DigiCert证书安全站点

不断发展，以提供最好的 SSL/TLS 解决方案

由digicert提供

digicert

digicert:

DigiCert安全站点SSL是那些认真对待保护其数据和身份的企业的新标准。凭借具有优先级的验证和支持、web上最受认可的信任标志以及行业领先的管理平台，DigiCert一直在不断发展，为我们的客户提供最好的SSL/TLS解决方案。

建立客户信任和维护安全的数字基础设施需要持续的努力，**但却可以**在几秒钟内**分崩离析**。对于大多数组织来说，跟上网络威胁的扩散根本是不可行的。与其自己动手，不如自信地依靠 DigiCert 作为网络安全方面的合作伙伴。

DigiCert 的新安全站点证书包括了组织所需的一切，以加强他们的电子商务操作和网上运营，同时也简化了管理和减轻**整**个网络的威胁
DigiCert 安全站点是一个**三步**解决方案：

1. 安全的站点 SSL 证书

唯一带有Norton Seal的证书，被证明是领先的信托标志，可以降低反弹率和增加客户信心。

给客户提供最好的 SSL/TLS 解决方案

$175 万回复方保证在证书相关的妥协下保护您，**给你提供**独家的VIP服务和验证，确保您不会在需要帮助时长时间等待。

2. 证书中央管理控制台

我们屡获殊荣的平台允许您从发行到更新一站式管理您的证书。

使用发现和漏洞扫描工具，您可以轻松地找到网络上的每个证书——内部和外部(甚至是那些没有由 DigiCert 颁发的证书)——并收到易于阅读的报告，**重点凸显**任何安全风险，如弱签名或配置错误的证书。
使用具有自定义角色的多用户帐户控制发行，并自动进行证书更新，以避免**造成**成本高昂的网络停机。

3. DigiCert 的不匹配的基础架构

CA 的投资价值都没有超过 DigiCert。我们已经构建了一个对开发人员友好的 REST 用于本地集成到进程和系统的 API，以及一个可扩展的后端，以支持高发行卷。也许你可能还不在财富 500 强公司**排行内**，但 DigiCert 是可以和你一起成长的 CA。

Digicert服务器:

由Digicert服务器驱动

身份认同的价值

每个人都担心网络钓鱼、网络诈骗和虚假信息的扩散。

无论你的组织规模有多大，你和你的客户都很容易受到社会工程的攻击，从假登录页面到 CEO 长矛式钓鱼。

通过安全网站证书和 DigiCert 独特的品牌保护功能来控制您的线上工作。我们的验证程序——超过了行业标准——确保没有人能够模拟您的组织或以您的名义获得证书。

使用 EV（扩展验证）证书清楚地与你的用户——客户和员工——**传达**他们确实是在你的合法网站上，而不是用**单**一浏览器UI显示你注册公司或品牌名称的冒名顶替者。

某某公司https:〃www.yourcompany.com

DigiCert 公司的严格验证过程允许您实施贵司的证书策略，确保只有授权员工才能请求和接收证书，且不会放慢证书的速度，也不需要 IT 部门进行耗时的管理。

DigiCert 安全站点为您的组织带来了更高的安全性、简化的管理和增强的性能。今天就和销售代表谈谈吧。

如需更多信息，请致电 1.855.800.3444 或发送电子邮件联系digicert证书销售代表sales@digicert.com。

网站安全问题的运营成本

手动管理证书的成本非常高昂。平均**算来**，$288 每个证书 外 加 4 小时的管理。[1]

全球 5000 人已经花费了高达 1500 万$来将企业从证书中断中恢复过来和高达 2500 万$的合规化成本。

全球至少有 255,065 次**新型**的网络钓鱼攻击，比去年增加了 10%。多为针对特定品牌或实体的网络钓鱼网站。[3]

https:

消费者比以往任何时候都更关注 网页安全。2017 年年**据统计13条链接中有一条就藏匿着**恶意攻击。~同比增长 3%。[4]

1 参考文献：1 案例研究：使用Cisco系统的可扩展密钥和证书生命周期管理，“会话ID：SPO1-303，RSA2011 年会议，Cisco系统公司。
2 参考网址：
https://www.theatlantic.com/technology/archive/2016/10/alot/505025/
3 参考网址：
http://docs.apwg.org/reports/APWG_Global_Phishing_Report_2015-2016.pdf
4 参考网址：
https://www.symantec.com/content/dam/symantec/docs/reports/istr23-2018-en.