CSC Security Center
快速入门指南

网络攻击每天都在发生，且有增无减。选择合适的合作伙伴和工具来保护品牌在线形象这项工作比以前任何时候都更重要。

众所周知，数字资产是网络罪犯和黑客利用的漏洞，所以选择基础管理服务，以及每年简单地复盘解决方案，已不再足够。

为了在与网络罪犯的较量中更胜一筹，并协助品牌所有人应对迅速演变的商业模式，CSC 开发了 CSC Security Center℠，从而化繁为简，让客户重新掌控全局。

有何风险?CSC Security Center 如何协助?

CSC Security Center 对一部分全球规模最大的组织进行了测试，通过运用多数据来源和复杂的算法，能识别和监控对您的业务生死攸关的数字资产，从而持续评估风险。这可让您立即识别和规避网络攻击对受监控资产的潜在威胁。

风险	后果	影响	CSC 解决方案
核算和管理欠佳	关键域名和安全套接层 (SSL) 数字证书过期	无网站解析服务、电子邮件、虚拟专用网络 (VPN) 或 IP 语音 (VoIP)；失去消费者的信任，以及可能容易受到恶意软件或勒索软件的攻击	审计和合并域名、域名系统 (DNS) 和 SSL
第三方提供商	社会工程、网络钓鱼或分布式拒绝服务 (DDoS) 攻击	无法控制网站解析服务、电子邮件、VPN 或 VoIP——且网络罪犯有可能克隆网站和盗取电子邮件	专注于安全性；我们在技术和人员方面投入了巨资
资产的可访问程度	社会工程、网络钓鱼攻击	无法控制网站解析服务、电子邮件、VPN 或 VoIP——且网络罪犯有可能克隆网站和盗取电子邮件	利用 IP 验证、双重验证和联合身份保护访问管理系统的权限
第三方威胁	无法规避 DDoS 和网络钓鱼攻击	无网站解析服务、电子邮件、VPN 或 VoIP——且充当着第二次攻击的烟幕	利用多重锁定、DDoS 规避、电子邮件认证和反钓鱼服务使资产免受已知的威胁
采用静态方法	无法识别关键域名和风险	无法控制网站解析服务、电子邮件、VPN 或 VoIP——且网络罪犯有可能克隆网站和盗取电子邮件	CSC Security Center