

Web 邮件与邮件客户端，谁更安全？

2026 年 8 月 13 日

这个话题网上有许多文章，大家一致的观点是各有各的好处，各用于不同的电子邮件收发应用场景，都离不开，需要同时使用 Web 邮件和邮件客户端。本文笔者从另一个角度来谈谈这个问题，并探讨理想的邮件客户端应该具备哪些特质。

一、什么是邮件客户端？什么是 Web 邮件？各自的优缺点是什么？

为何先讲邮件客户端？因为电子邮件发展史是先有邮件客户端。电子邮件诞生时就是使用专门的客户端软件，邮件客户端来收发电子邮件的，因为电子邮件是一个专门的协议，需要一个专门的软件来实现电子邮件的收发管理。电子邮件是互联网的第一个应用，当时还没有 Web 服务。

电子邮件客户端使用 POP3/IMAP 协议收取邮件服务器中的电子邮件，使用 SMTP 协议发送电子邮件，同时提供邮件管理、通讯录管理等服务，让用户可以离线查看和编写邮件，本地电脑保存电子邮件。第一个电子邮件客户端软件是 Larry Roberts 在 1972 年编写的，该软件具备了列表显示邮件、选择、转发和回复邮件的功能。第一个提供图形用户界面的电子邮件客户端软件是 Steve Dörner 在 1988 年编写的 Eudora。现在常用的邮件客户端有微软 Outlook、苹果邮件、Mozilla 雷鸟、腾讯 Foxmail 等。

电子邮件客户端软件是收发电子邮件的必备软件，直到 1996 年出现了 Hotmail，全球首家为用户提供 Web 邮件服务，用户无需使用电子邮件客户端软件，直接使用上网用的浏览器就可以收发电子邮件，并且免费给每个注册用户一个@hotmai.com 的电子邮件地址。Hotmail 不仅让用户可以免费拥有电子邮件地址，而且只要能上网就可以使用浏览器收发电子邮件，很快就风靡全球，仅用了一年时间就拥有了一千万用户，1998 年被微软以 4 亿美元收购，后来更名为现在的 Outlook.com。

Web 邮件的高潮事件是谷歌于 2004 年 4 月 1 日推出的 Gmail，全球首个提供高达 1GB 免费存储空间提供免费 Web 邮件服务，Gmail 现在仍然是全球排名第一位的免费 Web 邮件服务。Web 邮件以方便使用为特点，因为任何电脑和手机都有浏览器，都可以 Web 登录邮箱收发电子邮件。但是，仍然有许多不方便的地方，如无法离线查看邮件和发送邮件、每次都需要登录等。于是，所有 Web 邮件服务提供商都为用户提供了邮件客户端软件。

据最新第三方统计数据，全球前四大邮件客户端分别为苹果邮件、谷歌 Gmail、微软 Outlook、

雅虎邮件，市场份额分别为 53.67%、30.70%、4.38%、2.64%，合计 91.39%，其他所有邮件客户端软件的总和为 8.61%。而全球 Web 邮件服务提供商的排名是谷歌 Gmail、微软 Outlook、雅虎邮件、苹果 iCloud Mail，市场份额分别为 43%、19%、10%、8%，合计 80%，其他所有 Web 邮件服务提供商的总和为 20%。

可以看出：无论是邮件客户端还是 Web 邮件服务，前四大公司既是邮件客户端厂商又同时是 Web 邮件服务提供商，只是排名有一点不同，谷歌 Gmail 由于其第一位的免费 Web 邮件服务带来了第二位的邮件客户端市场份额。这也充分说明了 Web 邮件和邮件客户端在不断融合，相互为补充，但主流还是使用邮件客户端。而苹果邮件在邮件客户端软件中排名第一，这与移动互联网的流行有很大的关系，因为用户使用手机收发电子邮件已经成为第一刚需，这使得 Web 邮件从十分火爆变成了现在的只是一个无法使用邮件客户端时的补充手段。

二、电子邮件的核心安全是什么？是否还有未解决的难题？

Web 邮件和邮件客户端虽然看起来是两种不同的电子邮件使用方式，其实 Web 邮件也是使用了一个客户端软件——浏览器来处理电子邮件，不同之处在于：（1）使用通用客户端还是使用专用客户端；（2）在云端处理邮件还是在用户端处理邮件。

用户可能会问：到底是 Web 邮件安全还是邮件客户端安全呢？这其实不是一个好问题，邮件安全与使用何种邮件客户端无关。

电子邮件的核心安全是如何保证电子邮件内容在传输过程的安全和在云端邮件服务器的存储安全，简称为电子邮件的在途安全和在云安全。在途安全已经实现了 TLS 传输加密，能有效保证电子邮件无论用户是使用 Web 邮件或邮件客户端的传输安全。如果一个电子邮件服务不支持 TLS 加密传输（TLS IMAP 和 TLS SMTP），则是一个不合格的电子邮件服务，用户不应该选用这样的电子邮件服务，无论是免费的还是收费的。

如何保障电子邮件的在云安全，则是目前全球还没有解决的难题，或者说是一个云亦云的问题，所有电子邮件服务提供商都会说采取了很多技术措施来保障电子邮件的在云安全。笔者所讲的“在云安全”是指电子邮件在云端邮件服务器中是否是以加密邮件方式保存的，只有这种方式才能真正保证邮件的在云安全，其他的声称保障邮件在云安全都只是口头承诺而已，只要是明文电子邮件，采用任何措施都保证不了电子邮件的在云安全。

虽然目前市场上已经有了各种电子邮件加密解决方案，常用的邮件客户端也已经支持 S/MIME 邮件证书加密，但是由于很难使用而无法普及应用，使得目前的电子邮件都是明文存储在云端邮件服务器中，几乎所有 Web 邮件服务提供商都依赖机读用户邮件内容而展示相关的广告为盈利模式，用户 Web 查看邮件时出现一堆很烦人的广告，这也是许多用户不愿意使

用免费的 Web 邮件服务的原因之一。

目前需要重点解决的邮件安全问题是普及实现电子邮件的端到端加密，只有实现了端到端加密，才能真正保障电子邮件的在途安全和在云安全，才能有效防止电子邮件欺诈和 BEC 攻击。而实现电子邮件的端到端加密的可靠技术是 S/MIME 邮件加密技术，这个技术像 HTTPS 加密技术要求用户向 CA 购买和申请 SSL 证书一样，要求用户向 CA 购买和申请邮件证书，手动配置到支持 S/MIME 技术的邮件客户端中去使用，并同收件人实现交换公钥才能实现电子邮件端到端加密，使用过程非常繁琐，费时费力和费钱，无法实现普及应用。

三、传统邮件客户端的三大痛点

既然邮件客户端是处理邮件的主流工具，S/MIME 又是实现端到端加密的可靠技术，为什么加密邮件迟迟无法普及？根源在于传统邮件客户端存在三大痛点：

痛点一：证书申请和配置极其复杂。用户需要向 CA 机构申请 S/MIME 证书、验证身份、下载证书、手动配置到邮件客户端中，这一套流程足以让 99.99% 的用户望而却步。

痛点二：公钥交换困难。发送加密邮件前，收发双方需要事先交换公钥证书。这相当于在加密通信之前还需要一个“加密的准备工作”，大大增加了使用门槛。

痛点三：密钥管理繁琐。证书有有效期，到期需要续期；更换设备需要重新配置；私钥丢失则所有加密邮件无法解密，这些管理负担让普通用户难以承受。

四、理想的邮件客户端：自动化、标准化、智能化

基于以上分析，理想的邮件客户端应该具备三大特质：

自动化：邮件证书自动配置、公钥自动交换、密钥自动管理、证书自动续期。用户无需理解任何技术细节，加密成为默认行为。

标准化：基于 S/MIME 国际标准与国密标准，与 Outlook、Thunderbird、Apple Mail 等全球主流邮件客户端无缝加密互通。不锁定用户，不制造孤岛。

智能化：自由对接 AI 大模型，实现邮件摘要、智能起草、自动分类，让 AI 成为邮件处理的得力助手。

五、零信 AI 邮：让加密邮件不再有门槛

零信 AI 邮正是基于以上理念打造的全球首款自动加密 + 自主 AI 对接的邮件客户端。

自动化证书管理：用户在设置中点击“申请证书”后，系统自动完成证书申请并配置一张 RSA 算法 S/MIME 证书。有国密合规需求的用户可按需申请 SM2 双证书。密钥在本地生成，

私钥永不离开用户设备。

自动化公钥交换：发送加密邮件时，系统自动查询证书目录服务获取收件人公钥证书，收发双方无需事先交换公钥。

自动化密钥管理：密钥在本地生成和保存，支持一键加密导出备份到用户自己邮箱保管，并支持一键导入，实现用户自主管理密钥。

自主 AI 对接：自由选择 AI 模型、自带 API 密钥、AI 助理自己选。邮件摘要、智能起草、自动分类，AI 由用户自己掌控。

加密证书与签名证书，各司其职：零信 AI 邮为每封邮件配置两类证书，加密证书仅用于加解密，确保内容安全；签名证书决定收件人看到的身份级别（T1/T2/T3/T4），身份级别越高，可信度越高。

一封加密邮件，零信 AI 邮和 Outlook 都能看：用户可以在证书管理中手动导出零信 AI 邮自动配置的邮件证书，安装到 Windows 系统存储区，Outlook 就可以自动解密由零信 AI 邮加密的加密邮件。这是零信 AI 邮独有的跨客户端无缝体验。

零信 AI 邮的创新 UI 设计，采用清晰的图标展示每一封邮件的加密状态、加密算法、数字签名和发件人可信身份信息：T1 邮箱认证、T2 个人认证、T3 单位认证、T4 单位员工认证，身份级别越高，可信度越高。



免费自动化配置电子邮件证书，自动化实现端到端邮件加密，让普及电子邮件加密不再有门槛，普惠保障全球电子邮件安全。

零信 AI 邮，默认加密，天生智能。

王高华

2026 年 8 月 13 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 279 篇(共 82 万 8 千多字)和英文 121 篇(16 万 8 千多单词)。

