한눈에 보기

장점

- 이용가능한 가장 믿을 수 있는 이메일 암호화를 기반으로 모바일 사용자의 보안을 강화합니다.
- 최신 매커니즘을 사용하여 이메일 수신자를 믿을 수 있는 방식으로 인증 및 확인합니다.
- 안정적이고 사용하기 쉬운 제어 기능을 통해 이메일을 만료 및 회수하고 이메일이 언제 확인되었는지 알려줍니다.
- Apple iOS와 Google Android 스마트폰 및 태플릿에서도 구축할 수 있습니다.

Cisco Business-Class Email: 모바일 이메일 암호화

Cisco Business-Class Email이 필요한 이유

이메일은 어디에서나 사용합니다. 우리는 이를 당연시하며 사용하고 있습니다. 특히 모바일 디바이스에서의 이메일은 보안에 취약합니다. 많은 이메일 보안 기술이 있지만 기능에는 제약이 따르며 관리하기도 어렵습니다. Cisco Business-Class Email은 모바일 사용자에게 향상된 보안과 믿을 수 있는 제어 기능을 제공하며 가장 흔히 사용되는 이메일 기술과 사용자의 일상적인 이메일 이용 방식에 완전히 통합됩니다.

이메일 보안 기술에는 여러 가지 한계가 있습니다.

- 암호화되지 않은 정보가 이메일을 통해 전송될 경우 기밀을 유지하기 어렵습니다. 예를 들어 네트워크를 통해 전송되는 일반 텍스트 상태의 이메일은 가로채이기 쉽습니다.
- 이메일이 상대방에게 도착했는지, 언제 열어서 읽어 보았는지 알 수 없는 경우가 많습니다.
- 이메일 메시지를 확실하게 회수할 방법이 없습니다.
- 발신자에게는 수신자가 민감한 데이터를 포함하여 이메일을 전달하는 것을 통제할 방법이 없습니다.

iOS/Android 스마트폰 및 태블릿용 Cisco Business-Class Email은 기밀 유지, 사용자 인증 단순화, 이메일 제어 방식 강화 등을 지원하는 기능으로 이러한 기술적 한계를 해결합니다.

간편성, 유연성 및 확장성 제공

Cisco Business-Class Email에는 Cisco의 최신 클라우드 기반 암호화 키 서비스인 Cisco Registered Envelope Service가 포함되어 있습니다. CRES(Cisco Registered Envelope Service)를 통해 조직은 수신자 등록, 인증, 메시지별 암호화 키를 간편하게 관리할 수 있습니다. 암호화 및 키 관리의 복잡성이 제거되어 사용자는 보안 메시지를 비 암호화 이메일처럼 쉽게 주고 받을 수 있습니다. 이것은 조직이 추가 인프라에 투자하지 않고도 규정 준수 요구를 충족하고 지적 재산을 보호하면서 다양한 비즈니스 요구와 안전한 메시징 요구 사항을 지원할 수 있는 유연하고 확장 가능한 솔루션입니다.

Cisco Business-Class Email은 통제 방식이 강화되어 발송자가 원하는 이메일 클라이언트에서 이메일 사용자 경험을 바꿔줍니다. Cisco는 독특한 방식으로 스마트폰 및 태블릿을 지원하므로 모바일 사용자도 기업 사용자와 같은 환경에서 이용할 수 있습니다.

Cisco Business-Class Email 이용 방법

Cisco Business-Class Email은 스마트폰이나 태블릿, 데스크톱용 무료 앱으로 이용할 수 있습니다. iTunes나 Google Play 앱 스토어에서 iPhone이나 Android 폰에 다운로드하십시오. 이 애플리케이션을 이메일 앱에서 사용하려면 기업 CRES(Cisco Registered Envelope Service)가 가동되어야 합니다. CRES는 Cisco Email Security의 일부로 제공됩니다. 플래그 지정 기능을 사용하려면 플래그가 지정된 메시지를 찾아내어 서버에서 이를 암호화하도록 메일 서버를 구성해야 합니다.

다음 단계

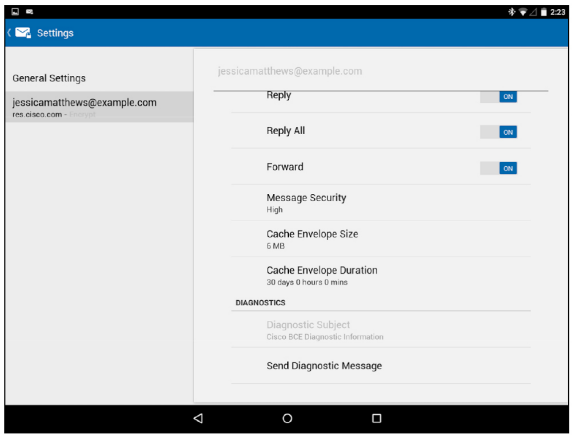
Cisco Business Class Email에 대한 자세한 내용은 http://www.cisco.com/go/emailsecurity를 참조하십시오.

풍부한 기능

Cisco Business Class Email의 기능은 표 1에 자세히 설명되어 있습니다.

공통 기능 - 설명	
비밀유지	Cisco Business-Class Email은 가장 믿을 수 있는 이메일 암호화 알고리즘을 사용합니다. 이 솔루션은 이메일이 네트워크를 통과하는 동안 기밀 보호를 위해 데이터를 암호화할 뿐 아니라 암호화 키에 쉽고 안전하게 액세스할 수 있는 최신 인증 방식을 적용합니다.
사용자 인증 단순화	이 솔루션은 SAML(Security Assertion Markup Language)을 사용하여 이메일 수신자를 인증하고 ID를 확인합니다. Cisco는 수신자의 사용 편의성을 유지하면서 강력한 인증 기능을 제공합니다. 사용자가 SAML 게이트웨이에 등록되어 있으면 회사 로그인 크리덴셜을 사용하여 회사의 다른 리소스에 액세스할 때처럼 암호화된 이메일에 간편하게 액세스할 수 있습니다.
이메일 제어 기능 강화	Cisco는 안전한 메시징을 통해 사용자에게 새로운 이메일 제어 방식을 제공합니다. 암호화된 이메일은 발송한 정보의 기밀이 유지되도록 보장합니다. 아울러 이 방식을 통해 발송자는 이메일 만료 시점을 지정하거나 회수하고 메일을 정확히 언제 열어보았는지 알 수 있습니다.
보안 기능 - 설명	
읽기 확인	수신자가 메시지를 열면(사용자의 인증이 완료되어 수신자가 암호 키를 받았다는 의미) Cisco는 수신자가 정보를 읽은 것을 확인하고 몇 초 안으로 읽음 확인을 발신자에게 보냅니다.
확실한 메시지 회수	발신자가 회수 옵션을 선택하면 데이터의 암호 해독 키가 만료되어 누구도 메시지 내용을 볼 수 없게 됩니다.
메시지 만료	발신자가 메시지의 만기일을 지정할 수 있습니다. 만기일이 지난 후에는 암호화 키가 삭제되므로 정보에 액세스할 수 없게 됩니다.
전달/답장 기능 제어	수신 후 이메일 메시지 처리 방식을 사전에 제어할 수 있습니다. 전달, 회신, 전체 회신을 비활성화하거나 발신자의 회사에서 인증할 경우에만 활성화되도록 할 수 있습니다.
뛰어난 수신자 환경	수신자는 암호화 사용 여부와 관계없이 메시지를 안전하게 회신, 전체 회신 또는 전달할 수 있습니다.

그림 1. 안전한 구성 및 봉투 설정



C45-720175-01 07/15