

설계의 관점에서 본 DELL EMC VXRAIL 어플라이언스의 종합 보안

개요

VxRail™ 어플라이언스는 IT 인프라스트럭처 및 보안 혁신을 위한 이상적인 플랫폼으로, 데이터 및 비즈니스 애플리케이션을 안전하게 보호하는 보호 계층을 제공합니다. Dell Technologies만이 진화하고 있는 오늘날의 위협 환경에 대처할 수 있는 완벽하고 포괄적인 솔루션을 제공할 수 있습니다. 이 가이드에서는 VxRail을 엣지에서 중앙 데이터 센터 그리고 클라우드까지 보호하는 통합 보안 기능과 옵션 보안 기능, 모범 사례, 검증된 기술을 모두 다룹니다.

2020 년 3 월

목차

목차	2
소개	4
Dell Technologies 와 함께 시작하는 보안 혁신	5
디지털 미래를 향한 가교	7
Dell EMC 제품 보안 프로그램을 통한 신뢰 구축	7
SDL(Security Development Lifecycle)	7
보안 개발	8
Dell EMC 의 취약성 대응	9
공급망 위험 관리	9
업계 협업으로 제품 보안 개선	10
업계 제품 보안 그룹에 참여	10
VxRail: 데이터 센터 현대화 및 IT 혁신을 위한 기반	12
Dell EMC VxRail HCI 시스템 소프트웨어	13
VMware vSphere	14
VMware vCenter Server	15
VMware ESXI 하이퍼바이저	15
VMware 가상 네트워킹	15
VMware vSAN	15
스토리지 정책 기반 관리(SPBM)	17
VMware vRealize Log Insight	17
NSX 를 포함한 VCF(VMware Cloud Foundation)	17
VxRail 보안 기능	18
데이터 보안	18
기밀 유지	18
무결성	21
가용성	21
시스템 보안	23
VxRail 인증, 권한 부여 및 계정 관리	23
VxRail 물리적 위치 보안	24
자동화	24

VxRail STIG 강화 패키지	25
VxRail ACE 에 내장된 보안	25
VxRail ACE 보안 개요	25
VxRail ACE 데이터 수집.....	26
Dell 에 전송되는 VxRail ACE 데이터.....	26
저장된 VxRail ACE 데이터	27
VxRail ACE 데이터 액세스 제어.....	27
VxRail ACE 에 대한 최종 사용자 액세스	27
Dell EMC IT 가 관리하는 VxRail ACE 인프라스트럭처에 대한 관리 액세스	27
표준 및 인증 준수	28
NIST 사이버 보안 프레임워크 및 VxRail.....	29
VxRail 보안 솔루션 및 파트너	31
ID 및 액세스 관리	31
보안 인시던트 및 이벤트 관리	31
키 관리 서버	32
기타 보안 파트너	32
결론	33

소개

모든 산업 전반에서 많은 조직이 차별화된 제품과 서비스를 운영 및 제공하는 방식을 현대화 및 혁신하고 있습니다. 데이터가 상주하는 위치, 액세스 방법, 엣지에서 중앙 데이터 센터 그리고 클라우드에 이르기까지 디바이스 수가 기하급수적으로 늘어나고 있습니다. 인증, 방화벽, 규정 준수 및 사이버 범죄 대응에 중점을 둔 보안은 언제나 IT의 한 부분일 것입니다. 보안은 이제 더 이상 일련의 프로젝트라 할 수 없으며 끊임없이 검토하고 분석해야 하는 지속적인 과제가 되었습니다. Dell Technologies는 보안이 성능을 저하시키지 않고 오히려 혁신을 가속화하여 고객이 새롭고 전략적인 방식으로 생각할 수 있게 도와 새로운 영업 기회를 확보할 수 있다고 생각합니다.

Dell EMC VxRail은 중앙 데이터 센터에서 엣지 그리고 클라우드에 이르기까지 가장 빠르고 간단한 방법으로 보안 혁신을 구현합니다. VxRail은 전체 스택 무결성 및 포괄적인 수명주기 관리로 비즈니스 변화에 신속하게 대응하는 인프라스트럭처를 제공하여 운영 효율성을 높이고, 위험을 줄이며, 팀이 비즈니스에 집중할 수 있도록 지원합니다. VxRail 시스템을 도입하여 운영 사일로를 제거하고 신속한 프로비저닝과 워크로드 배포로 지속적인 혁신을 가능하게 하면, 상당한 비용을 절감하고 운영 효율성을 높일 수 있어 단순히 비즈니스 운영을 지원하는 것이 아닌 IT 조직이 비즈니스 기회를 창출할 수 있게 됩니다. VMware 개선을 목적으로 VMware에 최적화되고 VMware를 사용하는 VxRail은 VxRail 하이퍼 컨버티드 인프라스트럭처 구축, 프로비저닝, 관리, 모니터링 및 업데이트에서 발생하는 운영 복잡성을 제거하기 위해 VMware와 공동으로 엔지니어링된 최초이자 유일한 HCI 시스템입니다.

VxRail은 모든 수준의 통합 기술 스택에서 기본으로 보안 기능을 제공합니다. 통합 VMware 소프트웨어를 비롯한 VxRail HCI 시스템 소프트웨어를 통해 각 프로세서 및 PowerEdge 서버부터 시작하여 중앙 데이터 센터에서 엣지 그리고 클라우드에 이르는 보안으로 기존 워크로드부터 클라우드 네이티브 워크로드까지 모든 워크로드에 대한 가용성, 무결성 및 신뢰성을 보장합니다.

Dell Technologies 와 함께 시작하는 보안 혁신

Dell Technologies의 보안 혁신이란 보안에 대해 다시 생각해보고 혁신을 가속화하는 것입니다. Dell Technologies는 Dell Technologies 회사 간의 협력에서부터 개발 및 출시된 제품에 이르기까지 모든 수준의 보안에 중점을 둡니다. VxRail도 예외가 아닙니다. 최고 수준의 제품 보안 보증을 바탕으로 구축되어 완벽하게 통합된 보안 기능을 제공하므로, 조직은 엣지에서 중앙 데이터 센터 그리고 클라우드에 이르기까지(아래 그림 참조) 사이버 보안 회복탄력성을 최적화하여 혁신을 가속화할 수 있습니다.

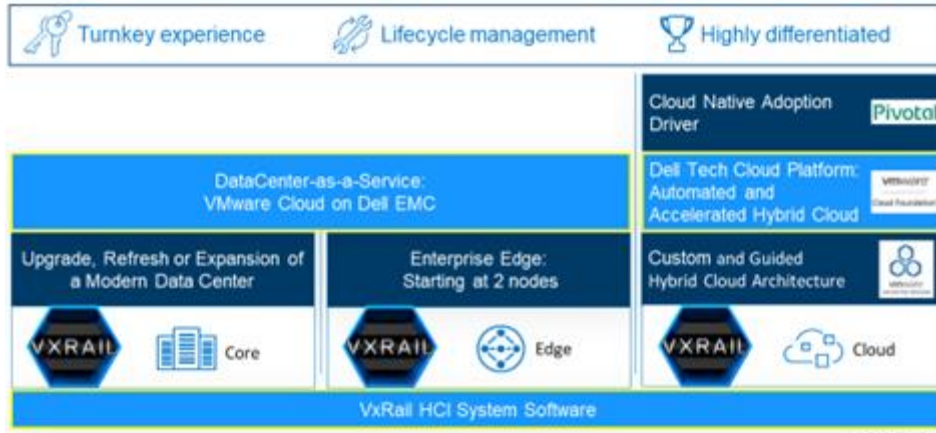


그림 1: 중앙 데이터 센터에서 엣지 그리고 클라우드에 이르는 보안

2019년 중반 Forbes [보고서](#), [2019 MidYear QuickView Data Breach Report](#)에 새로 발행된 Risk Based Security 연구 조사에 따르면, 2019년 상반기 동안 공개된 보안 침해 사례는 3,800건이 넘으며, 41억 건에 달하는 엄청난 양의 기록이 손상되었습니다. 이러한 수치를 바탕으로 2019년에 발생할 보안 침해 건수가 2018년에 같은 회사에서 보고한 공개된 데이터 손상 건수인 6,515건을 넘어설 것으로 보입니다.

Dell Technologies는 고객의 현대화 이니셔티브에 보안 전략이 부합할 수 있도록 지원하여 비즈니스 위험을 줄입니다.

1. 보안 프로그램을 전체적인 비즈니스 위험과 통합하여 허용할 가치가 있는 위험 요소를 파악합니다.
2. 변화하는 위험 환경에 맞게 조정되는 고급 보안 운영을 구현하여 위험에 효과적으로 대응할 수 있습니다.
3. 엔드포인트, 네트워크, 애플리케이션 및 데이터를 보호하는 복원력이 뛰어난 모던 인프라스트럭처를 구축합니다.
4. 신뢰할 수 있는 자문 서비스로 보안 혁신 프로그램의 설계 및 구현을 지원합니다. Dell Technologies는 이러한 모든 영역을 해결하도록 지원할 수 있는 독보적인 입지를 확보하고 있습니다.

여러 수준의 보안이 포함된 계층형 방어는 필수적이지만 이러한 모든 요소가 유기적으로 작동해야 합니다. 보안 혁신은 보안을 염두에 두고 설계 및 구축된 VxRail과 같은 사이버 복구 성능이 뛰어난 모던 인프라스트럭처에서 시작합니다.

오늘날의 진화하는 위험 환경에서는 이러한 위험을 방지 또는 완화하기 위해 접근 방식을 변경해야 합니다. 오래된 인프라스트럭처는 방어하기가 어려우며, 여러 공급업체의 포인트 제품을 사용하면 복잡성이 가중되고 악용할 수 있는 취약성의 위험이 높아집니다. 이러한 수준의 복잡성은 부정 행위자에게 여러 엔트리 포인트를 제공합니다.

보안 표준 및 규정 준수도 고려해야 하는 사항입니다. 규정 미준수로 인해 상당한 수준의 법적, 재정적 불이익이 종종 발생합니다. 사람들은 보안 침해가 발생한 회사와 사업을 하는 것을 꺼리므로, 비록 비용이 들더라도 이러한 벌금을 내는 것이 보안 침해로 인해 회사의 평판이 떨어지는 것보다 비즈니스에 미치는 영향이 적습니다.

- PCI DSS(Payment Card Industry Data Security Standard) – 신용카드 소지자 보호
- GDPR(General Data Protection Regulation) – 유럽 연합의 데이터 프라이버시 규정
- 독일 BDSG(Bundesdatenschutzgesetz) – 구체적인 데이터 보호법

- SOX(Sarbanes-Oxley Act) - 공공기업의 재무 보고와 관련된 기밀 데이터 보호
- GLBA(Gramm-Leach-Bliley Act) – 금융 서비스 산업의 NPPI(Nonpublic Personal Information) 보호
- HIPAA(Health Insurance Portability & Accountability Act) – 전자 환자 의료 데이터 및 정보 보호
- CCPA(California Consumer Privacy Act) - 캘리포니아 주민에 대한 개인 정보 보호 권리 및 소비자 보호 강화(2018년 6월 28일 제정)

Dell Technologies는 보안 혁신이 신뢰할 수 있는 파트너를 확보하는 것에 달려있다고 생각합니다. 디지털 위험 관리를 지원하고, 관리된 보안 서비스를 제공하며, 인프라스트럭처에서 애플리케이션에 이르는 전체 스택을 보호하는 전문 지식, 서비스, 솔루션 및 제품을 제공하고 운영을 간소화하여 보안이 비즈니스 전략에 필수 요소가 되도록 만드는 파트너가 필요합니다.

Dell Technologies는 보안 혁신을 위한 신뢰할 수 있는 보안 파트너입니다. 엔드포인트, 데이터 센터, 개발자, ID, 보안 운영, 클라우드, 가상화 등 어느 곳에 중점을 두든지 포괄적인 보안이 필요하며, Dell Technologies는 이를 지원할 수 있습니다. 보안 및 비즈니스 위험을 해결하고 보안 침해를 처리하며 랜섬웨어 공격으로부터 복구하고 보안 애플리케이션을 구축할 수 있습니다. 보안은 많은 사람들에게 있어 좋거나 나쁘거나 등의 다양한 의미를 갖습니다. 하지만 어떤 상황에서도 Dell Technologies는 조직의 보안 혁신에 함께하기를 원합니다.

디지털 미래를 향한 가교

오늘날 비즈니스 문제를 해결하기 위해 그 어느 때보다 IT를 많이 사용하고 있습니다. 조직은 데이터 분석, AI(Artificial Intelligence), 새로운 애플리케이션 및 스마트 디바이스를 구현하는 등 IT를 활용해 엄청난 양의 데이터를 생성하고 있습니다. 이 데이터를 활용하여 실용적인 통찰력과 차별화된 경쟁 우위를 확보합니다. 그렇지만 여전히 많은 조직에는 명확한 디지털 비전과 전략이 부족하고, 오래된 기술을 사용하며, 제약을 만들고, 변화에 저항하는 문화를 조성하고 있습니다. 적절한 계획이 없다면 일이 벌어진 후에 위험과 보안을 고려하거나 더 큰 전략적 논의에 포함시키지 않습니다. 기술적으로 중요한 이 시점에 사후 대응적인 비즈니스 방식은 더 이상 통하지 않습니다. 혁신을 가속화하고 디지털 미래에 대한 잠재력을 실현하려면 조직은 보안을 이해하는 방법을 다시 생각해야 합니다.

일반적으로 IT 세계에서는 보안을 긍정적인 변화의 촉진제로 보기보다는 장애물로 보는 경우가 더 많습니다. 매일 이루어지는 보안 작업은 까다롭지만 보상을 기대하기 힘들며, 경영진들은 ROI(Return on Investment)를 얻기 어렵습니다. 보안 직원은 커져가는 위협과 복잡한 시스템을 관리하고, 끊임없이 변하는 환경에 대한 실무 지식을 유지해야 합니다. 사이버 공격이 매일 빗발치는 것처럼 보도하는 뉴스를 보면 조직이 소유한 모든 것들이 한순간에 사라질 것 같아 불안해지고 스트레스가 가중됩니다. 그러나 보안이 이렇게 두려움과 좌절감을 불러일으키는 것만은 아닙니다. 보안은 항상 더욱 긍정적이고 사전 예방적인 방법을 추구하고자 하며, 이는 올바른 사고 방식과 기술로만 이뤄질 수 있습니다. 보안과 위험에 대해 계속 과거와 같은 방식으로 생각할 수는 없습니다. 이를 다른 관점에서 설명하자면 자동차의 브레이크와 비슷합니다. 브레이크는 속도를 늦추기 위해 존재한다고 생각할 수 있지만 브레이크를 사용하여 더 빨리 달릴 수도 있습니다. 브레이크를 이용해 장애물과 앞길에 대비하면서 자신 있게 속도를 올릴 수 있습니다. 보안과 위험 역시 조직의 속도를 늦추는 요인이 아니라 조직을 위한 가속기로 보아야 합니다.

Dell EMC 제품 보안 프로그램을 통한 신뢰 구축

Dell EMC는 2002년에 회사의 초점이 기존 스토리지 하드웨어 공급업체에서 엔터프라이즈급 소프트웨어 제공업체로 전환되면서 제품 보안 정책을 수립하기 시작했습니다. Dell EMC는 2004년에 취약성 대응 프로그램을 출시하고 2005년에 전사적 제품 보안 정책을 수립했습니다. 이 정책은 모든 Dell EMC 제품을 포괄하며, 광범위하지만 명확한 보안 표준을 준수합니다. 이 정책은 지속적으로 업데이트되었으며, 2007년에 Dell EMC의 새로운 SDL(Security Development Lifecycle)에 통합되었습니다. SDL은 제품 개발 및 배포의 모든 단계에 측정 가능하고 반복 가능한 일련의 보안 방침을 제공합니다. 또한 2012년에는 공급망 위험 관리 프로그램을 수립하여 보안 방침을 Dell EMC의 제품 구성 요소 공급업체로 확장했습니다. Dell EMC는 업계 표준 및 프로세스의 최첨단 제품 보안 프로그램을 계속해서 발전시키고 있습니다.

Dell EMC는 VxRail을 이용해 보안에 대한 노력을 계속하고 있습니다. VxRail의 개발 수명주기는 [Dell EMC 제품 보안](#) 개발 프로세스 및 Security Development Lifecycle 적용을 따릅니다. [Dell EMC Security Development Lifecycle](#)은 제품을 시장에 출시하기 전 경영진 수준의 위험 관리를 거치는 엄격한 보안 제품 개발 방식을 따릅니다. 또한 VMware vSphere는 이와 유사한 Security Development Lifecycle을 사용하여 개발된 VxRail 하이퍼 컨버지드 인프라스트럭처의 상당 부분을 차지합니다.

SDL(Security Development Lifecycle)

Dell EMC Security Development Lifecycle은 제품 수명주기 전반에 걸쳐 필요한 작업을 요약하여 제품에 보안 회복탄력성과 일관된 보안 기능을 구축하고 외부에 보고된 보안 취약성에 신속하게 대응합니다. 업계 모범 사례에 부합하는 Dell EMC는 제품 R&D 조직에서 구현한 제어 기능을 기반으로 합니다. 그림 2는 SDL의 일부로 수행되는 몇 가지 일반적인 작업을 보여줍니다.

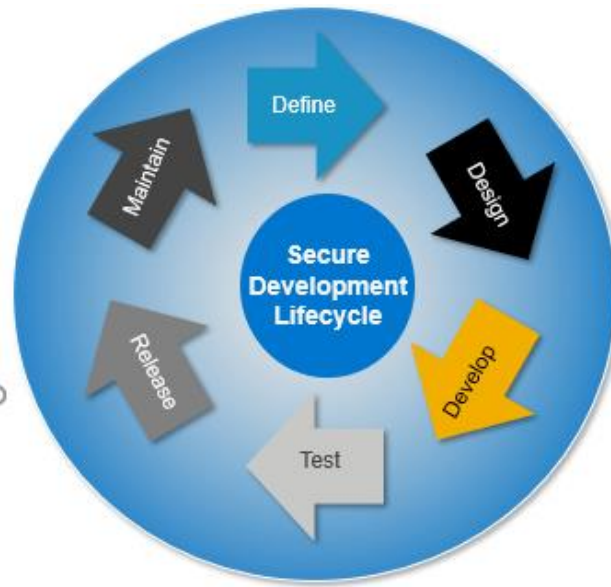


그림 2: Dell EMC SDL 작업

PSO(Product Security Office) 보안 고문과 긴밀히 협업하는 제품 R&D 조직 내 보안 담당자가 이러한 제어 기능의 구현과 검증을 주도합니다. 그림 3은 이러한 SDL이 일반적인 민첩한 수명주기에 어떻게 매핑되는지 보여줍니다.

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

그림 3: SDL 및 일반적인 민첩한 수명주기

스코어카드는 Dell EMC의 비즈니스 전반에서 사용되는 메커니즘으로, 제품/솔루션의 DA(Directed Availability)/GA(General Availability) 출시일에 제품 및 솔루션의 보안 상태를 파악합니다.

보안 개발

Dell EMC의 포괄적인 보안 개발 방식은 제품의 소프트웨어 취약성 및 설계상 약점의 위험을 최소화하는 데 중점을 둡니다.

보안 소프트웨어 개발을 위한 이러한 포괄적인 방식은 정책, 인력, 프로세스 및 기술 전반에 걸쳐 적용되며 다음을 포함합니다.

- Dell EMC 제품 보안 정책은 Dell EMC 제품 조직들이 시장의 기대치와 업계 모범 사례를 바탕으로 제품 보안을 벤치마크하고자 할 때 공통적으로 참조하는 기준입니다.
- Dell EMC 엔지니어링 팀은 보안의 중요성을 이해하는 엔지니어링 커뮤니티입니다. 모든 엔지니어는 직무 관련 보안 모범 사례와 관련 리소스 사용 방법을 교육하는 역할 기반 보안 엔지니어링 프로그램에 참석합니다. Dell EMC는 전체 엔지니어링 커뮤니티 전체의 보안 의식을 높이기 위해 최선을 다하고 있습니다.
- Dell EMC 개발 프로세스는 안전하고 반복 가능합니다. SDL은 표준 개발 프로세스를 적용하여 Dell EMC 제품 보안 규정을 철저하게 준수합니다.
- Dell EMC 개발 팀은 업계 최고 수준의 보안 기술을 기반으로 합니다. Dell EMC는 최첨단 RSA 기술을 활용하여 인증, 권한 부여, 감사, 책임 소재 파악, 암호화, 키 관리 등의 일반적인 소프트웨어 보안 요소에 대한 2개의 소프트웨어, 표준, 사양 및 설계를 개발했습니다. 필요한 경우 개방형 인터페이스를 사용하여 고객의 기존 보안 아키텍처와 통합할 수도 있습니다.
- Dell EMC의 SDL은 표준 개발 프로세스에 보안을 적용하여 Dell EMC 제품 보안 규정을 철저하게 준수합니다. Dell EMC SDL은 제품을 시장에 출시하기 전 경영진 수준의 위험 관리를 거치는 엄격한 제품 개발 방식을 따릅니다.
- SDL은 보안 설계 표준 내에 있는 더 광범위한 프로세스의 일부입니다. 안전한 설계 표준은 Dell EMC 제품에 보안을 구축하기 위한 벤치마크입니다. 이 표준은 모든 제품 기능의 보안과 관련이 있으며, Dell EMC가 고객에게 제공하는 모든 제품에 구축되어 있어야 하는 필수 보안 기능을 나타냅니다. 이 표준으로 Dell EMC 제품은 다음과 같은 이점을 얻을 수 있습니다.
 - 고객의 엄격한 보안 요구 사항을 충족하고,
 - 고객이 PCI, HIPAA 등의 규제 요건을 충족할 수 있도록 지원하며,
 - 보안 취약성으로 인해 Dell EMC 제품 및 고객 환경에 미치는 위험을 최소화합니다.
 - 소스 코드 보호는 제품 관련 지적 재산권에 대한 소스 코드를 포함하는 Dell EMC 엔지니어링 시스템을 올바르게 보호하고 고객 환경에 배포된 제품의 무결성을 보장하는 방법을 명시합니다.

Dell EMC의 취약성 대응

공격자는 모든 시스템 구성 요소의 보안 취약성을 이용하여 전체 IT 인프라스트럭처에 침투해 인프라스트럭처를 손상시킬 수 있습니다. 취약성을 초기에 발견한 시간부터 수정이 가능한 시간까지 공격자와 방어자는 서로 경쟁합니다. Dell EMC의 최우선 과제는 이러한 시간 격차를 최소화하여 위험을 줄이는 것입니다.

[Dell PSIRT\(Product Security Incident Response Team\)](#)에서 대응 조치를 조율하고 외부에서 발견된 Dell EMC 제품 취약성을 공개하는 업무를 담당합니다. PSIRT는 취약성으로 인해 발생하는 위험을 해결하기 위해 고객에게 적시에 정보와 지침, 완화 전략을 제공합니다.

누구든지 Dell의 웹사이트나 이메일을 이용해 제품의 잠재적인 보안 결함을 Dell에 알릴 수 있습니다. 모든 제보는 업계 가이드라인에 따라 조사, 검증, 문제 해결 및 보고됩니다.

Dell은 제품 취약성에 대한 정보를 모든 고객에게 동시에 공개합니다. Dell은 보안 권장 사항을 이용하여 취약성의 심각도를 파악하고 표준화된 여러 보고 시스템을 활용하여 정보를 전파합니다. Dell의 공개 정책은 다른 제품 보안 사례와 마찬가지로 업계 모범 사례를 기반으로 합니다.

공급망 위험 관리

성공적인 제품 보안 프로그램은 포괄적이며 아웃소싱된 구성 요소 및 소프트웨어로 확장됩니다. 공급망 내 무결성 테스트는 신뢰 구축 및 유지에 있어 필수적인 요소입니다. Dell Technologies에는 공식 공급망 위험 관리 프로그램이 있어 회사의 제품에 사용하는 하드웨어 구성 요소의 소스가 제대로 검증된 것인지 확인할 수 있습니다.

공급망 보안은 물리적 자산, 재고, 정보, 지적 재산, 사람을 보호하는 예방과 탐지 통제 방식의 실행과 적용을 말합니다. 물리적 자산, 정보, 개인 보안을 해결하면 멀웨어와 위조된 구성 요소가 공급망에 악의적으로 침입할 수 있는 기회를 줄여 공급망을 보증할 수 있습니다.

Dell의 공급망 위험 관리 프레임워크(아래)는 NIPP(National Infrastructure Protection Plan)의 포괄적인 위험 관리 프레임워크를 반영하며, 정부와 민간 부문이 어떻게 협력하여 위험을 줄이고 보안 목표를 달성할 수 있는지 설명합니다. Dell의 프레임워크에는 개방형 피드백 루프가 포함되어 있어 지속적인 개선이 가능합니다. 전체 솔루션 수명주기에서 위험 완화 계획의 적절한 우선 순위가 매겨지고 이행됩니다. 그림 4는 공급망 위험 관리 프로세스를 보여줍니다.

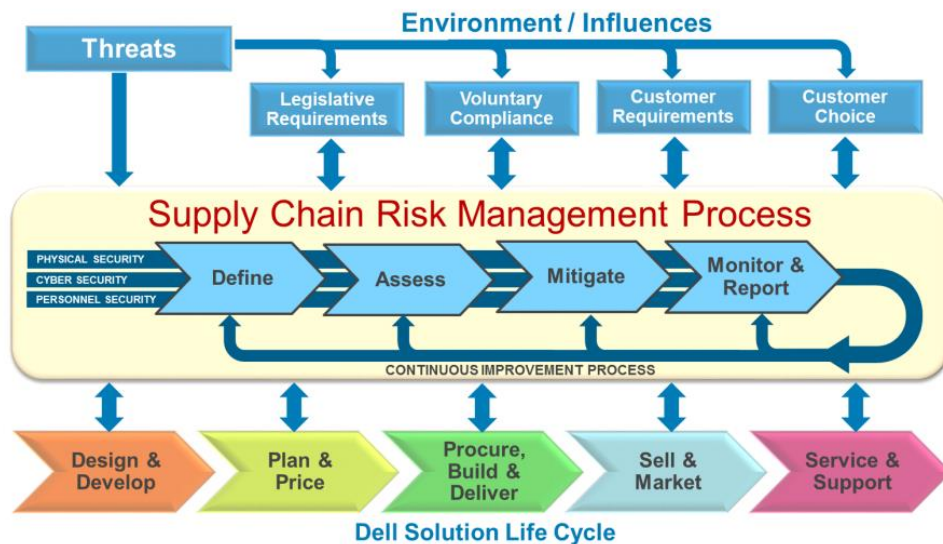


그림 4: Dell 공급망 위험 관리 프로세스

업계 협업으로 제품 보안 개선

Dell Technologies는 끊임없이 발생할 뿐만 아니라 상호 간에 밀접하게 연결된 시스템으로 조직 간에 빠르게 확산되는 보안 위협을 처리할 수 있는 가장 효율적이고 효과적인 방법은 협업을 통한 접근 방식이라고 생각합니다.

높아진 위험을 고려할 때 기술 공급업체는 제품 보안에 관해서는 시장에서의 경쟁 목표를 잠시 미뤄둬야 합니다. 모든 IT 제품 보안 문제를 단일 공급업체에서 자체적으로 해결할 수는 없습니다. IT 보안은 집단적이고 협력적인 노력입니다. Dell Technologies는 시장을 모두가 성장할 수 있는 장소로 유지하려면 다른 기업과 협력해야 한다고 생각합니다.

Dell Technologies는 수십 년 동안 제품 보안 분야에서 힘을 쏟으며 성공적인 개선과 통찰력을 얻는 등 많은 혁신을 달성했으며, 습득한 내용을 공개적으로 고객, 동료, 파트너와 공유하고 있습니다. Dell Technologies는 고객의 IT 시스템이 Dell Technologies 제품에서만 실행되는 것이 아니라는 점을 이해하고 있으므로, 제품이 운영되는 모든 지원 환경의 보안을 개선하기 위해 최선을 다합니다. 즉, 산업 전반에 적극적으로 참여하고 있으며, 긍정적으로 기여하기 위해 노력하고 있습니다.

제품 보안을 향상하기 위한 오랜 노력으로 Dell Technologies에는 새로운 업계 구성원을 지원하고 성장을 장려해야 할 의무가 생겼습니다. 회사의 제품 보안 책임자는 컨퍼런스, 블로그 포스트 및 기타 사교적, 공식적 공간을 활용하여 아이디어를 공개적으로 교환할 수 있습니다.

업계 제품 보안 그룹에 참여

Dell Technologies는 제품 보안 그룹에 활발히 참여하고 있으며, 이곳에서 진보적인 모범 사례를 배우고 가르치며, 제품 보안에 대한 공동 책임감을 양성하고 있습니다. Dell Technologies는 다음과 같은 업계 제휴에 참여하고 있습니다.

BSIMM - Building Security in Maturity Model 은 업계의 소프트웨어 보안 이니셔티브를 평가하여 조직이 자체 보안 노력 수준 및 보안을 발전시켜 나갈 방법을 확인할 수 있게 합니다.



Open Group - 이 400 명 규모의 컨소시엄은 IT 인력, 제품 및 서비스에 대해 인정받는 인증 프로그램을 운영하여 IT 표준을 설계 및 개선합니다. Open Group 은 현재 및 앞으로의 IT 요구 사항을 파악하고 이를 충족하기 위해 모범 사례를 수립하거나 공유하고 있습니다.



SAFECode - Dell EMC 가 공동 설립한 Software Assurance Forum for Excellence in Code 는 더 안전하고 신뢰할 수 있는 소프트웨어, 하드웨어 및 서비스를 제공하기 위한 모범 사례를 파악하고 증진하는 업계 선도 조직입니다.



CSA - Cloud Security Alliance 는 보안 클라우드 컴퓨팅 환경을 보장하는 모범 사례를 정의하고 이를 알리기 위해 노력하며 세계를 선도하는 조직입니다.



FIRST - Forum of Incident Response and Security Team 은 인시던트 대응에 있어 인정받는 글로벌 리더입니다. Dell PSIRT 는 FIRSTVxRailteam 의 구성원입니다.



VxRail: 데이터 센터 현대화 및 IT 혁신을 위한 기반

지속적으로 진화하는 보안 위협 환경과의 경쟁에서 승리하기 위해, VxRail은 현재와 미래의 위협에 대비해 방어할 수 있는 적응력을 갖추고 있습니다. VxRail은 현세대의 Dell PowerEdge 서버와 보안 플랫폼 및 유연한 구성 옵션을 제공하는 최신 프로세서 기술을 기반으로 합니다. vSphere는 스토리지 및 서버 가상화를 제공합니다. 워크로드 요구 사항이 증가해도 VxRail은 쉽게 확장할 수 있습니다. 규정이 변경돼도 VxRail의 유연한 구성 옵션을 이용하여 변경 사항에 신속하게 적응할 수 있습니다.

VxRail은 조직이 어떤 업계에 종사하든 관계없이 조직이 사이버 복원력을 최적화하고, 위험을 관리하며, 규정 준수 요건을 충족할 수 있도록 지원합니다. VxRail은 VMware vSAN을 기반으로 하여, 완벽하게 통합 및 사전 구성되고 테스트를 거친 유일한 하이퍼 컨버지드 인프라스트럭처 어플라이언스입니다. VxRail이 데이터 센터든 엣지든 하이브리드 클라우드 솔루션의 일부에 배포되든 관계없이 VxRail은 비즈니스 크리티컬 애플리케이션, VDI 및 원격 인프라스트럭처를 더욱 간단하고 효율적이며 보다 안전하게 제공할 수 있습니다. VxRail을 이용하여 Dell EMC는 고객의 전체 배포 환경에서 사이버 회복탄력성을 최적화하는 데 필요한 기능을 제공할 수 있습니다. 아래 그림 5는 VxRail의 내장 보안 기능을 보여줍니다.

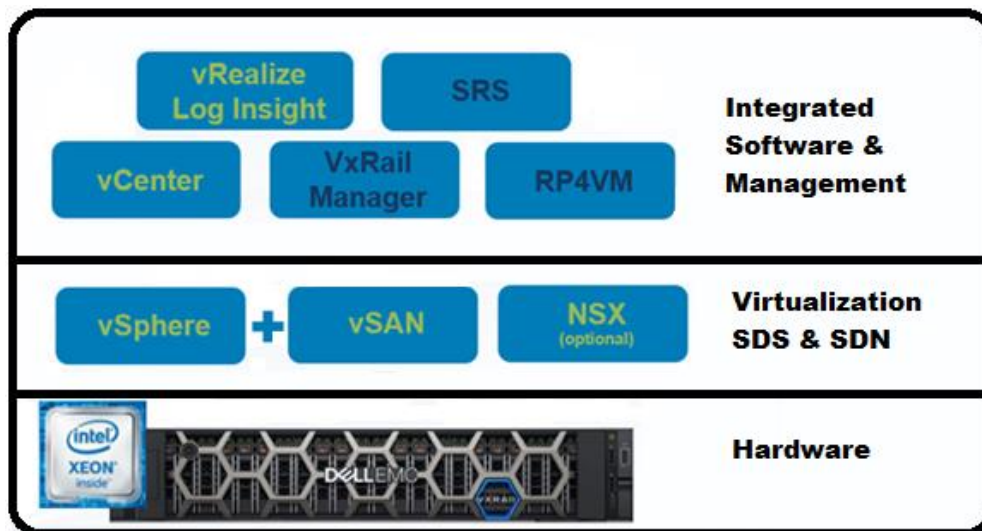


그림 5: VxRail의 내장 보안 기능

Dell EMC PowerEdge 서버

VxRail은 하드웨어 및 시스템 수준 보안 기능을 갖춘 Dell PowerEdge 서버 플랫폼에 구축되며 방어 계층을 이용해 인프라스트럭처를 보호합니다. 보안 침해를 빠르게 탐지하여 시스템을 신뢰할 수 있는 기준으로 복구할 수 있습니다. PowerEdge 서버의 차별화된 보안 기능은 다음과 같습니다.

- 무단 변경 또는 의도하지 않은 변경을 방지하도록 시스템을 잠급니다. 업계 최초로 제공되는 이 기능을 이용하여 보안 취약성을 유발하고 기밀 데이터를 유출시키는 구성 변경을 방지할 수 있습니다.
- UEFI 보안 부팅, BIOS 복구 기능 및 서명된 펌웨어와 같은 기능을 갖춘 사이버 복구 아키텍처는 공격에 대한 향상된 보호 기능을 제공합니다.
- 서버 수준의 System Erase 기능은 서버를 폐기할 때 드라이브 및 모든 비휘발성 메모리에서 모든 사용자 데이터를 신속하고 안전하게 지워 개인 정보를 보호합니다.

Dell EMC PowerEdge 서버는 VxRail 클러스터의 노드를 구성하는 중요한 하드웨어입니다. 각 노드의 CPU, 메모리 및 디스크 리소스는 클러스터에 대해 풀링된 리소스를 제공하고 네트워크 인터페이스는 연결성을 제공합니다. 따라서 안전한 Dell EMC PowerEdge 서버는 VxRail 보안의 토대입니다.

PowerEdge 서버에는 iDRAC라고 하는 통합 원격 액세스 컨트롤러가 있습니다. iDRAC는 안전한 통신, 인증 및 역할 기반 액세스 제어를 사용하여 물리적 시스템의 안전한 원격 관리 및 구성을 지원합니다. 구성 가능한 알림을 이용하여 iDRAC에서 하드웨어에 액세스하거나 구성을 변경할 때마다 SIEM(Security Incident and Event Management) 시스템에 이벤트 정보를 보낼 수 있습니다. 승인되지 않은 변경 사항을 탐지하고 보고하여 VxRail의 무결성을 보호합니다. 자세한 내용은 [Cyber Resilient Security in 14th generation of Dell EMC PowerEdge servers](#)를 참조하십시오.

PowerEdge 서버는 암호화로 서명 및 검증된 펌웨어를 사용하여 신뢰할 수 있는 시스템을 구축합니다. 실리콘에 바로 내장된 보안 기술을 활용합니다. 인텔의 TXT(Trusted Execution Technology)와 같은 기능을 이용하여 서버가 원하는 버전의 펌웨어, BIOS 및 하이퍼바이저만 실행하고, 탐지하지 못한 멀웨어의 유입을 막도록 합니다. 아래 그림 6은 하드웨어 기반의 트러스트를 보여줍니다.

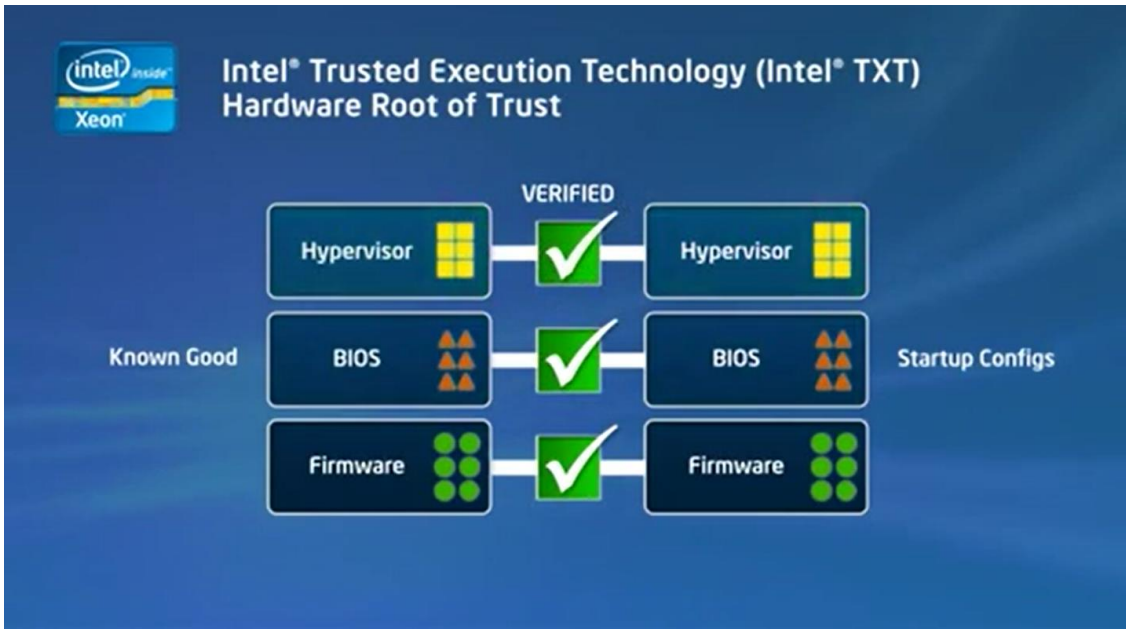


그림 6: 하드웨어 기반의 트러스트

VxRail은 TPM(Trusted Platform Management) 모듈(TPM v1.2 및 v2.0) 옵션으로 노드를 구성하여 서버 무결성에 대한 보호 수준을 더 높일 수 있습니다. TPM은 보안 암호화 프로세스의 국제 표준으로 암호화 키에 높은 보안을 제공하고, 모든 VxRail 노드에 대한 옵션을 제공하도록 설계된 전용 마이크로컨트롤러입니다.

Dell EMC VxRail HCI 시스템 소프트웨어

VxRail HCI 시스템 소프트웨어는 VxRail의 가치 차별화 기능을 위한 기반입니다. 인프라스트럭처 스택 관점에서 보면 VxRail은 VMware 소프트웨어와 PowerEdge 서버에서 실행되는 관리 소프트웨어로 작동하고 VxRail은 단일 통합 시스템으로 작동합니다.

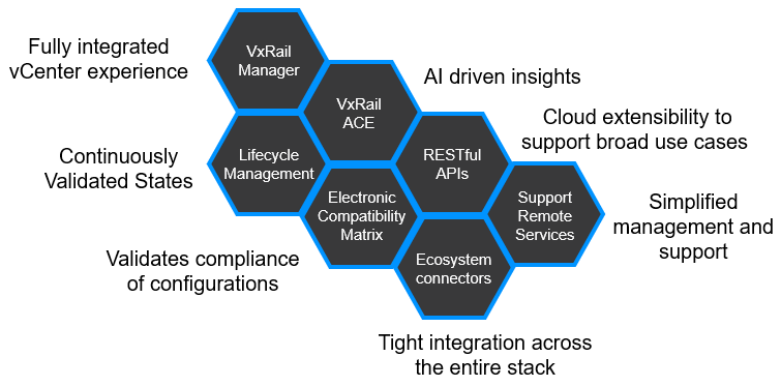


그림 7: VxRail HCI 시스템 소프트웨어

지속적으로 검증된 상태 – VxRail은 VMware 소프트웨어 및 PowerEdge 서버 구성 요소를 포함하여 전체 VxRail 스택에 대해 사전 테스트 및 검증된 소프트웨어 및 펌웨어에서 실행됩니다. VxRail 수명주기 관리 기능은 클러스터가 최신 VMware 소프트웨어 혁신, 보안 수정 또는 버그 수정을 활용하기 위해 지속적으로 변화하는 동안, VxRail 클러스터가 전체 수명주기에 걸쳐 양호한 상태로 실행되도록 합니다. 지속적으로 검증된 상태라는 용어에는 VxRail 클러스터에서 제공하는 구성 안정성이 함축되어 있습니다.

전자 호환성 매트릭스 – 이러한 모든 다양한 소프트웨어 및 하드웨어 구성 요소가 스택에 저장된 상태에서 VxRail 팀이 전체 스택을 지속적으로 테스트하고 검증하므로, VMware 호환성 매트릭스에서 사용자가 결정한 모든 상태를 지속적으로 검증된 상태로 검증합니다. 또한, VxRail은 이 매트릭스를 참조하여 클러스터 구성이 규정을 준수하도록 합니다. 이러한 이점은 고객이 투자해야 하는 테스트 노력과 리소스를 획기적으로 줄여주며 애플리케이션 워크로드에 영향을 주지 않아, 고객은 마음 편히 VxRail 클러스터를 예측 가능한 상태에서 안전하게 발전시킬 수 있습니다.

지원 환경 커넥터 – 광범위한 전자 호환성 매트릭스를 구축하기 위해서는 VxRail이 vSphere, vSAN, vCenter, PowerEdge 서버 및 여러 하드웨어 구성 요소를 포함하는 스택의 생태계 구성 요소와 통신할 수 있어야 합니다. 커넥터를 이용하여 VxRail은 각 구성 요소에서 실행되는 소프트웨어/펌웨어 버전을 파악하고 이러한 구성 요소를 수명주기 전체에 걸쳐 관리할 수 있습니다. 자동화 및 오케스트레이션 기능을 이용하여 VxRail을 단일 통합 시스템으로 관리할 수 있습니다.

VxRail Manager – VxRail의 기본 관리 사용자 인터페이스는 VxRail Manager라고 하는 vCenter 플러그인입니다. VxRail 사용자는 인터페이스를 이용하여 초기 클러스터 구성, 하드웨어 구성 요소 모니터링, 정상적인 클러스터 종료 수행, 노드를 추가하여 클러스터 확장, VxRail HCI 시스템 소프트웨어 업데이트 등 모든 VxRail 활동을 수행할 수 있습니다. 인터페이스에서는 완벽하게 통합된 vCenter 환경을 제공합니다.

VxRail ACE(Analytical Consulting Engine) – VxRail 수명주기 관리 환경을 향상하기 위한 개선 사항으로, VxRail ACE의 분석 컴퓨팅 기능에 따라 대부분의 작업을 수행합니다. ACE는 분석 컨설팅 엔진을 의미합니다. HCI 시스템 소프트웨어가 VxRail 클러스터에 대해 수집한 고급 텔레메트리를 이용하여, ACE는 AI 기반 통찰력을 제공하여 사용자가 클러스터를 사전 예방적으로 관리하여 성능 및 가용성을 개선할 수 있도록 합니다. 또한 AI 기반 통찰력을 이용해 ACE에서 더 능동적인 다중 클러스터 관리 기능을 사용할 수 있으며, HCI 상면이 확장되고 규모에 따른 관리가 필요해짐에 따라 HCI 사용자는 ACE에 더 많은 관심을 보이고 있습니다.

REST API – IT 팀이 클라우드 기반 IT 서비스 제공 모델에 집중하려면 IT 운영 단순화에 초점을 맞추는 것이 중요하므로, VxRail의 수명주기 관리에 대한 이점을 활용하여 VxRail은 이상적인 인프라스트럭처 플랫폼으로 자리매김할 수 있었습니다. API를 이용하여 VxRail 플랫폼을 확장할 수 있게 하면 고객은 서비스형 인프라스트럭처 솔루션을 기반으로 구축할 수 있습니다. 또한 API를 사용하면 규모에 맞게 관리가 가능하므로 다양한 위치에 많은 수의 VxRail 클러스터를 배포하고 사내 스크립트 솔루션을 활용해 규모에 맞게 관리하려는 고객에게 이점을 제공합니다.

원격 서비스 지원 – 지원 환경은 올바른 HCI 솔루션을 선택하는 데 중요한 요소가 될 수 있습니다. VxRail은 Dell 기술 지원을 이용하여 VMware 소프트웨어, PowerEdge 서버 및 VxRail 소프트웨어에 대한 단일 공급업체 지원을 제공합니다. VxRail 지원에는 Call-home을 위한 Dell EMC Secure Remote Service와 전체 수명주기에 대한 원격 모니터링, 진단 및 수리를 위한 사전 예방적 양방향 원격 연결이 포함되어 있어 가용성을 극대화합니다.

VMware vSphere

VMware vSphere 소프트웨어 제품군은 VxRail에 가용성이 높고 회복탄력성을 갖춘 온디맨드 가상 인프라스트럭처를 제공합니다. ESXi, vSAN 및 vCenter Server는 vSphere의 핵심 구성 요소입니다. ESXi는 물리적 VxRail 서버 노드에 설치되어 출고되는 하이퍼바이저로서, 단일 물리 서버가 여러 개의 논리적 서버나 VM을 호스팅할 수 있도록 지원합니다. vSAN은 VM에서 사용하는 소프트웨어 정의 스토리지이며 VMware vCenter Server는 ESXi 호스트, vSAN, VM용 관리 애플리케이션입니다.

vSphere Platinum은 애플리케이션, 인프라스트럭처, 데이터 및 액세스를 보호하도록 설계된 특수 제작된 보안 솔루션입니다. 여기에는 검증된 두 가지 제품이 결합되어 있습니다. vSphere는 인프라스트럭처, 데이터 및 액세스를 보호하고 AppDefense는 VM에서 실행되는 애플리케이션을 보호합니다. [AppDefense](#)는 위협을 탐지하고 예방하기 위해 머신 러닝을 사용해 애플리케이션 및 시스템의 의도된 상태와 행동을 파악하여 vSphere에서 실행 중인 애플리케이션의 무결성을 보호합니다. VMware에서 Platinum 라이선스(구독 포함)를 구매한 VxRail 고객은 vSphere Enterprise Plus를 실행하는 VxRail에서 Platinum 라이선스를 사용할 수 있습니다. vSphere Platinum의 AppDefense 부분에 대한 LCM은 고객의 책임이라는 점을 확인하시기 바랍니다.

Dell EMC와 마찬가지로 VMware는 엄격한 보안 소프트웨어 개발 수명주기 프로세스 및 Security Response Center를 따릅니다. VxRail은 VMware와 공동으로 개발 및 지원되므로 솔루션에 포함된 모든 구성 요소는 보안을 최우선으로 설계, 구축, 테스트 및 배포됩니다. 더 자세한 내용은 [VMware Product Security](#)을 참조하십시오.

VMware vCenter Server

vCenter Server는 서버 가상화와 vSAN 스토리지 모두를 기본적으로 관리할 수 있는 툴입니다. 단일 vCenter 인스턴스는 엔터프라이즈 수준으로 확장되어 수백 개의 VxRail 노드와 수천 개의 VM을 지원할 수 있습니다. VxRail은 VxRail 클러스터 내에 배포된 vCenter 인스턴스를 사용하거나 기존 vCenter 인스턴스를 사용할 수 있습니다.

vCenter는 데이터 센터, 클러스터 및 호스트의 논리적 계층을 제공합니다. 이 계층은 사용 사례 또는 비즈니스 라인별로 리소스를 분류하며, 필요에 따라 리소스를 동적으로 옮길 수 있습니다. 이 모든 작업은 직관적인 단일 인터페이스에서 수행됩니다.

vCenter Server는 인벤토리 서비스, 작업 스케줄링, 통계 로깅, 경고 알림 및 이벤트 관리, VM 프로비저닝 및 구성과 같은 VM 및 리소스 서비스를 제공합니다. 또한 vCenter Server는 다음과 같은 고급 가용성 기능을 제공합니다.

- vSphere vMotion – 다운타임 없이 실시간 VM 워크로드 마이그레이션 가능
- vSphere DRS(Distributed Resource Scheduler) – 클러스터의 노드에서 VM 컴퓨팅 리소스 할당에 대한 지속적인 밸런싱 및 최적화
- vSphere HA(High Availability) – VM 페일오버 및 재시작 기능 제공

VMware ESXi 하이퍼바이저

VxRail에서 ESXi 하이퍼바이저는 클러스터 노드의 VM을 호스팅합니다. VM은 안전하고 이식 가능하며, 각 VM은 프로세서, 메모리, 네트워킹, 스토리지 및 BIOS를 갖춘 완벽한 시스템입니다. VM은 서로 격리되어 있으므로 VM에서 실행되는 게스트 운영 체제에 장애가 발생해도 같은 물리적 호스트의 다른 VM은 영향을 받지 않고 계속 실행됩니다. VM은 CPU에 대한 액세스를 공유하고 ESXi는 CPU 일정을 담당합니다. 또한, ESXi는 VM에 가용 메모리 영역을 할당하고 물리적 호스트와 연결된 물리적 네트워크 카드 및 디스크 컨트롤러에 대한 공유 액세스를 관리합니다. 모든 x86 기반 운영 체제를 지원하며, 동일한 물리적 서버 하드웨어의 VM은 다양한 운영 체제 및 애플리케이션을 실행할 수 있습니다.

VMware 가상 네트워킹

네트워크 트래픽을 격리하는 것이 기본적인 보안 요구 사항입니다. VxRail에서 vSphere의 가상 네트워킹 기능은 유연한 연결 및 격리 기능을 제공합니다. VxRail VM은 동일한 클러스터의 여러 노드에서 단일 논리 스위치로 작동하는 VMware VDS(Virtual Distributed Switch)를 사용해 서로 통신합니다. VDS는 표준 네트워크 프로토콜과 VLAN 구현을 사용하며, 데이터 링크 계층에서 프레임을 전달합니다.

VDS는 데이터 센터 수준에서 vCenter Server에 구성되어 VM이 여러 호스트로 마이그레이션될 때 안전하고 일관적인 네트워크 구성을 유지합니다. VxRail 어플라이언스는 어플라이언스 트래픽과 관련하여 VDS를 사용하며, vSAN은 네트워크 액세스와 관련하여 VDS를 사용합니다.

또한, VxRail을 NSX와 함께 구성하여 초세분화를 활용해 소프트웨어 정의 네트워크 보안 및 더 세밀한 수준의 액세스 제어를 제공할 수 있습니다.

VMware vSAN

VxRail 어플라이언스는 엔터프라이즈급 소프트웨어 정의 스토리지용 VMware vSAN을 기반으로 합니다. vSAN은 vSphere 클러스터에 있는 호스트의 로컬로 연결된 디스크를 취합하여 분산 공유 스토리지 풀을 생성합니다. 클러스터에 디스크를 추가하여 용량을 확장하고, VxRail 노드를 추가하여 용량을 확장할 수 있습니다. vSAN은 vSphere와 완벽히 통합되어 있으며 다른 vSphere 기능과도 원활하게 작동합니다.

vSAN은 뛰어난 효율성과 성능으로 유명합니다. vSAN은 워크로드, 활용도 및 리소스 가용성에 따라 자체적으로 최적화되고 할당을 밸런싱합니다. vSAN은 다양한 워크로드에 적합하며 플래시에 최적화된 고성능 HCI를 제공합니다. 엔터프라이즈급 스토리지 기능은 다음과 같습니다.

- 중복 제거와 압축, 삭제 코딩을 비롯한 효율적인 데이터 정리 기술
- 사용자가 정의한 한계에 따라 워크로드 소비를 제어하는 QoS 정책
- 소프트웨어 체크섬 및 장애 도메인을 포함한 데이터 무결성 및 데이터 보호 기술
- vSAN 저장된 데이터 암호화를 통한 보안 강화

vSAN을 사용하면 각 VxRail 노드의 디스크가 자동으로 단일 캐시 드라이브 및 하나 이상의 대용량 드라이브가 있는 디스크 그룹으로 구성됩니다. 이러한 디스크 그룹은 단일 vSAN 데이터 저장소를 형성하는 데 사용되며, VxRail 클러스터의 모든 노드에서 액세스할 수 있습니다.

VxRail은 두 가지 다른 vSAN 노드 스토리지 구성 옵션을 제공하며, 플래시 SSD와 기계식 HDD를 모두 사용하는 하이브리드 구성과 올플래시 SSD 구성 중에 선택할 수 있습니다. 하이브리드 구성은 캐싱에 플래시 SSD를 사용하고, 용량이 크고 영구적인 데이터 스토리지에는 기계식 HDD를 사용합니다. 올플래시 구성은 캐싱 및 대용량 스토리지 모두에 플래시 SSD를 사용합니다. 그림 8은 vSAN의 기본 개념을 보여줍니다.

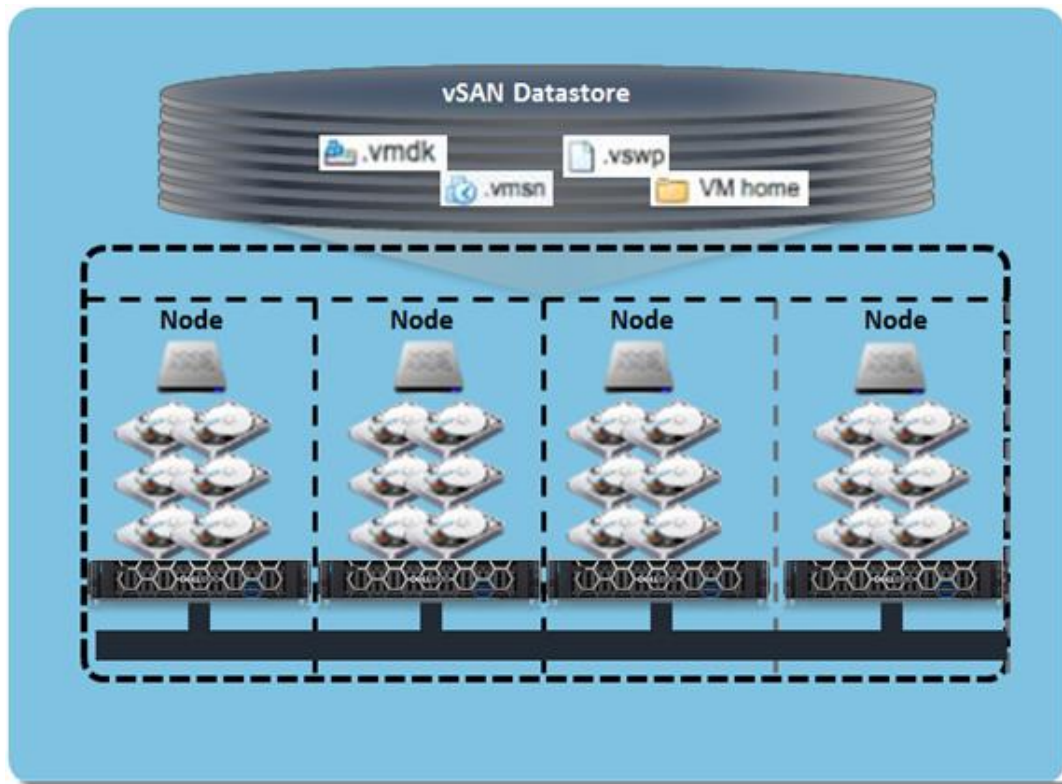


그림 8: vSAN의 기본 개념

vSAN은 VxRail 클러스터가 처음 초기화되고 vCenter를 이용하여 관리되는 경우에 구성됩니다. vSAN은 VxRail 어플라이언스 초기화 프로세스 중에 각 ESXi 노드의 로컬로 연결된 디스크에서 분산 공유 데이터 저장소를 생성합니다. 데이터 저장소의 스토리지 용량은 클러스터에 있는 모든 대용량 드라이브를 포함합니다. 사용할 수 있는 스토리지 용량은 사용하는 보호 수준에 따라 다릅니다. 시스템 초기화의 일부로 수행되는 오케스트레이션된 vSAN 구성 및 검증은 일관되고 예측 가능한 성능과 모범 사례를 따르는 시스템 구성을 보장합니다.

스토리지 정책 기반 관리(SPBM)

vSAN은 정책 중심 스토리지로, 스토리지 프로비저닝 및 관리를 단순화할 수 있도록 설계되었습니다. vSAN 스토리지 정책은 VM의 스토리지 요구 사항을 정의하는 규칙 세트를 기반으로 합니다. 관리자는 요구 사항의 변화에 따라 VM 스토리지 정책을 동적으로 변경할 수 있습니다. SPBM 규칙의 예로는 허용 가능한 오류의 수, 사용할 데이터 보호 기술, 스토리지 수준의 체크섬 활성화 여부 등이 있습니다.

VMware vRealize Log Insight

VxRail과 함께 번들로 제공되는 VMware vRealize Log Insight는 시스템 이벤트를 모니터링하고 가상 환경 및 어플라이언스 하드웨어의 상태에 대한 전반적인 알림 기능을 제공합니다. vRealize Log Insight는 로그 모니터링, 인텔리전트 그룹화 및 분석을 포함해 VxRail 어플라이언스에 대한 실시간 자동 로그 관리 기능을 제공해 VxRail의 물리적, 가상 및 클라우드 환경 전체의 문제 해결을 간소화합니다. 중앙 집중식 로깅은 보안 인프라스트럭처의 기본 요구 사항입니다. 이미 로깅 기능 또는 SIEM(Security Incident and Event Management)을 보유한 고객의 경우, 업계 표준 syslog 프로토콜을 사용하여 VxRail에 쉽게 통합할 수 있습니다.

NSX 를 포함한 VCF(VMware Cloud Foundation)

VxRail의 VMware Cloud Foundation은 Dell EMC가 VMware와 공동으로 엔지니어링한 통합 솔루션으로 0일차부터 2일차까지 전체 SDDC(Software Defined Datacenter)의 운영을 간소화, 효율화 및 자동화하는 기능을 갖추고 있습니다. 새로운 플랫폼은 컴퓨팅(vSphere 및 vCenter 지원), 스토리지(vSAN 지원), 네트워킹(NSX 지원), 보안 및 클라우드 관리(vRealize Suite 지원)을 위한 소프트웨어 정의 서비스 세트를 프라이빗 환경과 퍼블릭 환경 모두에 제공하므로, 이를 하이브리드 클라우드용 운영 허브로 사용할 수 있습니다.

VxRail의 VMware Cloud Foundation은 완벽하게 통합된 하이브리드 클라우드 플랫폼으로 하이브리드 클라우드를 구축하는 가장 간편한 방법을 제공합니다. 이 플랫폼은 기본 VxRail 하드웨어 및 소프트웨어 기능과 vCenter 플러그인 및 Dell EMC 네트워킹 같은 VxRail의 기타 고유한 통합을 활용합니다. 이러한 구성 요소는 함께 작동하여 전체 스택 통합과 함께 새로운 터키 방식의 하이브리드 클라우드 사용자 경험을 제공합니다. 전체 스택 통합을 이용하여 고객은 완전하고 자동화된 수명주기의 단일 터키 형태로 HCI 인프라스트럭처 계층과 클라우드 소프트웨어 스택을 모두 경험할 수 있습니다.

VMware NSX 데이터 센터는 가상 클라우드 네트워크를 지원하는 네트워크 가상화 및 보안 플랫폼입니다. 이는 네트워킹에 대한 소프트웨어 정의 접근 방식으로 데이터 센터, 클라우드, 엔드포인트 및 엣지 위치 전반에 걸쳐 확장됩니다. NSX 데이터 센터를 이용한 스위칭, 라우팅, 방화벽, 로드 밸런싱을 비롯한 네트워크 기능은 애플리케이션에 더 가까이 다가가 환경 전체에 분산됩니다. VM의 운영 모델과 마찬가지로 네트워크를 기본 하드웨어와 독립적으로 프로비저닝하고 관리할 수 있습니다.

NSX 데이터 센터는 소프트웨어에서 전체 네트워크 모델을 재현하여 간단한 네트워크부터 복잡한 다중 계층 네트워크까지 모든 네트워크 토폴로지를 몇 초 만에 생성하고 프로비저닝할 수 있습니다. 사용자는 다양한 요구 사항을 충족하는 여러 개의 가상 네트워크를 생성하고, 초세분화를 비롯해 NSX로 제공되는 서비스 조합을 활용하거나, 차세대 방화벽부터 성능 관리 솔루션에 이르는 광범위한 타사 통합 지원 환경을 활용하여 본질적으로 더 변화 대응 능력과 보안성이 뛰어난 환경을 구축할 수 있습니다. 그런 다음 이러한 서비스를 클라우드 내부와 클라우드 전반의 여러 엔드포인트로 확장할 수 있습니다. 더 자세한 내용은 [VMware Cloud Foundation on VxRail Architecture Guide](#)를 참조하십시오.

VxRail 보안 기능

보안 기능은 2개 섹션 즉, 데이터 보안과 시스템 보안으로 나뉩니다. 그런 다음 VxRail의 보안 시스템 구성 및 관리에 따라 CIA(Confidentiality-Integrity-Availability) 원칙 3요소를 따릅니다.

VxRail은 모든 보안 기능에 완벽히 사전 구성되고 테스트를 거친 스택을 제공합니다. 이러한 보안 기능은 어플라이언스에 통합 및 포함되어 있습니다.

데이터 보안

데이터 보안은 CIA 3요소를 따라 권한이 있는 계정이나 규정 준수 및 사양을 충족하는 특별한 계정에서만 데이터를 사용할 수 있도록 합니다. 이는 데이터에 대한 물리적 및 사용자 수준 액세스를 모두 포함합니다.

기밀 유지

기밀 유지 또는 개인 정보 보호에 있어 가장 기본적인 과제는 기밀 정보가 잘못된 사람에게 도달하는 것을 방지하면서 회사의 데이터에 대해 적절하고 승인된 액세스 권한을 보장하는 것입니다. VxRail은 여러 가지 방법으로 사용 중인 데이터, 이동 중인 데이터, 저장된 데이터의 기밀을 유지합니다.

암호화

암호화는 인증되지 않은 수신자가 이해할 수 없도록 인코딩하여 기밀 정보를 보호합니다. VxRail을 사용하면 vSAN의 D@RE(Data at Rest Encryption)를 이용하여 데이터 저장소를 암호화할 수 있으며, 이는 FIPS 140-2 Level 1 검증 보호 기능을 제공합니다. vSphere 암호화를 사용해 개별 VM을 암호화할 수 있으며, vMotion 암호화를 사용해 이동 중인 VM을 암호화할 수 있습니다. 애플리케이션 요구 사항에 따라 추가적인 암호화 수준을 구성할 수 있습니다.

전체 vSAN 데이터 저장소는 단일 설정으로 암호화되므로 vSAN 암호화는 저장된 데이터를 암호화하는 가장 쉽고 유연한 방법입니다. 이는 데이터 저장소를 사용하는 모든 VM에 대한 클러스터 전체 암호화입니다. 일반적으로 암호화된 데이터는 중복 제거나 압축과 같은 공간 축소 기술의 이점을 누릴 수 없습니다. 하지만 vSAN을 사용하면 중복 제거 및 압축 후 암호화가 수행되므로 이러한 공간 축소 기술의 모든 이점을 유지할 수 있습니다.

VM 암호화는 유연성을 제공하므로 개별 VM 암호화가 가능합니다. 즉, 단일 클러스터에 암호화된 VM과 암호화되지 않은 VM을 둘 수 있습니다. VM 암호화는 호스팅되는 위치와 관계없이 VM을 따라갑니다. 따라서 VM이 VxRail 외부 데이터 저장소로 이동했더라도 암호화된 상태는 유지됩니다.

또한 VM 암호화를 켜고 끌 수 있습니다. 암호화된 VM을 vSphere vMotion으로 마이그레이션하면 항상 암호화된 vSphere vMotion을 사용합니다. 암호화되지 않은 VM은 vMotion을 사용할 때 암호화 옵션이 있어 비활성화, 재량적, 필수 중에 선택할 수 있습니다. vMotion을 사용하는 동안 암호화되지 않은 VM에는 기본적으로 재량적 옵션이 적용됩니다. 아래 그림 9는 VM 암호화 및 vSAN 암호화의 차이점을 요약해서 보여줍니다.

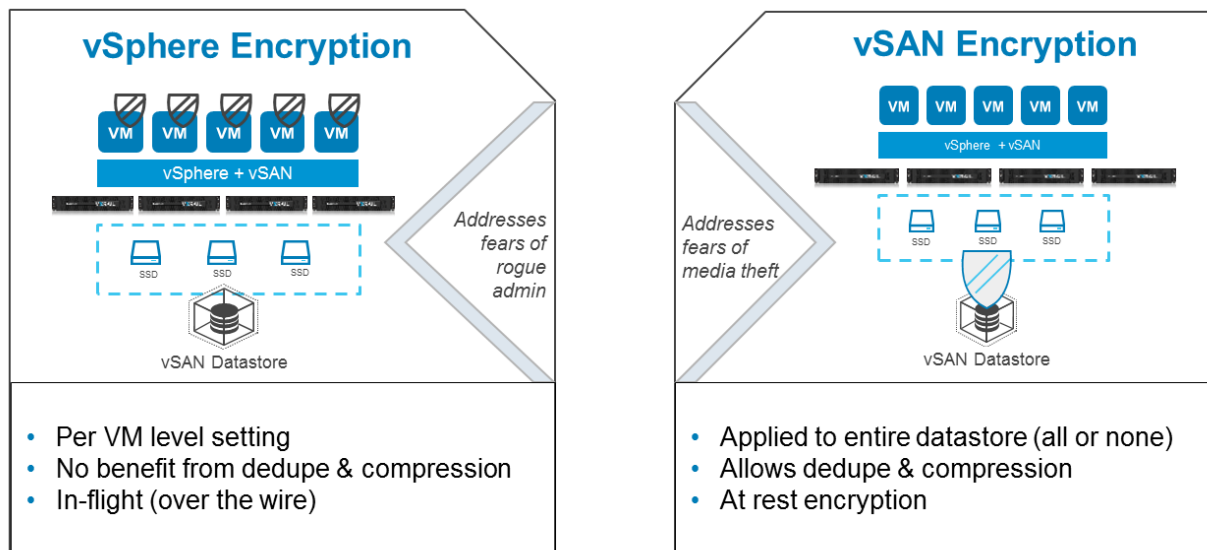


그림 9: VM 암호화 대 vSAN 암호화

또한 VxRail은 호스트 간에 VM을 이동시킬 때 VM을 암호화하는 암호화된 vMotion을 지원합니다. 이는 VxRail 내의 vMotion 마이그레이션뿐만 아니라 vCenter 인스턴스 내에서 VxRail 클러스터로의 vMotion 마이그레이션을 포함합니다. 암호화된 vMotion을 vSAN 암호화와 함께 사용하여 저장된 데이터 암호화 및 전송 중인 데이터 암호화를 모두 수행할 수 있습니다. 암호화된 vMotion은 vSphere 암호화가 활성화된 VM에 적용됩니다.

vSphere가 이동 중인 데이터 암호화에 사용되는 임시 키를 제공하는 vMotion 암호화를 제외하면, 암호화 키의 안전한 생성, 스토리지 및 배포를 위해서는 KMS(Key Management Server)가 필요합니다. 암호화가 활성화되면 vCenter는 KMS와의 신뢰 관계를 구축하고 KMS 연결 정보를 ESXi 호스트에 전달합니다. ESXi 호스트는 KMS에 바로 암호화 키를 요청하고 데이터 암호화 및 복호화를 수행합니다. vCenter 연결은 초기 설정에만 필요합니다.

KMS는 보안 인프라스트럭처의 중요한 구성 요소이기 때문에 DNS, NTP 및 Active Directory와 같은 다른 중요한 인프라스트럭처 구성 요소에 일반적으로 적용되는 것과 동일한 수준의 이중화 및 보호 기능을 갖추어야 합니다. 여기서 중요한 것은 KMS를 암호화하는 요소와 물리적으로 분리하여 실행해야 합니다. 시작하는 동안 ESXi 호스트는 KMS에 키를 요청합니다. KMS를 사용할 수 없는 경우 시스템이 시작을 완료할 수 없습니다.

VxRail 및 VMware는 [Dell EMC CloudLink](#)와 같은 KMIP(Key Management Interoperability Protocol) v1.1 이상과 호환되는 KMS를 지원합니다. VMware는 vSphere로 검증된 KMS의 호환성 가이드를 유지 보수합니다.

vSphere 내 암호화는 FIPS 140-2 검증이 완료된 공통 모듈 세트에서 처리합니다. 이러한 공통 모듈은 VMware Secure Development Lifecycle:에서 설계, 구현 및 검증합니다. VxRail은 암호화를 위한 공통 모듈 세트를 이용하여 암호화를 더 쉽게 구현, 관리 및 지원할 수 있습니다.

vCenter에서 간단한 구성을 설정하면 VxRail에서 암호화가 활성화됩니다. 액세스 제어를 사용하면 인증된 개인만 암호화를 활성화 또는 비활성화할 수 있습니다. "암호화 관리자 없음"이라는 역할을 하는 관리자는 일반적인 관리 작업을 할 수 있지만 암호화 설정은 변경할 수 없습니다.

NSX 옵션을 사용하는 VxRail 소프트웨어 정의 네트워킹

VxRail과 같은 동적 가상 환경은 SDN(Software Defined Networking) 서비스가 제공하는 유연성의 이점을 누릴 수 있습니다. VxRail에 SDN을 적용하는 가장 쉬운 방법은 소프트웨어 라이선스(옵션, VxRail에 미포함)인 VMware NSX를 사용하는 것입니다. NSX는 완벽한 네트워크 가상화 및 보안 플랫폼으로, 관리자가 라우터, 방화벽 및 로드 밸런서를 비롯한 전체 가상 네트워크를 소프트웨어 내에서 만들 수 있습니다. 이 소프트웨어 정의 네트워킹은 기본 물리적 네트워크 인프라스트럭처와 분리되기 때문에 특정 스위치 공급업체에 연결되는 VxRail에 의존하지 않습니다.

VxRail에서 NSX는 추가적인 보안 하드웨어나 소프트웨어 구성 요소를 구축/배포할 필요성을 줄여주는 통합 보안 솔루션입니다. NSX를 함께 사용하면 VxRail 관리자는 초세분화 구성을 이용하여 다양한 테넌트 워크로드를 보호 및 격리하고, 수신 및 송신을 제어하며, 기존의 다중 계층 애플리케이션과 범용 VM, VDI 환경을 비롯한 모든 워크로드에 대해 향상된 보안을 제공할 수 있습니다. NSX를 VxRail과 함께 사용하면 다음과 같은 이점이 있습니다.

- 워크로드에 가장 알맞은 보안 정책을 적용할 수 있습니다. 보안 정책은 소프트웨어에 적용되며, 보안 제어는 워크로드와 함께 클러스터 내 호스트 사이를 이동합니다.
- 보안을 통한 단순화된 관리는 vSphere 스택과 통합되며 vSphere HTML5 웹 클라이언트 및 NSX Manager 플러그인을 이용하여 중앙에서 관리됩니다.
- 그룹 및 정책을 사용하여 일관되고 자동화된 보안 제어가 가능합니다. 워크로드를 자동으로 식별하고 올바른 보안 상태에 동적으로 배치합니다.
- 하이퍼바이저 수준에서 보안 제어를 효율적으로 구현하면 외부 또는 경계 기반 보안 제어와 비교할 때 애플리케이션 레이턴시와 대역폭 소비가 줄어듭니다.
- 트래픽을 제어하기 위해 적절한 허용 및 거부 규칙을 사용하여 인터넷에서 내부 및 외부 클라이언트 모두에 대한 수신 및 송신을 제어할 수 있는 DMZ 수준의 격리가 가능합니다.
- SpoofGuard 기능을 사용하여 스푸핑된 VM IP 주소를 탐지하고 차단합니다. 이 기능에 대한 자세한 내용은 VMware의 [Using SpoofGuard](#) 설명서를 참조하십시오.
- ID 방화벽을 이용해 NSX 관리자가 Active Directory 사용자 기반 DFW 규칙을 만들 수 있습니다. 이 기능에 대한 자세한 내용은 [VMware NSX Documentation](#)를 참조하십시오.
- 침입 탐지 및 침입 방지(IDS/IDP)와 같은 타사 보안 서비스와 통합됩니다.

NSX는 환경의 보안 상태를 개선하고 다음과 같은 인증 및 표준을 준수합니다.

- Common Criteria 인증 - EAL 2+
- ICSA Labs 인증 방화벽
- FIPS 140-2
- 가상화된 워크로드 보호에 대한 모든 NIST 사이버 보안 권장 사항 충족

보안에 VxRail과 함께 VMware NSX 플랫폼(옵션)을 활용하면 방화벽과 보안 정책이 내장되어 있어, 외부로부터 지키는 경계 보안과는 달리 진정한 컨버지드 어플라이언스를 제공할 수 있습니다. NSX를 VxRail과 함께 배포하면 보안 제어가 추가적인 하드웨어나 소프트웨어 구성 요소가 아니라 어플라이언스의 일부가 되므로 새로운 애플리케이션 이니셔티브 배포에 소요되는 시간이 크게 줄어듭니다.

잠금 모드

유연하게 적용되는 강력한 보안이 필요한 환경의 경우, ESXi에 대해 잠금 모드를 구성할 수 있습니다. 잠금 모드에서는 개별 호스트에 수행할 수 있는 관리 작업이 제한되므로 vCenter를 이용하여 관리 작업을 완료해야 합니다.

"일반" 모드에서 잠금 기능을 사용하면 선택된 사용자 그룹을 허용 목록에 추가할 수 있어 vCenter를 통하지 않고 로컬에서 서버를 관리할 수 있습니다. 이 허용 목록에는 특정 VxRail 관리 계정이 포함되어야 합니다.

엄격한 잠금 모드에서는 사용자가 로컬에서 서버를 관리할 수 없습니다. "엄격" 모드의 잠금은 VxRail에서 지원되지 않습니다.

HTTPS로 보안 관리

안전하지 않은 관리 트래픽은 심각한 보안 위험입니다. 따라서 VxRail은 TLS(Transport Layer Security) "TLS 1.2" vCenter, iDRAC 및 HCI 시스템 소프트웨어로 보안된 관리 인터페이스를 사용하며 일반 텍스트 HTTP 인터페이스를 비활성화하고 TLS 1.2를 사용하는 HTTPS를 사용해야 합니다. 또한 ESXi 서버의 명령줄에 액세스하려면 SSH를 사용해야 합니다. SSH 및 HTTPS 사용은 VxRail에 대한 보안 명령과 제어의 중요한 부분입니다.

무결성

회사 데이터의 무결성은 비즈니스 운영에 기본적으로 요구되는 사항입니다. VxRail은 사용자 액세스를 제어하고 데이터 체크섬과 같은 내장된 무결성 기능을 사용하여 수명주기에 걸쳐 데이터의 일관성, 정확성 및 신뢰성을 유지함으로써 데이터 무결성을 보장합니다.

네트워크 세분화

네트워크 세분화는 공격 지점을 줄이기 위해 공용 트래픽에서 전용 네트워크 트래픽을 격리하는 데 사용됩니다. 그리고 네트워크를 통한 공격자의 이동을 제한하는 효과적인 보안 제어 기능이기도 합니다.

VxRail은 하드웨어 관리 네트워크의 물리적 세분화, 애플리케이션 및 인프라스트럭처 네트워크의 가상 세분화, VMware의 NSX 소프트웨어 옵션을 사용한 VM 및 애플리케이션 레벨에서의 초세분화를 비롯해 여러 수준의 네트워크 세분화를 이용하여 엔지니어링되었습니다. 세분화를 하면 중요한 관리 톨의 가시성이 제한되므로 공격자가 시스템에 관리 톨을 사용할 수 없습니다. 적절한 네트워크 분할은 시스템 초기화의 일부로 기본 자동 구성되며, 관리자는 애플리케이션 환경에 필요한 만큼 추가 세분화 수준을 유연하게 정의할 수 있습니다. 네트워크 구성에 대한 모범 사례는 [Dell EMC VxRail Network Guide](#)에서 확인할 수 있습니다.

VxRail은 기본적으로 관리, vSAN, vMotion 및 애플리케이션 트래픽에 대해 별도의 VLAN을 사용하여 트래픽을 세분화하는 VMware Distributed Virtual Switches를 기본으로 사용합니다. vSAN 및 vMotion 네트워크는 라우팅할 수 없는 전용 네트워크입니다. VxRail 네트워크에서 지원하는 애플리케이션에 따라 여러 애플리케이션, 운영/비운영 트래픽 또는 기타 요구 사항을 기반으로 트래픽을 더 세분화할 수 있습니다.

VxRail의 Distributed Virtual Switch는 vSphere NIOC(Network I/O Control)로 기본 구성됩니다. NIOC를 사용하면 서로 다른 VLAN에 물리적 대역폭을 할당할 수 있습니다. 서비스 거부 및 웜과 같은 일부 사이버 공격은 리소스의 과도한 사용을 유도할 수 있습니다. 이로 인해 공격받고 있지 않은 다른 서비스에 대해 리소스 거부가 발생할 수 있습니다. NIOC는 일부 서비스에 공격이 발생한 경우 다른 서비스가 무결성을 유지하는 데 필요한 네트워크 대역폭을 할당 받도록 보장합니다. NIOC 설정은 시스템 초기화 시 권장 모범 사례에 따라 자동으로 구성됩니다. [Dell EMC 네트워크 가이드](#)에서 기본 VxRail VLAN의 NIOC 설정에 대한 자세한 정보를 확인할 수 있습니다.

각 VxRail 노드에는 iDRAC 하드웨어 관리 인터페이스를 위한 별도의 물리적 이더넷 포트가 있습니다. 이 네트워크를 물리적으로 세분화하게 되면 공격자가 하드웨어 관리에 액세스하기가 어려워집니다. 분산된 서비스 거부 공격이 발생한 경우, 물리적으로 세분화된 네트워크는 영향을 받지 않아 잠재적 공격의 범위가 제한됩니다.

UEFI 보안 부팅

UEFI 보안 부팅은 손상 및 루트 키트 공격으로부터 운영 체제를 보호합니다. UEFI 보안 부팅은 펌웨어, 부팅 로더 및 VMkernel이 모두 신뢰할 수 있는 기관에 의해 디지털 서명되었는지 확인합니다. 또한, ESXi용 UEFI 보안 부팅은 VIB(VMware Install Bundle)가 암호화 방식으로 서명되었는지 확인합니다. 이렇게 하여 서버 부트 스택이 모든 정품 소프트웨어를 실행하고 있고 변경되지 않았다는 것을 확인할 수 있습니다.

소프트웨어 체크섬

데이터 무결성의 핵심은 스토리지에서 검색된 데이터가 작성된 이후 변경되지 않았음을 검증하는 것입니다. VxRail은 기본적으로 블록 수준의 포괄적인 데이터 무결성 체크섬을 사용합니다. 체크섬은 데이터와 함께 생성됩니다. 그런 다음 읽기 시 체크섬이 검증되며, 데이터가 작성된 시점으로부터 변경 사항이 있다고 체크섬이 표시하면 RAID 그룹의 다른 구성원에서 재구성됩니다. 또한 vSAN은 사전 예방적 스크러버 메커니즘을 사용하여 자주 액세스하지 않는 데이터에서도 잠재적인 데이터 손상을 탐지 및 수정합니다.

가용성

IT 시스템을 최신 상태로 유지하고, 하드웨어가 제대로 작동하는지 확인하며 적절한 대역폭을 제공하는 것은 모두 권한이 부여된 사용자에게 기업의 데이터 가용성을 유지하기 위한 키스톤입니다. VxRail 수명주기 관리, vSphere 가용성 기능, 사전 예방적 모니터링, 기본 복구 기능뿐만 아니라 하드웨어의 보안 관제 및 보안 시스템 구성을 이용하여 최대 시스템 가용성을 보장합니다.

VxRail 소프트웨어 수명주기 관리

IT 인프라스트럭처를 안전하게 유지하기 위해 조직이 취할 수 있는 가장 중요한 작업 중 하나는 소프트웨어 업데이트와 패치를 최신 상태로 유지하는 것입니다. 업데이트 및 패치는 단순히 잠재적으로 다운타임을 일으키는 문제를 수정하거나 성능을 개선하기 위한 것만이 아니라 보안 취약성을 해결하기 위함이기도 합니다. 보안 커뮤니티 내에서는 엄청난 양의 협업이 이뤄지고 있습니다. VxRail이 VMware와 함께 공동 엔지니어링된 덕분에 보안 수정을 위한 계획을 미리 확인할 수 있어 VxRail 팀은 사전에 인증된 보안 패치를 신속하게 검증하고

준비할 수 있습니다. 하지만 모두가 같은 편일 수는 없으므로 위협을 완화하고 해결하려는 방어자와 취약성을 악용하려는 공격자는 서로 경쟁하게 됩니다. VxRail은 VMware와 함께 공동 엔지니어링되어 보안 수정을 위한 계획을 미리 확인할 수 있어 VxRail 팀은 사전에 인증된 보안 패치를 신속하게 검증하고 준비할 수 있습니다.

VxRail 소프트웨어 수명주기 관리를 이용하여 복잡하고 위험할 수 있는 업데이트 작업을 쉽게 설치하고 안전하게 구현할 수 있습니다. VxRail HCI 시스템은 모든 소프트웨어 구성 요소를 엔지니어링하고 테스트를 거쳤으며 번들로 릴리스한 유일한 시스템입니다. VxRail 소프트웨어 번들은 BIOS, 펌웨어, 하이퍼바이저, vSphere 또는 기타 포함된 관리 구성 요소의 업데이트를 포함할 수 있습니다. 취약성이 발견되면 수정 개발이 신속하게 진행되어 발견된 위치에 관계없이 위협을 완화할 수 있습니다. 업데이트 번들은 고객에게 릴리스되기 전에 VxRail 하드웨어 플랫폼과 전체 VxRail 소프트웨어 스택에서 광범위한 테스트를 거칩니다.

업데이트가 가능하면 HCI 시스템 소프트웨어를 이용하여 관리자에게 알립니다. 관리자는 업데이트 번들을 직접 다운로드하고 오케스트레이션된 업데이트 프로세스를 시작하거나 예약할 수 있습니다. 시스템이 온라인 상태로 비즈니스를 제공하는 동안 업데이트를 롤링 프로세스로 진행할 수 있습니다. 재부팅이 필요한 경우 업데이트를 계속하기 전에 클러스터의 다른 노드로 VM이 자동 마이그레이션됩니다.

HCI 시스템 소프트웨어 수명주기 관리는 복잡성을 줄일 뿐만 아니라 시스템 패치 및 위험 제거에 소요되는 시간과 어려움을 줄여 인프라스트럭처를 더 안전하게 보호합니다.

VxRail vSphere 가용성 기능

VxRail은 VMware HA(High Availability), VMware DRS(Distributed Resource Scheduler) 및 VMware 확장 클러스터를 포함하는 기본 제공 vSphere 가용성을 활용합니다. 이러한 기능을 이용해 VxRail의 자동화 소프트웨어를 지원하며, VxRail에서 호스팅되는 서비스에 지속적인 가용성을 제공합니다. 따라서 이러한 기능이 포함된 vSphere 버전을 사용하는 것이 권장됩니다.

VMware HA는 VxRail 클러스터에서 실행 중인 VM을 모니터링합니다. VM 또는 노드에 오류가 발생하면 HA가 클러스터의 다른 노드에서 다시 시작됩니다. VM에는 사이버 공격, 기본 하드웨어 오류 또는 손상된 소프트웨어 등 여러 가지 이유로 오류가 발생할 수 있습니다. VMware HA에서 운영 중단을 방지하지는 않으나, 서비스를 복원하는 데 걸리는 시간을 최소화합니다.

VMware DRS는 클러스터의 모든 호스트에 VM 워크로드를 분산시킵니다. VM 리소스 요구가 변경되면 DRS는 vSphere vMotion을 사용하여 VM 워크로드를 클러스터 내의 다른 호스트로 마이그레이션합니다. 사이버 공격은 공격 대상이 아닌 VM에 대한 리소스 문제를 일으킬 수 있습니다. 사이버 공격은 종종 공격받는 VM에 과도한 리소스 활용을 유발하여 호스트 수준에서 리소스 활용도가 매우 높아지며, 이로 인해 해당 호스트에 대해 다른 VM이 활용 가능한 리소스에 영향을 미칩니다. DRS는 리소스에 제약이 있는 호스트에서 VM을 마이그레이션하여 VM을 보호하므로 VM은 계속해서 서비스를 제공할 수 있습니다.

VMware 확장 클러스터는 단일 사이트에서 VxRail 클러스터를 두 사이트에 걸쳐 확장하여 더 높은 가용성을 제공합니다. 단 하나의 VM 인스턴스만 존재하지만, 해당 데이터의 완전한 사본을 두 사이트 모두에서 유지 보수합니다. VM이 현재 실행 중인 사이트를 사용할 수 없게 되면 다른 사이트에서 VM을 재시작합니다.

Data Protection

강력한 보안 방어도 매우 중요하지만 강력하고 신뢰할 수 있는 복구 계획도 역시 중요합니다. 백업 및 복제는 보안 침해를 입은 경우 복구의 초석이 됩니다. 복구를 지원하기 위해 HCI 시스템 소프트웨어는 파일 기반 백업 및 복원을 포함합니다. 모든 VxRail 어플라이언스는 동급 최고의 로컬 및 원격 복제와 세분화된 복구를 제공하는 VM용 Dell EMC RecoverPoint(RP4VM) 스타터 팩을 포함하고 있습니다.

HCI 시스템 소프트웨어의 파일 기반 백업 및 복원은 실수로 가상 어플라이언스가 삭제되거나 어플라이언스가 내부적으로 손상되는 것을 방지합니다. 백업을 정기적으로 또는 필요에 따라 수행하도록 구성할 수 있습니다. 이는 vSAN 데이터 저장소 내부의 파일을 백업하는 포괄적인 기능으로 추가 하드웨어 및 소프트웨어가 필요하지 않습니다.

예를 들어, RP4VM을 사용하면 VM이 훼손되거나 데이터가 손상되거나 랜섬웨어에 감염된 경우, VM과 데이터 세트를 공격 이전 시점으로 신속하게 롤백하여 비즈니스를 빠르게 복구할 수 있습니다. VxRail 관리자에서 직접 설치할 수 있는 RP4VM은 신속한 배포가 가능하며, 익숙한 vCenter 플러그인을 이용하여 일상적인 모니터링을 할 수 있습니다. 복구도 익숙한 vSphere 인터페이스를 사용하여 손쉽게 수행할 수 있습니다.

개선했던 포괄적인 데이터 보호 기능이 필요한 조직을 위해, VxRail은 Dell EMC Data Protection Suite For VMware, Dell EMC Power Protect, Dell EMC Data Domain Virtual Edition을 포함한 옵션을 지원합니다.

VxRail HCI 시스템 소프트웨어의 파일 기반 백업은 VxRail VM을 재구축해야 하는 드문 경우에도 비즈니스 연속성 보장을 지원합니다.

시스템 보안

VxRail 인증, 권한 부여 및 계정 관리

AAA(Authentication, Authorization and Accounting) 프레임워크가 내장되어 있습니다. AAA는 적절한 사용자가 시스템을 사용하고 있는지, 어떤 수준의 액세스 권한 가지고 있는지를 확인하고, 누가 어떤 작업을 수행했는지 계정에 활동을 기록하여 액세스를 제어하도록 설계되었습니다.

인증

HCI 시스템 소프트웨어에 대한 인증은 vCenter 플러그인을 이용하여 SSO로 처리됩니다. VxRail vCenter는 인증 보안 정책에 따라 조직의 중앙 집중식 ID 관리 시스템을 지원합니다.

조직은 종종 LDAP를 사용하는 Microsoft AD(Active Directory)와 같은 디렉토리 서비스를 이용하여 ID 관리를 중앙 집중화합니다. VxRail이 도메인의 일부가 아니라 독립 실행형 환경인 경우, vSphere와 iDRAC에서 사용자와 암호를 로컬로 관리할 수 있습니다. 모범 사례를 고려할 때 중앙 집중식 인증을 사용하는 것이 좋습니다.

물리적 서버, VxRail 수명주기 관리, 서버 및 스토리지, 네트워크 가상화 환경의 관리를 담당하는 개인이 다를 수 있습니다. 따라서 VxRail은 iDRAC, HCI 시스템 소프트웨어 및 vSphere에 대해 세분화된 역할 기반 액세스 제어를 사용합니다.

권한 부여

"POLP(Principle of Least Privilege)"를 사용하면 사용자가 역할을 수행하는 데 필요한 권한을 필요한 만큼만 사용자에게 부여할 수 있습니다. vSphere에는 적절한 권한을 부여하는 데 사용할 수 있는 미리 정의된 여러 역할이 포함되어 있습니다. 예를 들어 사용자에게 vSphere 관리자나 HPCIA 관리, 혹은 두 역할 모두를 부여할 수 있습니다. HCIA 관리 역할은 vCenter 내의 VxRail 관리 플러그인에서 VxRail 수명주기 관리 작업을 수행할 수 있는 사용자 권한을 부여합니다. vSphere 관리자는 vCenter에서 관리자 작업을 수행할 수 있는 권한을 부여합니다. 또한 vSphere로 사용자 지정 역할을 생성하여 더욱 세밀한 수준의 액세스 제어가 가능합니다. 예를 들어 권한이 있는 사용자가 경보를 확인하거나 스토리지 프로파일을 생성할 수 있지만 VM을 배포할 수는 없도록 권한을 부여할 수 있습니다.

역할은 사용자, 그룹 및 특정 개체와 관련이 있으며, 여기서 개체란 사물 또는 사물 그룹을 의미합니다. 예를 들어 사용자 또는 그룹은 특정 VM 또는 포트에 대한 경고를 확인할 수 있지만 다른 개체는 확인할 수 없습니다. 또한 "액세스 없음"과 같은 제한적인 역할을 사용자에게 할당하여 vCenter 내의 특정 영역을 볼 수 없게 할 수도 있습니다. 동일한 개체에 대한 같거나 다른 수준의 액세스 권한을 여러 사용자 또는 그룹에 부여할 수 있습니다. 하위 개체에 부여된 권한을 사용해 상위 개체에서 상속된 권한을 재정의할 수 있습니다.

vSphere 역할 기반 액세스 제어는 "최소 권한"과 "책임 분리"의 세분화된 보안 원칙을 지원하며, 보안 관리자가 조직의 시스템 관리 구조에 따라 정확한 권한을 정의하여 보안을 강화할 수 있도록 지원합니다.

회계

구성 및 구성 요소 상태에 대한 변경 사항을 파악하는 것은 시스템을 안전하게 유지하는 데 매우 중요합니다. 변경 사항은 구성 이탈을 유발하는 임시 수정으로 인해 발생할 수도 있고, 침입 발생을 나타내는 것일 수도 있습니다. 인프라스트럭처를 사전 예방적으로 모니터링하는 것은 중요한 보안 활동입니다.

침입이 발생했을 때 이를 적시에 탐지하면 몇 달 동안 침입이 계속되어 여러 중요 시스템이 손상되지 않고, 공격자가 중요 시스템을 손상시킬 수 없는 중단이 잠깐 발생하는 것으로 끝낼 수 있습니다. 감사 로그 시스템을 유지 보수하지 못하면 공격에 대한 적절한 정보를 제공받을 수 없어 공격의 심각도를 결정할 수 없습니다. [2019 Trustwave Global Security Report](#)(로그인 필요)에 따르면 조사한 인사면접의 57%가 기업 및 내부 네트워크와 관련 있습니다. 이는 2017년 50%에서 증가한 수치입니다.

구성 이탈은 모든 시스템에 영향을 주는 문제입니다. 시스템을 안전한 구성 기준으로 시작할 수 있지만 시간이 지남에 따라 변경 사항이 발생해 시스템이 취약해질 수 있습니다. 이러한 변경 사항은 문제 해결 중 발생하는 일시적인 변경이나 기준 구성의 일부에 대한 승인된 변경 등 다양한 이유로 발생할 수 있습니다. 모니터링을 하지 않으면 이러한 변경 사항을 탐지하기는 매우 어렵습니다.

정보 모니터링의 당면 과제는 개별 VM, 물리적 서버, 가상화 인프라스트럭처, 네트워크, 보안 구성 요소 또는 애플리케이션 자체 등 다양한 소스의 정보를 모니터링해야 한다는 것입니다. 이러한 정보를 이해하려면 활동과 변경 사항에 대한 통합된 시각이 필요합니다. VxRail은

vRealize Log Insight를 포함합니다. Log Insight는 서버, 네트워크 디바이스, 스토리지 및 애플리케이션을 포함한 VMware 로그를 컴파일합니다. 아래 이미지에서 볼 수 있듯이, Log Insight는 로그의 데이터를 기반으로 그래프와 함께 대시보드를 생성합니다. 그 결과 관리자는 문제의 근본 원인을 쉽고 빠르게 드릴다운할 수 있습니다. 아래 그림 10은 vRealize Log Insight 대시보드를 보여줍니다.

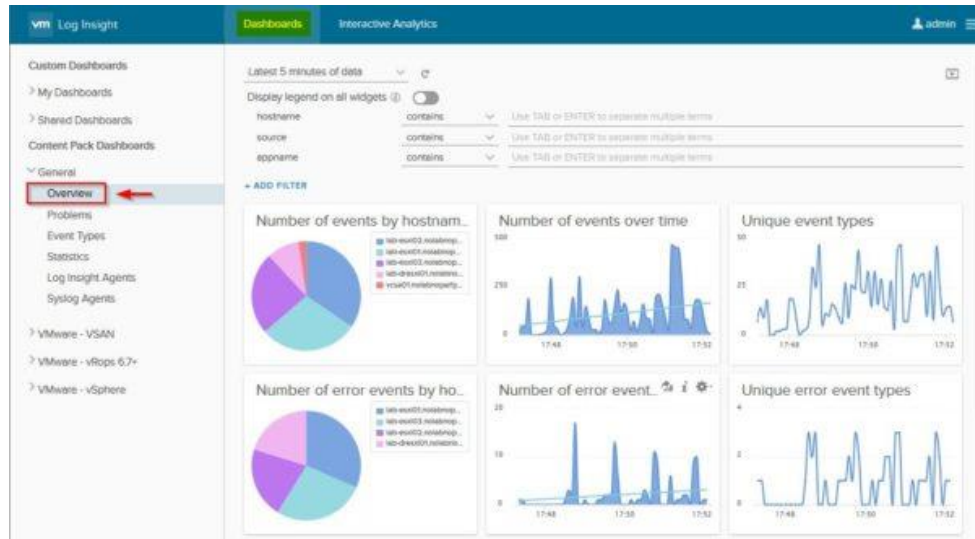


그림 10: Realize Log Insight

모든 정보를 상호 연관시키는 것은 VxRail이 구성 요소 클럭을 동기화 상태로 유지하기 위해 업계 표준 NTP(Network Time Protocol)를 사용하는 많은 이유 중 하나입니다.

이미 로그 관리 시스템 또는 SIEM(Security Incident and Event Management) 시스템을 보유한 조직의 경우, 표준 syslog 프로토콜을 사용하여 VxRail에 쉽게 통합할 수 있습니다.

VxRail 물리적 위치 보안

보안 관제는 포괄적인 보안 솔루션의 핵심적인 부분입니다. VxRail은 기존 데이터 센터 외부에 구축될 수 있기 때문에 보안 관제는 더욱 중요합니다. 멀웨어 또는 감염된 소프트웨어가 USB 드라이브로 유입되는 것을 방지하기 위해, VxRail의 USB 포트를 비활성화했다가 필요할 때만 활성화할 수 있습니다.

또한 VxRail 노드는 새시 열기, 부품 고장 또는 교체, 펌웨어 변경, 온도 경고와 같은 기타 이벤트를 모니터링합니다. 이 정보는 iDRAC 수명주기 로그에 기록됩니다. 대부분의 경우, 새시가 생산에 투입된 후 새시를 열 필요가 없기 때문에 이러한 활동을 추적되는 경우, 이는 시스템을 훼손시키려는 시도를 나타내는 것일 수 있습니다.

자동화

보안 유지 보수에 있어 중요한 부분은 모든 관련 보안 구성 요소가 환경에 있는 모든 개체에 구현되어야 한다는 것입니다. 개별 VxRail 클러스터는 최대 64개의 물리적 노드를 포함할 수 있으며, 하나의 vCenter를 이용하여 여러 개의 VxRail 클러스터를 관리할 수 있으므로 수천 개의 VM을 지원할 수 있습니다. 단순한 변경 사항조차도 모든 VM에 구성해야 하는 경우 상당한 시간이 소요 될 수 있습니다. 또한 반복적인 작업을 수행할 경우 실수가 발생할 수 있습니다. 따라서 자동화가 중요합니다.

자동화를 사용하면 환경에 발생하는 구성 오류가 줄어들고, 더 일관된 구성을 유지하면서 효율성을 높이고, 의사 결정을 내린 후 실제로 구현하는 데까지의 시간을 줄여 의사 결정의 가치 창출 시간을 늘릴 수 있습니다.

vRealize Automation과 같은 호환 툴을 사용하면 vSphere 및 vSAN을 자동화할 수 있습니다. 이러한 툴을 사용해 VM 또는 스토리지 정책 생성과 같은 일상적인 작업을 자동화할 수 있습니다. 또한 vRealize Automation를 사용하여 보안 구성이 적절한 설정을 이탈하지 않았는지 확인할 수 있습니다. 구성이 변경된 경우, vRealize Automation을 이용하여 ESXi 서버, vCenter 또는 개별 VM을 재구성할 수 있어 필수

보안 구성을 다시 충족할 수 있습니다. 또한 vRealize Automation은 표준 VMware 툴이기 때문에 많은 IT 가상화 팀은 vRealize Automation 사용법을 쉽게 익힐 수 있으며, VxRail 클러스터와 함께 사용할 수 있는 프로파일을 쉽게 만들 수 있습니다.

VxRail STIG 강화 패키지

보안 구성은 완화해야 할 동일한 위험이 많은 복잡하고 오류가 발생하기 쉬운 프로세스일 수 있습니다. VxRail 인프라스트럭처 보안 프로세스를 간소화하는 세 가지 요소가 있습니다. 먼저 vSphere를 “기본 보안” 방식으로 구성할 수 있습니다. 둘째, DISA(Defense Information Systems Agency) STIG(Security Technical Implementation Guides)는 보안 강화를 위한 청사진을 제시하며 다양한 자동화 툴을 이용하여 보안 매개변수의 모니터링과 구성을 필요에 따라 확인하고 구성할 수 있습니다. 따라서 비즈니스 요구에 맞게 적절한 위험 프로파일을 구성할 수 있습니다. 마지막으로 예기치 않은 변경 사항이 발생하는 경우 구성을 알려진 보안 상태로 자동으로 되돌리는 기능은 VxRail 보안의 핵심입니다.

VMware는 vSphere 6.0부터 보안을 vSphere의 기본 설정으로 만드는 이니셔티브를 시작했습니다. 이로 인해 VxRail을 처음 사용할 때부터 더 안전하게 보호할 수 있습니다. 이 이니셔티브의 일환으로, 가장 권장되는 보안 설정은 사이트별 설정으로 분류되거나 기본 보안 설정으로 변경되었습니다. 기존에는 설치 후 변경해야 했던 설정이 이제는 업데이트되어 보안 설정이 기본으로 설정됩니다.

사이트별 설정으로 분류되는 구성 설정은 기본 보안 설정으로 구성할 수 없습니다. 원격 syslog 또는 NTP 서버의 호스트 이름을 예로 들 수 있습니다. VxRail을 사용하면 VMware가 사이트별로 분류하는 대부분의 설정이 설치될 때 HCI 시스템 소프트웨어에 의해 구성됩니다.

많은 조직이 STIG를 기준으로 삼아 시스템을 강화합니다. 이러한 STIG는 체크리스트를 사람이 읽을 수 있는 PDF와 자동화된 스크립트로 제공합니다. 따라서 최소한의 수동 개입만으로도 자동화 툴이 STIG를 읽고 권장 구성과 일치하게 환경을 구성할 수 있습니다. 기존 VMware SITG는 vSphere, ESXi 및 vSAN을 포함한 VxRail 구성 요소를 다루며 매우 쉽게 구현할 수 있습니다. VxRail 어플라이언스 소프트웨어 v4.5.x 또는 4.7.x를 실행 중인 Dell VxRail 어플라이언스는 관련 DISA STIG(Security Technical Implementation Guides)의 요구 사항을 준수합니다.

시간이 지남에 따라 보안성이 떨어지는 방향으로 구성이 이탈할 수 있습니다. 따라서 구성을 모니터링하는 것뿐만 아니라 초기 보안 상태로의 환경 복원을 자동화하는 것도 중요합니다. VxRail은 필요한 자동화 수준에 따라 다양한 옵션을 지원합니다. VxRail은 현재 구성을 STIG와 비교하여 확인하는 자동 강화 툴을 제공하며, 구성이 변경된 경우 구성을 알려진 보안 상태로 되돌립니다. 더 강력한 자동화 툴이 필요한 경우, VMware vRealize Suite는 VxRail 환경과 연동하여 규정 준수 및 제어를 유지하면서 구성 관리를 자동화합니다. 또한 VMware는 머신 러닝을 사용하여 VM과 지원하는 애플리케이션에 대해 알려진 양호한 상태에 대한 정보를 수집하는 애플리케이션 중심 툴인 AppDefense를 제공합니다. 이 툴을 사용하면 알려진 양호한 상태의 변형을 탐지했을 때 이를 관리자에게 알리고, 인시던트 대응 작업 라이브러리로 대응을 자동화할 수 있습니다.

VxRail ACE 에 내장된 보안

VxRail ACE(Analytical Consulting Engine)는 VxRail 클러스터를 위한 운영 인텔리전스로 Dell EMC VxRail 에 내장된 운영 편의성을 보완합니다. VxRail ACE 는 운영 편의성 및 운영 인텔리전스를 기본 보안과 결합하여 기업의 IT 인프라스트럭처 혁신을 지원합니다.

VxRail ACE 는 Dell EMC IT 관리형 클라우드 플랫폼에서 실행됩니다. 클라우드 기반 SaaS 솔루션으로서, VxRail ACE 는 중단 없이 자주 새로운 기능을 제공하여 뛰어난 고객 경험을 지원하는 유연성을 제공합니다. VxRail 이 클러스터에 대해 취합할 수 있는 풍부한 메타데이터를 수집함에 따라 딥 러닝을 위한 신경망의 예측 능력은 지속적으로 개선됩니다.

VxRail 사용자는 Dell EMC 지원 자격 증명으로 <https://vxrailace.emc.com> 에서 VxRail ACE 에 액세스할 수 있습니다.

VxRail ACE 보안 개요

VxRail ACE 는 조직의 VxRail 클러스터 전체의 VxRail 노드에서 텔레메트리 데이터를 수집하고, 그림 011 에 나와있는 것처럼 Dell EMC 가 관리하는 SaaS 솔루션에 해당 데이터를 안전하게 전송합니다.

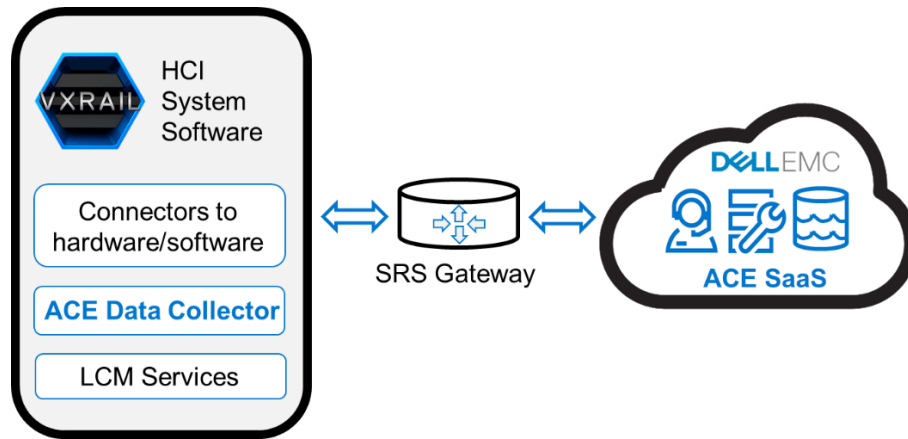


그림 11: VxRail ACE 의 개괄적인 아키텍처 다이어그램

Dell EMC 는 데이터 보안 유지에 대한 고객의 우려를 파악하고 있습니다. 데이터 수집부터 데이터 전송 및 저장까지 VxRail ACE 보안은 기본 사항입니다. 또한, VxRail ACE 는 Dell EMC 표준 Security Development Lifecycle 의 일부로 아키텍처 제어를 사용하여 안전하게 개발되었습니다. 이 표준은 Dell EMC 제품이 보안 취약성으로 인한 제품 및 고객 환경에 미치는 위험을 최소화하기 위해 제품을 구축하고 릴리스할 때 Dell EMC 제품 팀이 준수해야 하는 보안 중심 활동을 정의합니다.

VxRail ACE 데이터 수집

각 VxRail 클러스터에는 VxRail 하드웨어 및 소프트웨어 커넥터를 이용하여 HCI 시스템 소프트웨어에서 텔레메트리 데이터를 가져오는 ADC(Adaptive Data Collector)가 실행되고 있습니다. ADC 는 PII(Personally Identifiable Information)를 수집하지 않습니다. ADC 가 수집하는 텔레메트리 데이터는 표 1 에서 확인할 수 있습니다.

기본 텔레메트리 (하드웨어 토폴로지: 어플라이언스, 드라이브, 펌웨어, PSU)	성능 정보	경보	하드웨어 센서 데이터
- 클러스터 정보 - 어플라이언스 정보	- 클러스터(CPU, 메모리, 디스크) - VM(CPU, 메모리, 디스크) - vSAN(디스크, 네트워크)	- vCenter - VxRail	- 센서 유형 - 상태 - 이름 - 현재 판독값

표 1 ACE 가 수집하는 VxRail 텔레메트리 데이터

ADC 에서 수집한 텔레메트리 데이터는 로컬에 저장되지 않으며, 데이터는 Dell EMC SRS(Secure Remote Support) 게이트웨이를 이용하여 안전하게 전송됩니다.

Dell 에 전송되는 VxRail ACE 데이터

ADC(Adaptive Data Collector)가 수집한 데이터만 Dell EMC 의 SRS(Secure Remote Service) 게이트웨이를 이용하여 Dell EMC 백엔드로 전송됩니다. VxRail ACE 는 SRS 게이트웨이를 이용하여 HCI 시스템 데이터 도착 알람을 수신합니다. VxRail ACE 고객은 게이트웨이를 이용하여 HCI 시스템 데이터를 전송하는 시스템을 제어합니다. Dell EMC SRS 게이트웨이를 이용하여 전송되는 모든 데이터는 전송 중에 업계 표준 모범 사례에 따라 보호됩니다. SRS 게이트웨이는 RSA® 디지털 인증서를 고객 제어 액세스 정책 및 상세한 감사 로그와 함께 사용하여 양방향으로 인증됩니다. P2P(Point to Point) 통신은 모든 데이터가 Dell EMC IT 관리형 인프라스트럭처로 안전하게 전송되도록 보장하는 AES(Advanced Encryption Standard)-256 비트 암호화를 사용하여 이루어집니다. 또한 SRS 는 전용 VPN 및 다단계 인증을 제공합니다. 데이터가 Dell 에 도착하면, VxRail ACE 는 자체 Dell EMC IT 관리형 인프라스트럭처에서 ACE 데이터를 암호화하고 저장합니다.

저장된 VxRail ACE 데이터

VxRail ACE 관리형 시스템에서 수신한 HCI 시스템 데이터는 Dell EMC IT 관리형 Dell 인프라스트럭처에 암호화되어 저장됩니다.

Dell EMC IT 인프라스트럭처:

- 각 고객의 텔레메트리 데이터가 격리되도록 보장하는 안전한 플랫폼을 제공합니다.
- 고가용성, 내결함성 및 재해 복구 기능을 제공합니다.
- 고객의 텔레메트리 데이터(백업 포함)를 미국 내에 보관합니다.
- ACE 에서 도출해 낸 유용한 정보를 포함하여 ACE 가 적극적으로 모니터링하는 시스템에 대한 기간별 데이터를 무기한 보유합니다.
- 각 사용자는 Dell EMC MyService360 에 정의된 대로 사용자의 사이트 액세스에 속하는 VxRail ACE 에서만 해당 시스템을 볼 수 있는 독립된 보안 포털에 대한 액세스 권한을 고객에게 제공합니다.

Dell 의 최고 보안 책임자가 이끄는 Dell Technologies SRO(Security and Resiliency Office)는 VxRail ACE SaaS 솔루션을 호스팅하는 Dell EMC 의 정보 기술 인프라스트럭처에 대한 보안과 보호를 책임지고 있습니다. 이는 다중 계층 방화벽, 침입 탐지 시스템, 업계를 선도하는 안티바이러스 및 멀웨어 보호와 같은 조치를 포함하는 확립된 보안 정책 및 절차와 정보 보안 제어의 시행으로 이루어집니다. Dell EMC 사이버 보안 팀은 애플리케이션 및 기본 환경에 대한 지속적인 취약성 검사를 실행합니다. 필요한 모든 문제 해결 조치는 소프트웨어 업그레이드, 패치 또는 구성 변경과 같은 지속적인 취약성 문제 해결 프로그램을 이용하여 처리됩니다.

VxRail ACE 로 전송된 모든 데이터는 Dell EMC 데이터 센터에 호스팅된 인프라스트럭처에 저장됩니다. 정보 보안 정책은 모든 Dell EMC 정보와 리소스를 올바르게 보호하며, 정보 소유자는 모든 리소스를 고려해야 하며, 각 리소스에는 지정된 관리자가 있습니다. 모든 인프라스트럭처 구성 요소는 외부 액세스에 노출되지 않고 방화벽으로 보호되는 고립된 전용 Dell EMC 네트워크에 위치합니다. 시스템 관리자 및 데이터베이스 관리자 팀의 구성원이 아니면 데이터베이스 서버 및 데이터베이스에 직접 개별 로그인할 수 없습니다. 데이터베이스 애플리케이션 계정은 표준 데이터베이스 암호 인증을 사용하여 관리됩니다. Dell EMC 는 Dell EMC 인프라스트럭처 하드웨어를 안정적으로 제어 및 보호하기 위해 변경 관리 프로세스를 업계 모범 사례를 따라 구현했습니다. 변경 관리는 이러한 변경 사항을 관리하는 데 필요한 정책, 절차 및 툴을 제공하여 변경 사항에 대한 적절한 검토 및 승인을 거쳐 이를 사용자에게 효과적으로 전달합니다.

VxRail ACE 데이터 액세스 제어

VxRail ACE 데이터 액세스는 다음 두 가지 경우로 나뉩니다.

- 고객이 시스템 데이터 및 ACE 파생 통찰력을 보기 위해 VxRail ACE 에 액세스하는 경우
- 내부 Dell EMC IT 시스템 관리자 및 데이터베이스 관리자가 Dell EMC 에서 관리하는 VxRail ACE 인프라스트럭처에 액세스하는 경우

아래의 하위 섹션에서는 이 두 경우에 해당하는 사용자가 데이터에 액세스하는 방법을 설명합니다.

VxRail ACE 에 대한 최종 사용자 액세스

고객은 기존 지원 계정을 사용하여 VxRail ACE 에 로그인합니다. VxRail ACE 포털에서 VxRail ACE 데이터에 액세스하려면 각 최종 사용자는 유효한 Dell EMC 지원 계정을 보유하고 있어야 합니다. 인증은 Dell EMC 의 SSO(Single Sign-on) 인프라스트럭처에서 처리합니다. VxRail ACE 는 액세스 제어에 Dell EMC MyService360 고객 사용자 프로파일을 사용합니다. 사용자 Dell EMC 에 계정을 등록하면 사용자 프로파일이 생성되고 유효한 고객 프로파일과 연결됩니다. VxRail ACE 는 각 고객에게 시스템에 대한 독립적인 보안 보기를 제공하여 고객이 VxRail ACE 를 이용하여 자신의 데이터만 볼 수 있도록 합니다. 각 사용자는 Dell EMC MyService360 의 사용자 구성에 따라 사용자 사이트 액세스에 해당하는 시스템만 VxRail ACE 에서 볼 수 있습니다.

Dell EMC IT 가 관리하는 VxRail ACE 인프라스트럭처에 대한 관리 액세스

Dell EMC 는 고객의 독점 및 기밀 정보 보호를 매우 중요하게 생각하고 있습니다. 이에 따라 모든 Dell EMC 직원은 고객 기밀 정보에 관한 조항이 포함된 직원 계약서에 서명하게 됩니다. 이 계약의 의무는 유지 보수 서비스에 종사하는 중이거나 Dell EMC 와의 고용이 종료된 후에도 그대로 유지되며, 어떠한 방식이나 형식으로든 직원이 인지한 모든 시스템 저장 데이터에 적용됩니다.

표준 및 인증 준수

VxRail은 조직이 규정 준수 요건을 충족하도록 구성할 수 있는 강력하고 유연한 하이퍼 컨버지드 인프라스트럭처입니다. 일부 HCI 공급업체는 자사 제품의 호환성이 높다고 주장할 수 있지만, Dell EMC는 고객에게 중요한 보안 표준에 대한 완전한 인증을 받도록 적극적으로 노력하고 있습니다. VxRail이 가장 엄격한 비즈니스 및 규제 요건을 충족하는 방법에 대한 자세한 내용은 Dell EMC 담당자에게 문의하십시오. 다음은 VxRail이 준수하는 몇 가지 표준 및 인증 목록입니다.

FIPS 140-2 저장된 데이터 암호화 –FIPS PUB 140-2(Federal Information Processing Standard Publication 140-2)는 암호화 모듈의 하드웨어 및 소프트웨어 구성 요소에 대한 요구 사항 및 표준을 설정합니다. FIPS 140-2는 미국 정부와 기타 금융 및 의료 기관 등 중요하지만 분류되지 않은 정보를 수집, 저장, 전송, 공유 및 유포하는 규제가 엄격한 업종에서 요구됩니다. VxRail 이 사용하는 PowerEdge 서버는 검증을 받았습니다.



Common Criteria EAL 2+ – 정보 기술 보안 평가를 위한 Common Criteria는 컴퓨터 보안 인증에 대한 국제 표준(ISO/IEC 15408)입니다. Common Criteria 평가는 컴퓨터 보안 제품 및 시스템을 대상으로 하며 시스템의 보안 기능을 평가하고, SAR(Security Assurance Requirements) 또는 EAL(Evaluation Assurance Level)를 이용하여 제품의 보안 기능에 대한 신뢰 수준을 제공합니다. Common Criteria 인증은 보안을 보장하지는 않지만 보안 속성에 대한 주장을 독립적으로 확인할 수 있습니다. VxRail 이 사용하는 PowerEdge 서버 및 vSphere 구성 요소는 현재 완전한 인증을 **보유하고** 있습니다.



NIST 사이버 보안 프레임워크 – 주요 인프라스트럭처 개선을 위한 NIST 프레임워크는 조직이 사이버 보안, 위험 관리 및 시스템의 회복탄력성을 개선할 수 있도록 개발된 자발적 지침입니다. NIST는 1년 넘게 정부, 업계 및 학계의 수많은 파트너와 협력하여 합의에 기반하여 믿을 만한 지침과 관행을 구축했습니다. 특별 간행물 800-131A는 암호화 키 길이에 대한 권장 사항을 제시합니다.



NSA Suite B – Suite B는 암호 현대화 프로그램의 일환으로 National Security Agency에서 발표한 암호화 알고리즘 세트입니다. VxRail 이 사용하는 ESXi 및 vCenter의 현재 버전은 NSA Suite B를 지원합니다.



508 조 VPAT – 미국 접근성 위원회의 재활법 508 조 표준은 연방 정부가 조달하는 전자 및 정보 기술에 적용되며, 신체적 장애나 감각 또는 인지 장애가 있는 사용자에게 대한 액세스 요구 사항을 정의합니다. VxRail 이 사용하는 PowerEdge 서버와 vSphere 소프트웨어 구성 요소 모두 재활법 508 조를 준수합니다.



TAA(Trade Adjustment Assistance) – 무역조정 지원조치 프로그램은 대외 무역으로 인해 실직한 미국 노동자들을 지원하여 고용 성장과 기회를 제공하는 연방 프로그램입니다. 시스템으로 판매되는 VxRail은 TAA를 준수합니다.



DISA-STIG – 미국 DOD(Department of Defense)의 DISA(Defense Information Systems Agency)는 국방부의 IT 인프라스트럭처 보안 유지를 위한 방법 중 하나로 STIG(Security Technical Implementation Guides)라는 구성 표준을 개발합니다. 이 가이드는 공격에 대해 취약할 수 있는 정보 시스템 및/또는 소프트웨어를 폐쇄하기 위한 기술 지침을 제공합니다. Dell EMC 는 DoD 의 정보 네트워크(DISA) STIG 요구 사항을 준수하기 위해 VxRail 어플라이언스를 구성하는 수동 및 자동 단계를 제공합니다.



IPv6 – IPv6 은 인터넷에서 사용되는 차세대 프로토콜입니다. IPv4 의 주소 지정 제한 문제를 해결하는 것 외에도 IPv6 에는 여러 가지 보안상의 이점이 있으며, 많은 환경이 IPv6 도입을 추진하고 있습니다. VxRail 은 이중 스택 모드에서 IPv6 에 대한 USGv6 상호 운용성 테스트와 IPv6 지원 테스트에 대한 높은 표준을 통과했습니다.



Trusted Platform Module – Trusted Computing Group 은 TPM (Trusted Platform Module)에 대한 사양을 정의합니다. TPM 1.2 및 2.0 을 VxRail 에서 옵션으로 사용할 수 있습니다. 두 가지 모두 FIPS 140-2, TCG 및 Common Criteria 보안 요구 사항을 갖춘 인증입니다. vSphere 는 TPM 1.2 및 TPM 2.0 을 지원합니다.



NIST 사이버 보안 프레임워크 및 VxRail

NIST CSF(Cybersecurity Framework)는 민간 부문 조직이 사이버 공격을 방지, 탐지 및 대응하는 능력을 자체적으로 진단 및 개선할 수 있는 방법에 대한 컴퓨터 보안 지침 정책 프레임워크를 제공합니다. 이 자발적 프레임워크는 사이버 보안과 관련된 위험을 관리하는 표준, 지침 및 모범 사례로 구성됩니다. 사이버 보안 프레임워크의 우선 순위가 지정된 유연하고 비용 효율적인 접근 방식은 중요한 인프라스트럭처를 보호하고 복원하는 능력을 키울 수 있도록 지원합니다.

NIST CSF의 "핵심" 자료는 다섯 가지의 "기능"으로 구성되며 아래 그림 12와 같이 세분화된 범주가 있습니다.

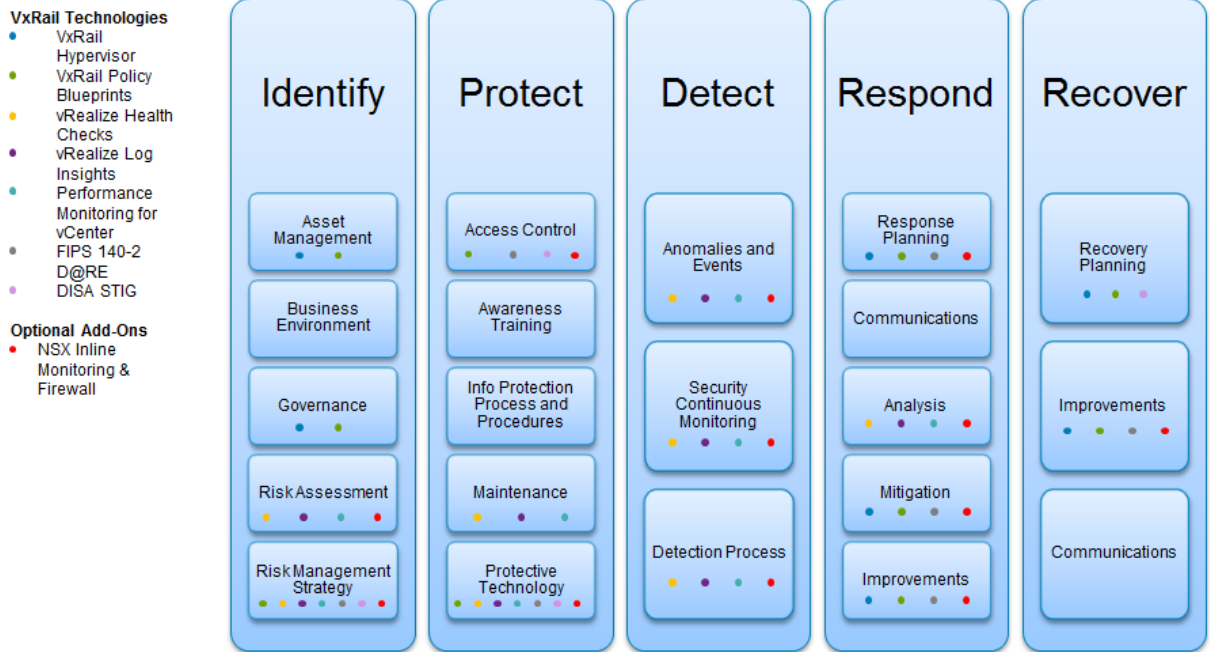


그림 12: National Institute of Standards and Technology, 사이버 보안 프레임워크

NIST CSF에 대한 자세한 내용은 [NIST 웹사이트](#)를 참조하십시오. VxRail을 NIST CSF와 연계하는 방법에 대한 자세한 내용은 여기 [보안 프레임워크](#)에서 백서 VxRail Features Supporting NIST Cyber Security Framework를 참조하십시오.

VxRail 보안 솔루션 및 파트너

VxRail은 보안 모범 사례에 따라 내장 및 배포된 보안 기능과 함께 설계되었습니다. 사용자는 적절한 액세스 수준으로 인증되고 권한이 부여됩니다. VxRail 클러스터를 저장된 데이터 암호화 기능과 함께 쉽게 구성할 수 있어 포함된 정보의 기밀 유지, 기본 네트워크 구성 세부 트래픽을 안전하게 보호할 수 있습니다. 또한 데이터의 무결성이 훼손됐을 때 애플리케이션 및 서비스의 빠른 복구를 지원하는 VM용 RecoverPoint와 같은 툴과 함께 구성할 수도 있습니다. 이러한 보안 기능은 VxRail 어플라이언스에 기본으로 내재된 기능입니다.

하지만 오늘날의 위협으로부터 환경을 완전하게 보호하려면 여러 계층의 보안을 통한 "심층 방어"가 필요합니다. VxRail 어플라이언스에서 실행되는 애플리케이션 및 서비스와 이를 사용하는 사용자를 연결하는 네트워크는 보호되어야 하며, 애플리케이션과 서비스 자체도 안전해야 합니다. 방화벽, 침입 탐지 및 예방 시스템, 안티바이러스/멀웨어, 엔드포인트 보호, 보안 운영 및 관리는 모두 다중 계층 방어의 일부입니다. Dell Technologies는 유일하게 고객의 환경을 완전히 보호할 수 있는 광범위한 기술과 서비스를 보유하고 있습니다.

조직이 IT 혁신의 어떤 단계에 있는지와 조직의 규모에 따라 적절한 접근 방식이 결정됩니다. 일부 환경은 기존 보안 프레임워크 내에서 작동 중일 수 있지만, IT 인프라스트럭처 혁신에 따라 일부 환경은 보안 운영을 혁신할 절호의 시기일 수 있습니다. 조직은 종종 보안 프로그램을 위해 여러 공급업체를 활용하기도 하지만, 이럴 경우 복잡성이 증가하여 위험도 함께 증가합니다. Dell Technologies 계열사에는 RSA 및 SecureWorks가 포함되어 있으며, 두 회사 모두 위험을 관리하고 고객의 디지털 자산을 보호합니다. Dell Technologies는 유일하게 세계적인 심층 보안 전문 지식과 수천 개 회사와의 파트너 협력 체계를 보유하고 있어 단일 공급업체 관계를 제공할 수 있습니다. 아래 그림 13은 위험 관리와 데이터 보호를 지원하는 Dell의 강력한 기능을 보여줍니다.

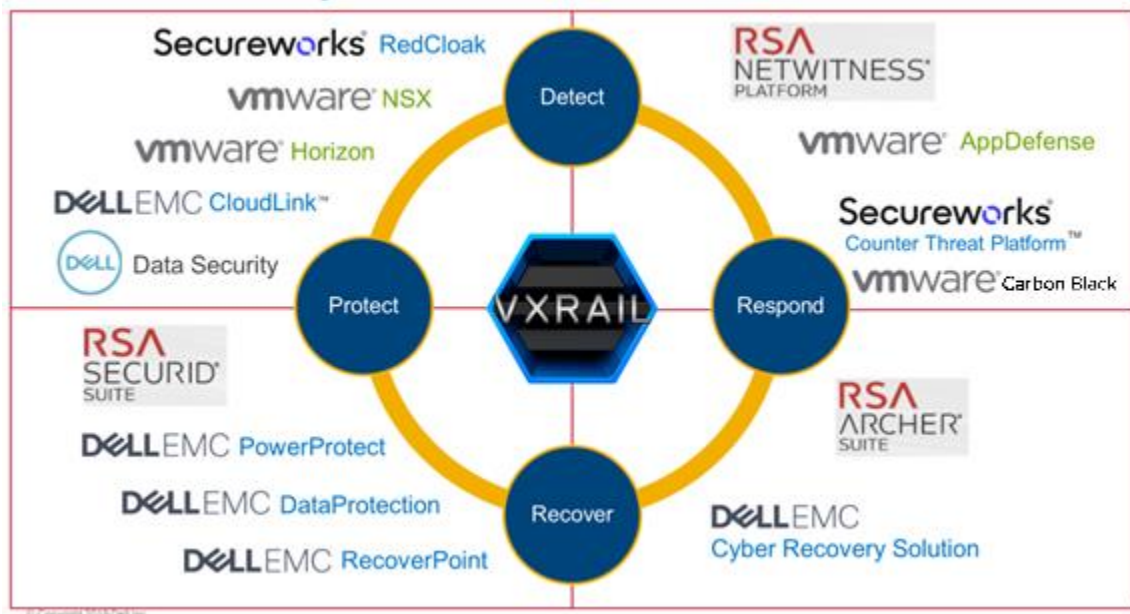


그림 13: 위험 관리와 데이터 보호를 지원하는 Dell의 강력한 기능

ID 및 액세스 관리

VxRail은 로컬 사용자 계정, LDAP 통합 및 SSO(Single Sign On)를 지원합니다. 독립 실행형 VxRail을 사용할 수도 있지만, 대부분의 환경은 Microsoft Active Directory와 같은 디렉토리 서비스를 사용하는 IAM(Identity and Access Management) 시스템을 통합합니다.

보안 인시던트 및 이벤트 관리

VxRail 어플라이언스는 vRealize Log Insight를 포함하고 있어 시스템의 로그 관리를 중앙 집중화합니다. 이미 Splunk 또는 SIEM(Security Incident and Event Management) 시스템과 같은 중앙 집중식 로그 관리 기능을 보유한 조직의 경우, 표준 syslog 프로토콜을 사용하여

VxRail에 쉽게 통합할 수 있습니다. RSA NetWitness 제품군은 로그 수집, 분석 및 기타 다양한 보안 기능을 제공하여 VxRail의 보안 기능을 향상시킵니다.

보안 이벤트를 자체적으로 관리하고 싶지 않은 고객을 위해 SecureWorks는 VxRail 및 실질적으로 중요한 정보 자산 또는 보안 기술에 대한 로그 관리 서비스를 제공합니다. SecureWorks는 비즈니스 보안 유지에 필요한 보안 정보를 수집하고 모니터링합니다. 또한 SecureWorks의 매우 숙련된 보안 전문가들이 각자의 통합 위험 대응 운영 센터에서 근무하며 모든 악의적인 행위를 24시간 연중무휴 즉시 조사하고 대응합니다.

키 관리 서버

암호화는 정보의 기밀 유지를 보호하기 위한 강력한 툴이며, VxRail은 암호화 기능이 내장되어 있어 사용 중인 데이터, 이동 중인 데이터 및 저장된 데이터를 보호합니다. 단, 암호화 기술을 통해 제공되는 데이터 보안 기능의 성능은 암호화 프로세스에 사용되는 키의 생성, 보호 및 관리가 얼마나 효과적으로 이루어지는지에 따라 좌우됩니다.

암호화 키는 필요할 때 사용할 수 있어야 하며, 복호화 작업을 실행하는 동안 키에 대한 액세스가 데이터 수명주기 내내 보존되어야 합니다. 따라서 암호화 키를 효과적으로 사용하려면 암호화 키를 올바르게 관리해야 합니다. 대부분의 조직은 전사에 걸쳐 중앙 집중화된 키 관리를 이용하여 관리를 간소화하고, 정책을 시행하며, 규정 준수에 대한 보고 및 감사를 제공합니다.

VxRail과 vSphere는 KMIP(Key Management Interoperability Protocol)가 여러 기업 키 관리 시스템과 작동하도록 이를 지원합니다. [Dell EMC CloudLink](#)는 KMIP 호환 키 관리는 물론 퍼블릭 클라우드, 프라이빗 클라우드, 하이브리드 클라우드에 대한 암호화 기능을 제공합니다. 이미 키 관리 서비스를 보유한 조직의 경우, VxRail과 vSphere에 쉽게 통합하여 기업 전체에 단일 키 관리 지점을 제공할 수 있습니다. VMware는 [호환되는 키 관리 서버 목록](#)을 제공합니다.

기타 보안 파트너

오늘날 IT 인프라스트럭처와 디지털 자산을 보호하는 것은 복잡한 작업입니다. 단일 솔루션은 강력한 방어를 제공할 수 없습니다. 그래서 Dell Technologies는 고객 환경의 고유한 위험과 취약성을 해결하기 위해 협력하는 파트너 협력 체계를 제공합니다. Dell은 고객이 사이버 보안 목표를 달성할 수 있도록 업계 전체가 협력해야 한다는 사실을 인식하고 있습니다.

Dell EMC VxRail 어플라이언스와 VMware vSphere는 개방형 보안 표준을 지원하며 파트너는 고객이 안전한 가상 클라우드 및 멀티 클라우드 IT 세계로 전환하도록 지원하는 데 중요한 역할을 담당하고 있습니다.

부록 A에 링크된 "[VMware Integrated Partner Solutions for Networking and Security](#)" 백서에서 VMware vSphere®, vCenter™, vShield Endpoint™, vCloud® Networking and Security™와 통합된 네트워킹, 보안 및 규정 준수 솔루션을 제공하는 몇몇 파트너 솔루션 목록과 vSphere 지원 애플리케이션 및 소프트웨어 세트 목록을 확인할 수 있습니다. vShield Endpoint가 제공하는 안티바이러스/안티멀웨어 보호를 위한 EPSEC API 외에도 VMware vCloud Ecosystem Framework는 vNIC 및 가상 엣지 수준에서 서비스 삽입을 제공합니다. [VMware Compatibility Guide](#)에서 올바른 구성 요소를 쉽게 찾을 수 있습니다.

결론

보안 혁신은 안전한 IT 인프라스트럭처에서 시작됩니다. VxRail은 엣지에서 중앙 데이터 센터 그리고 클라우드로 이르기까지 안전한 모던 인프라스트럭처를 제공합니다. 하이퍼 컨버지드 인프라스트럭처인 VxRail은 인프라스트럭처에 관련된 구성 요소의 수를 줄임으로써 공격을 받을 수 있는 부분을 줄이기 위해 하나의 제품으로 설계, 엔지니어링, 제작, 관리됩니다. VxRail 소프트웨어 수명주기 관리 VxRail 복합 번들은 BIOS, 펌웨어, 하이퍼바이저, vSphere 또는 기타 포함된 관리 구성 요소의 업데이트를 포함할 수 있으며, 전체 소프트웨어 스택을 훨씬 간단하게 업데이트할 수 있어 공격에 대한 취약성이 줄어듭니다.

오늘날의 위협으로부터 환경을 완전하게 보호하려면 여러 계층의 보안을 통한 "심층 방어"가 필요합니다. VxRail 어플라이언스에서 실행되는 애플리케이션 및 서비스와 이를 사용하는 사용자를 연결하는 네트워크는 보호되어야 하며, 애플리케이션과 서비스 자체도 안전해야 합니다. 방화벽, 침입 탐지 및 예방 시스템, 안티바이러스/멀웨어, 엔드포인트 보호, 보안 운영 및 관리는 모두 다중 계층 방어의 일부입니다.

Dell Technologies은 보안을 이해하고 고객이 환경을 진단하고 고유한 요구 사항에 맞게 보안 계획을 세울 수 있도록 지원하는 전문가를 세계 곳곳에 보유하고 있습니다. 자세한 내용은 Dell Technologies 담당자에게 문의하시기 바랍니다.

부록 A: 참조

이 백서에 인용된 모든 링크 및 참조는 아래에 표시되어 있습니다.

자산	URL
Risk Based Security:	https://www.riskbasedsecurity.com/2019/02/13/over-6500-data-breaches-and-more-than-5-billion-records-exposed-in-2018/
EMC 제품 보안:	https://www.dellemc.com/ko-kr/products/security/index.htm
Dell EMC Security Development Lifecycle:	https://www.dellemc.com/ko-kr/products/security/index.htm#tab0=2
Dell PSIRT(Product Security Incident Response Team):	https://www.dell.com/support/contents/kr/ko/19/article/product-support/self-support-knowledgebase/security-antivirus/alerts-vulnerabilities/dell-vulnerability-response-policy
Cyber Resilient Security in 14th generation of Dell EMC PowerEdge servers:	http://en.community.dell.com/techcenter/extras/m/white_papers/20444755/download
AppDefense:	https://www.vmware.com/kr/products/appdefense.html
VMware Cloud Foundation on VxRail Architecture Guide:	https://www.dellemc.com/resources/ko-kr/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/ko/pdf/VMware-Product-Security.pdf
Dell EMC VxRail Network Guide:	https://www.dellemc.com/resources/ko-kr/asset/technical-guides-support-information/products/converged-infrastructure/h15300-VxRail-network-guide.pdf
VMware's Using SpoofGuard guide:	https://docs.vmware.com/kr/VMware-NSX-for-vSphere/6.4/com.vmware.nsx.admin.doc/GUID-06047822-8572-4711-8401-BE16C274EFD3.html
VMware NSX Documentation:	https://docs.vmware.com/kr/VMware-NSX-Data-Center-for-vSphere/6.4/com.vmware.nsx.admin.doc/GUID-B5C70003-8194-4EC3-AB36-54C848508818.html
Security for Hyper-Converged Solutions:	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 2017 Data Breach Investigation Report.	http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017
*2 PWC "20thCEO Survey" of 5,351 members of the public, in 22 countries.	https://www.pwc.com/jg/en/publications/pwc-ceo-report-2017%20(2).pdf
NIST Cyber Security Framework:	https://www.nist.gov/cyberframework
list of compatible key management servers:	https://www.vmware.com/resources/compatibility/search.php?deviceCategory=kms&details=1&page=1&display_interval=10&sortColumn=Partner&sortOrder=Asc

VMware Integrated Partner Solutions for Networking and Security:	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vcns/vmware-integrated-partner-solutions-networking-security.pdf
VMware Compatibility Guide:	https://www.vmware.com/resources/compatibility/search.php
VxRail Techbook:	https://www.emc.com/collateral/technical-documentation/h15104-VxRail-appliance-techbook.pdf
Security Features of the integrated Dell Remote Access Controller (iDRAC):	http://en.community.dell.com/techcenter/extras/m/white_papers/20441744/download
vSAN 설명서:	https://docs.vmware.com/kr/VMware-vSAN/index.html
Four business transformations:	https://www.youtube.com/watch?v=TcKJ39_4Rwc
VMware encryption certifications:	https://www.vmware.com/kr/security/certifications/fips.html
VMware vRealize Log Insight:	https://www.vmware.com/content/dam/digitalmarketing/vmware/ko/pdf/products/vrealize-log-insight/vrealize-log-insight-datasheet.pdf
NIST certifications for FIPs 140-2 search by Vendor for Dell EMC and VMware:	https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search
VMware Secure Development Lifecycle:	https://www.vmware.com/kr/security/sdl.html
VMware Key Management:	https://blogs.vmware.com/vsphere/2017/10/key-manager-concepts-topology-basics-vm-vsan-encryption.html
vSphere 6.5 Security Guide:	https://docs.vmware.com/kr/VMware-vSphere/6.5/vsphere-esxi-vcenter-server-65-security-guide.pdf
Dell EMC 제품 보안 프로그램을 통한 신뢰 구축:	https://www.emc.com/ko-kr/products/security/index.htm
	ACE Resources
ACE Overview video demo	https://vxrail.is/acedemo
Smart update bundle staging video demo	https://vxrail.is/aceupdates
솔루션 개요	https://www.dell EMC.com/resources/ko-kr/asset/offering-overview-documents/products/converged-infrastructure/vxrail-ace-solution-brief.pdf
Dell Technologies MyService360 overview	https://www.delltechnologies.com/et-ee/services/support-deployment-technologies/my-service-360.htm
VxRail Comprehensive Security by Design(백서)	https://www.dell EMC.com/resources/ko-kr/asset/white-papers/products/converged-infrastructure/VxRail_Comprehensive_Security_by_Design.pdf
Dell Technologies Product Security practices	https://www.delltechnologies.com/ko-kr/products/security/index.htm
	YouTube - Security Resource
Youtube - VxRail Security Overview	https://www.youtube.com/watch?v=ZTNmYBgJv4s
Youtube - VxRail Security Hardening and Compliance	https://www.youtube.com/watch?v=ZjhfCE5nq6U