# Battle Card – Check Point vSEC

## 개요

Check Point vSEC와 VMware NSX 통합 솔루션은 모든 데이터센터 트래픽의 진보된 위협 방어를 위해 동적인 결합을 제공합니다. 소프트웨어 정의 데이터센터(SDDC) – 추상적으로 물리적인 인프라스트럭처를 자원을 할당하고, 목적에 맞게 다시 자원을 할당 할 수 있습니다. 가상머신을 동적으로 생성하고 관리 할 수 있는 프로그램 컨트롤을 제공합니다.

VMware NSX는 미세 분할을 실행 가능하게 만드는 네트워크 가상화 플랫폼입니다. NSX는 자동화된 배포, 결합 및 진보된 보안 서비스의 스케일아웃을 지원 하는 SDDC를 위한 기반을 제공합니다.

고급 위협 방어 기능(Advanced Threat Prevention)을 갖춘 Check Point vSEC는 맬웨어와 제로 데이(zero-day) 공격을 선행적으로 차단시키기 위해 다계층 방어를 제공합니다. Check Point의 가상 및 물리 게이트웨이에 대한 통일된 관리는 데이터센터 전체에 걸친 보안 관리와 제어를 단순화합니다.

## 엘리베이터 피치 – 3대 셀링 포인트

- vCenter와 NSX의 완전한 통합은 보안 정책에서 모든 데이터센터 오브젝트에 대한 완전한 가시성을 제공합니다.
- 사이버 위협으로부터 보호하기 위해 차세대 위협 방어를 이용한 완전한 보호를 제공하고 자동 교정을 위해 감염된 VM의 보안 상태를 NSX와 공유합니다.
- 로그와 이벤트에 상세히 기록된 vCenter 및 NSX 컨텍스트(VM 이름)

## 핵심 메시지

**1.소프트웨어 정의 데이터센터 내부에서 원활하게 강제되는 보안 보호**

a. 맬웨어에 대한 가장 높은 탐지율의 고급 위협 방어, VM 내부 트래픽 보호

b. 감염된 가상 머신(VM) 탐지 및 태그 부착, 자동 검역 및 교정을 위한 NSX 업데이트

c. 동적 트래픽 워크로드에 맞게 조정하기 위해 보안 용량을 탄력적으로 확장

**2.자동화된 보안 프로비저닝과 조정**

a. NSX 보안 그룹 및 vCenter VM 오브젝트와 동적으로 연결된 세밀한 보안 정책이 네트워크 토폴로지 변경에 관계 없이 가상 어플리케이션의 보안을 보장합니다.

b. 간편한 정책 분할이 NSX 미세 분할과 일치하는 세밀한 규칙 정의, 자동화 및 권한 분리를 지원합니다.

c. 새로운 ESX 호스트가 배포되고 VM이 SDDC 내에서 이동함에 따라 보안은 자동 프로비저닝됩니다.

**3.SDDC 전체의 포괄적인 위협 가시성**

a. 가상 및 물리 게이트웨이 모두에 대한 단일 정책이 보안 시행을 단순화합니다.

b. 집중식 모니터링, 로깅 및 이벤트 분석이 SDDC 전체의 포괄적인 위협 가시성을 보장합니다.

## vSEC의 특별한 점

**업계 최고의 고급 보안 보호**

- 다계층에 걸친 진보된 고급 위협방어에 업계 최고의 탐지율과 실시간 인텔리전스는 물리적 네트워크만큼 안전한 가상 네트워크 보안을 보장합니다.
- 보안 용량은 변화하는 트래픽 워크로드에 부합하도록 탄력적으로 확장됩니다.

**가상 트래픽 위협 포렌식**

- 가상 데이터센터 오브젝트 ID는 간편한 트래픽 모니터링과 분석을 위해 로그에 저장됩니다.
- 포괄적인 보안 이벤트 분석이 가상 트래픽 변칙과 제로 데이(zero-day) 위협을 탐지합니다.

**민첩한 자동화 보안 프로비저닝**

- 세밀한 보안 정책을 구현할 목적으로 NSX 정의 오브젝트를 동적으로 끌어당기기 위해 NSX 및 vCenter와 통합
- 보안을 몇 시간이 아닌 몇 분 내에 자동 프로비저닝
- 네트워크 세그먼트 수준의 검사 및 권한의 분리를 위해 하위정책을 사용하여 보안정책을 쉽게 분할 할 수 있다.

**가상 및 물리 환경의 관리 통합**

- 가상 및 물리 게이트웨이를 위한 단일 정책이 보안 시행을 단순화합니다.
- 집중식 관리는 보안 태세에 대한 포괄적 가시성을 보장하고 운영 간접비를 최소화합니다.

## 영업 지원 리소스

**제품 정보**

- 고객 프레젠테이션
- 제품 페이지
- 영업 가이드
- 경쟁 팩트 시트

**기타 리소스:**

- 데이터센터를 위한 최고의 보안
- NSX 데모 – CP vSEC와 PAN VM-시리즈 비교

추가 정보가 필요하십니까?
vsec@checkpoint.com으로 연락하십시오.

# Battle Card – Check Point vSEC

## 경쟁 방법...

### VM-시리즈 NSX 판

- 비 NSX 환경(vCNS & vCenter)의 하이퍼바이저 모드에 대한 지원 없음
- 보안 정책에서 데이터센터 객체의 번거로운 프로비저닝 – 데이터센터 오브젝트를 가져와 보안 정책에서 사용하려면 NSX와 Panorama에 대해 복잡한 수동 작동이 필요
- PAN은 NSX(VM 보안 태깅)를 통해 제3자 솔루션과 호환되지 않음 – 감염된 머신에 대한 교정 조치를 자동으로 트리거할 수 없음
- 로그에 데이터센터 오브젝트 ID가 없는 제한적 포렌식

### FortiGate-VMX

- 불완전한 솔루션 - 통합형 NSX 솔루션 없음
- 기상 및 물리 게이트웨이를 위한 별개의 관리 콘솔. 보안 관리자 간접비 추가

### VMware NSX 분산 방화벽

- NGFW 및 NGTP 기능이 없는 L2-4 보안(방화벽만)
- 가상 및 물리 게이트웨이를 같은 보안 정책에서 관리할 수 없음
- 전용 로그 뷰어 또는 SIEM이 없는 제한적 포렌식 기능
- 참고: VMware는 경쟁업체가 아니라 Check Point의 강력한 파트너입니다. SDDC를 위한 최고 수준의 보안은 Vsec와 NSX가 함께 제공합니다.

| 네트워크 보안 | Check Point | Palo Alto | Fortinet | VMware |
|---|---|---|---|---|
| **고급 위협 방어 매트릭스** | | | | |
| vCNS 인증 | ● | ○ | ● | N/A |
| NSX 인증 | ● | ◔ [1] | ◔ [2] | N/A |
| 가상 및 물리 게이트웨이를 위한 통합 관리 | ● | ● | ○ | ○ |
| 데이터센터 정책을 계층 및 하위 정책으로 분할(R80) | ◒ [3] | ◔ [4] | ○ | ○ |
| 글로벌 보안 정책에서 사용하기 위해 vCenter 및 NSX 데이터센터 오브젝트 패치 | ● | ◒ [5] | ◔ [6] | N/A |
| 가상 데이터센터를 위해 다계층 방어로 위협 방어 | ● | ◒ [7] | ◔ [8] | ○ |
| 자동 교정을 위한 NSX 보안 상태 업데이트 및 감염된 VM 태그 부착 | ● | ○ | ○ | ◔ [9] |
| 보안 로그에서 VM 오브젝트 보기 | ◔ [3] | ○ | ○ | ◒ [10] |
| 프라이빗 클라우드 보안 보고서(R80) | ◒ [3] | ○ | ○ | ○ |
| **요약** | | | | |
| **완전한 데이터센터 보안 솔루션** | ◔ | ◔ | ◔ | ○ |

취약 ○ ◔ ◒ ◔ ● 강력

1) 인증 안된 솔루션
2) NSX 호환만
3) R80에서 지원
4) 통일된 보안만
5) 오직 NSX와 통합
6) NSX 보안 그룹을 볼 수 없음
7) 우회 공격에 취약한 IPS
8) IPS 건너뛰기
9) 자동화 안됨
10) Log Insight 필요

추가 정보가 필요하십니까?
vsec@checkpoint.com으로 연락하십시오.

# Battle Card – Check Point vSEC

## 대상 청중 및 질문

| 최고정보책임자(CIO), 최고정보보호책임자(CISO) | IT/정보보안 부서장 | 보안 관리자 |
|---|---|---|
| 기존의 보안 솔루션으로 데이터센터 내부의 보안 및 가시성을 어떻게 확보합니까? | 물리 게이트웨이와 같은 보안 인프라를 이용해서 소프트웨어 정의 데이터센터를 보호할 수 있습니까? | NSX 및 vCenter 데이터센터 오브젝트를 기존 보안 정책에 어떻게 간편하게 추가합니까? |
| 최신 사이버 위협으로부터 데이터센터를 어떻게 보호합니까? | 데이터센터 내부에 맬웨어가 전파되어 있는지 어떻게 알 수 있습니까? | 맬웨어에 감염된 VM을 어떻게 식별하고 교정할 수 있습니까? |
| 소프트웨어 정의 데이터센터에서 실행되고 있는 비즈니스 애플리케이션의 보안을 어떻게 유지합니까? | 데이터센터 애플리케이션을 보호하기 위해 어떻게 보안을 자동으로 프로비저닝합니까? | 가상화된 데이터센터 네트워크 내부의 VM 간 트래픽 보안을 어떻게 유지합니까? |

## 이의 처리

| | |
|---|---|
| 저는 네트워크 보안과 방화벽만을 담당하고 있으며 데이터센터 인프라는 다루고 있지 않습니다. | 가상화된 데이터센터 내부의 East/West 트래픽을 어떻게 보호하시겠습니까? 데이터센터 내부에서 사이버 위협과 보안 인시던트를 어떻게 하실 생각입니까? |
| 소프트웨어 정의 데이터센터 솔루션에 기본으로 가지고 있는 보안 기능으로 이미 구축했습니다. | SDDC는 기본적인 보안 기능(방화벽만)을 갖추고 있지만 오늘날의 보다 정교한 위협으로부터 보호하기에는 충분하지 않습니다. 가상 데이터센터 보안은 물리 네트워크 보안과 대등해야 합니다. |
| 데이터센터 보안 솔루션으로 Check Point를 이용해야 하는 이유는 무엇입니까? | Check Point는 VMware 뿐만 아니라 다른 여러 프라이빗/퍼블릭 클라우드 플랫폼과의 원활한 통합을 제공합니다. 예를 들어, 잠재적 위협에 대한 자동 교정을 위해 위협 방어 메커니즘을 활용하는 능력이 있습니다(VM 태깅). |
| 데이터센터 보안을 관리할 리소스가 충분하지 않습니다. | 소프트웨어 정의 데이터센테에 대한 보안 삽입은 새로운 VM을 스핀업하는 것만큼이나 간단해야 합니다. Check Point vSEC와 VMware 하이퍼바이저의 통합과 프로비저닝은 물리 및 가상 게이트웨이 모두에 대해 동일한 '황금 기준' 통합 관리를 활용하는 동안 vCenter/NSX에 대한 즉각적 가시성과 함께 자동으로 수행됩니다. |

## 요약 - 승리 보장

Check Point는 소프트웨어 정의 데이터센터에 맞춰 구성된 업계 최고의 고급 보안 솔루션을 제공합니다. Check Point vSEC와 VMware의 독특한 통합은 물리 및 가상 게이트웨이 모두를 위한 단일의 '황금 기준' 통합 관리 플랫폼을 활용하는 보안의 동적 삽입, 분산 및 조정을 지원합니다. vSEC는 향상된 가시성과 세밀한 제어를 위해 보안 정책, 로그 및 이벤트에서 vCenter 및 NSX 오브젝트를 활용합니다. 또한 감염된 VM에 대해 차세대 위협 방어 메커니즘을 사용해 사이버 위협에 대한 고급 보호 기능을 제공함으로써 잠재적 위협에 대한 자동 교정을 시작할 수 있습니다.

## 중요 포지셔닝 팁

1. Check Point와 VMware의 강력한 통합과 vCenter 및 NSX 모두에 대한 연결 능력을 강조하십시오.
2. 보안 정책, 로그 및 이벤트에서 데이터센터 오브젝트에 대한 향상된 가시성을 보여주십시오.
3. Check Point는 차세대 위협 방어 기능을 통해 사이버 위협에 대한 최상의 보호를 제공할 뿐만 아니라 자동 교정을 위해 NSX와 보안 상태를 공유할 수 있는 능력(VM 태깅)도 제공한다는 점을 강조하십시오.