestrutura hiperconvergente, o VxRail é projetado, desenvolvido, criado e gerenciado como um produto único para reduzir a possível superfície de ataque ao diminuir o número de componentes que estão envolvidos na infraestrutura. Os pacotes compostos de gerenciamento do ciclo de vida do software VxRail podem incluir atualizações de BIOS, firmware, hypervisor, vSphere ou qualquer um dos componentes de gerenciamento incluídos, o que torna a atualização da pilha de software completa muito mais simples e reduz a vulnerabilidade aos ataques.

A proteção total de um ambiente contra as ameaças de hoje exige “defesa profunda” com várias camadas de segurança. As redes que conectam os aplicativos e serviços executados no equipamento VxRail para os usuários que os consomem devem ser protegidas, e os próprios aplicativos e serviços também devem ser protegidos. Firewalls, sistemas de prevenção e detecção de invasão, antivírus/antimalware, proteção de endpoints, além de operações de segurança e gerenciamento fazem parte de uma defesa multicamada.

A Dell Technologies compreende a segurança e tem especialistas em todo o mundo que podem ajudar a avaliar seu ambiente e projetar um plano de segurança para atender a seus requisitos exclusivos. Entre em contato com um representante de vendas da Dell Technologies para obter mais informações.

Apêndice A: Referências

Todos os links e referências mencionados neste white paper são exibidos abaixo.

Controle	URL
Segurança baseada em risco:	https://www.riskbasedsecurity.com/2019/02/13/over-6500-data-breaches-and-more-than-5-billion-records-exposed-in-2018/
Segurança dos produtos EMC:	https://www.dellemc.com/pt-br/products/security/index.htm
O ciclo de vida de desenvolvimento da segurança da Dell EMC:	https://www.dellemc.com/pt-br/products/security/index.htm#tab0=2
Equipe de resposta a incidentes de segurança de produtos Dell (PSIRT):	https://www.dell.com/support/contents/us/en/19/article/product-support/self-support-knowledgebase/security-antivirus/alerts-vulnerabilities/dell-vulnerability-response-policy
Segurança da resiliência cibernética na 14ª geração de servidores Dell EMC PowerEdge:	http://en.community.dell.com/techcenter/extras/m/white_papers/20444755/download
AppDefense:	https://www.vmware.com/products/appdefense.html
VMware Cloud Foundation on VxRail Architecture Guide:	https://www.dellemc.com/resources/pt-br/asset/technical-guides-support-information/products/converged-infrastructure/vmware_cloud_foundation_on_vxrail_architecture_guide.pdf
VMware Product Security:	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/VMware-Product-Security.pdf
Guia de sistema de rede do Dell EMC VxRail:	https://www.dellemc.com/resources/en-us/asset/technical-guides-support-information/products/converged-infrastructure/h15300-VxRail-network-guide.pdf
Guia Using SpoofGuard da VMware:	https://docs.vmware.com/en/VMware-NSX-for-vSphere/6.4/com.vmware.nsx.admin.doc/GUID-06047822-8572-4711-8401-BE16C274EFD3.html
Documentação do 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
Segurança para soluções hiperconvergentes:	https://communities.vmware.com/servlet/JiveServlet/download/36084-3-183512/Security for Hyper-Converged Solutions_NSX.pdf
2019 Trustwave Global Security Report:	https://www.trustwave.com/Resources/Library/Documents/2019-Trustwave-Global-Security-Report/
*1 Relatório de investigação sobre violações de dados de 2017.	http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017
*2 “20th CEO Survey” da PWC com 5.351 membros do público em 22 países.	https://www.pwc.com/jg/en/publications/pwc-ceo-report-2017%20(2).pdf
Estrutura de Segurança Cibernética do NIST:	https://www.nist.gov/cyberframework
Lista de servidores de gerenciamento de chaves compatíveis:	https://www.vmware.com/resources/compatibility/search.php?deviceCategory=kms&details=1&page=1&display_interval=10&sortColumn=Partner&sortOrder=Asc

Soluções de parceiros integradas da VMware para sistema de rede e segurança:	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vcns/vmware-integrated-partner-solutions-networking-security.pdf
Guia de compatibilidade da VMware:	https://www.vmware.com/resources/compatibility/search.php
Livro técnico do VxRail:	https://www.emc.com/collateral/technical-documentation/h15104-VxRail-appliance-techbook.pdf
Recursos de segurança do integrated Dell Remote Access Controller (iDRAC):	http://en.community.dell.com/techcenter/extras/m/white_papers/20441744/download
Documentação do vSAN:	https://docs.vmware.com/en/VMware-vSAN/index.html
Quatro transformações dos negócios:	https://www.youtube.com/watch?v=TcKJ39_4Rwc
Certificações de criptografia da VMware:	https://www.vmware.com/en/security/certifications/fips.html
VMware vRealize Log Insight:	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vrealize-log-insight/vrealize-log-insight-datasheet.pdf
Certificações do NIST para a pesquisa do FIPS 140-2 por fornecedor para Dell EMC e VMware:	https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search
Ciclo de vida de desenvolvimento seguro da VMware:	https://www.vmware.com/security/sdl.html
Gerenciamento de chaves da VMware:	https://blogs.vmware.com/vsphere/2017/10/key-manager-concepts-toplogy-basics-vm-vsan-encryption.html
Guia de fortalecimento do vSphere 6.5:	https://docs.vmware.com/en/VMware-vSphere/6.5/vsphere-esxi-vcenter-server-65-security-guide.pdf
Como conquistar a confiança com os programas de segurança de produto da DELL EMC:	https://brazil.emc.com/products/security/index.htm
	Recursos do ACE
Demonstração em vídeo de visão geral do ACE	https://vxrail.is/acedemo
Demonstração em vídeo de preparo do pacote de atualizações inteligentes	https://vxrail.is/aceupdates
Visão geral da solução	https://www.dellemc.com/resources/pt-br/asset/offering-overview-documents/products/converged-infrastructure/vxrail-ace-solution-brief.pdf
Visão geral do Dell Technologies MyService360	https://www.delltechnologies.com/en-us/services/support-deployment-technologies/my-service-360.htm
Segurança abrangente por padrão do VxRail (white paper)	https://www.dellemc.com/resources/pt-br/asset/white-papers/products/converged-infrastructure/VxRail_Comprehensive_Security_by_Design.pdf
Práticas de segurança dos produtos Dell Technologies	https://www.delltechnologies.com/pt-br/products/security/index.htm
	YouTube — recursos de segurança
YouTube — Visão geral da segurança do VxRail	https://www.youtube.com/watch?v=ZTNmYBgJv4s
YouTube — Fortalecimento e conformidade de segurança do VxRail	https://www.youtube.com/watch?v=ZjhfCE5nq6U