Symantec™ Email Security.cloud

서비스 설명

2019년 3월

본 서비스 설명은 시만텍의 Email Security.cloud(“서비스”)를 대상으로 합니다. 이 설명에서 대문자로 표시된 모든 용어는 계약(아래 정의됨) 또는 정의 섹션에 부여된 의미를 가집니다.

본 서비스 설명은 참조로 포함된 첨부 파일과 함께 서비스 사용을 통제하는, 고객이 직접 서명 또는 디지털 서명한 시만텍과 계약(서명 계약이 없는 경우 시만텍 온라인 서비스 사용 약관)(이하 “계약” 이라 칭함)의 일부이거나 해당 계약에 통합됩니다.

목차

Symantec™ Email Security.cloud

서비스 설명

2019년 3월

1: 기술/비즈니스 기능

서비스 개요

Symantec™ Email Security.cloud는 이메일 메시지를 필터링하고 멀웨어(표적 공격, 피싱 포함), 스팸, 원치 않는 대량 이메일로부터 기업을 보호하는 호스팅 서비스입니다. 이 서비스는 암호화 및 데이터 보호 옵션을 제공하여 이메일을 통해 전송되는 중요 정보를 제어할 수 있게 합니다. 또한 다양한 벤더의 각종 편지함 유형을 지원합니다.

서비스 기능

- 고객 관리자는 안전한 암호로 보호되는 로그인을 통해 서비스 관리 콘솔에 액세스할 수 있습니다. 관리 콘솔은 고객이 서비스를 구성하고 관리하며 리포트에 액세스하고 서비스의 일부로 사용 가능한 데이터와 통계를 볼 수 있는 기능을 제공합니다.
- 서비스는 24시간 연중무휴 관리되며 하드웨어 가용성, 서비스 용량, 네트워크 리소스 사용률에 대한 모니터링이 수행됩니다. 서비스는 정기적인 모니터링을 통해 서비스 수준을 준수하는지 확인하고 필요에 따라 조정합니다.
- 서비스에 대한 보고는 관리 콘솔을 통해 가능합니다. 보고에는 작업 로그 및/또는 통계가 포함될 수 있습니다. 고객은 관리 콘솔을 사용하여 리포트 생성을 선택할 수 있습니다. 이렇게 생성된 리포트는 정기적으로 이메일이 전송되도록 구성하거나 관리 콘솔에서 다운로드할 수 있습니다.
- 이 서비스는 고객이 적합하고 실행 가능한 시스템 사용 정책 또는 그에 상응하는 것을 구현할 수 있도록 지원합니다.
- 시만텍에서 제공하는 추천어 목록, 템플릿 규칙이나 정책에 부적절한 단어가 포함될 수도 있습니다.
- 어떤 이유로든 서비스가 일시 정지 또는 종료된 경우 시만텍은 서비스 프로비전 중에 변경된 모든 구성을 되돌릴 수 있습니다. 서비스가 복구될 때 필요한 다른 모든 구성 변경을 수행하는 것은 고객의 책임입니다.

서비스 옵션 및 기능

이 서비스는 Email Protect 또는 Email Safeguard 2가지 옵션으로 제공됩니다. 서비스는 (본 서비스 설명에 기술된 모든 제한 사항에 따라) 선택된 옵션 또는 애드온 사용자 각각에 대해 구매해야 합니다.

서비스 옵션별 기능

	Email Protect	Email Safeguard
이메일 멀웨어 차단: 피싱 및 표적 공격 방어를 포함한 멀웨어 차단	✓	✓
이메일 스팸 차단: 스팸 및 피싱 차단(실시간 링크 추적), 대량 메일 차단	✓	✓

Email Data Protection: 커스터마이즈 가능한 컨텐트 필터링 정책 제어		✓
이메일 이미지 제어: 부적절한 이미지 탐지		✓
아웃바운드 필터링	✓	✓
강제 TLS 암호화		✓
기회주의적 TLS 암호화	✓	✓
주소 등록: 잘못된 수신자 처리	✓	✓
사용자 및 그룹 LDAP 동기화 툴	✓	✓
메시지 추적	✓	✓
리포팅 대시보드	✓	✓
요약(PDF) 및 상세(CSV) 리포팅	✓	✓
엔드유저 스팸 검역소 포털 및 알림	✓	✓
면책 조항 관리	✓	✓
Policy Based Encryption Essentials		✓
이메일 가장 제어		✓

개별 서비스 기능에 대한 자세한 내용은 온라인 도움말(http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=KO_KR)을 참조하십시오.

서비스 애드온

	Email Protect	Email Safeguard
Advanced Threat Protection: 이메일	사용 가능	사용 가능
Policy Based Encryption Advanced	–	사용 가능
Email Fraud Protection	사용 가능	사용 가능

Symantec™ Email Security.cloud

서비스 설명

2019년 3월

Email Threat Isolation	사용 가능	사용 가능

개별 서비스 애드온에 대한 자세한 내용은 온라인 도움말(http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=KO_KR)을 참조하십시오. Email Fraud Protection 관련 서비스 설명을 다음 위치에서 확인할 수 있습니다. https://www.symantec.com/about/legal/repository.

Advanced Threat Protection: Email은 Symantec Cynic™ 샌드박스로 이메일에 의해 유포되는 지능형 보안 위협을 탐지하고 수신 조직 또는 사용자를 노리는 표적 이메일 공격을 식별하며 Symantec Click-time™ URL 보호로 이메일 전달 후 악성으로 변하는 URL을 식별합니다. O365 고객용 Cynic™ 샌드박스를 통해 전달 후 악성으로 식별된 이메일을 풀백할 수 있습니다. 또한 고객이 침해 지표를 기반으로 이메일을 차단 목록에 추가하여 이메일 공격을 교정할 수 있도록 도움을 줍니다. URL 정보, 멀웨어 카테고리, 탐지 방법, 파일 해시를 포함하여 멀웨어에 대한 세부적인 보고를 제공합니다. 데이터 피드 API가 포함되어 있어 파일을 가져오거나 이메일로 데이터를 보내지 않고도 인증된 URL을 통해 멀웨어 보고를 활성화할 수 있습니다. Advanced Threat Protection: 이메일은 Phishing Readiness 서비스에 대한 액세스도 제공합니다. 이 서비스는 개인이 피싱 공격에 대한 민감도를 확인하는 데 사용되는 피싱 공격 시뮬레이터입니다. Phishing Readiness 서비스 사용에는 https://www.symantec.com/about/legal/repository의 이용 약관이 적용됩니다.

Policy Based Encryption Advanced는 (i) 풀(Pull) 웹 픽업 포털, (ii) PGP 및 S/MIME 전달 지원, (iii) 투명성이 더 낮은 암호화 기술로 변경하기 전 TLS 암호화 시도 기능, (iv) 암호화된 .pdf 푸시 전달(Email Safeguard 계획의 Policy Based Encryption Essentials 기능의 일부분으로 제공되는 유일한 암호화 방식) 기능을 제공합니다. Policy Based Encryption Advanced는 발신 사용자 단위로 라이센스를 제공하는데, 이러한 발신 사용자 수는 Email Safeguard 옵션의 전체 사용자 수보다 적거나 같습니다. 고객이 안전한 명세서 전달을 위해 Policy Based Encryption Advanced 옵션을 사용해야 할 경우 전달할 명세서 수를 기준으로 시만텍이 정의한 공식에 따라 추가 사용자 라이센스 구매가 가능할 수 있습니다.

Symantec™ Email Fraud Protection은 DMARC(도메인 기반 메시지 인증, 보고 및 적합성)를 자동화하는 클라우드 서비스입니다. Symantec Email Fraud Protection은 수동 방법에 비해 DMARC 시행에 대한 모든 단계를 보다 간편하고 원활하게 합니다. 시행하면 인증되지 않은 출처에서 온 모든 이메일이 검역소에 보관되거나 거부되므로 인바운드 가장 공격의 위험이 줄어듭니다. 일단 시행이 되면 이메일 수신인 또는 메일 전송 에이전트는 고객의 도메인을 신뢰하고 이메일 전달률을 높일 수 있다는 사실을 알게 됩니다.

Symantec™ Email Threat Isolation은 악성 링크를 격리하고 위험한 웹 페이지를 안전하게 렌더링하여 스피어 피싱, 인증 정보 도용 및 고급 이메일 공격에 대비한 보호 기능을 강화합니다. 시만텍은 Email Threat Isolation을 통해 고급 스피어 피싱 또는 인증 정보 도용 공격과 같이 악성 링크를 이용하는 정교한 이메일 위협에 대비하여 한층 강화된 보호 기능을 제공합니다.

Email Threat Isolation은 웹 세션을 원격으로 실행하고 사용자의 브라우저에 안전한 렌더링 정보만 보내는 방식으로 사용자와 해당 이메일 링크 또는 첨부 파일 간에 안전한 실행 환경을 구축합니다. . 결과적으로 시만텍은 악성 링크 및 첨부 파일이 포함된 위협 요소가 사용자에게 도달하지 못하게 합니다. 또한 Email Threat Isolation은 피싱 웹 사이트를 읽기 전용 모드에서 렌더링하여 사용자가 회사 인증 정보 및 기타 중요 정보를 입력하는 것을 방지함으로써 인증 정보 피싱 공격을 차단합니다.

서비스 수준 계약

- 시만텍은 별첨 A에 명시된 대로 서비스에 대해 적용 가능한 서비스 수준 계약(“SLA”)을 제공합니다.

지원되는 플랫폼 및 기술 요구 사항

- 서비스에 대한 지원되는 플랫폼 및 기술 요구 사항은 http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=KO_KR에 제공되어 있습니다.

호스팅 서비스 소프트웨어 구성 요소

- 이 서비스에는 관리 콘솔에서 제공되는 소프트웨어 서비스 구성 요소가 포함되며, 해당 요금을 결제하면 이용할 수 있습니다.

2: 고객의 책임

시만텍은 고객이 필요한 정보를 제공하거나 필요한 조치를 수행하는 경우에만 서비스를 수행할 수 있습니다. 그렇지 않은 경우 아래에 명시된 대로 시만텍의 서비스 성능이 지연되거나 장애가 발생하거나 금지될 수 있으며 서비스 수준 계약 수혜 자격이 무효화될 수도 있습니다.

- 설정 지원: 고객은 시만텍이 서비스 수행을 시작할 수 있도록 필요한 정보를 제공해야 합니다.
- 지정 고객 담당자: 고객은 시만텍의 합당한 요청이 있을 경우 시만텍의 서비스 수행을 지원할 적임자를 제공해야 합니다.
- 고객은 계정 정보, 암호 또는 기타 로그인 인증 정보에 대한 책임이 있습니다.
- 고객은 인증 정보를 보호하기 위해 합당한 방법을 사용하는 것에 동의하며 고객 계정이 무단으로 사용된 것을 알게 되면 즉시 그 사실을 시만텍에 통지할 것입니다.
- 갱신 인증 정보: 해당되는 경우 고객은 서비스를 계속 받거나 서비스 약관에 제공되는 계정 정보 및 고객 데이터를 유지 관리할 목적으로 계정 관리에서 제품 정보 사용 기간 안내(Subscription Instrument) 또는 주문 확인(Order Confirmation)을 통해 제공되는 갱신 인증 정보를 적용해야 합니다.
- 고객 구성 및 기본 설정 비교: 고객은 해당되는 경우 관리 콘솔을 통해 서비스 기능을 구성해야 합니다. 그렇지 않으면 기본 설정이 적용됩니다. 기본 설정이 없어서 고객이 설정을 선택할 때까지 서비스가 제공되지 않는 경우도 발생할 수 있습니다. 서비스 구성 및 사용은 전적으로 고객이 제어합니다. 즉 시만텍은 고객의 서비스 사용에 대해 책임지지 않으며 서비스 운영의 결과로 고객에게 발생할 수 있는 민형사상 책임과 무관합니다.

사용 제한 정책

- 고객은 시만텍 온라인 서비스 사용 제한 정책을 준수할 책임이 있습니다.

3: 자격 및 제품 정보 사용 기간 정보

요금 부과 메트릭

서비스는 주문 확인서에 명시된 다음 단위에 따라 제공됩니다.

- “**사용자**”는 서비스를 이용하거나 그 이용에 따른 혜택을 받도록 허가 받은 또는 실제로 서비스의 일부를 사용하는 개인이나 장치를 의미합니다.

제품 정보 사용 기간에 대한 변경

고객이 시만텍으로부터 직접 제품 정보 사용 기간 또는 자격을 얻은 경우 고객의 제품 정보 사용 기간 또는 자격에 대한 허용된 변경 사항이 있으면 고객과 시만텍의 계약에 별도로 명시되지 않는 한 CLD_cancellations_MLABS@symantec.com(또는 시만텍에서 게시한 대체 주소)으로 이를 알려야 합니다. 위 절차에 따라 제공된 고지는 수령 시 제공된 것으로 간주됩니다. 고객이 시만텍 리셀러를 통해 제품 정보 사용 기간 또는 자격을 얻은 경우 고객의 리셀러에게 문의하십시오.

4: 지원 및 기술 지원

참고: 이 조항은 시만텍으로부터 직접 고객 지원(“지원”)을 받을 자격이 있는 고객에게만 적용됩니다. 고객이 시만텍 대리점으로부터 지원을 받을 자격이 있는 경우 해당 지원에 대한 자세한 내용은 해당 대리점과 고객의 계약을 참조해야 하며, 여기에 설명된 지원은 고객에게 적용되지 않습니다.

고객 지원

시만텍은 현지 영업 시간 중에 서비스의 일부로 다음 지원 서비스를 제공합니다.

- 서비스 이행에 대한 주문 접수 및 처리
- 서비스의 기능에 대한 허가된 수정 요청 접수 및 처리
- 청구 및 송장 관련 문의에 응답

기술 지원

아래에 명시된 것과 같이 서비스에는 기본 수준의 지원이 포함됩니다.

- 지원은 서비스 기능 구성 및 서비스와 관련하여 보고된 문제와 관련하여 고객을 돕기 위해 24x7 연중무휴로 제공됩니다. 서비스에 대한 지원은 https://support.symantec.com/ko_KR/article.TECH236428.html에 게시된 약관 및 기술 지원 정책에 따라 수행됩니다.
- 고객의 지원 제출에 심각도 수준이 할당되면 시만텍은 아래의 표에 정의된 응답 목표에 따라 최선의 노력을 다해 응답합니다. 고객의 조치로 인해 또는 다른 서비스 제공자의 조치가 필요하여 장애가 발생한 경우는 시만텍의 통제 범위를 벗어나며 이 지원 약정에서 명시적으로 제외됩니다.

문제 심각도	**24x7 연중무휴 지원 응답 목표***
심각도 1: 다음 상황 중 하나에서 즉각적인 해결 방법을 사용할 수 없는 문제가 발생한 경우: (i) 고객의 프로덕션 서버 또는 기타 미션 크리티컬 시스템이 중단되거나 심각한 서비스 손실이 발생한 경우, 또는 (ii) 고객의 미션 크리티컬 데이터의 상당 부분이 심각한 손실 또는 손상 위험에 처한 경우	30분 내

심각도 2: 주요 기능이 심각하게 손상되는 문제가 발생한 경우 장기적인 생산성에 부정적인 영향이 있더라도 고객이 제한된 방식으로 영업을 계속할 수 있는 경우	2시간 내
심각도 3: 고객의 영업에 제한된 부작용을 미치는 문제가 발생한 경우	영업일 기준 익일 동일 시간까지**
심각도 4: 고객의 영업에 부작용을 미치는 문제가 발생한 경우	영업일 기준 익일 이내. 시만텍은 고객이 새로운 기능 또는 개선 사항에 대한 고객 제안을 시만텍 포럼에 제출해줄 것을 권장합니다.

위의 지원 응답 목표는 정상적인 서비스 운영 중에 달성 가능하며 아래의 유지 보수 조항에 설명된 것과 같이 서비스 및/또는 지원 인프라에 대한 유지 보수 중에는 적용되지 않습니다.

** 목표 응답 시간은 해결 시간(요청을 종결하는 데 소요되는 시간)이 아닌 요청에 대한 응답 시간과 관련됩니다.*

*** "영업일"은 고객의 현지 표준 시간대를 기준으로 각 지역의 영업 시간 및 요일을 의미하며 주말과 현지 공휴일은 제외됩니다. 대부분의 경우 "영업 시간"은 고객의 현지 표준 시간대를 기준으로 오전 9:00 ~ 오후 5:00 입니다.*

서비스 및/또는 지원 서비스 인프라에 대한 유지 보수

시만텍은 수시로 유지 보수를 수행해야 합니다. 시만텍은 중단을 최소화하기 위해 집합적으로 고객 작업이 적은 시간에 일상적인 유지 보수를 수행하도록 상업적으로 타당한 노력을 기울입니다. 고객은 이러한 일상적인 유지 보수 작업에 대한 사전 통지를 받지 않습니다. 기타 모든 유형의 유지 보수의 경우 아래에 나열된 바와 같이 시만텍은 시만텍 상태 페이지(https://status.symantec.com/)에 경고를 게시하여 사전에 영향을 받은 당사자에게 알리려고 노력합니다. 서비스 상태, 계획된 유지 보수 및 알려진 문제에 대한 자세한 내용을 보려면 시만텍 상태 페이지를 방문하고 Symantec Email Security.cloud 페이지를 구독하여 최신 업데이트를 받으십시오. **보안 검사 및 이메일 전송과 같은 핵심 서비스 기능은 모든 유지 보수 작업 중에 중단되지 않습니다.**

- ***계획된 유지 보수:*** 계획된 유지 보수는 서비스 인프라의 가용성 중지로 인해 서비스가 중단 또는 차단될 수 있는 예약된 유지 보수 기간을 의미합니다. 시만텍은 해당 인프라가 있는 지역의 표준 시간대에서 집합적으로 고객 작업이 적은 시간에 네트워크 전체가 아닌 일부에서만 계획된 유지 보수를 수행하기 위해 최선을 다합니다. 계획된 유지 보수 중에 서비스 중단을 방지할 수 있도록 유지 보수가 진행되지 않는 인프라 일부로 서비스가 전환될 수 있습니다. 시만텍은 계획된 유지 보수가 있을 때 7일 전부터 시만텍 상태 페이지에 고객 대상 통지를 게시하도록 상업적으로 타당한 노력을 기울입니다. 고객은 시만텍 상태 페이지를 구독하여 SMS, 이메일 또는 Twitter를 통해 통지를 받을 수도 있습니다.
- ***계획되지 않은 유지 보수:*** 계획되지 않은 유지 보수는 서비스 인프라의 가용성 중지로 인해 서비스가 중단 또는 차단될 수 있는 예약된 유지 보수 기간을 의미하며, 표준 7일 통지가 가능하지 않을 수 있습니다. 시만텍은 상업적으로 타당한 노력을 기울여 고객에게 최소 하루(1일) 전에 알릴 수 있도록 시만텍 상태 페이지에 통지를 게시합니다. 계획되지 않은 유지 보수 중에 서비스 중단을 방지할 수 있도록 유지 보수가 진행되지 않는 인프라 일부로 서비스가 전환될 수 있습니다. 경우에 따라 시만텍은 비상 유지 보수를 수행합니다. 비상 유지 보수는 *주요 인시던트를 해결하거나 예방하기 위해 최대한 빨리 구현되어야* 하는 유지 보수로

정의됩니다. 시만텍은 유지 보수를 시작하기 최소 1시간 전부터 시만텍 상태 페이지에 알림을 게시하는 방법으로 영향을 받는 당사자에게 이 사실을 알리기 위해 노력합니다.

- ***관리 콘솔 유지 보수:*** 시만텍은 관리 콘솔 유지 보수가 있을 때 14일 전부터 시만텍 상태 페이지에 고객 대상 통지를 게시하도록 상업적으로 타당한 노력을 기울입니다. 시만텍은 관리 콘솔 가용성의 중단을 최소화할 목적으로 집합적으로 고객 활동량이 적은 시점에 관리 콘솔에 대한 유지 보수를 수행하기 위해 노력합니다. 경우에 따라 시만텍은 관리 콘솔에 대한 사소한 업데이트를 수행할 수 있으며 고객은 이러한 일상적인 유지 보수 작업에 대한 사전 통지를 받지 않습니다.

5: 추가 약관

- 이 서비스는 전 세계적으로 해당 시점의 시만텍 기준에 따라, 관련 수출 제한 및 기술 제한 규정에 의거하여 액세스하거나 이용할 수 있습니다.
- 시만텍은 서비스의 핵심 기능을 실질적으로 축소하지 않는 한 동등하거나 향상된 서비스를 제공할 목적으로 서비스의 기능을 수정 및 업데이트할 권리가 있습니다. 고객은 시만텍이 제공되는 서비스를 정확히 반영하기 위해 제품 정보 사용 기간 중 언제든지 본 서비스 설명을 업데이트할 권한을 보유하고 있으며 업데이트된 서비스 설명은 게시와 함께 효력을 발생한다는 것을 인정하고 이에 동의합니다.
- 소프트웨어 형태로 서비스 구성 요소를 이용할 경우 해당 소프트웨어의 라이센스 계약이 적용됩니다. 서비스 구성 요소에 대한 EULA가 없을 경우 http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf에 명시된 약관이 적용됩니다. 그러한 서비스 구성 요소의 이용에 관한 추가적인 권리 및 의무는 이 서비스 설명에 명시된 바를 따라야 합니다.
- 서비스 설명에 달리 명시되지 않는 한, 서비스(서비스와 함께 제공되는 호스팅 서비스 소프트웨어 구성 요소 포함)에서 별도의 라이센스가 적용되는 오픈 소스 및 타사 자료를 사용할 수 있습니다.
- 시만텍은 서비스의 실효성을 유지하기 위해 언제든지 서비스를 업데이트할 수 있습니다.
- 시만텍이 제공하는 모든 템플릿은 고객이 자신의 사용자 정의 정책 및 기타 템플릿을 생성하는 지침으로만 사용됩니다.
- 서비스에는 아래와 같은 한도가 적용됩니다.
    - 사용자당 월 기준 인바운드 및 아웃바운드 메시지 = 10,000건. 이러한 한도에는 고객에게 전송된 스팸 및 멀웨어가 포함되지 않습니다.
    - 시만텍은 사용량이 서비스 계약의 메시지 한도를 초과할 경우 고객에게 통지하고 나머지 기간(월)과 추가 사용자에 대한 요금을 청구할 수 있습니다.
    - 인바운드 및 아웃바운드 메일 재시도 일정 = 7일.
    - 기본 최대 이메일 크기 = 50MB. 고객은 1,000MB 한도에서 최대 이메일 크기를 지정할 수 있습니다. 서비스에서 지정된 한도를 초과하는 이메일을 수신할 경우 해당 이메일을 차단하고 삭제한 후 발신자, 수신 예정자, 관리자에게 이를 알리는 이메일을 보냅니다.
    - 메시지 추적 = 이 데이터는 30일간 문제 해결 검색을 위해 사용할 수 있습니다. 여기에는 단일 검색에서 반환할 수 있는 결과 수에 대한 한도가 추가로 적용됩니다.
    - 멀웨어 검역소 = 30일 후 이메일이 자동으로 삭제됩니다.
    - 스팸 검역소 = 달리 구성되지 않는 한 14일 후 이메일이 자동으로 삭제됩니다.

  - 대시보드 보고 데이터 제공 기간 = 상세 정보의 경우 40일, 요약 정보의 경우 12개월.
  - 요약(PDF) 보고 데이터 제공 기간 = 12개월.
  - 상세(CSV) 보고 데이터 제공 기간 = 40일.

- Policy Based Encryption에는 아래와 같은 한도가 적용됩니다.
  - Policy Based Encryption(Z) 사용자당 월 기준 아웃바운드 이메일 = 300건.
  - Policy Based Encryption Essentials/Advanced 사용자당 월 기준 아웃바운드 이메일 = 480건.
  - 여러 수신자에게 보낼 경우 각각의 고유한 주소가 보안 이메일 1개로 계산됩니다. 고객이 임의의 월에 허용된 보안 이메일 수를 초과할 경우 시만텍은 실제 사용량에 대해 고객에게 청구할 수 있습니다.
  - Policy Based Encryption 서비스를 통해 라우팅되는 이메일의 최대 크기는 50MB입니다.
  - Policy Based Encryption(Z) 서비스에서 Pull 암호화를 사용할 경우 이메일은 기본적으로 90일간 보안 픽업 포털에 저장된 후에 만료됩니다.
  - Policy Based Encryption Advanced 서비스에서 Pull 암호화를 사용할 경우 이메일은 기본적으로 30일간 보안 픽업 포털에 저장된 후에 만료됩니다.
  - 가용성 및 대기 시간 서비스 수준은 이 서비스에 적용되지 않습니다.

- 전송 중 모든 지점에서 메시지를 보호하기 위해 고객이 Policy Based Encryption에 사용할 도메인을 구성하여 서비스 인프라를 통해 주고받는 모든 아웃바운드 및 인바운드 메시지에 TLS 암호화를 강제적으로 적용하는 것이 좋습니다.
- 고객은 시만텍이 제공한 라우팅 정보를 사용하여 시만텍을 통해 인바운드 이메일을 라우팅해야 하며 특정 타워 또는 IP 주소로 이메일을 라우팅해서는 안 됩니다.
- 이 서비스는 자체 이메일 도메인 이름이 있고 해당 도메인 이름에 대해 MX 레코드 또는 DNS를 구성할 수 있는 고객만 이용할 수 있습니다.
- 고객은 인프라의 일부를 사용하지 못하는 상황에 서비스의 연속성을 보장할 수 있도록 모든 필수 IP 범위에서 전송되는 인바운드 이메일을 수락해야 합니다.
- 고객이 해당 조직에 인바운드 이메일을 전달하려면 메일 서버 IP 주소 또는 호스트 이름을 지정해야 합니다.
- 고객은 서비스를 필요로 하는 모든 도메인(하위 도메인 포함)이 프로비저닝되었는지 확인해야 합니다. 고객은 프로비저닝되지 않은 도메인에 대해서는 서비스 기능이 올바르게 작동하지 않고 이메일이 전달되지 않을 수 있음을 인정합니다. 고객은 서비스를 받을 유효한 이메일 주소의 목록("유효성 검사 목록")을 제공하고 관리하는 데 동의합니다. 서비스 제공 전과 서비스 기간 동안 유효성 검사 목록을 확인하는 것은 고객의 책임입니다. 유효성 검사 목록에 없거나 잘못 입력된 이메일 주소로 전송된 이메일은 서비스에 의해 거부됩니다. 고객은 잘못된 주소로 전송된 이메일에 SLA가 적용되지 않음을 인정합니다. 확실을 기하기 위해 스팸 검역소 시스템 사용 고객은 유효성 검사 목록을 관리하고 주소 등록 기능을 사용하도록 설정해야 합니다. 고객이 그러한 유효성 검사 목록을 제공하지 못하고 주소 등록 기능의 실행 중지를 요청할 경우 시만텍은 개별적으로 그러한 요청을 검토하고 시만텍 단독의 재량에 따라 요청을 거부할 권리를 갖습니다.

- 고객은 멀웨어 또는 스팸을 포함한 것으로 분류된 이메일을 해제하거나 시만텍이 고객의 도메인에서 그러한 이메일을 해제하도록 요청할 수 있습니다. 고객은 시만텍이 고객의 요청에 따라 그러한 이메일을 해제하는 것과 관련하여 어떠한 책임도 지지 않는다는 데 동의합니다.
- 시만텍은 서비스에서 스팸을 식별하지 못해 직간접적으로 발생한 피해나 손실에 대해 또는 어떤 이메일을 멀웨어나 스팸으로 잘못 식별하는 것에 대해 책임지지 않습니다. 시만텍은 모든 아웃바운드 이메일을 검사할 권리를 가집니다.
- 기본 면책 조항 메시지는 서비스를 프로비저닝하는 시점부터 서비스에서 검사를 수행하고 고객이 관리 콘솔을 통해 해당 텍스트를 편집할 수 있는 이메일에 적용됩니다. 시만텍은 언제든지 기본 면책 조항 메시지를 업데이트할 권리가 있습니다.
- 고객은 서비스 사용과 관련하여 해당하는 모든 법률을 준수해야 합니다. 특정 국가에서는 개인의 동의를 얻어야 할 수 있습니다. 서비스 구성 및 사용은 전적으로 고객이 제어합니다. 따라서 시만텍은 고객의 서비스 사용에 대해 책임지지 않으며 서비스 운영의 결과로 고객에게 발생할 수 있는 민형사상 책임과 무관합니다.
- 고객에 대한 지속적인 서비스 제공이 고객의 도메인을 겨냥하거나 고객의 도메인으로부터 발생하는 해킹 시도, 서비스 거부 공격, 메일 폭탄, 기타 악성 활동 등 서비스의 보안 기능 저해로 이어질 경우 고객은 시만텍이 잠정적으로 고객에 대한 서비스를 중지할 수 있다는 데 동의합니다. 그러한 경우 시만텍은 즉시 고객에게 알리고 고객과 함께 문제를 해결할 것입니다. 시만텍은 보안 위협 요소를 제거하는 즉시 서비스를 재개합니다.
- 어떤 이유로든 서비스가 일시 중지될 경우 서비스는 더 이상 고객의 이메일에 적용되지 않으며 이메일이 시만텍의 인프라를 통해 라우팅되지 않습니다. 고객은 일시 중지 기간에 이메일을 리디렉션하고 서비스가 재개될 경우 모든 구성의 정확성을 확인할 책임이 있습니다.
- 어떤 이유로든 서비스가 해지될 경우 고객의 계정은 삭제되고 고객은 서비스에 액세스할 수 없게 됩니다.
- 고객은 본인의 시스템이 (i) 오픈 릴레이 또는 오픈 프록시 역할을 하거나 (ii) 스팸을 전송하도록 허용해서는 안 됩니다. 시만텍은 언제든지 고객이 이 조항을 준수하는지 검토할 권리를 가집니다. 확실을 기하기 위해 본 조항의 위반은 중대한 계약 위반으로 간주되며, 시만텍은 즉시, 그리고 위반이 시정될 때까지 서비스의 전체 또는 일부를 일시 중지하거나 관련 서비스에 대한 계약을 해지할 권리를 가집니다.
- 언제든지 (i) 고객의 이메일 시스템이 블랙리스트에 오르거나 (ii) 고객의 스팸 전송으로 인해 시만텍 시스템이 블랙리스트에 오르거나 (iii) 고객이 이 서비스 설명에 명시된 의무 중 하나라도 이행하지 않을 경우 시만텍은 고객에게 그 사실을 알릴 것이며 시만텍의 자유 재량에 따라 즉시 서비스의 전체 또는 일부의 제공을 보류하거나 일시 중지하거나 해지할 권리를 가집니다.
- 고객은 오로지 본인의 비즈니스 목적을 위해서만 서비스를 이용할 수 있습니다. 고객은 서비스 및 관련 문서를 제3자에게 재판매하거나 라이센스를 재부여 또는 임대하고 그 밖의 형태로 제공하지 않는다는 데 동의합니다. 고객은 시만텍의 사전 서명 허가 없이는 경쟁 제품 또는 서비스 구축, 서비스 기능 또는 사용자 인터페이스 복사, 고객 조직 외부에 게시하기 위한 서비스 평가, 벤치마킹 또는 기타 비교 분석을 수행할 목적으로 서비스를 사용하지 않는다는 데 동의합니다.

6: 정의

"**주소 등록(Address Registration)**"은 서비스의 필수 기능으로 고객의 유효 이메일 주소 목록("유효성 검사 목록")에 포함되지 않은 이메일 주소로 전송된 인바운드 이메일을 거부합니다.

"**관리자**"는 고객을 대신하여 서비스를 관리할 수 있는 권한을 가진 고객 사용자를 의미합니다. 관리자는 고객이 지정한 대로 서비스의 일부 또는 전체를 관리할 수 있습니다.

"**스팸 차단 베스트 프랙티스 설정(AntiSpam Best Practice Settings)**"은 프로비저닝 프로세스에서 고객에게 제공되었거나 온라인 도움말 리소스에 게시된 서비스에 대해 시만텍이 권장하는 구성 지침을 의미합니다.

"**연결 관리자(Connection Manager)**"는 SMTP 핸드셰이크 단계에서 수행되는 탐지 방법을 의미합니다.

"**크레딧 요청(Credit Request)**" 은 시만텍이 다르게 통지하지 않는 경우 고객이 "Credit Request" 라는 제목 줄을 사용하여 이메일로 시만텍(support.cloud@symantec.com)에 제출해야 하는 통지를 의미합니다.

"**지정 타워 클러스터(Designated Tower Cluster)**"는 고객에게 이메일 보안 서비스를 제공하도록 지정된 둘 이상의 타워를 의미합니다.

""**도메인 레벨 설정(Domain Level Settings)**")"**은 이메일 보안 서비스의 관리 콘솔 내에서 특정 도메인에 대해 사용자 정의할 수 있는 도메인 설정을 의미합니다.**

"**이메일(Email)**"은 서비스를 통과하는 인바운드 또는 아웃바운드 SMTP 메시지를 의미합니다.

"**이메일 보안 서비스(Email Security Services)**"는 Email Safeguard와 Email Protect의 옵션 및 제공되는 애드온 서비스입니다.

"**이메일 멀웨어 오탐지(Email Malware False Positive)**"는 적법한 이메일이 멀웨어를 포함한 것으로 잘못 식별되는 것을 의미합니다.

"**최종 사용자 라이센스 계약(EULA: End User License Agreement)**"은 (아래에 정의된) 소프트웨어에 수반되는 약관을 의미합니다.

"**글로벌 설정(Global Settings)**"은 관리 콘솔에서 수행되는 작업으로 서비스의 모든 도메인 및 그룹 레벨에 적용되는 것입니다.

"**그룹 레벨 설정(Group Level Settings)**"은 해당 서비스 기능의 관리 콘솔 내에서 특정 그룹에 대해 사용자 정의할 수 있는 그룹 설정을 의미합니다.

"**인프라**"는 서비스 제공에 사용되는 시만텍 또는 라이센스 제공자의 기술과 지적 재산을 의미합니다.

"**알려진 멀웨어(Known Malware)**"는 시만텍이 구축한 바이러스 차단 기술에서 사용한 시그니처가 시만텍에서 컨텐트를 수신한 시점을 기준으로 최소한 1시간 전부터 제공된 멀웨어를 의미합니다.

"**멀웨어(Malware)**" 또는 "**악성 소프트웨어(malicious software)**"는 시스템 또는 모바일 작동을 중단시키는 데 이용되거나 적합한 승인을 받지 않고 중요 정보를 수집하거나 개인 컴퓨터 시스템에 접근하는 데 이용되는 모든 소프트웨어를 의미합니다.

"**멀웨어 오탐(Malware False Positive)**"은 적법한 이메일이 멀웨어를 포함한 것으로 잘못 식별되는 것을 의미합니다.

"**회원(Member)**"은 고객 및 고객이 이메일 경계 암호화 애드온 서비스를 활용하여 암호화 네트워크를 생성한 제3자를 의미합니다.

"**월간 요금(Monthly Charge)**"은 계약에 정의된 해당 서비스에 대한 월 단위 요금을 의미합니다.

"**온라인 도움말(Online Help)**" 은 http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=KO_KR에서 제공하는 추가 정보를 의미합니다.

"**오픈 프록시(Open Proxy)**"는 확인되지 않았거나 승인되지 않은 제3자가 서비스를 위한 DNS, 웹 페이지, 기타 데이터에 액세스하고 이를 저장하거나 전달하는 것을 허용하도록 구성된 프록시 서버를 의미합니다.

"**오픈 릴레이(Open Relay)**"는 확인되지 않았거나 승인되지 않은 제3자로부터 이메일을 수신하고 본인이 연결된 이메일 시스템의 사용자가 아닌 수신자 1명 이상에게 해당 이메일을 전달하도록 구성된 이메일 서버를 의미합니다. 오픈 릴레이는 "스팸 릴레이" 또는 "공개 릴레이"라고도 합니다.

"**주문 확인(Order Confirmation)**"은 시만텍 온라인 서비스 약관(해당되는 경우)에 정의된 의미를 갖습니다. 서비스에 대해 그러한 약관이 없을 경우 "주문 확인"은 여기에 정의된 제품 정보 사용 기간 안내를 의미합니다.

"**서비스(Service)**"는 고객이 구매한 Symantec Email Security.cloud의 Protect 또는 Safeguard 옵션을 의미합니다.

"**서비스 구성 요소**"는 시만텍에서 서비스의 부수적 요소로 별도로 제공할 수 있는 특정 지원 소프트웨어, 하드웨어 주변 기기, 관련 문서를 의미합니다.

"**서비스 크레딧(Service Credit)**"은 고객이 크레딧 요청을 제출하고 시만텍이 유효성 검사를 거쳐 고객의 크레딧 수령을 결정한 후 고객의 다음 청구서에서 크레딧으로 처리될 금액을 의미합니다.

"**서비스 소프트웨어**"는 서비스를 받기 위해 서비스에서 요구하는 대로 고객 시스템에 설치되어야 하는 소프트웨어(아래 정의)를 의미합니다. 서비스 소프트웨어에는 서비스의 일부로 시만텍이 별도로 제공할 수 있는 연관된 문서 및 소프트웨어가 포함됩니다.

"**소프트웨어(Software)**" 는 시만텍이 고객에게 사용을 허가하는 객체 코드 형식의 각 시만텍 또는 라이센스 부여자 소프트웨어 프로그램을 의미하며, 해당 EULA의 약관이 적용되고 그에 따라 제공되는 새로운 릴리스 또는 업데이트도 포함합니다.

"**스팸(Spam)**" 은 원치 않은 상업용 이메일을 의미합니다.

""스팸 미탐(Spam False Negative)")"는 서비스에서 스팸으로 식별하지 않은 스팸 이메일을 의미합니다.

""스팸 오탐(Spam False Positive)")"는 서비스에서 스팸으로 잘못 식별한 이메일을 의미합니다.

"**스팸 권장 설정(Spam Recommended Settings)**"은 프로비저닝 프로세스에서 고객에게 제공되었거나 온라인 도움말 리소스에 게시된 서비스에 대해 시만텍이 권장하는 구성 지침을 의미합니다.

"**제품 정보 사용 기간 안내(Subscription Instrument)**"는 서비스와 관련된 고객의 권리 및 의무를 추가적으로 정의하는 하나 이상의 문서를 의미하며, 여기에는 서비스에 수반되거나 선행 또는 후속 단계에 제공되는 시만텍 인증서나 이와 유사한 시만텍 발행 문서 또는 고객과 시만텍 간의 서면 계약이 포함됩니다.

"**시만텍 호스팅 서비스 약관(Symantec Hosted Service Terms)**" 은 시만텍 호스팅 서비스 약관으로, https://www.symantec.com/about/legal/service-agreements.jsp에서 확인할 수 있습니다.

"**시만텍 온라인 서비스 약관(Symantec Online Service Terms and Conditions)**"은 온라인 서비스 약관으로, https://www.symantec.com/about/legal/service-agreements.jsp에서 확인할 수 있습니다.

"**시만텍 추적기(Symantec Tracker)**"는 서비스에 대한 서비스 가용성 및 대기 시간을 측정하는 시만텍 툴을 의미합니다.

"**타워(Tower)**"는 로드 밸런싱된 이메일 서버의 클러스터를 의미합니다.

""**사용자(User)**")"는 이메일을 보내고 받는 개인을 의미하며 서비스의 일부분에 의해 보호됩니다.

별첨 A

서비스 수준 계약

일반 사항

- 시만텍이 규정된 서비스 수준을 달성하지 못할 경우 고객은 서비스 크레딧을 받을 수 있습니다. 고객이 판단하기에 서비스 크레딧을 받을 자격이 될 경우 서비스 수준 미달 의심 사례가 발생한 해당 월의 말일로부터 업무일 기준 10일 이내에 크레딧 요청을 제출해야 합니다. 고객은 로그가 일 수를 기준으로 한시적으로 보관되므로 기한을 경과하여 제출된 크레딧 요청은 무효로 간주됨을 인정합니다.
- 크레딧을 요청하려면 시만텍 기술 지원에 문의해야 합니다. 자세한 내용은 https://support.symantec.com/en_US/email-security-cloud..html.
- 모든 크레딧 요청은 시만텍이 이 서비스 수준 계약의 조항에 따라 확인합니다. 시만텍은 크레딧 요청의 유효성을 확인하기 위해 고객에게 추가 정보를 요청할 수 있습니다.
- 이 서비스 수준 계약은 (i) 계획된 유지 보수 또는 비상 유지 보수 기간 동안 불가항력이나 고객 또는 제3자의 행위 또는 누락으로 인해 서비스를 이용할 수 없는 경우, (ii) 시만텍이 계약 약관에 따라 서비스를 일시 중지한 기간 동안, (iii) 고객이 계약을 위반했을 때(고객의 지불 기한을 경과한 경우 포함), (iv) 고객이 계약에 따라 서비스를 구성하지 않았을 때, 그리고 (v) 평가 서비스 기간 동안에는 적용되지 않습니다.
- 이 SLA에 명시된 구제책은 고객이 이 서비스 수준 계약과 관련하여 계약, 불법 행위(부주의 포함), 기타 근거로 행사할 수 있는 유일한 구제책입니다.
- 이 서비스 수준 계약에서 시만텍의 매월 최대 누적 부담액은 월간 요금의 100% 또는 (고객 청구서상 통화에 따라) 1만 달러/5천 파운드/1만 유로($10,000/£5,000/€10,000) 중 더 적은 금액입니다.
- 영향을 받는 서비스가 서비스 번들의 일부로 구매된 경우 서비스 크레딧은 전체 서비스 번들이 아닌 영향을 받는 서비스를 기반으로 계산됩니다.

이메일 보안 서비스에 대한 서비스 수준 계약 예외 조항

이 서비스 수준 계약은 (i) 서비스를 거치지 않은 이메일(고객이 시만텍 인프라에서 보낸 인바운드 이메일만 수신하기 위해 적절한 조치를 취하지 않은 경우 포함) 또는 (ii) 원래 시만텍에 전송되었지만 SMTP 세션당 수신자 수가 500명을 초과하는 인바운드 또는 아웃바운드 이메일, (iii) 벌크 클러스터 타워(Bulk Cluster Tower)로 지정된 타워에서 프로비저닝된 고객, 그리고 (iv) 서비스가 프로비저닝되지 않은 고객 도메인에 대한 인바운드 또는 아웃바운드 이메일에는 적용되지 않습니다.

서비스 가용성

서비스 가용성 서비스 수준은 RFC5321에 따라 포트 25를 사용하여 고객 MTA에서 시만텍 인프라로 SMTP 세션을 설정하는 기능에 의해 정의됩니다. 서비스 가용성 서비스 수준은 관리 포털이나 스팸 검역소 시스템에 적용되지 않습니다. 이 서비스 수준은 고객이 서비스를 잘못 구성한 경우 또는 천재지변, 전쟁, 테러, 폭동, 정부 조치, 시만텍 데이터 센터의 외부에 있는 네트워크 또는 장치(고객 사이트에 있거나

고객 사이트와 시만텍 데이터 센터의 사이에 있는 경우 포함) 오류 등 예기치 못한 상황이나 시만텍이 합당하게 제어할 수 없는 원인이 발생하면 적용되지 않습니다.

임의의 월에 서비스 가용성이 100% 미만일 경우 고객은 크레딧 요청을 제출하고 월간 요금의 100% 또는 (고객 청구서에 명시된 통화에 따라) 1만 달러/5천 파운드/1만 유로($10,000/£5,000/€10,000) 중 더 적은 금액에 해당하는 백분율 크레딧에 대한 서비스 크레딧을 받을 수 있습니다.

월 단위 가용성 비율	월간 요금에 대한 백분율 크레딧
100% 미만, 99% 이상	25%
99% 미만, 98% 이상	50%
98% 미만	100%

임의의 월에 시만텍이 확인한 서비스 가용성이 98% 미만으로 떨어질 경우 고객은 해당 서비스를 해지하고 이미 결제한 요금 중 해지 시점 이후의 나머지 기간에 대해 비례 정산한 금액을 환불받을 수 있습니다.

이메일 전달

이메일 전달(Email Delivery) 서비스 수준은 시만텍이 아래 조건에 따라 고객의 수발신 이메일을 100% 전달하는 기능으로 정의됩니다.

a) 이 이메일은 시만텍에서 수신했어야 하며

b) 서비스에서 이메일을 차단하는 원인이 되는 멀웨어, 스팸 또는 기타 컨텐트가 이메일에 포함되어서는 안 됩니다.

위 조건에 따라 시만텍이 고객의 수발신 이메일을 전달하지 못할 경우 고객이 계약의 약관을 위반하지 않았으면 30일 이전에 서면으로 통지한 후 서비스를 해지할 수 있습니다.

이메일 대기 시간

이메일 대기 시간(Email Latency) 서비스 수준은 임의의 월에 고객의 지정 타워 클러스터(Designated Tower Cluster)에 속한 각 타워에서 5분 간격으로 수발신하는 이메일에 대해 시만텍 추적기에서 측정한 평균 왕복 시간이 아래의 표에 명시된 지연 시간을 초과하는지 여부로 정의됩니다. 고객이 판단하기에 대기 시간 서비스 수준에 미달한 경우 크레딧 요청을 제출하고 아래의 표에 따라 서비스 크레딧을 받을 수 있습니다.

평균 왕복 시간(초)	월간 요금에 대한 백분율 크레딧
60 초과, 90 이하	25%
90 초과, 120 이하	50%

120 초과, 180 이하	75%
180 초과	100%

아래와 같은 경우 이 대기 시간 서비스 수준이 적용되지 않습니다.

a) 고객이 시만텍에 유효성 검사 목록을 제공하지 않았고 고객에 대한 서비스 거부 공격이 발생했습니다.

b) 지연의 원인이 고객 시스템과의 메일 루프에 있습니다.

c) 고객의 기본 이메일 서버가 최초 전달 시도에서 이메일을 받지 못합니다.

스팸 오탐

스팸 오탐(Spam False Positive) 서비스 수준은 최대 스팸 오탐 캡처율을 정의합니다. 스팸 오탐 서비스 수준은 고객이 온라인 도움말 리소스에 제시된 스팸 차단 베스트 프랙티스 설정을 구현한 경우에만 적용됩니다. 평균 스팸 오탐 캡처율이 임의의 월에 고객 인바운드 이메일 트래픽의 0.0003%를 초과할 경우 고객은 크레딧 요청을 제출하고 아래의 표에 따라 서비스 크레딧을 받을 수 있습니다.

스팸 오탐 캡처율(%)	월간 요금에 대한 백분율 크레딧
0.0003 초과, 0.003 이하	25%
0.003 초과, 0.03 이하	50%
0.03 초과, 0.3 이하	75%
0.3 초과	100%

아래 이메일은 이 서비스 수준의 스팸 오탐 이메일에 해당되지 않습니다.

a) 적법한 비즈니스 이메일이 아닌 이메일

b) 수신자가 20명을 초과하는 이메일

c) 발신자가 고객의 차단된 발송인 목록에 있는 이메일. 고객이 사용자 레벨 설정을 활성화한 경우 개별 사용자가 정의한 차단된 발송인도 해당됩니다.

d) 감염된 시스템에서 전송된 이메일

e) 제3자의 차단 목록에 있는 시스템에서 보낸 이메일

f) 아웃바운드 스팸 검사에서 차단된 이메일

고객이 서비스 크레딧을 받으려면 오탐 의심 이메일을 받은 날로부터 5일 이내에 시만텍 기술 지원에 보고해야 합니다. 시만텍은 이메일의 스팸 오탐 여부를 조사하여 확인하고 그 결과를 기록합니다.

스팸 캡처율

스팸 캡처율(Spam Capture Rate) 서비스 수준은 최소 스팸 캡처율을 정의합니다. 이 서비스 수준은 고객이 온라인 도움말 리소스에 제시된 스팸 차단 베스트 프랙티스 설정을 구현한 경우에만 적용됩니다. 이 서비스 수준은 해당 월에 측정된 스팸 미탐지(Spam False Negative) 수를 가리킵니다. 고객은 아래의 표에 따라 크레딧 요청을 제출하고 서비스 크레딧을 받을 수 있습니다.

스팸 캡처율(%)	월간 요금에 대한 백분율 크레딧
98 초과, 99 이하	25%
97 초과, 98 이하	50%
96 초과, 97 이하	75%
96 미만	100%

이 스팸 캡처율 서비스 수준은 이메일이 유효한 이메일 주소로 전송되지 않은 경우 적용되지 않습니다. 더블바이트 문자 집합이 50%를 초과하는 이메일에는 더 낮은 95%의 스팸 캡처율이 적용됩니다. 스팸 캡처율이 95% 미만으로 떨어질 경우 고객은 월간 요금의 25%에 해당하는 서비스 크레딧을 받을 수 있습니다. 스팸 캡처율이 90% 미만으로 떨어질 경우 고객은 월간 요금의 100%에 해당하는 서비스 크레딧을 받을 수 있습니다.

고객이 서비스 크레딧을 받으려면 미탐지 의심 이메일을 받은 날로부터 5일 이내에 시만텍 기술 지원에 보고해야 합니다. 시만텍은 이메일의 스팸 미탐지 여부를 조사하여 확인하고 그 결과를 기록합니다.

멀웨어 차단

고객 시스템이 클라우드 검사 서비스를 통과하여 전달된 이메일에 의해 알려진 멀웨어 또는 미확인 멀웨어에 감염될 경우 고객은 아래에 정의된 금액의 서비스 크레딧을 받을 수 있습니다. 고객은 그러한 멀웨어에 대해 알게 된 날로부터 5일 이내에 시만텍에 알려야 하며, 시만텍은 그러한 알림을 로그에 기록하고 조사 및 검증을 실시해야 합니다. 고객은 크레딧 요청을 제출해야 하며, 유효성 검사를 거친 후 월간 요금의 100% 또는 (고객 청구서상 통화에 따라) 1만 달러/5천 파운드/1만 유로($10,000/£5,000/€10,000) 중 더 적은 금액의 서비스 크레딧을 받습니다. 이 조항에 명시된 구제책은 고객이 서비스를 통해 고객 또는 제3자에게 유포된 멀웨어 감염과 관련하여 계약, 불법 행위(부주의 포함), 기타 근거로 행사할 수 있는 유일한 구제책입니다. 단, 이 조항에 명시된 구제책은 고의적인 직접 감염 사례에는 적용되지 않습니다.

서비스를 통과하여 수신한 이메일에 포함된 멀웨어가 고객 시스템에서 자동으로 또는 수작업에 의해 활성화된 경우 고객 시스템이 감염된 것으로 간주합니다. 시만텍이 멀웨어 첨부 파일이 있는 이메일을 탐지했으나 차단하지 않고 시만텍 상태 페이지에 업데이트를 게시하거나 그 밖의 방식으로 고객에게 알려 고객이 감염된 이메일을 찾아 삭제할 수 있도록 충분한 정보를 제공한 경우 위에 명시된 구제책이 적용되지 않습니다.

이 서비스에서는 최대한 많은 이메일과 그 첨부 파일을 검사합니다. 발신자가 직접적으로 제어하는 컨텐트가 있는 첨부 파일(예: 첨부 파일이 암호로 보호되거나 암호화된 경우 또는 암호가 이메일과 별도로 전송된 경우)은 검사하지 못할 수 있습니다. 그러한 이메일 및/또는 첨부 파일은 서비스 수준에서 제외되며 위에 명시된 구제책이 적용되지 않습니다.

멀웨어 차단 서비스 수준은 고객이 또는 고객의 요청을 받아 시만텍이 고의적으로 유포한 멀웨어에 대해서는 적용되지 않습니다.

멀웨어 차단 서비스 수준은 이 서비스 설명에 정의된 멀웨어에만 적용되며 스파이웨어, 애드웨어, 악성 컨텐트를 호스팅하는 웹 사이트의 URL 링크 또는 미확인 트로이 목마에는 적용되지 않습니다.

멀웨어 오탐지

멀웨어 오탐지(Malware False Positive) 서비스 수준은 최대 멀웨어 오탐지 캡처율을 정의합니다. 이메일 멀웨어 오탐지 캡처율이 임의의 월에 고객 이메일 트래픽의 0.0001%를 초과할 경우 고객은 크레딧 요청을 제출하고 아래의 표에 따라 서비스 크레딧을 받을 수 있습니다.

악성 코드 오탐지 캡처율(%)	월간 요금에 대한 백분율 크레딧
0.0001 초과, 0.001 이하	25%
0.001 초과, 0.01 이하	50%
0.01 초과, 0.1 이하	75%
0.1 초과	100%

24x7 기술 지원 및 장애 조치

기술 지원은 아래와 같은 목적으로 연중무휴 24시간 이용할 수 있습니다.

a) 고객에게 서비스 관련 문제에 대한 기술 지원 제공

b) 그러한 문제의 해결을 위해 고객과 소통