Advanced Malware Protection을 통해 Office 365를 개선하는 Cisco Email Security

개요

Microsoft Exchange는 전 세계의 중간 규모~대규모 조직에서 사용하는 표준 이메일 시스템으로 자리잡았습니다. 클라우드 애플리케이션이 등장함에 따라 Microsoft는 Office 365를 도입했습니다. 이 문서에서는 Office 365 고객이 Cisco® CES(Cloud Email Security)를 통합하여 이메일 보안을 개선할 수 있는 방법을 설명합니다.

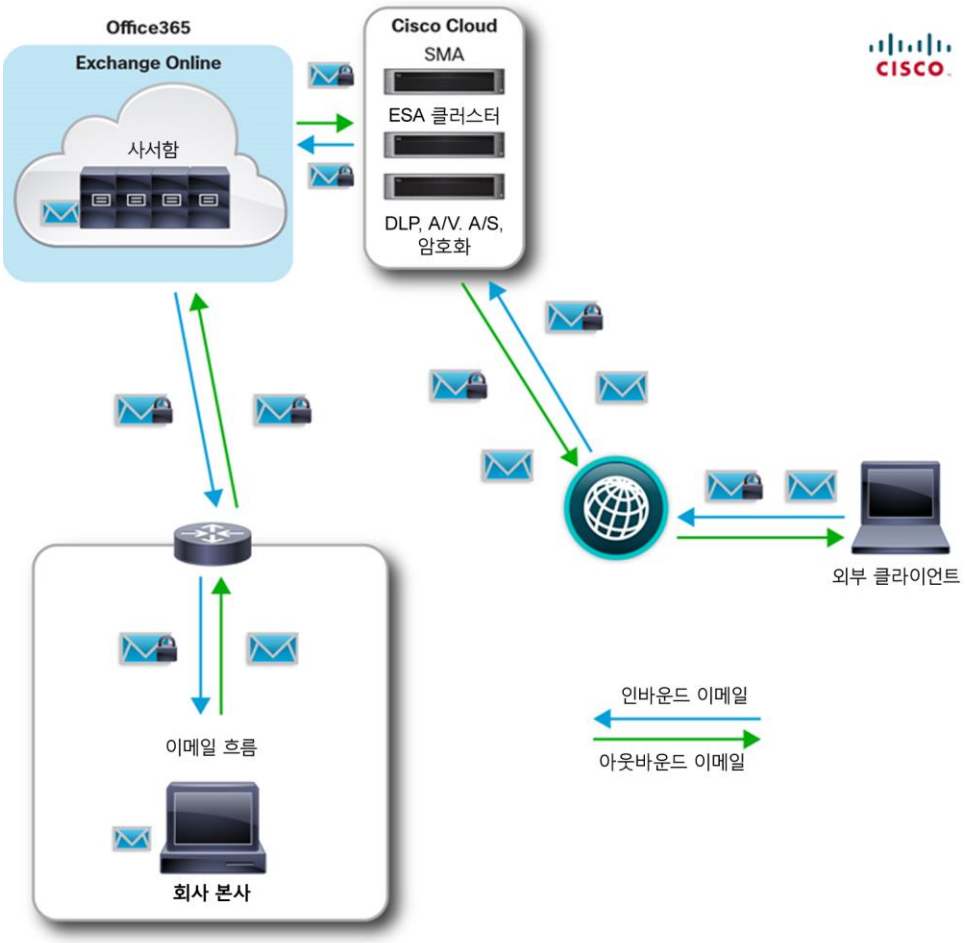
백서 결론: Office 365에 CES가 필요한 이유

CES는 다음과 같은 기능을 제공합니다.

- 최고의 효율성(차단율 99%, 이메일 1백만 건당 오탐 수 1건 미만)을 자랑하는 업계 최고의 이메일 기반 위협(피싱/표적 공격 포함) 방지 기능
- AMP Threat Grid를 통한 정적 및 동적 악성코드 분석(샌드박싱)
- 데이터 유출 방지 및 매우 안전한 메시징을 위한 통합 컨트롤
- 메시지 수준 암호화(서드파티 제품 불필요)
- 다중 벡터 고급 악성코드 공격 방지를 위한 Cisco Talos 서비스의 동적 업데이트
- 실시간에 가까운 그래픽 메시지 추적(명령줄 인터페이스에서 실시간 추적 기능 제공)
- 전용 클라이언트 인프라(다른 고객으로 인한 중단 위험 감소)
- 호스팅된 Email Security 고객을 위한 전용 모니터링 및 지원
- 필요한 경우 Cisco 지원을 통해 고객 제어 보고 기능 제공

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

그림 1. Office 365와 통합된 Cloud Email Security



메모: Cisco Cloud Email Security 구성 요소에는 Content Security Management Appliance, Email Security Appliance 클러스터, 데이터 유출 방지, 안티바이러스/안티 스팸 툴 및 암호화 기능이 포함됩니다.

현재 환경

클라우드는 획기적으로 발전해 왔습니다. 기존에는 내부에서 제공되었던 서비스를 제공하기 위해 작업과 리소스를 사이트 외부로 이동하는 조직이 갈수록 증가하고 있습니다. 온라인 서비스로 마이그레이션한 기업에는 많은 혜택이 제공되었습니다. 현재는 소규모 기업도 통신, 네트워크 및 서버 리소스에 자본을 지출하지 않고도 엔터프라이즈급 이중화 및 재해 복구 기능을 사용할 수 있습니다.

경쟁 우위를 확보하고자 하는 기업은 이전에는 재무 관련 문제만큼 미션 크리티컬 요소가 아닌 것으로 간주되었던 이메일이 이제는 비즈니스 크리티컬 요소로 자리잡았음을 인식하고 있습니다. 기업은 이메일을 통해 많은 양의 업무를 수행합니다. 금융, 거래, 판매 계약, 법률 문서가 보안 여부에 관계없이 모두 전자 메일을 통해 전송됩니다. 기업은 클라우드로 이전하기 위한 논리적 단계가 사서함을 클라우드로 이동하는 것임을 깨달았습니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

클라우드 이메일을 사용하는 경우 운영상 많은 이점이 제공되지만, 이러한 시스템에서도 온프레미스(구내 장비)에서 호스팅되는 이메일과 마찬가지로 정교한 공격으로 인해 보안 침해가 발생할 수 있습니다. 이러한 위협에는 현재 널리 확산되어 있는 신규 악성코드 배포와 표적이 지정된 소규모 공격을 비롯한 제로 데이 악성코드가 포함됩니다. 스노우슈(Snowshoe) 스팸은 보안 탐지를 피하기 위해 대량의 IP 주소에서 소량의 스팸을 발송하는 새롭게 등장한 위협입니다. 이러한 모든 방법은 효율성이 매우 높은 것으로 확인되었으며 기능성이 떨어지는 스팸 필터를 통과하는 경우가 많습니다.

이로 인해 클라우드를 사용하는 조직 역시 기업과 고객의 데이터를 도용하려는 매우 정교한 악성코드 위협을 통한 이메일 공격을 끊임없이 받고 있습니다.

Microsoft EOP(Exchange Online Protection)

Office 365 보호 기능을 제공하는 호스팅된 필터링 서비스인 Microsoft EOP는 다음과 같은 기능을 제공합니다.

- 안티 스팸 필터
- 안티바이러스 보호
- 정책 시행
- 재해 복구
- 디렉토리 서비스

자세한 내용은 https://technet.microsoft.com/en-us/library/dn762130%28v=exchg.150%29.aspx를 참고하십시오.

이러한 SLA 및 Microsoft Exchange의 시장 점유율을 고려할 때 Office 365와 EOP를 이메일 보안 솔루션으로 사용하는 것이 효율적이라고 생각하는 고객이 많습니다. 하지만 보다 심도 있는 보안 솔루션에 대한 고객의 수요가 증가함에 따라 Microsoft는 서드파티 시스템과의 연동을 위한 Office 365용 메커니즘을 제공하게 되었습니다. 여기에는 Cisco Email Security 클라우드 및 온프레미스(구내 장비) 솔루션과 같은 업계 최고의 솔루션 및 RSA Data Loss Prevention이 포함됩니다.

Cisco Cloud Email Security

Cloud Email Security는 Fortune 1000대 기업의 40%를 인바운드 및 아웃바운드 이메일 위협으로부터 보호하는 업계 최고의 기술을 기반으로 합니다. 고객은 온사이트 데이터 센터 설치 공간을 절약하고 이메일 보안 관리를 신뢰할 수 있는 보안 전문가에게 위임할 수 있습니다. Cloud Email Security는 여러 장애복구형 Cisco 데이터 센터의 전용 인프라를 통해 최고 레벨의 서비스 가용성 및 데이터 보호 기능을 제공합니다. 고객은 호스팅된 인프라에 계속 액세스할 수 있으며 인프라를 확인할 수 있습니다. 포괄적인 보고 및 메시지 추적 기능이 매우 유연한 관리 작업을 지원합니다. 이 고유한 서비스에는 소프트웨어, 하드웨어, 지원이 모두 번들로 포함되어 더욱 간편하게 이용할 수 있습니다.

이 서비스는 다음과 같은 동급 최고의 기능을 제공합니다.

- **Talos/SenderBase:** 알려진 위협과 새롭게 등장하는 위협으로부터 기업을 보호할 수 있도록 전 세계의 트래픽을 스캔하며 3~5분마다 Cisco Email Security 솔루션을 업데이트합니다.
- **안티 스팸:** 스팸이 받은 편지함에 전송되지 않도록 하기 위해 발신자 평판을 기준으로 하는 외부 필터링 레이어가 결합된 멀티레이어 방어 기능이 제공됩니다. 또한 메시지 심층 분석을 수행하는 내부 필터링 레이어도 실행됩니다. 평판 필터링을 통해 80% 이상의 스팸이 회사의 네트워크에 도달하기도 전에 차단됩니다. 이로 인해 99.999%가 넘는 업계 최고의 스팸 차단율이 제공되며, 오탐률은 메시지 1백만 건당 1건 미만입니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

- **그레이메일 탐지:** 그레이메일은 마케팅, 소셜 네트워킹, 벌크 메시지로 구성됩니다. 그레이메일 탐지 기능은 조직에 유입되는 이메일을 정확하게 분류하고 모니터링합니다. 이를 토대로 관리자는 각 카테고리의 그레이메일에 대한 적절한 조치를 취할 수 있습니다.
- **그레이메일 안전 수신 거부:** 이 기능은 안전한 "수신 거부" 옵션으로 그레이메일에 태그를 지정합니다. 이 옵션은 클라우드를 사용하여 최종 사용자 대신 수신 거부 요청을 안전하게 처리합니다. 또한 여러 가지 다른 그레이메일 수신 거부 요청도 모니터링합니다. 이러한 모든 요청을 LDAP 그룹 레벨의 정책에서 관리할 수 있습니다.
- **안티바이러스:** Sophos 또는 McAfee 안티바이러스 엔진 중 하나를 유동적으로 구축할 수 있습니다. 이러한 엔진을 동시에 실행할 수도 있으므로 추가적인 안티바이러스 보호를 위한 레이어 방식을 사용할 수 있습니다.
- **Outbreak 필터:** Outbreak 필터는 새로운 위협 및 복합적인 공격으로부터 방어합니다. 이러한 필터는 파일 유형, 파일 이름, 파일 크기, 메시지의 URL을 포함하여 6가지 파라미터의 조합에 대한 규칙을 모두 작성할 수 있습니다. Talos가 보안 침해에 대해 더 많은 정보를 입수하면 그에 따라 규칙을 수정하고 격리된 메시지를 해제할 수 있습니다. Outbreak 필터는 의심스러운 메시지에 링크된 URL을 다시 작성할 수도 있습니다. 새 URL을 클릭하면 수신자는 Cisco Web Security 프록시를 통해 리디렉션됩니다. 그런 다음 웹사이트 콘텐츠를 철저히 검사하며, Outbreak 필터는 차단 화면을 표시하여 사용자에게 사이트에 악성코드가 포함되어 있는지 알립니다.
- **웹 상호작용 추적:** 완전히 통합된 이 솔루션을 통해 IT 관리자는 Cisco Email Security에서 재작성한 URL을 클릭하는 최종 사용자를 추적할 수 있습니다. 링크를 클릭한 사용자와 해당 작업의 결과를 비롯해 악성 링크가 포함된 메시지를 추적할 수 있습니다.
- **DLP:** Cisco는 DLP 기술 분야의 선두 업체인 RSA와 협력하여 통합형 올인원 DLP 솔루션을 제공합니다**.** 이 솔루션을 사용하면 전 세계적으로 업계 및 정부 규정을 준수하고 기밀 데이터가 네트워크를 벗어나지 못하도록 방지할 수 있습니다. 이 통합 솔루션에서는 60초 내에 DLP 정책을 구현할 수 있습니다.
- **이메일 암호화:** Cisco의 암호화된 이메일은 이메일 기밀 유지 기능을 제공하므로 발신자와 수신자만 이메일을 읽을 수 있습니다. S/MIME(Secure/Multipurpose Internet Mail Extension) TLS(Transport Layer Security) 암호화 지원도 포함되어 있습니다.
- **AMP 애드온:** 이 기능을 통해 향상된 인바운드 위협 탐지 및 모니터링을 수행할 수 있습니다. 이 기능은 침입의 영향을 받는 네트워크 영역을 식별하여 신속하게 정상 작동 상태로 되돌리는 회귀 방식의 보안을 제공합니다.
  - AMP 라이센스에는 다음의 세 가지 기능이 포함됩니다.
    - 파일 평판: 파일의 모든 측면을 점검하여 보안 위험을 확인합니다.
    - 파일 분석(샌드박싱): 파일이 네트워크에 진입하기 전에 보안 공간에서 분석하여 악의적인 의도를 확인합니다.
    - 회귀 보안: 확인된 파일을 지속적으로 모니터링하여 특성이 변경되면 동적 평판 분석을 트리거하고 관리자에게 알림을 보냅니다. 또한 악성코드에 대한 상세 정보가 제공되므로 치료 우선순위를 지정할 수 있습니다.

이러한 기능 외에도 역할 기반 관리, 99.999%의 업타임, 공동 관리, 이중화를 위한 미국과 유럽의 여러 데이터 센터, 다른 고객과 함께 차단 목록에 포함되는 현상 방지를 위한 전용 IP 주소, 자금 지원 SLA 등의 추가 혜택이 제공됩니다.

Cisco는 2015년의 Gartner Magic Quadrant® for Email Gateways에서 1위 업체로 선정되었습니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Cisco Talos(Talos Security Intelligence and Research Group)

Email Security는 Cisco의 포괄적인 네트워크 보안 제품 및 서비스 제품군의 일부입니다. 단일 벤더에서 제공하는 업계 최고의 제품과 서비스를 사용하는 조직은 위협을 보다 효율적으로 탐지하고 대응할 수 있습니다.

Email Security는 Talos를 활용합니다. Talos는 전 세계 기업 이메일 트래픽의 35%, 75TB의 일별 웹 데이터, 130억 개의 웹 요청, 160만 개의 구축된 서비스 및 1억 5천만 개 이상의 엔드포인트를 감시하고 있습니다. Cisco 제품에 통합되어 있는 Cisco Web Security 및 Cisco AMP(Advanced Malware Protection) Threat Grid와 같은 솔루션의 기능은 이메일에서 악의적일 수 있는 원치 않는 URL과 첨부 파일을 처리합니다. 동급 최고의 보안 기능을 사용하고 복합적인 최신 위협을 방지하려는 조직은 이와 같은 다중 벡터 인텔리전스 솔루션을 사용해야 합니다.

Cisco Cloud Email Security와 Office 365 통합

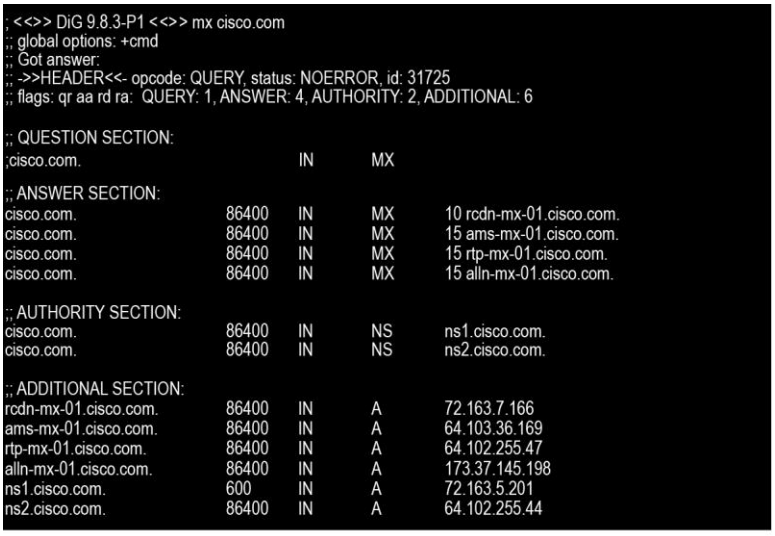
Office 365 고객의 경우에는 다행히 Microsoft에서 서드파티 시스템을 비교적 쉽게 통합했습니다. 이러한 시스템으로 이메일을 라우팅하기 위한 EOP용 스마트 호스트 커넥터 생성 기능이 상세하게 나와 있는 설명서가 제공됩니다. Microsoft Exchange 라이브러리를 참고하십시오.

스팸 필터링을 위해 Cloud Email Security로 인바운드 메일 라우팅

이메일 라우팅은 MX(mail exchange) 레코드를 사용하여 수행됩니다. 이러한 레코드는 이메일을 배달할 위치를 시스템에 알려 주는 DNS 항목입니다. MX 레코드는 IP 주소(대개 방화벽의 인바운드 NAT 변환 주소)를 가리키며, 이 IP 주소는 수신(SMTP) 연결을 수락합니다. MX 레코드는 대개 MTA(메시지 전송 에이전트)를 가리킵니다. MTA는 ESA, Microsoft Exchange, Lotus Notes 또는 오픈 소스 솔루션(예: Sendmail)과 같은 보안 이메일 게이트웨이일 수 있습니다.

그림 2에 나와 있는 것처럼 고객은 이중화를 위해 여러 MX 레코드가 다수의 IP 주소를 가리키도록 지정할 수 있습니다. Cisco Cloud Email Security는 데이터 센터 이중화 외에 MX 이중화도 제공하기 위해 고객에게 MX 레코드 2개를 제공합니다.

그림 2. IP 주소의 MX 레코드



© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Acme Inc.의 사례

Acme Inc. 고객(가상 기업)이 이메일 보안을 Microsoft Office 365 및 Cisco Cloud Email Security로 마이그레이션하는 방법을 살펴보겠습니다.

현재 Acme는 내부의 이메일 시스템을 사용 중이며 모든 메시지는 자체 개발 애플리케이션을 통해 필터링됩니다. 하지만 이 애플리케이션은 Acme 직원에게 필요한 보호 레벨을 제공하지 못합니다. Acme는 직원 사서함과 이메일 보안 인프라를 모두 클라우드로 이동하기 위해 Microsoft Office 365와 Cisco Cloud Email Security를 선택했습니다.

Acme의 IT 담당자는 두 서비스를 모두 활성화했으며 사용자의 사서함이 포함된 Office 365 환경을 구성했습니다. Acme의 현재 MX 레코드는 mail.acme.com을 가리킵니다. Cloud Email Security 환경은 이미 구성되었으며 프로덕션 트래픽에 사용할 수 있는 상태입니다. 그리고 MX 레코드 mx1.acme.iphmx.com 및 mx2.acme.iphmx.com이 생성되었습니다. 이러한 레코드는 이중화된 Cisco 데이터 센터에서 호스팅되는 Email Security Appliance를 가리킵니다. Acme와 비즈니스 파트너는 Acme 도메인에 대해 수신되는 이메일을 Office 365 서버로 라우팅하도록 Cisco 클라우드 보호를 구성했습니다. 이러한 서버에서 이메일은 최종 사용자 사서함으로 배달됩니다.

Acme의 IT 담당자가 회사 DNS(Domain Name System) MX 레코드를 mail.acme.com에서 mx1.acme.iphmx.com 및 mx2.acme.iphmx.com으로 변경합니다. 인터넷의 DNS 서버는 최대 24시간 동안 이 변경을 탐지하여 이메일을 Acme의 Cloud Email Security Appliance로 전달하기 시작합니다.

수신 메시지를 스캔하여 스팸, 바이러스, 악의적인 첨부 파일 및 악의적인 URL을 확인합니다. Office 365로 이메일을 배달하기 전에 기타 이메일 검사도 수행합니다.

Cloud Email Security로 아웃바운드 메일 라우팅

Acme의 중역은 조직 외부로 보내는 이메일이 HIPAA(Health Insurance Portability and Accountability Act) 및 Sarbanes-Oxley Act와 같은 여러 정부 규정을 준수해야 함을 명확하게 지시했습니다. 이러한 규정을 준수하기 위해 Acme의 IT 담당자는 Cisco 클라우드를 통해 아웃바운드 이메일을 라우팅합니다. Cisco 클라우드에서는 RSA DLP 모듈 및 통합 Cisco Email Encryption을 사용하여 정책이 시행됩니다.

Office 365 사서함에서 Cisco로 이메일 메시지를 라우팅하려면 EOP 시스템에서 아웃바운드 커넥터를 구성해야 합니다. 이를 위해 고객은 다음과 같은 단계를 수행할 수 있습니다.

1. EOP Admin Center(EOP 관리 센터)에서 Exchange를 선택한 다음 Mail Flow(메일 흐름)로 이동하여 Connectors(커넥터)를 클릭합니다.
2. Connectors(커넥터)에서 Outbound Connectors(아웃바운드 커넥터)를 선택하고 Add(추가)를 선택합니다.
3. 커넥터의 이름을 Outbound to Cisco Cloud로 지정합니다.
4. 수신자 도메인을 *.*로 지정합니다
5. mx1.acme.iphmx.com 및 mx2.acme.iphmx.com 대상으로 모든 메시지를 배달합니다.
6. TLS(Transport Layer Security)를 선택하고 Validation Against Self-Signed Certificate(셀프 서명 인증서 기준 검증)를 선택합니다.
7. 변경 내용을 저장합니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Cisco Cloud Email Security에서 다음 항목을 구성합니다.

1. 메일 정책/HAT 개요
2. Office 365 도메인 acme.onmicrosoft.com을 RELAYLIST 정책에 추가하고 변경 사항을 커밋합니다.

자세한 내용은 https://technet.microsoft.com/enus/library/ms.exch.eac.connectorselection%28v=exchg.150%29.aspx를 참고하십시오.

결론

Acme는 두 솔루션을 통합함으로써 Office 365에서 제공하는 호스팅된 사서함의 모든 이점과 Cisco Cloud Email Security에서 제공하는 업계 최고의 이메일 보호 기능을 모두 활용할 수 있습니다.

추가 정보

O365용 Cisco Cloud Email Security에 대한 자세한 내용을 확인하려면 http://www.cisco.com/go/cloudemail을 참고하거나 무료 Cisco Email Security를 사용해 보십시오.

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 확인하려면 www.cisco.com/go/trademarks로 이동하십시오. 언급된 타사 상표는 해당 소유주의 재산입니다. "파트너"라는 용어는 Cisco와 기타 회사 간의 파트너 관계를 의미하지는 않습니다. (1110R)

Printed in USA C11-727691-01 07/15

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.