한눈에 보기

Cisco Firepower 9300

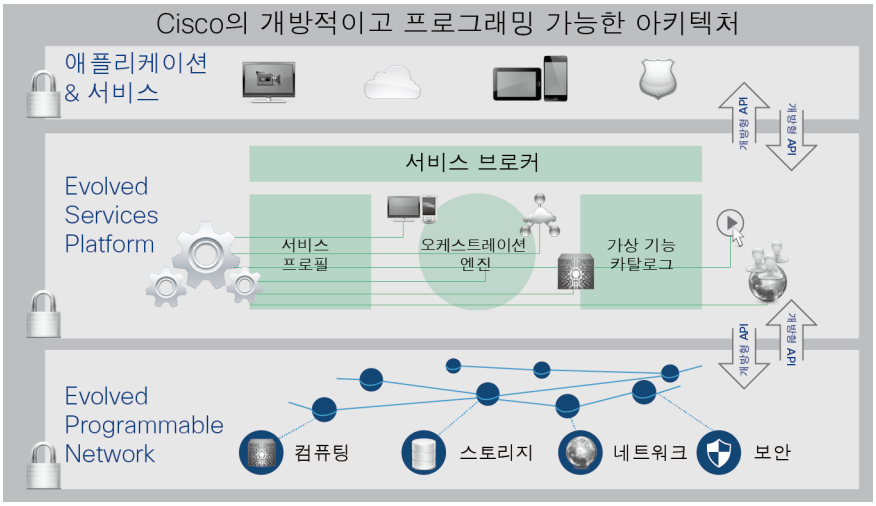
통신 사업자를 위한 위협 대응형 보안

더 이상 API만으로는 충분하지 않다고 통신 사업자들은 말합니다. 보안 서비스 통합에는 막대한 비용이 들지만 효과는 미흡합니다.

지금까지 통신 사업자가 실행할 수 있는 유일 보안 접근 방법은 확장 가능한 포인트 솔루션을 구축하는 것이었습니다. 이 방식은 통합을 제한하므로 위협 가시성과 상관성 분석에 허점이 있었습니다. 게다가 각기 다른 보안 어플라이언스 때문에 워크로드 및 데이터 흐름을 물리적, 가상, 클라우드 토폴로지를 지나는 동안 동적으로 보호할 수 없습니다.

Cisco는 자체 보안 서비스와 파트너의 서비스를 통합하여 통신 사업자 보안의 새로운 기준을 제시합니다. 지능적으로 서비스를 구성함으로써 위협 방어 및 네트워크 성능을 모두 최적화할 수 있습니다. 이러한 방식으로 개방적이고 프로그래밍 가능한 네트워크를 완벽하게 구현할 수 있습니다. 네트워크 패브릭의 전반에서 데이터 흐름 및 워크플로우를 따라 일관성 있게 보안 정책이 적용됩니다.

통신 사업자를 위한 Cisco® Evolved Programmable Network 아키텍처에서 보안은 중심적 역할을 합니다. 이 아키텍처는 통신 사업자와 그 고객의 데이터 및 가용성을 보호합니다. 또한 Cisco의 신속한 프로비저닝으로 새로운 보안 서비스를 현실성 있게 구축할 수 있습니다. 따라서 보안이 부가 가치를 창출하는 전략적 비즈니스 차별화 요소가 됩니다.



앞선 Cisco ASA 방화벽 및 Radware DDoS(분산 서비스 거부 공격) 완화 기능을 갖춘 고성능 캐리어급 플랫폼인 Firepower 9300에서 Cisco의 특별한 방식이 하드웨어적으로 구현됩니다. Cisco의 NGIPS(Next-Generation IPS), Cisco AMP(Advanced Malware Protection)를 비롯하여 Cisco 및 서드파티 보안 서비스가 추가될 예정입니다.

이점

- Cisco와 그 파트너의**보안 서비스**를 캐리어급 NBES 지원 플래폼에서 **통합**
- 확장 가능한 방식으로 **가시성의 틈새를 해결하여** 운영 및 고객 보호
- 물리적 환경과 가상 환경을 포괄하는 민첩성으로 새로운 서비스 솔루션의 **출시 일정 단축**

Firepower 9300은 캐리어급 플랫폼입니다. 보안 모듈을 통해 확장하면서 비즈니스 요구 사항을 해결할 수 있습니다.

다음과 같은 혜택을 제공합니다.

- Cisco ASA 5585-X Adaptive Security Appliance보다 600% 우수한 성능, 30% 높은 포트 집적도
- 테라비트 백플레인 및 최대전력 효율
- 멀티서비스 및 멀티벤더(Cisco 및 서드파티) 보안 애플리케이션에 대한 지능적인 서비스 구성으로 낮은 레이턴시 및 고효율성 실현
- 스완형 애플리케이션 블레이드 아키텍처에서 유연한 구성 및 편리한 성능 확장
- 10Gb 및 40Gb 이더넷(GE) I/O 및 네트워크 지원

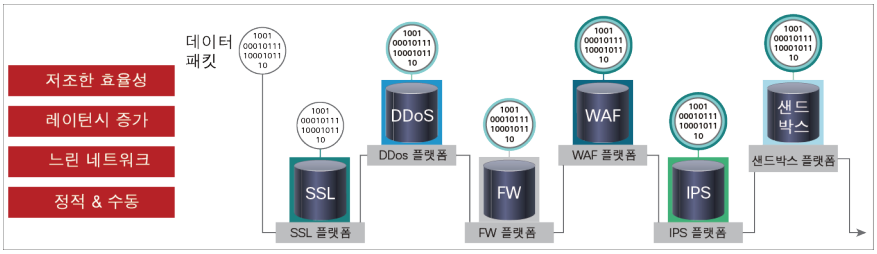
다음 단계

Cisco Firepower 9300에 대한 자세한 내용은 https://www.cisco.com/go/sp 를 참조하십시오.

혁신적인 동급 최고의 솔루션

포인트 솔루션 구축은 SLA(service-level agreement) 충족에 매우 중요했습니다. 하지만 이 방식에서는 수동적이고 비효율적인 프로세스가 주를 이루었습니다.

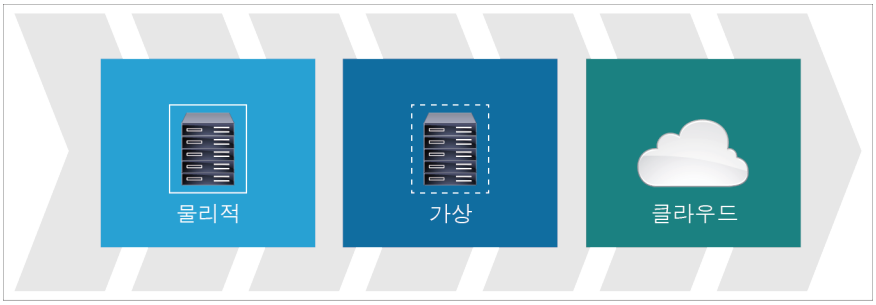
과거의 방식



Cisco의 특별한 방식

강력한 통합 및 지능적인 서비스 구성

Cisco의 위협 대응형 보안 방식은 물리적, 가상, 클라우드 토폴로지의 전 범위에서 API뿐 아니라 보안 서비스까지 강력하게 통합합니다.



Cisco의 방식으로 비용을 줄일 수 있으며 통신 사업자 및 그 고객의 운영 환경을 확장 가능하고 탄력적인 위협 대응형 보안으로 보호할 수 있습니다.

C45-734810-00 06/15