

# 思科安全状况评估

技术应用支持

产品简介

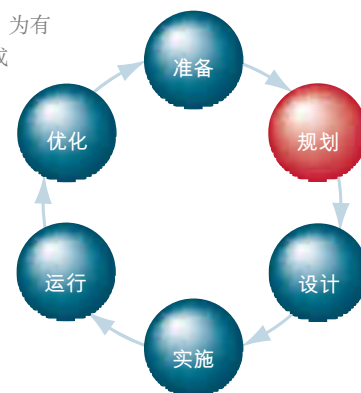


思科安全状况评估能够帮助企业成功地部署安全解决方案,以防止网络遭受黑客、病毒和蠕虫的攻击。

## 服务概述

对企业而言,网络基础设施的安全性正变得越来越重要。为有效保护企业安全,必须将安全性作为网络的一个有效组成部分,贯穿在整个环境中,才能抵御各种安全威胁。

为帮助企业消除安全威胁,大大提高网络生产率,并降低总拥有成本,思科?网络安全高级服务提供多种专家咨询和服务,并全面帮助企业规划、设计、实施、运行和优化网络安全解决方案。目前,只有思科系统公司能够提供将安全作为网络一部分的全面服务。



## 网络安全规划

作为网络安全规划的第一步,思科将全面评估网络安全状况。安全状况评估(SPA)服务由经验丰富的安全专家提供,它能够全面评估网络设备、服务器、台式机和数据库,抓拍网络安全状况。思科专家将参照公认的行业最佳实践对网络安全有效性进行分析,以揭示客户环境的相对优势和弱势。

## 思科安全状况评估的优点

### 消除网络安全风险

- 确定潜在的非法接入点,提出有助于减少安全漏洞的建议,保护专有信息;
- 帮助企业随时了解最新安全威胁,包括帮助企业了解安全漏洞,以及需要修改的地方(最好根据网络的复杂程度定期执行安全状况评估);
- 设计出来的基础设施能够有效应对各种威胁,包括发现漏洞和缺口,并提出安全改进措施;
- 揭示集成带来的漏洞和缺口,在保持网络安全的同时将新产品和技术集成到现有架构中;
- 依据行业实践确定安全需求,找出网络安全状况与实践建议之间的差距;
- 在网络扩展之后保护网络安全,包括查找网络改动之后可能出现的新缺口,并提出解决这些问题的建议。

### 提高生产率

- 消除安全漏洞，减少攻击数量，防止因安全问题而中断对客户和员工提供服务；
- 采纳专门负责安全漏洞研究的工程师提出的建议，提高网络安全和 IT 人员的生产率。

### 降低网络安全基础设施的总拥有成本

- 提供实现安全设计所需要的信息，例如网络上应该运行哪些服务，以及存在哪些安全漏洞等，从而避免以很高的代价重新设计网络安全基础设施。

思科安全状况评估服务注重内外威胁分析，包括对无线基础设施以及所有拨号连接的专家测试。

## 外部安全状况评估

外部安全状况评估用于查找外部可疑网络访问内部网络和系统的安全漏洞，并提出改进解决方案。

外部安全状况评估的目标是量化互联网连接系统的安全风险。为有效查找外部可疑网络访问内部网络和系统的安全漏洞，思科将模仿恶意攻击者的典型行为，并试图突破周边设备和互联网的安全控制。首先，思科专家将利用功能远强于标准商业工具的专业自动工具对机构的互联网连接设备执行远程安全漏洞扫描。检查完互联网设备注册之后，思科专家还将扫描外部可见设备。由于多数服务都具有固有的和已知的安全漏洞，因此，思科工程师可以帮助企业确定外部可见设备是否容易遭受攻击，并尝试人工核实可能导致安全问题的安全漏洞。外部安全状况评估提供的服务和进行的操作如表 1 所示。

表 1 外部安全状况评估提供的服务和进行的操作

提供的服务	进行的操作
查找、验证和确认外部 IP 网络上的安全漏洞	<ul style="list-style-type: none"><li>● 研究并核实目标 IP 地址空间的注册</li><li>● 分析外部可见 IP 地址空间，查找主计算机及其操作系统的号码；使用 ICMP（呼叫）答复或其它技术发现防火墙等过滤设备之后的主机</li><li>● 全部扫描 65,535 个可行端口，确定是否存在外部可见的服务</li></ul>
检查已知安全薄弱环节的安全漏洞，以便更加有效地确定非法接入可能性	<ul style="list-style-type: none"><li>● 利用提示和协议协商符号对外应用服务</li><li>● 确定所提供的服务是否存在安全漏洞，并试图通过非破坏途径核实是否存在服务安全漏洞，以及安全漏洞的程度</li></ul>
分析并提供外部评估结果	<ul style="list-style-type: none"><li>● 分析和审核数据，将外部安全状况评估结果与当前运营要求进行比较，查找主要问题</li><li>● 分析和审核数据，将外部评估结果与向企业推荐的安全实践和特殊策略、控制或运营要求进行比较</li><li>● 现有安全漏洞和建议总结</li></ul>
编写外部安全漏洞和建议报告	<ul style="list-style-type: none"><li>● 最重要的安全漏洞发现结果</li><li>● 与单个系统和安全漏洞相关的数据和统计数据</li><li>● 改进建议</li></ul>

## 内部安全状况评估

内部安全状况评估的目的是预防内部人员发动故意攻击或出现意外错误，以便更好地保护宝贵的信息资源。

很多企业和媒体都十分重视远程黑客滥用互联网发动的攻击和发生的事故，但却忽略了内部网络的安全性。内部安全状况评估是一种可以控制的网络模拟攻击，可用于揭示内部系统、应用和网络设备的暴露程度。内部安全状况评估的目的是探寻防止内部人员发动故意攻击或发生意外错误的步骤，以便更好地保护宝贵的信息资源。

思科工程师将会通过利用各种方法非法接入内部资源发现安全漏洞。除自动检测安全漏洞外，思科专家还将模拟真正的入侵过程，以可控制的安全方式人工查找安全漏洞，并利用结构化方法寻找可能漏网的安全漏洞。这种二级攻击包含攻击主机之间的可信关系，利用密码弱点，以及获得对系统的管理权等。内部安全状况评估提供的服务和进行的操作如表 2 所示。

表 2 内部安全状况评估提供的服务和进行的操作

提供的服务	进行的操作
查找、验证和确认内部 IP 网络上的安全漏洞	<ul style="list-style-type: none"><li>• 执行对客户查找到的网络的快速呼叫</li><li>• 扫描快速呼叫过程中发现的主机上的主要已知 TCP 和 UDP</li><li>• 检查可用端口，确定潜在的安全漏洞</li><li>• 确认已发现的安全漏洞</li></ul>
检查已知安全薄弱环节的安全漏洞，以便更加有效地确定非法接入可能性	<ul style="list-style-type: none"><li>• 利用主机之间的信任关系</li><li>• 利用用户引发的问题，例如在 Windows 和 UNIX 中使用相同密码</li><li>• 利用从已侵占系统收集到的应用信息和路由器配置</li><li>• 试图破坏密码文件并获得管理员（Windows）、根（UNIX）或管理员（Novell）访问权限</li></ul>
分析并提供内部评估结果	<ul style="list-style-type: none"><li>• 分析和审核数据，将测试结果与当前运营要求进行比较，查找主要问题</li><li>• 分析和审核数据，将评估结果与所推荐的安全实践和特殊策略、控制或运营要求进行比较</li><li>• 现有安全漏洞和建议总结</li></ul>
编写内部安全漏洞和建议报告	<ul style="list-style-type: none"><li>• 最重要的结果</li><li>• 与单个系统和安全漏洞相关的数据和统计数据</li><li>• 改进建议</li></ul>

## 拨号安全状况评估

拨号安全状况评估用于确定远程接入服务的安全风险。

拨号安全状况评估的目的是确定远程接入服务的安全风险。拨号服务为攻击者侵入网络开启了后门，使攻击者能够绕过防火墙等有效互联网保护。思科工程师将查找远程接入服务器上使用的服务器软件和验证方法，并试图非法接入。人工绕过接入服务器之后，思科工程师将尝试确定受攻击设备与网络的连接地点，如有可能，将进一步接入其它设备。拨号安全状况评估提供的服务和进行的操作如表 3 所示。

表 3 拨号安全状况评估提供的服务和进行的操作

提供的服务	进行的操作
查找、验证和确认远程拨号网络上的安全漏洞	<ul style="list-style-type: none"> <li>研究并核实电话号码的清单或范围</li> <li>拨打电话号码清单上的号码，成功接入电信商网络，找到主计算机及其操作系统的号码</li> <li>使用调制解调器设置和推式字串或其它技术找到电信商连接背后的主机</li> <li>重新拨打占线的电话号码</li> </ul>
检查已知安全薄弱环节的安全漏洞，以便更加有效地确定非法接入可能性	<ul style="list-style-type: none"> <li>记录白天和晚上与主计算机相连的电信商连接</li> <li>试图通过拨号连接访问主计算机</li> <li>通过非破坏性手段确定主计算机的接入难易度</li> </ul>
分析并提供拨号评估结果	<ul style="list-style-type: none"> <li>分析和审核数据，将拨号安全状况评估结果与当前运营要求进行比较，查找主要问题</li> <li>分析和审核数据，将拨号评估结果与向企业推荐的安全实践和特殊策略、控制或运营要求进行比较</li> <li>执行安全漏洞和建议总结</li> </ul>
编写拨号安全漏洞和建议报告	<ul style="list-style-type: none"> <li>最重要的安全漏洞发现结果</li> <li>与单个号码和主计算机接入难易度相关的数据和统计数据</li> <li>改进建议</li> </ul>

## 无线安全状况评估

无线安全状况评估的目的是查找风险和暴露点，并提出改进解决方案，以便增强对无线基础设施的安全保护。

无线安全状况评估的目的是评价企业无线网络的安全状况，查找与无线部署相关的风险和暴露点。思科专家将分析无线技术架构和配置，寻找合法和不合法的接入点，提出解决方案，增强对无线基础设施的安全保护。

首先，思科专家将调查客户端设备，以便发现并记录所有接入点。然后，思科将把发现的接入点和现场调查过程中收集到的数据与合法设备清单进行对比，找出恶意设备。调查完接入点之后，思科工程师将把无线网络架构和配置与业界最佳实践进行对比，并记录已知安全漏洞和威胁。

之后，工程师将转移到大楼以外，用先进无线天线查找大楼的泄露无线局域网（WLAN）流量。如果必要，工程师还将转移到大楼的可控区域，继续查找泄露的 WLAN 流量。发现流量之后，工程师将确定所使用的加密和验证方法，以便接入 LAN 网段。无线安全评估状况所提供的服务和进行的操作如表 4 所示。

表 4 无线安全评估状况所提供的服务和进行的操作

提供的服务	进行的操作
查找、验证和确认 IP WLAN 网络上的安全漏洞	<ul style="list-style-type: none"><li>● 检查无线接入点配置，并将其与安全实践建议进行比较</li><li>● 部署先进的无线天线，查找客户大楼的泄露 WLAN 流量</li><li>● 检测到 WLAN 流量后，使用全球定位卫星（GPS）技术绘制区域图，记录信号覆盖范围</li><li>● 检查大楼内公共区域的信号可视性和强度，如果未能在大楼外检测到 WLAN 流量，可根据需要检查大楼可控区域的流量</li><li>● 确定是否支持 WEP 加密，或者传输的无线流量是否使用了加密</li></ul>
检查已知安全薄弱环节的安全漏洞，以便更加有效地确定非法接入可能性	<ul style="list-style-type: none"><li>● 试图破译 WEP</li><li>● 试图获取客户 IP 地址，并评价接入点的安全性</li></ul>
分析并提供 IP WLAN 评估结果	<ul style="list-style-type: none"><li>● 分析和审核数据，将无线安全状况评估结果与当前运营要求进行比较，查找主要问题</li><li>● 分析和审核数据，将无线评估结果与所推荐的安全实践和特殊策略、控制或运营要求进行比较</li><li>● 执行安全漏洞和建议总结</li></ul>
编写 IP 无线局域网安全漏洞和建议报告	<ul style="list-style-type: none"><li>● 最重要的安全漏洞发现结果</li><li>● 与单个系统和安全漏洞相关的数据和统计数据</li><li>● 改进建议</li></ul>

## 上市日期

安全状况评估现已在全球范围内上市。

## 总结

为帮助客户快速取得成功,思科系统公司推出了多种服务计划。这些全新的服务计划通过人员、流程、工具和合作伙伴的独特组合提供,能显著提高客户满意度。思科服务不但能帮助客户保护网络投资,优化网络运作,还能使客户的网络不断支持新应用,以便扩展网络智能,增强企业的竞争优势。

## 订购

思科安全状况评估属于菜单式服务,不需要与任何其它服务一起订购。

## 详情垂询

如果想详细了解思科安全状况评估或其它思科服务,请访问:

[www.cisco.com/en/US/products/svcs/ps11/services\\_segment\\_category\\_home.html](http://www.cisco.com/en/US/products/svcs/ps11/services_segment_category_home.html)

或者与思科服务客户经理联系。



### 思科系统（中国）网络技术有限公司

#### 北京

北京市东城区东长安街1号东方广场  
东方经贸城东一办公楼19-21层  
邮编: 100738  
电话: (8610)85155000  
传真: (8610)85181881

#### 上海

上海市淮海中路222号  
力宝广场32-33层  
邮编: 200021  
电话: (8621)33104777  
传真: (8621)53966750

#### 广州

广州市天河北路233号  
中信广场43楼  
邮编: 510620  
电话: (8620)85193000  
传真: (8620)38770077

#### 成都

成都市顺城大街308号  
冠城广场23层  
邮编: 610017  
电话: (8628)86961000  
传真: (8628)86528999

如需了解思科公司的更多信息, 请浏览<http://www.cisco.com/cn>

思科系统（中国）网络技术有限公司版权所有。

2005©思科系统公司版权所有。该版权和/或其它所有权利均由思科系统公司拥有并保留。Cisco, Cisco IOS, Cisco IOS标识, Cisco Systems, Cisco Systems标识, Cisco Systems Cisco Press标识等均为思科系统公司或其在美国和其他国家的附属机构的注册商标。这份文档中所提到的所有其它品牌, 名称或商标均为其各自所有人的财产。合作伙伴一词的使用并不意味着在思科和任何其他公司之间存在合伙经营的关系。