사례 연구: Symantec과 Napatech의 파트너쉽 - 기업 내 정보유출 위험성에 대한 이해.

Symantec 소개

정보유출방지에 대한 가트너 매직 쿼드런트(Gartner's Magic Quadrant)에 의하면 Symantec은 기업 정보유출방지(DLP) 솔루션 제공 분야의 리더입니다. DLP는 데이터 침해의 증가와 함께 시간과 비용이 소모되고 브랜드 가치를 훼손시키는 큰 보안 문제가 되었습니다. 정보유출 사각지대를 확인하기 위해 Symantec 정보유출방지(DLP) 네트워크 모니터는 기밀 정보가 IT 네트워크를 떠나기 전에 지속적으로 비즈니스 통신을 검사합니다.

도전: 정보유출 위험의 범위 이해하기

오늘날, 기업들은 생성 및 수집되는 데이터 양이 폭발적으로 증가함에 따라 보안에 대한 필요성을 인식합니다. 기업이 자신들의 지적 재산(IP)을 보호하여 경쟁력을 유지하고 고객의 정보를 보호하는 일은 IT 경영진에서 큰 우선 순위(최우선이 아니면)를 두어야 하는 일입니다. 특히 전 세계에서 2016년 한해 동안 발생한 데이터 침해 횟수만 보면 이메일 제공업체, 소셜 네트워킹, 제조, 건강, 교육, 정부, 소프트웨어, 소매업 등 안전한 분야는 어디에도 없습니다.

모든 기업의 정보유출 위험은 IT 제어 영역 밖에서 기기 및 네트워크(특히 모바일 기기 및 클라우드)를 사용하면서 크게 증가합니다. 잠재적 데이터 영역의 수가 증가할 뿐만 아니라 모니터링해야 할 데이터 양도 크게 증가합니다. 정보유출을 평가하는 데 필요한 모든 데이터를 수집하는 일은 점점 더 어려워지고 있습니다.

해결 방법: Symantec 네트워크 모니터와 함께 Napatech 가속기를 사용

Symantec의 네트워크 모니터를 사용하면 기업에서 정보유출이 발생하는 위치를 정확하게 파악할 수 있습니다. 이 솔루션은 네트워크를 통과하는 데이터를 소극적으로 모니터링하기 때문에 일상 작업에 영향을 미치지 않습니다. 궁극적으로는 고객이 보안 허점을 확인하면 미래에 그러한 정보유출을 차단하는 방법을 정확하게 정할 수 있습니다.

네트워크 모니터가 정보유출 범위를 정확하게 나타낼 수 있도록 Napatech 가속기가 항상 전체 데이터 패킷을 캡처합니다. Napatech를 통해 네트워크 모니터는 현재까지 IT 네트워크 밖으로 전송된 모든 데이터를 완벽하게 파악합니다.

도전

정보유출 위험은 IT 제어 영역 밖에서 기기 및 네트워크를 사용하면서 크게 증가합니다. 반면 정보유출을 평가하는 데 필요한 데이터를 수집하는 일은 점점 더 어려워지고 있습니다.

솔루션

Napatech 가속기 및 Symantec DLP 네트워크 모니터를 사용하면 패킷 손실 없이 기업 IT 네트워크 밖으로 전송 중인 기밀 데이터를 감지할 수 있습니다.

장점

Napatech 가속기 및 Symantec DLP 네트워크 모니터를 사용하면 모든 기업 통신을 확인할 수 있기 때문에 민감한 정보를 잘못 처리하여 기업을 정보유출 위험에 빠뜨릴 수 있는 고위험 사용자를 식별할 수 있습니다.

DN-1037 Rev. 1-KO

장점

Napatech 가속기로 기업 네트워크를 드나드는 모든 패킷을 캡처할 수 있습니다. 그 후 Symantec 네트워크 모니터는 캡처한 모든 관련 데이터를 검사하고 기업은 정보유출 위험에 대한 포괄적인 그림을 얻을 수 있습니다. 전송되는 데이터의 양과 유형이 계속 증가함에 따라 위험을 철저하게 평가하는 일이 매우 중요합니다.

이 솔루션의 장점은 모든 분야에 적용됩니다.

사례 1:

EHR(전자 건강 기록)의 등장으로 미국 건강 관리에서는 환자의 비밀을 보장하는 것이 가장 중요한 일입니다. EHR은 의사가 환자에게 종합적이고 원활한 서비스를 제공하는 것을 도와주지만(의료 시설이 개인 의료 기록을 빠르게 확인할 수 있음) 이러한 기록에 포함된 개인 의료 정보(PHI)는 HIPAA(Health Insurance Portability and Accountability Act: 건강 보험 양도 및 책임에 관한 법)를 통해 비밀로 유지하도록 법으로 정해져 있습니다.

PHI를 무단으로 액세스하면 신원 정보(생일, 주민번호)뿐만 아니라 법적으로 의사와 환자 사이에서만 공유할 수 있는 진단 내용도 유출됩니다. 예를 들어, 보험 회사는 환자의 보장 내용을 확인하기 위해 의료 서비스 제공자로부터 정보를 요청할 수 있습니다.

의료 서비스 제공자는 신속한 처리를 위해 환자의 암호화되지 않은 파일을 보낼 수 있습니다. 네트워크 모니터가 있다면 자동으로 이 통신에는 미준수 플래그가 실시간으로 표시되고 제공자는 즉시 조치를 취할 수 있습니다.

사례 2:

소매업계의 정보유출 위험은 쉽게 잠재적인 수익 손실로 변환되기 때문에 기업은 자신들의 지적 재산(IP)을 보호하여 경쟁력을 유지해야 합니다. 오늘날의 대규모 소매업체는 전 세계 고객들에게 서비스를 제공하기 때문에 수많은 지역의 유통업자와 IP를 공유해야 합니다. 경쟁사에서 장점(예: 도용)으로 사용할 수 있는 데이터 유출 가능성을 최소화하기 위해 정보 교환은 보안이 철저해야 합니다.

소매업체는 최신 가격 정보를 제공하는 것이 중요합니다. 일부 소매업체에서는 유통업자가 액세스할 수 있는 중앙 문서 보관소를 제공하기도 합니다. 유통업자는 고객과의 미팅을 위해 최신 가격 정보가 필요할 수 있으며 현장에 보관소에 액세스할 수 없기 때문에 소매업체에 정보를 보내줄 것을 직접 요청하게 됩니다.

하지만, 소매업체에서는 예를 들어, 이메일이나 ftp를 통해 유통업자에게 가격 정보를 직접 보내줄 수 없습니다. Napatech는 네트워크 모니터를 통해 미준수 사례를 캡처하므로 IP가 도용될 위험이 없습니다.

사례 3:

대학교에서도 정보유출을 우려해야 합니다. 이러한 기관도 정부 기관 및 민간 부문으로부터 지원 받는 연구를 통해 IP를 생성합니다. 그러나, 대학은 항상 부족한 예산으로 운영되는 것으로 알려져 있어 포괄적인 DLP 솔루션을 구현할 시간이나 리소스가 없을 수 있습니다.

Napatech 가속기가 있으면, 네트워크 모니터는 상대적으로 짧은 시간 안에 실제 DLP 위험을 평가할 수 있습니다. 효율적인 패킷 캡처를 통해 조직에서 정보유출 위험 범위를 완전히 파악할 수 있습니다. 이러한 파악을 통해 대학에서 DLP용 아키텍처 구현에 대한 비즈니스 사례를 만들고 장단기 문제를 해결하기 위한 실용적인 계획을 세울 수 있습니다.

Symantec 정보유출방지에 대한 자세한 내용은 다음을 방문하십시오.
go.symantec.com/dlp

Napatech 가속기에 대한 자세한 내용은 다음을 방문하십시오.
www.napatech.com/products/accelerators

추가적인 고객 사례는 다음을 참조하십시오.
www.napatech.com/resources/case-studies

유럽, 중동 및 아프리카
Napatech A/S
덴마크, 코펜하겐

전화: +45 4596 1500
info@napatech.com
www.napatech.com

북미
Napatech Inc.
매사추세츠, 보스턴
캘리포니아, 로스앨터스
워싱턴 D.C.

전화: +1 888 318 8288
info@napatech.com
www.napatech.com

아시아태평양
Napatech China/South Asia
타이완, 타이베이
전화: +886 2 28164533 Ext. 319

Napatech Japan K.K.
일본, 도쿄
전화: +81 3 5326 3374

Napatech Korea
서울
전화: 02 6001 3545

ntapacsales@napatech.com
www.napatech.com