불분명한 네트워크 경계,
어떻게 해야 할까요?

클라우드 애플리케이션, 모바일 디바이스, 원격 작업자들이 네트워크 경계라는 개념을 제거하면서 보안 문제가 대두됩니다.

Symantec™

클라우드 세대의 보안

클라우드 세대의 네트워크 보호 관련 심각한 보안 문제를 해결하십시오.

모바일 사용자, 원격 사무실, 클라우드 애플리케이션을 보호하려면 어떻게 해야 할까요? 컴플라이언스 의무를 충족하면서 갈수록 지능화되는 끊임없는 사이버 보안 공격에 대응하려면 어떻게 해야 할까요?

지점/지사 및 원격 인터넷 트래픽은 보안 및 보안 위협 차단 정책이 적용되는 기업 데이터 센터로 백홀(backhaul)됩니다. 기업이 클라우드로 운영을 이전함에 따라 이 모델은 점차 사라지는 추세입니다. 이는 한편으로 사설 MPLS(Multiprotocol Label Switching) 링크가 상당히 고가인데다 백홀로 인해 클라우드 애플리케이션 및 웹을 확보하려는 오프사이트 직원에게 영향을 미치는 지연 문제가 발생하기 때문입니다. 또는 직원들이 직접 클라우드 기반 보안 서비스에 액세스하여 백홀을 제거할 수 있으므로 트래픽이 웹 및 클라우드 애플리케이션으로 이동하는 시점에 보안 정책이 적용됩니다.

2017년

13건중1건

분석 결과 악성으로 밝혀진 게이트웨이 URL

2016년의 20건 중 1건에서 증가

제안 사항

- 클라우드 기반 보안 웹 게이트웨이를 보안 인프라트럭처의 기반으로 삼으십시오. 위치에 관계없이 모든 사용자와 데이터를 보호할 수 있습니다.
- 네트워크 성능 및 경제성을 훼손하지 않고 필요한 보안을 확보하십시오.
- 업계 최고의 보안 위협 차단 기술을 채택하십시오.
- 통합 보안 정책으로 온프레미스 및 원격/모바일 사용자를 보호하십시오.
- 유연하고 효과적인 보호를 위한 통합 솔루션을 선택하십시오.

암호화된 트래픽에 숨겨진 경우 악성 코드가 기존 네트워크 방어 체계를 침투하여 공격할 수 있습니다. 오늘날 대부분의 인터넷 트래픽이 암호화되고 점차 많은 공격자들이 암호화를 사용하여 악성 코드를 확산시키고 있습니다.

2장

첨단 클라우드 기반 Secure Web Gateway를 중심으로 방어 체계 구축

클라우드 세대에는 웹 및 클라우드 애플리케이션 보안 기본 조치를 넘어서는 Secure Web Gateway(SWG)가 필요합니다.

SWG(Secure Web Gateway)를 통해 웹 및 클라우드 애플리케이션에 유입되는 데이터를 신속하게 보호하면서 악성 코드가 있거나 정보 보안 컴플라이언스를 위반하는지 트래픽을 검사합니다(암호화된 경우 포함). 이것이 바로 SWG가 네트워크 보안 스택의 완벽한 기본을 형성하는 이유입니다. 첨단 클라우드 기반 Secure Web Gateway는 기업에 허용 가능한 웹 사용 정책을 적용하는 등 기존의 기본적인 기능을 능가합니다. 여기서는 보안 위협 인텔리전스 데이터를 통해 URL의 리스크를 평가하고 직원들이 위험한 사이트를 방문하지 않도록 하는 동시에 검사 기술을 통합하여 사이버 보안 위협 및 데이터 유출 여부를 확인합니다. 일부 SWG는 웹 격리와 같은 혁신적인 기술을 통합하여 사용자를 위한 추가적인 보안 위협 차단 기능을 제공합니다. 모든 기능을 갖춘 SWG는 사용자가 주요 보안 및 컴플라이언스 과제를 해결하는 데 필요한 통합적인 기능을 제공합니다. 무엇보다 클라우드에서 제공되는 경우 이 기능을 통해 상시 사용자의 트래픽을 라우팅하여 사용 중인 디바이스 유형 및 그 위치에 관계없이 모든 디바이스를 보호합니다.

제안 사항

- **선택적으로 암호화된 트래픽을 검사하여 해당 컨텐트에 악성 코드가 포함되거나 컴플라이언스를 위반하는지 확인하십시오.**
  - SSL/TLS 암호화 트래픽을 신속하고 안전하게 검사하여 기업에 필요한 보호를 제공하고 사용자가 요구하는 성능을 제공하십시오. 대부분의 인터넷 트래픽이 암호화되므로 네트워크 보안 솔루션을 사용하여 보안 및 데이터 컴플라이언스 검사 엔진을 기준으로 트래픽을 복호화 및 조정하는 것이 중요합니다. 사용자의 웹 브라우저를 표적으로 하는 신종 보안 위협 클래스로부터 보호하는 것 역시 중요 요건입니다.
- **직원이 잠재적으로 위험한 웹 사이트에 액세스하지 않도록 보호하십시오. 이메일에 포함된 URL에 안전하게 액세스하고 기업 액세스 자격 증명이 피싱 사이트에 액세스할 수 없도록 하십시오.**
  - 웹 격리 기술을 통해 사용자의 웹 브라우저를 표적으로 하는 보안 위협과 직원의 디바이스를 대상으로 하는 피싱 공격을 차단하십시오. 웹 격리 기술은 엔드포인트 외부에서 웹 세션을 실행하여 사용자의 브라우저에 안전한 렌더링 정보만 전송하는 방식으로 웹 사이트에서 전달된 제로데이 악성 코드가 사용자의 디바이스에 도달하지 않도록 방지합니다.

2장

첨단 클라우드 기반 Secure Web Gateway를 중심으로 방어 체계 구축

- **암호화 여부에 관계없이 모든 웹 트래픽에 데이터 개인 정보 보호 및 차단 정책을 자동으로 적용하고 대시보드 및 온라인 리포트를 사용하여 활동을 모니터링하십시오.**
  - 정확하고 신속한 분석을 위해 복호화된 SSL/TLS 트래픽을 Data Loss Prevention(DLP) 시스템에 전송하십시오. 규정 준수 컴플라이언스를 지원하고 데이터를 보호하십시오.
- **사용 중인 클라우드 애플리케이션을 정확하게 식별하고 관련 리스크를 평가하며 사용자, 그룹, 위치를 기반으로 액세스를 제어하십시오.**
  - CASB(Cloud Access Security Broker) 제어를 통해 퍼블릭 클라우드와 상호 작용하는 데이터와 클라우드 애플리케이션을 보호하십시오. Office 365와 같이 "알려진" 클라우드를 비롯하여 직원이 직접 프로비저닝한 "섀도우 IT" 클라우드와 같이 사용 중인 모든 클라우드 애플리케이션에 대한 가시성을 확보하여 기업의 클라우드 사용 정책을 준수하도록 하십시오.
- **클라우드 SWG를 온프레미스 및 모바일 엔드포인트 보호와 통합하십시오.**
  - 네트워크 보안과 엔드포인트 설치 보안을 통합하여 완벽한 다계층 네트워크 및 엔드포인트 보호와 간소화된 모바일 디바이스 애플리케이션 관리 기능을 확보하십시오. 인터넷에 직접 연결하는 모바일 및 원격 사용자를 포함하여 모든 엔터프라이즈 엔드포인트를 보호하는 멀티티어 방어 체계를 구축하십시오.
- **SD-WAN 성능 및 유연성을 활용하면서 지점/지사/원격 사무실 직원을 네트워크에 연결하십시오.**
  - 원격 트래픽을 클라우드 보안으로 라우팅하는 선택적인 SD-WAN(및 유사) 디바이스를 사용하여 원격 사무실 및 모바일 직원을 안전하게 보호하십시오. 방화벽 또는 프록시에서 구성을 변경하거나 사용자 디바이스에서 간단히 조정을 수행하면서 손쉽게 시작할 수 있습니다.

3장

고비용 없이 보안 및 성능 획득

클라우드의 네트워크 보안 서비스(Network Security as a Service)를 사용하여 직원을 보호하는 데 필요한 모든 기능을 확보하십시오.

위치나 사용 중인 디바이스에 관계없이 모든 사용자에게 일관된 정책이 적용됩니다. 무엇보다 클라우드 기반 네트워크 보안 스택으로, 클라우드 속도 및 간소화를 기반으로 한 통합적인 보안이 제공됩니다. 또한 필요한 모든 항목이 비용 효율적인 단일 서비스에 통합되므로 새로운 사용자를 위해 제품 사용 기간을 간단히 추가하면서 필요에 따라 구축을 확장할 수 있습니다.

Direct-to-net 효용성

클라우드 기반 보안은 직원들이 소위 "direct to net" 보안이라는 웹 위치 또는 클라우드 애플리케이션에 대한 액세스를 시도하는 중에 보안 서비스에 연결하게 되므로 사무실과 모바일 사용자를 위해 탁월한 성능을 제공할 수 있습니다. 또한 사무실과 클라우드를 간단히 연결하는 SD-WAN 솔루션 통합 서비스를 모색합니다.

효율적인 SSL/TLS 암호화 검사

주요 SSL/TLS 트래픽 검사 시 원치 않는 대기 시간이 발생하거나 컴퓨팅 리소스가 낭비되지 않도록 하십시오. 차세대 방화벽과 같이 적합하지 않은 디바이스를 사용하는 경우 성능이 심각하게 저하될 수 있습니다.

단일 에이전트 네트워크 보안 액세스

대부분의 직원들은 갈수록 증가하는 원격 및 모바일 디바이스를 통해 네트워크에 연결하려 합니다. 에이전트를 추가하여 각각을 클라우드 기반 네트워크 서비스에 연결할 수 있도록 허용하는 이유는 무엇일까요? 통합 엔드포인트 보안을 제공하는 가벼운 단일 에이전트는 웹 트래픽을 클라우드의 네트워크 보안 스택으로 리디렉션하여 성과를 거둘 수 있습니다.

4장

Office 365 등의 애플리케이션에 대한 가시성 확보, 리스크 최소화, 컴플라이언스 유지

CASB 제어를 통해 사용 중인 클라우드 애플리케이션을 정확하게 식별하고 관련 리스크를 평가하며 사용자, 그룹, 위치를 기반으로 액세스를 제어하십시오.

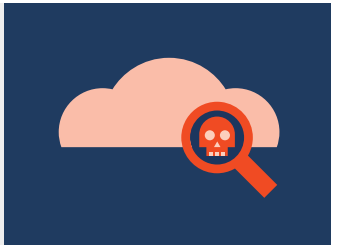
규정을 준수하려면 중요 데이터의 위치에 관계없이 어디서든 모니터링하고 제어할 수 있어야 합니다. 여기에는 소위 섀도우 IT라고 불리는 IT 팀의 허가 없이 직원이 채택한 애플리케이션을 포함하여 클라우드 애플리케이션에 공유된 문서 데이터가 포함됩니다. CASB 기능은 Office 365와 같은 퍼블릭 클라우드 애플리케이션과 연동하는 데이터를 보호합니다.

사용 중인 애플리케이션을 정확하게 식별

다양한 클라우드 애플리케이션 및 서비스 전반에서 사용자 활동을 심층 모니터링하고 세부적인 컨텐트 및 컨텍스트 기반 정책을 시행합니다. 클라우드 애플리케이션 사용을 지속적으로 모니터링하고 중요 데이터 공유 시 이를 탐지합니다. 직원이 클라우드 사용 정책을 준수하는지 확인하십시오.

클라우드 애플리케이션 리스크 평가

직원들이 사용하는 모든 클라우드의 다양한 속성을 검사합니다. 위험한 활동, 악성 행위 또는 악성 코드 보안 위협을 실시간으로 찾아 차단하면서 정보를 보호합니다.



클라우드 애플리케이션 액세스 제어

사용자, 그룹, 위치, 클라우드 속성 데이터를 기반으로 액세스 및 제어 정책을 설정합니다. 중요 컴플라이언스 관련 데이터를 식별하고 분류한 다음 해당 데이터가 클라우드 애플리케이션에서 어떻게 업로드, 다운로드, 공유되는지 모니터링합니다.

5장

간소화 및 일관성 확보를 위한 보안 정책 관리 통합

급속도로 변화하는 규제 요건 및 기업 정책을 채택하면서 온프레미스 및 클라우드 환경 전반에서 빠르게 정책을 정의하고 구현하십시오.

보안 인프라스트럭처를 변경할 경우 운영 복잡성이 발생할 수 있습니다. 이후 계획을 수립하지 않으면 서로 다른 정책을 요구하는 클라우드와 온프레미스 플랫폼을 사용하면서 별도의 두 가지 시스템을 유지 보수하게 될 수 있습니다. 단일 정책 세트를 통해 이 두 가지 시스템을 관리하면서 온프레미스와 클라우드에 유사한 기능을 구축하도록 허용하는 솔루션을 선택하여 간소화를 실현하십시오. 100% 클라우드로 이전하는 경우 버튼 한 번으로 기존 보안 정책을 클라우드 네트워크 서비스로 마이그레이션할 수 있는 솔루션을 모색하십시오.

간편하게 클라우드 기반 보안으로 전환

새로운 클라우드 기반 보안으로 자동 마이그레이션이 가능한 온프레미스 정책을 지정하십시오.

일관성 있는 정책 생성 및 관리

새로운 정책을 생성해야 할 경우 한 번만 정의한 다음 모든 시만텍 게이트웨이에 푸시하여 하이브리드 온프레미스와 클라우드 보안 환경에서 일관성 있게 시행할 수 있습니다.

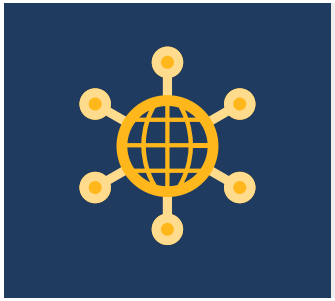
기존 투자 효과 극대화

가능한 경우 기존 보안 시스템을 활용하십시오. DLP 투자를 활용하면서 클라우드로 확장하십시오. 가능한 경우 주요 데이터 센터에서 온프레미스 SWG를 유지 보수하면서 지점/지사 및 모바일 사용자를 클라우드로 이전하십시오. 단일 관리 콘솔에서 프라이빗/퍼블릭, 물리적, 가상 또는 클라우드, 이 모두를 조합한 환경을 관리하십시오.

6장

결론: 경계가 무색합니까? 걱정하지 마십시오. 클라우드 기반 종합 네트워크 서비스

시만텍의 클라우드 기반 Web Security Service는 고성능 글로벌 클라우드 서비스에서 제공되는 강력한 엔터프라이즈급 보안 기능을 사용하여 위치에 관계없이 주요 위치, 지점/지사, 원격 및 로밍 사용자를 보호합니다.



탁월한 네트워크 보안 기능

클라우드 기반 Web Security Service는 Gartner Secure Web Gateway Magic Quadrant에서 11년 동안 리더로 선정된 Symantec ProxySG와 동일한 첨단 프록시 기술에서 실행됩니다. 전체 네트워크 보안 스택의 기반인 첨단 Secure Web Gateway를 중심으로 고유한 보안 위협 인텔리전스인 악성 코드 분석, 샌드박싱, 웹 격리, 클라우드 애플리케이션 제어(CASB), 데이터 유출 방지, 통합 SD-WAN을 결합하여 직원이 방문하려는 모든 웹 사이트의 리스크를 검사합니다.

글로벌 클라우드 네트워크: 입증된 성능

시만텍은 분산된 탄력적인 글로벌 클라우드 데이터 센터 인프라스트럭처를 통해 "거의 완벽한"(99.999%) 업타임 SLA를 제공합니다. 또한 Microsoft, Amazon, Google, 기타 애플리케이션과의 네트워크 피어링, 클라우드 스토리지 애플리케이션 간의 신속한 대용량 파일 이동을 지원하는 TCP 윈도우 최적화를 통해 성능을 최적화합니다.

통합 보호 솔루션으로 운영 간소화

시만텍은 엔드포인트도 보안 솔루션을 구축해야 할 필요성을 절감하고 있습니다. 시만텍이 업계 최고의 Symantec Endpoint Protection(SEP)과 Web Security Service를 통합한 이유입니다. 이러한 제품을 함께 사용하면 엔드포인트에 설치 및 관리할 에이전트 수를 줄일 수 있습니다. 웹 트래픽이 Web Security Service로 라우팅되도록 SEP를 구성하여 네트워크 보안 정책을 적용할 수도 있습니다. 시만텍은 고유한 엔드포인트 및 네트워크 보안 심층 서비스를 제공하여 경계가 모호한 환경에서 사용자를 안전하게 보호합니다.

자세한 내용은 아래에서 확인하십시오.

symantec.com/ko/kr/products/web-and-cloud-security

시만텍 소개

글로벌 사이버 보안 분야를 선도하는 시만텍은 기업, 정부 기관 및 개인의 중요한 데이터가 어디에 있든 안전하게 보호될 수 있도록 지원한다. 시만텍은 엔드포인트, 클라우드, 인프라 전반을 정교한 공격으로부터 방어할 수 있는 전략적인 통합 솔루션을 전 세계 기업과 기관에 제공하고 있다. 또한, 전 세계 5천만 이상의 개인사용자와 가정에서 시만텍 노턴 제품과 라이프록(LifeLock) 제품을 이용해 가정과 다양한 기기에서 디지털 라이프를 보호하고 있다. 시만텍은 세계 최대 규모의 민간 사이버 인텔리전스 네트워크를 통해 고도화된 지능형 위협을 탐지하고 고객들을 보호한다. 보다 자세한 정보는 시만텍 웹사이트(www.symantec.com/ko/kr)와 페이스북, 트위터, 링크드인을 통해 확인할 수 있다.

서울시 강남구 테헤란로 152강남파이낸스센터 28층 | TEL: 02-3468-2000 | FAX: 02-3468-2001 | www.symantec.com/ko/kr

19C210137_SB_VANISHING_PERIMETER_KR