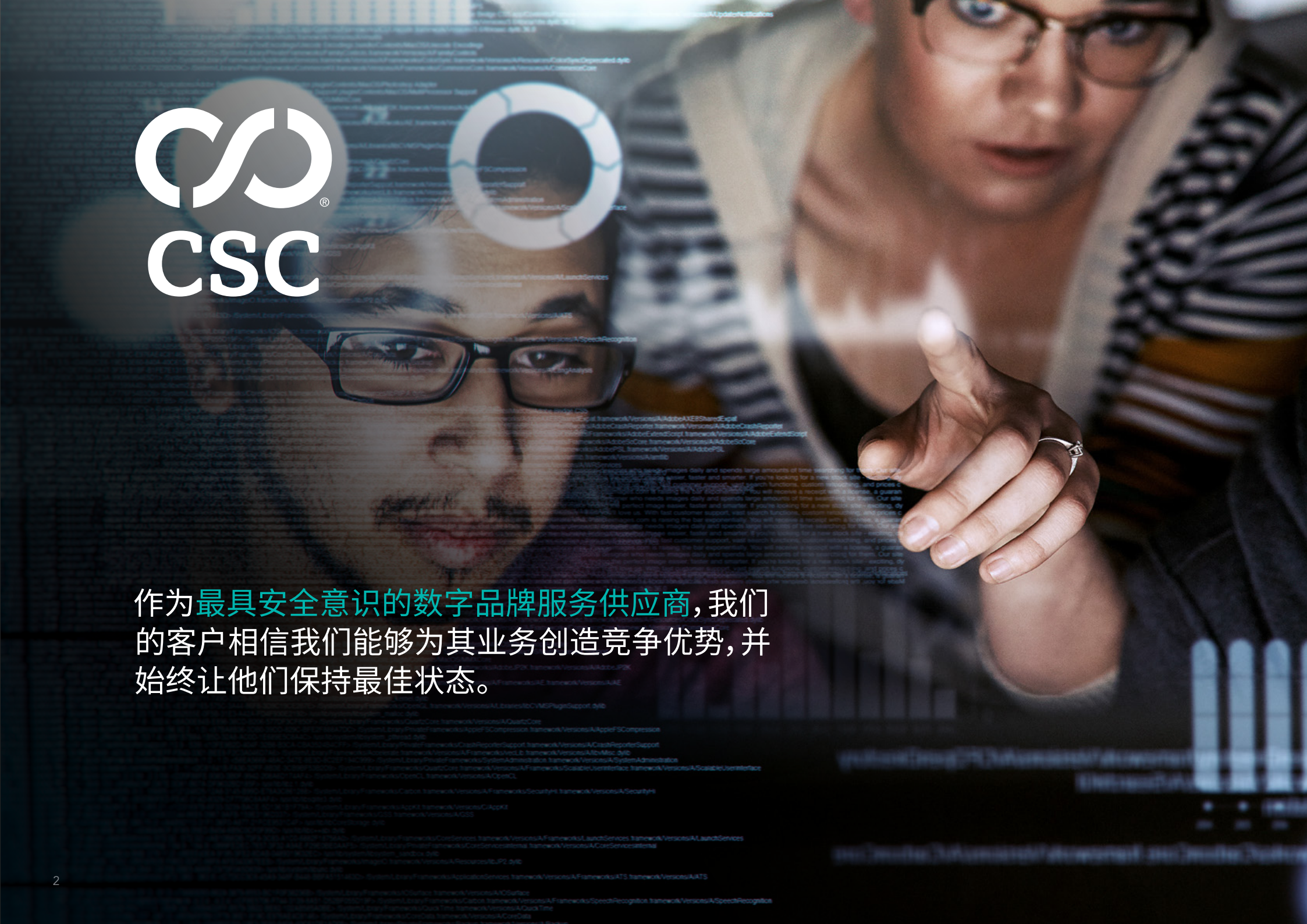
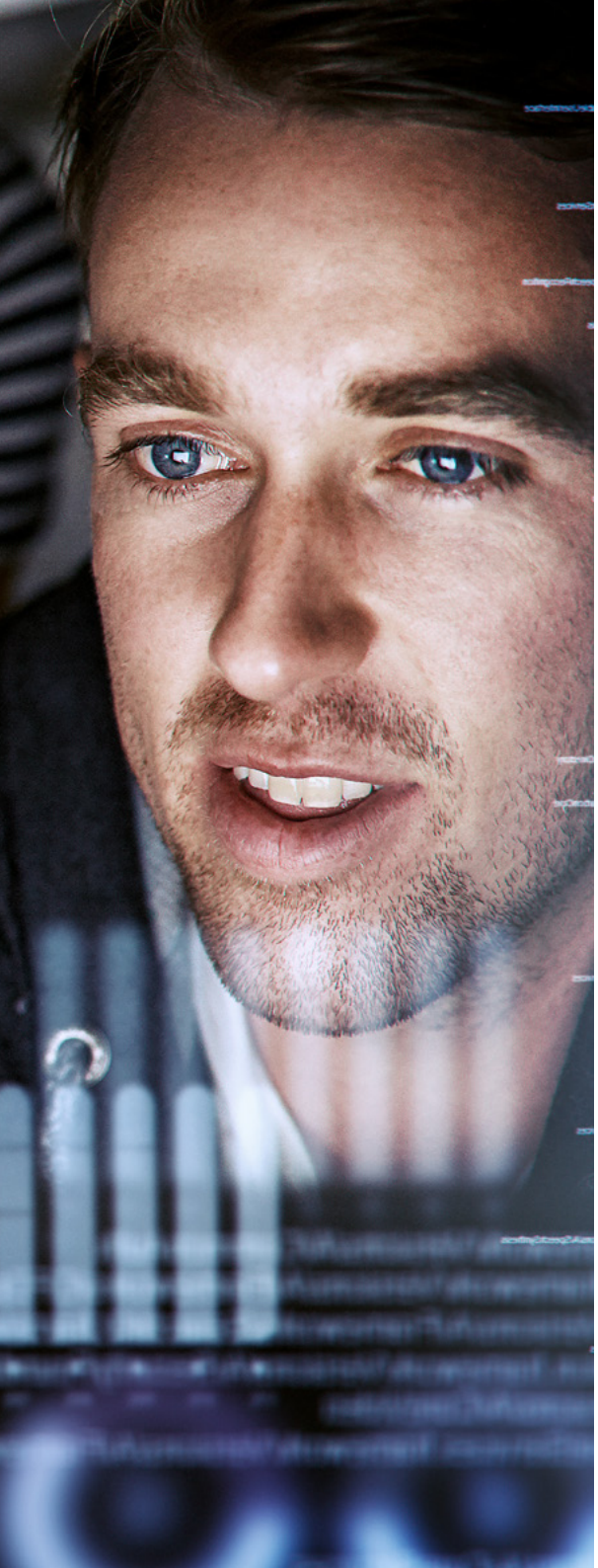
将关键在线品牌资产的安全放在首位

cscdbs.com/cn



作为最具安全意识的数字品牌服务供应商，我们的客户相信我们能够为其业务创造竞争优势，并始终让他们保持最佳状态。



持续的安全漏洞每天都可能出现在新闻报道中，贵公司可能也是受害者。事实上，并非每家公司都在竭尽全力来遏制网络犯罪。

各大公司都以指数级的速度投资了各种安全解决方案，以保护其自身免受不断演变的网络安全威胁。然而，许多公司仍然容易在安全专家所说的“至关重要的安全盲点”上受到攻击。网络罪犯正利用这些安全盲点进行更高频、更复杂和更严重的攻击，即：访问公司域名、域名系统（DNS）和数字证书。它们是使公司能够在线运营，支持其网站、电子邮件、虚拟专用网络（VPN）和其他公司应用程序运转的基本组件。如果这些组件受到损害，罪犯可以重定向网站以获取经济利益。他们还可能拦截电子邮件以从事间谍活动，甚至获取登录证书以入侵公司的网络。显然，这将对公司的收入和声誉产生巨大的影响，使公司因违反《通用数据保护条例》（GDPR）等政策而遭受巨额罚款。

法规可能令人无所适从，但 CSC 可助您从容守法。

引入CSC Security Center℠。它保护了超过 65% 的全球顶级品牌，是在线品牌保护服务的领先提供商。 CSC Security Center通过识别对您的关键资产的威胁，尽量降低未知风险，减少业务中断次数，从而使您的业务得以不间断运营。

CSC Security Center

CSC Security Center 已颠覆了网络安全态势——正如我们数十年如一日的坚持，CSC 将继续创新，率先满足市场需要，并向客户提供可靠、可扩展和定制的解决方案，为保护世界各地的品牌尽一份力。

针对那些需要了解并减轻其传统防火墙解决方案中未包含的网络风险的公司，CSC Security Center揭露安全盲点，以便能够针对危及网络存在、客户数据及关键业务功能（如电子邮件）的真实世界在线威胁采取快速行动。

CSC Security Center满足了之前从未实现的行业需求——对品牌核心域名进行全面的安全监督。其经由CSC先进的专有算法创建，是市场上最全面的域名安全解决方案。CSC Security Center将：

识别及监控

提供持续的威胁评估

发生变化时发送通知

降低威胁更加简单

我们是您的商务基石和最佳后盾®

降低网络攻击的风险

降低网络攻击的风险 DNSSEC保护您的关键域名

- 根据 CSC 的专有算法，对域名的 20 个属性进行评估，以识别该域名是否正在为您的企业开展业务关键型工作。
- 我们会对您的重要域名组合进行持续监控，因为评估会不断发生变化。
- DNS 安全扩展（DNSSEC）可保护您的网站访客免受伪造的 DNS 数据的侵害，并防止出现 DNS 缓存中毒攻击。

降低未经授权访问您关键域名所带来的风险

- 确保企业内关键域名的提升访问权限公开透明，具有访问权限的人员名单也应如此，以确保进行适当的安全控制。
- 将通过电子邮件提醒发送新用户和现有用户的权限变更。

降低 DNS 损害和中断的风险

- 突出显示 DNS 提供商的数量和风险状况。
- 由于使用了不能保证 100% 正常运行时间的低质量域名系统（DNS）提供程序，因此针对特定域名特别强调了分布式拒绝服务（DDoS）攻击的风险。

监控和减少电子邮件诈骗的风险

- 您为关键域名采取的电子邮件安全措施（包括发件人策略框架（SPF）、域名密钥识别邮件（DKIM）和基于域的消息身份验证、报告和一致性（DMARC））可用于您的风险评估。

评估整个组合中数字证书带来的风险

- 可以根据没有数字证书、低验证证书或不受信任的发行来评估处于风险中的域名。
- 存在多个数字证书提供商会增加特定域名的过期风险（疏于续订）。

CSC 是企业域名、域名系统 (DNS)、数字证书管理以及数字品牌和欺诈防御领域值得信赖的供应商，位列福布斯全球 2000 强企业和“全球最具价值 100 大品牌®”。随着全球公司加大安全性方面的投资，CSC 可以帮助他们了解存在的已知安全盲点，并帮助他们保护域名、DNS 和数字证书。CSC 的专有安全解决方案可保护公司在线资产免受网络威胁，避免重大经济损失、品牌声誉受损，或因不遵守《通用数据保护条例》（GDPR）之类的政策而受到重大经济处罚。我们还提供在线品牌保护（在线品牌监控和执行活动的结合），采用全面的数字资产保护方法，并提供欺诈防御服务来抵御网络钓鱼攻击。

cscdbs.com/cn

DBS07062021