Gigamon®

솔루션 소개
위협 차단

50%

모바일 데이터 트래픽은 폭증하고 있습니다.[1]

핵심 이점

- ✓ 인프라 전반의 네트워크 트래픽에 대한 가시성을 제공함으로써 사이버보안 툴의 효과를 높입니다.
- ✓ 보안 툴 최적화를 통해 비용을 절감함으로써 네트워크 트래픽과 애플리케이션을 더욱 잘 보호합니다.
- ✓ 새로운 보안 기술과 툴을 시험하고 배포하는 데 필요한 시간과 노력을 크게 줄여줍니다.
- ✓ SSL 트래픽을 효율적으로 복호화하여 검사할 수 있게 해줍니다.
- ✓ 네트워크를 지연시키거나 유지보수 기간까지 기다릴 필요 없이 NetOps 및 SecOps 팀이 안전한 애플리케이션과 새 보안 툴을 더욱 빨리 배포할 수 있습니다.

인라인 위협 차단 전략은 보안 툴의 집합체 그 이상입니다. 이는 통합적인 인텔리전트 접근법이어야 합니다. 완전한 위협 차단 솔루션은 차단 툴의 성능을 향상시킬 뿐만 아니라 네트워크 성능에 영향 미치거나 유지보수 기간에 의존하지 않고 패치를 신속하게 배포하여 신기술을 구현할 수 있게 함으로써 운영팀의 효율성도 높여줍니다. 기가몬 인라인 바이패스 위협 차단 솔루션은 비용을 낮추는 데 도움이 되면서 동시에 차단 툴 성능, 네트워크 복원력, 운영 효율성을 극대화시켜 줍니다.

기가몬 인라인 바이패스 위협 차단 솔루션은 보안을 위해 특별히 개발된 차세대 네트워크 패킷 브로커인 기가시큐어® 보안 전달 플랫폼(기가시큐어)의 일부입니다. 이를 활용하면 온프레미스 환경과 가상의 클라우드 환경에서 인프라 전반의 데이터에 접근할 수 있습니다. 보안 툴에서 검사하도록 설계된 트래픽만 전달함으로써 보안 툴을 최적화하고, 여러 툴에 걸쳐 부하를 분산하며, SSL 복호화와 같은 프로세스 집약적인 작업을 줄일 수 있습니다. 통합형 물리적 및 논리적 바이패스 기능은 최고 수준의 이중화를 제공할 뿐만 아니라 네트워크 가용성과 성능에 영향을 미치지 않으면서 인라인 툴의 단순한 시험과 복구를 원활하게 해줍니다.

기존 사이버보안 툴의 효과 향상

위협을 감지하여 그에 대응하기 위해 데이터에 효율적으로 접근할 수 있는 능력을 갖추는 것은 어려운 문제입니다. 보안 툴을 추가로 구매하거나 직원을 충원하지 않고 이 문제를 해결하기 위해, 사용자는 기가시큐어를 활용하여 다음과 같이 할 수 있습니다.

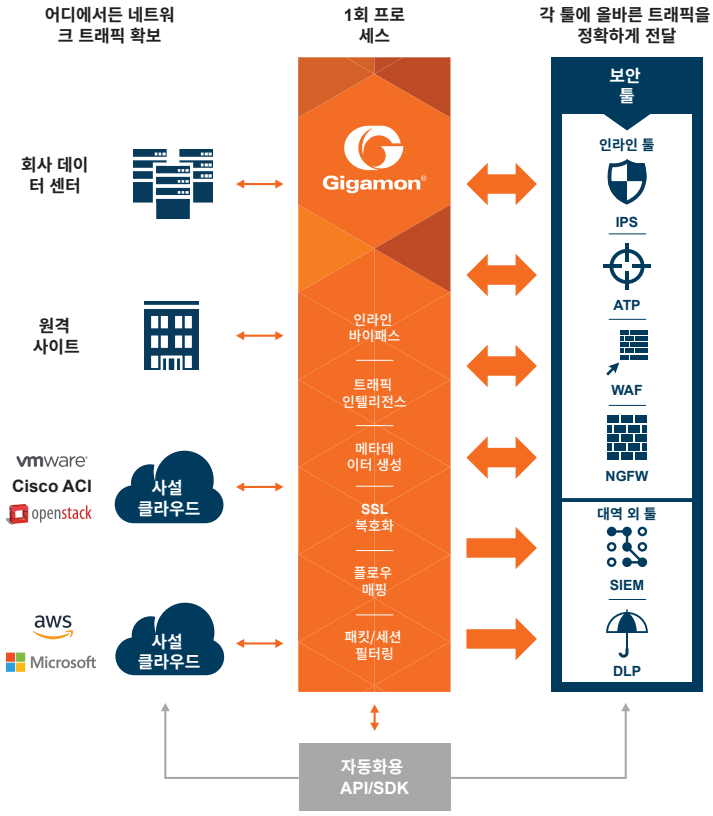
- 툴 관련 데이터만 전송하여 성능을 최적화합니다.
- 네트워크 속도와 업그레이드를 활용하여 차단 툴을 조정합니다.
- 더욱 빨리 감지할 수 있도록 조직 전반에 걸쳐 데이터에 접근합니다.
- 1회 복호화로 모든 툴과 데이터를 공유합니다.

사이버보안 툴 비용 절감

네트워크 트래픽이 증가하면 기업은 보안 툴을 늘리거나 업그레이드해야만 합니다. 이는 하드웨어와 소프트웨어 예산을 올리는 요인이 되며 사이버보안 인프라의 복잡성과 관리 비용을 높입니다. 기가시큐어 보안 전달 플랫폼은 다음을 가능하게 지원함으로써 이를 해결할 수 있습니다.

- 중복 제거 및 SSL 복호화와 같은 작업의 부하를 제거합니다.
- 필요한 정보만을 툴에 전송합니다. 그 이상은 전송하지 않습니다.
- 여러 툴에 대한 부하 분산을 통해 용량 낭비 문제를 제거합니다.
- 복잡성을 줄이고 보안 관리 비용을 낮춥니다.

[1]기가몬의 전체적인 경제 효과(The Total Economic Impact)™, 기가몬의 의뢰로 Forrester Consulting이 진행한 연구, 2016년 4월



기가시큐어 보안 전달 플랫폼: 사각지대를 제거하고, 성능을 높이며, 복원력을 향상시킵니다.

더욱 빨라진 새 사이버보안 기술의 시험과 배포

매일 새로 등장하는 위협에 대응하기 위해 IT 조직은 자주 업그레이드하거나 새 사이법안 툴과 기술을 도입할 필요가 있습니다. 보안 전달 플랫폼을 통해 다음과 같이 할 수 있습니다.

- 성능을 저해하지 않고 새 보안 툴을 시험합니다.
- 여러 보안 툴을 나란히 평가합니다.
- 네트워크 성능에 영향을 미치지 않고 보안 툴을 배포합니다.
- 고비용의 네트워크 카드를 사용하지 않고 새 툴을 롤아웃합니다.

기가몬 에코시스템 능력 적극 활용

기가시큐어는 시스코 FirePOWER 침입 방지 시스템(IPS), FireEye 네트워크 보안 고급 위협 차단(ATP) 솔루션 및 Imperva SecureSphere 웹 애플리케이션 방화벽(WAF)과 같은 인라인 보안 툴의 기능을 강화하여 네트워크 트래픽이 증가하는 상황에서 그리고 소프트웨어 업그레이드 시 침입을 감시하고 차단하여 시스템을 보호할 수 있도록 지원합니다. 또한 위협 트래픽을 최전방에 배치하고, SSL 복호화 부하를 제거하며, 복원력을 향상시킴으로써 기가몬은 생태계 파트너와 더불어 네트워크를 좀 더 정확하고 효율적으로 만듭니다.

기가시큐어 보안 전달 플랫폼

다이어그램에 나와 있듯이 기가시큐어 보안 전달 플랫폼은

- 조직 전반에 걸쳐 네트워크 트래픽에 대한 간단한 액세스를 제공합니다.
- 인라인과 대역 외 모두에 대해 개별 보안 툴의 요구에 따라 선택한 관심 트래픽을 전달합니다.
- SSL 복호화 및 중복 제거와 같은 프로세서 집약적인 작업을 대신 수행하여 개별 툴의 부하를 줄여줍니다.
- 트래픽 인텔리전스를 활용하여 네트워크 트래픽을 최적화하거나 네트워크 트래픽에서 메타데이터를 추출하여 적합한 보안 툴에 전달합니다.
- 보안 및 인프라 스택과의 통합을 위해 프로그래밍 방식의 인터페이스를 제공하여 인프라 변동, 이벤트 및 기타 조기 저해 징후에 동적으로 대응할 수 있게 해줍니다.

상세 정보

기가시큐어 보안 전달 플랫폼이 보안을 향상시키고 비용을 절감하는 데 어떤 도움을 줄 수 있는지 알아보려면 **www.gigamon.com** 에서 확인하시기 바랍니다.

6114-01 04/18

Gigamon® 3300 Olcott Street, Santa Clara, CA 95054 USA | +1 (408) 831-4000 | www.gigamon.com