사업 소개

기존 사이버보안 툴의 효과 향상

기업은 기술 분야의 최고 전문가가 개발한 사이버보안 툴에 상당한 자금을 투자해 왔습니다. 하지만 매일 5백만 건 이상의 데이터 기록이 분실되거나 도난당하고 있습니다.[1]

문제는 오늘날 사이버보안 툴의 설계가 잘못되었거나 필요한 기능이 없다는 것이 아닙니다. IT 조직이 게으르다거나 보안에 관심이 없다는 것은 더욱 아닙니다. 한편, 가장 자주 발생하는 문제는 폭증한 네트워크 트래픽 양이 보안 툴을 압도해서 관리자가 애플리케이션 성능을 유지하고자 샘플링을 사용하거나 고급 기능을 비활성화해야 한다는 것입니다. 보편적으로 발생하는 다른 문제는 보안 툴과 IT 직원이 데이터 수집 시 "사각지대"에 직면하기 때문에 외부 공격과 내부 사고를 탐지하여 이에 대응하기 위해 필요한 모든 데이터를 얻지 못한다는 것입니다.

보안 툴을 추가로 구매하거나 직원을 충원하지 않고 이 문제를 해결할 수 있도록 기가몬은 보안을 위해 특별히 개발된 차세대 네트워크 패킷 브로커인 기가시큐어® 보안 전달 플랫폼을 제공합니다. 기가시큐어 보안 전달 플랫폼은 기존 보안 툴이 네트워크 트래픽에 압도되지 않게 하고 이동 중인 데이터에 퍼베이시브 가시성을 제공하여 기존 보안 툴의 효율성을 높여줍니다.

트래픽 인텔리전스와 로드 밸런싱을 활용한 고성능 유지

트래픽 양이 증가하면 관리자는 SSL 복호화, 심층 패킷 검사 등의 중요 보안 기능을 끄는 경우가 많습니다. 이는 장치가 네트워크와 애플리케이션 성능을 저해하는 병목 현상이 발생하지 않도록 하기 위함입니다.

기가시큐어 보안 전달 플랫폼은 트래픽 인텔리전스를 활용하여 각 보안 툴에 불필요한 트래픽을 걸러냅니다. 예를 들어 이메일이 들어 있는 트래픽은 이메일 보안 제품에만 보내고 비디오 스트림이 들어 있는 패킷은 비디오를 검사하도록 설계된 툴에만 보냅니다. 기가시큐어 보안 전달 플랫폼은 동적 로드 밸런싱도 제공하며, 이를 통해 여러 장치의 용량 사용을 최적화할 수 있습니다. 관리자는 네트워크 성능을 저하시키지 않고도 보안 툴의 최대 성능을 유지할 수 있습니다.

1회 복호화를 통해 모든 툴과 공유

전자프런티어재단에 따르면 웹 트래픽 절반 이상이 HTTPS와 기타 SSL 변형물로 암호화됩니다.[2] 하지만 일부 보안 툴은 SSL 트래픽을 복호화할 수 없습니다. 다른 툴은 SSL 트래픽이 미검사 조직에 들어갈 수 있도록 관리자가 선택하기에 복호화 비용이 너무 "높습니다."[3] 이러한 한계로 인해 해커는 탐지되지 않을 것을 알고서 멀웨어를 숨겨 암호화된 트래픽의 통신을 명령하고 제어할 수 있습니다.

기가시큐어 보안 전달 플랫폼은 어느 기업에 진입하든 간에 필요에 따라 SSL 트래픽을 매우 효율적으로 복호화했다가 다시 암호화합니다.[4] 복호화된 트래픽은 검사를 위해 기업 내 필요한 모든 보안 툴에 제공되었다가 침입 차단 시스템(IPS)과 같은 인라인 차단 툴을 위해 다시 암호화됩니다. 멀웨어와 명령 및 제어 트래픽은 보안 툴을 회피할 목적으로 더 이상 SSL 암호화를 사용할 수 없습니다.

네트워크 사각지대 제거

대부분 보안 툴은 위치해 있는 네트워크 세그먼트를 가로질러 이동 중인 데이터에 대해서만 접근할 수 있습니다. 이로 인해 첨단 공격을 식별하는 데 필요한 모든 데이터를 연관 짓기가 매우 어렵습니다. 주변 보안 툴은 데이터 센터 내 "East-West" 트래픽뿐만 아니라 가상 머신에서 작동하는 애플리케이션 서비스 간 트래픽에 대해 가시성을 거의 갖지 않기 때문에 특히 부적합합니다.

기가시큐어 보안 전달 플랫폼은 기존 서버, 가상화된 서버 팜 내 가상 머신 및 네트워크 장치(예: 스위치, 라우터)간 이동하는 네트워크 트래픽을 확보하여 그 트래픽을 조직의 모든 보안 툴에 전달하여

[1]침해 레벨 인덱스, 2018년 1월
[2]우리는 전체 웹을 암호화하는 과정 중에 있습니다.
[3]주요 차세대 방화벽 8개에 대한 NSS 연구소의 연구 결과에 따르면 SSL 트래픽을 스캐닝하는 경우 방화벽 성능이 80%까지 저하됩니다.
[4]개인식별정보(PII)와 같은 데이터는 규제 기관의 요구사항을 충족하기 위해 암호화하거나 가린 상태로 둘 수 있습니다.

"퍼베이시브 가시성"을 제공합니다. 보안 정보 및 이벤트 관리 시스템(SIEM)뿐만 아니라 보안 분석 툴은 네트워크상 어디에서라도 모든 첨단 공격 징후에 대한 가시성을 확보합니다. 멀웨어 방지 툴, 방화벽, 침입 탐지 시스템, 데이터 누출 보호 툴과 같은 제품은 멀웨어, 스폿 측방향 움직임 그리고 외부 공격자로부터의 통신을 탐지하는 데 필요한 모든 데이터를 확보하여 악성 내부자의 의심되는 동작을 추적합니다.

관리 단순화를 통해 오류 축소

네트워크가 커지고 더욱 세분화됨에 따라 대부분 기업은 보안 장치를 추가로 구매할 수밖에 없습니다. 이로 인해 비용이 높아질 뿐만 아니라 보안 인프라가 더욱 복잡해져서 관리하기가 어려워집니다. 복잡함으로 인해 오류가 증가하고 기업 전반의 데이터를 포착하여 분석하기가 더욱 어려워집니다.

그러나 기가시큐어 보안 전달 플랫폼을 활용하여 조직은 그 외 방식의 경우 필요한 보안 툴 1/4만 가지고 스스로를 보호할 수 있습니다.[5] 이 플랫폼은 이를 위해 프로세서 집약적인 작업의 부하 제거, 각 툴에 대한 트래픽 필터링, 툴의 트래픽에 대한 로드 밸런싱과 같은 기법을 활용합니다.

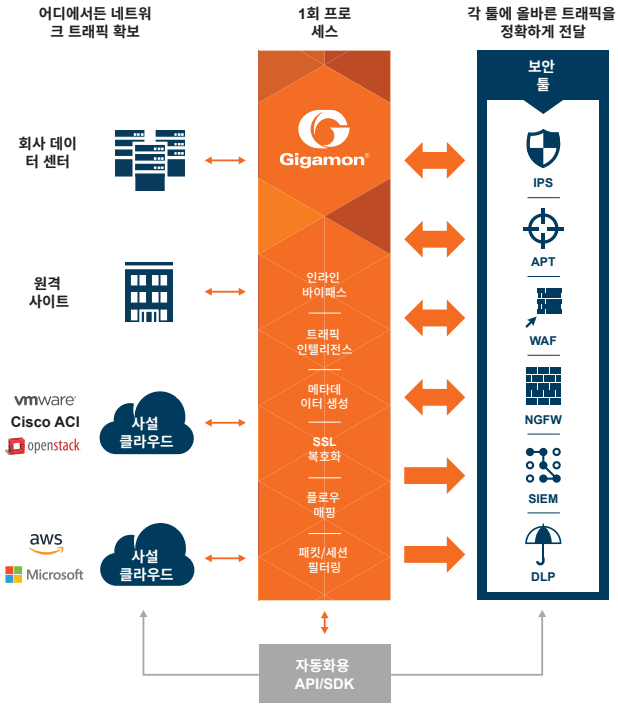
툴이 더 적다는 것은 덜 복잡하고 관리가 용이하다는 것을 의미합니다. 이를 통해 더 정확한 구성, 더욱 신뢰할 수 있는 업데이트, 보다 나은 보안 데이터 수집 그리고 기존 보안 툴의 효과를 높이는 기타 개선을 이룰 수 있습니다.

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

기가시큐어 보안 전달 플랫폼

다이어그램에 나와 있듯이 기가시큐어 보안 전달 플랫폼은

- 기업 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 작업의 부하를 개별 툴에서 제거합니다.
- "트래픽 인텔리전스"를 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.



기가시큐어 보안 전달 플랫폼은 보안 툴이 물리적 및 가상의 환경뿐만 아니라 클라우드 환경에서 보다 효율적으로 작동할 수 있도록 특별히 개발된 차세대 네트워크 패킷 브로커입니다. 인라인 위협 차단 툴을 위해 이 플랫폼은 보안 태세를 강화하고, IT를 단순화하며, 비용을 줄여줍니다. 모든 보안 툴이 사이버공격을 신속하게 탐지하여 분석하고 차단할 수 있도록 기업 주변 내 모든 활동에 대한 퍼베이시브 가시성도 제공합니다. 또한 조직의 특정 보안 툴에 정밀 데이터를 전달하기 전에 기업 내 어디에서든 네트워크 트래픽을 확보하여 트래픽 인텔리전스를 적용함으로써 부분적인 가시성과 사각지대를 제거해줍니다.

[5]Forrester사의 산업 분석자와 면담한 기가몬 고객은 자사가 기가몬 기술을 확보하지 않았더라면 기기를 4배 더 많이 구입했을 것이라고 추정했습니다. 기가몬의 전체적인 경제 효과(The Total Economic Impact)™ 연구에서 인용함: 비용 절감 및 사업적 이익

3254-02 03/18

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