天翼云安全体检
产品手册

天翼云科技有限公司

2024 年 10 月

目录

1. 产品介绍

1.1. 产品定义

安全体检是一款面向具备互联网业务的用户，提供周期性、精准、全面的互联网 IP 安全检查的产品，帮助用户监测、发现业务风险，生成体检报告，实时掌握业务安全状况。

安全体检产品支持弱口令检测、漏洞开放检测、高危端口开放检测等，帮助用户全面掌握互联网业务安全状况，并结合体检报告提供处置建议，帮助用户快速完成加固。

1.2. 产品优势

全面的互联网 IP 风险识别

兼容 CVE、CNVD、CNNVD 漏洞库，支持高危端口开放检测及弱口令检测，全面发现互联网暴露情况，识别安全风险。

易用的体检报告

自动生成 PDF 体检报告，包含总体安全状态、漏洞情况、端口开放情况，弱口令等内容，全面易读。

便捷的使用体验

多体检引擎支持，一键快速开始体检任务，减少排队等待时间，体检完毕自动发送体检报告，方便快捷。

1.3. 功能特性

一键启动体检

每次只需点击立即体检，即可全面检测系统健康状况与安全隐患。操作简单直观，快速生成报告，助您即时掌握设备安全状态，轻松维

护系统稳定与安全。

弱口令检测

弱口令检测是一项重要的安全措施，旨在帮助用户识别和避免使用易于被猜解或破解的密码。弱口令通常是指那些简单、常见或者容易被猜测的密码，例如“123456”、“password”或与用户个人信息相关的简单组合。安全体检弱口令检测能力可以提高系统的整体安全性，减少因密码被破解而导致的安全事件。

漏洞开放检测

对于攻击者来说，IT 系统的方方面面都存在脆弱性，这些方面包括常见的操作系统漏洞、应用系统漏洞、弱口令，也包括容易被忽略的错误安全配置问题，以及违反最小化原则开放的不必要的账号、服务、端口等。

安全体检能够全方位检测 IT 系统存在的脆弱性，全面发现网络安全建设过程中存在的各种脆弱性问题，同时可发现系统开放的账号、应用、服务、端口等，形成整体安全风险报告。帮助安全管理人员先于攻击者发现安全问题，及时进行修补。

高危端口开放检测

在 IT 系统安全管理中，经常会遇到由于业务需要而改变默认应用服务端口的情况，改变协议默认端口能够规避业务冲突、减少设备投入、充分利用资源，但某种协议在非标准端口上如何识别和扫描也成为安全管理产品需要解决的问题。

安全体检产品应用先进的非标准端口识别技术、以及丰富的协议

指纹库，能够快速准确识别非标准端口上的应用服务类型，并进一步进行漏洞检测，极大避免了扫描过程中的漏报和误报。

1.4. 应用场景

重要时期安全保障

重保期间，安全体检可以助您完成关键业务安全检查，分析业务互联网暴露情况及漏洞开放情况。您可以根据体检结果完成安全加固。

新业务上线检查

新业务上线前，安全体检可以帮助您全面检查新业务安全状况，减少新增高危漏洞及开放端口暴露，降低新业务带来的安全问题。

日常安全监控

日常安全运营工作中，您可以通过安全体检定期对互联网 IP 开展安全检查，全面了解业务安全风险，结合报告自动发送能力及时通知业务部门完成整改加固。

1.5. 术语解释

CVE

CVE（Common Vulnerabilities and Exposures）的全称是公共漏洞和暴露，是公开披露的网络安全漏洞列表。

CNVD

国家信息安全漏洞共享平台，简称 CNVD，国家计算机网络应急技术处理协调中心联合建立的信息安全漏洞信息共享知识库。

CNNVD

中国国家信息安全漏洞库（英文简称：CNNVD）是中国信息安全测评中心为切实履行漏洞分析和风险评估的职能，负责建设运维的国家信息安全漏洞库，为我国信息安全保障提供基础服务。

连通性检测

检测体检出口 IP 到目标 IP 的网络连通性，减少因防火墙、黑白名单等导致的网络不通，造成体检失败。

2. 计费说明

2.1. 计费模式

安全体检产品采用预付费，默认购买周期为一年，用户可自订单生效之日起享受购买期限内的服务，当购买的服务到期后，服务自动停止。服务为按照 IP 数量定价，单个互联网安全体检规格包含 5 个互联网 IP 授权，详细价格参考如下表格（以下表格中的月价格仅方便您参考，本服务当前仅支持按年购买、不支持按月付费）：

产品规格	产品描述	标准价格(元/月)	年付价格(元/年)
互联网安	提供 5 个及以	280	2800

全体检	内互联网 IP 安全体检服务，发现 IP 风险暴露情况、漏洞开放情况，推送安全体检报告。		

2.2. 产品订购

购买须知

安全体检产品是针对您天翼云上弹性 IP（EIP）提供服务，购买安全体检前，请确认您已有或计划购买天翼云弹性 IP 产品，并绑定业务使用，否则可能导致安全体检产品无法正常提供服务。

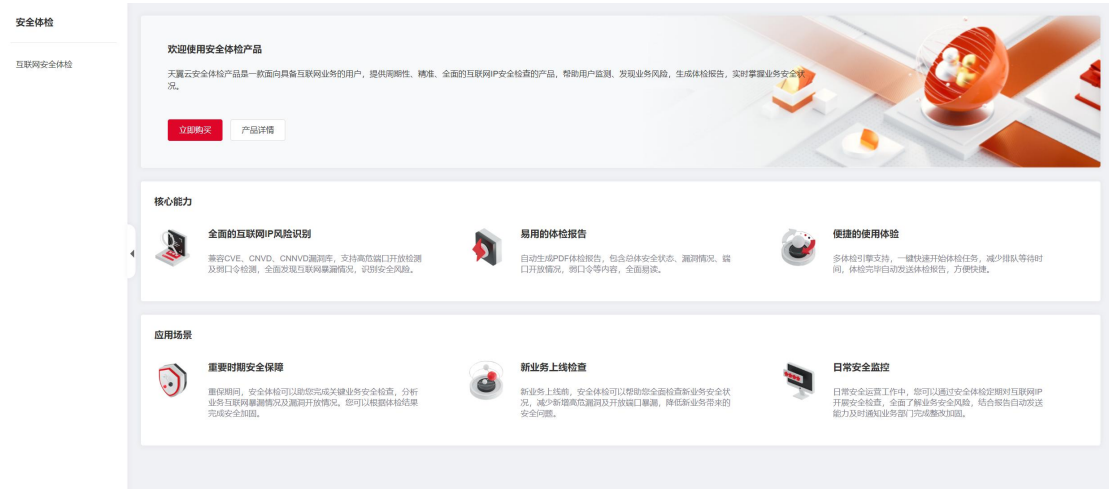
服务内容

- 高危端口、弱口令、漏洞开放检测。
- 提供安全体检报告，报告含处置加固建议。
- 自动发送邮件通知，您需要提前配置通知信息。
- 单个互联网安全体检规格包含 5 个 IP 授权，您可根据业务规模增减订购规格数量。

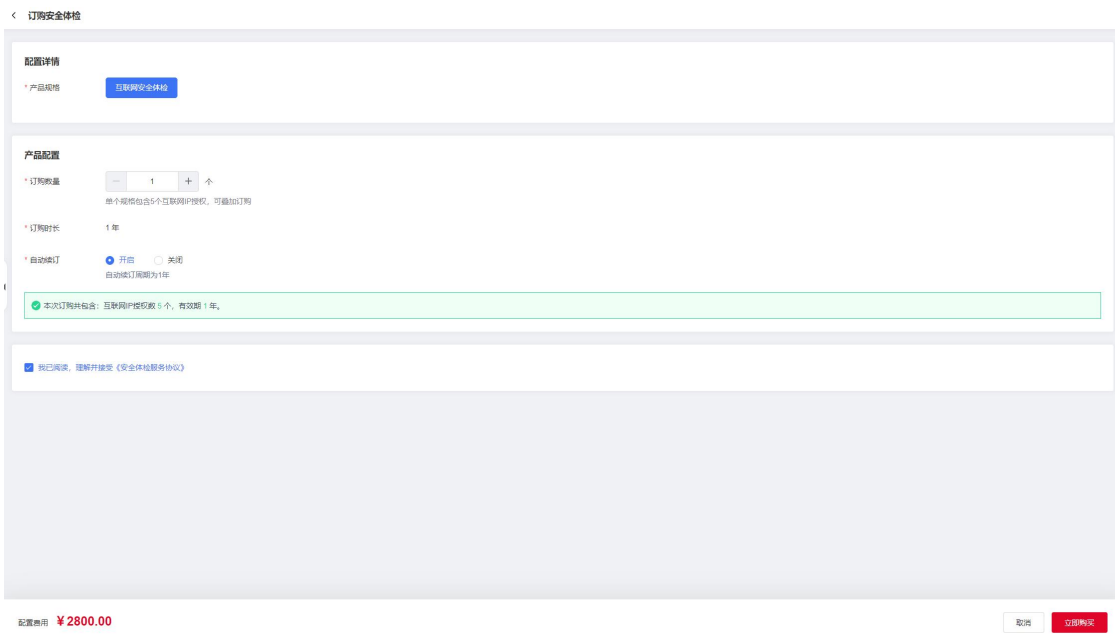
操作步骤

登录产品控制台。

点击“立即购买”按钮，跳转到安全体检订购页面。



在订购页面根据实际需要体检的互联网 IP 数量，选择订购数量（请注意单个规格包含 5 个互联网 IP 授权，如果您有 3 个互联网 IP，仅购买 1 个互联网安全体检体检即可），安全体检当前仅支持按年订购，开通自动续订后，服务到期将为您自动续订 1 年。阅读并勾选服务协议，点击右下角“立即购买”跳转到支付页面。



在“支付”页面，请选择付款方式进行付款。

付款成功后，返回安全体检产品控制台，查看订购状态。

订购并开通完成后，即可开始录入体检 IP 及通知信息。

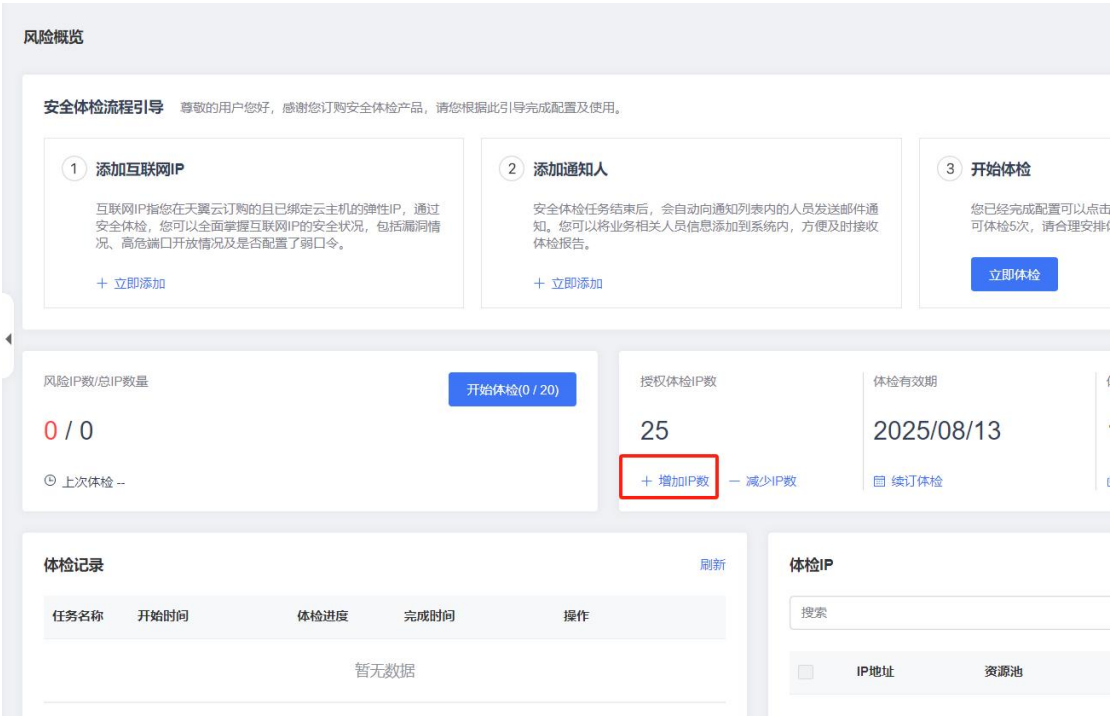
2.3. 产品升配

安全体检支持增加授权体检 IP 数量，在控制台页面，点击“增加 IP 数”按钮，进入安全体检升配页面，用户可根据自身需求输入要增加的规格数量（请注意单个规格包含 5 个互联网 IP 授权，如果您需要增加 6 个互联网 IP，仅购买 2 个互联网安全体检体检即可）。然后点击立即升配并支付。

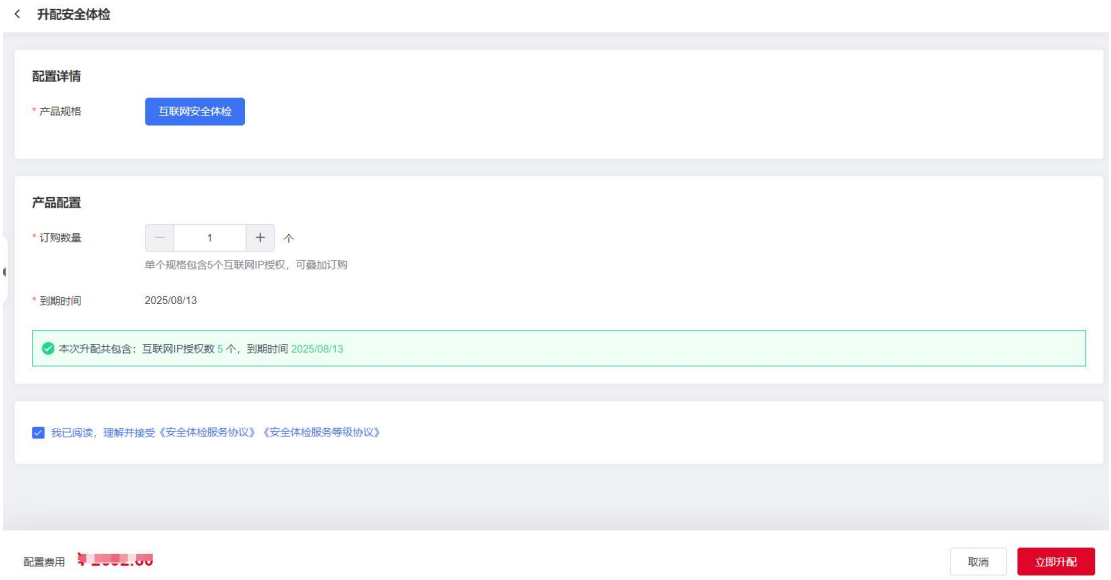
操作步骤

登录产品控制台。

点击控制台增加按钮，跳转到安全体检产品增项页面。



在升配页面，输入互联网安全体检规格订购数量，并点击“立即升配“按钮，跳转到支付页面。



在“支付”页面，请选择付款方式进行付款。

付款成功后，返回产品控制台，查看升配结果。

订购完成后，即可开始录入体检 IP 及通知信息。

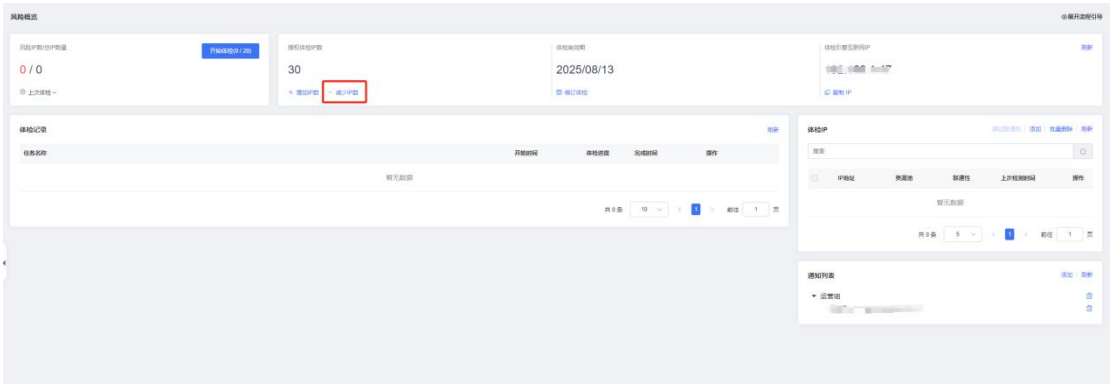
2.4. 产品降配

安全体检支持减少授权体检 IP 数量，在控制台页面，点击减少 IP 数按钮，进入安全体检降配页面，用户可根据自身需求输入要减少的规格数量（最低可减少至 1）。降配后，请您及时访问控制台，清理多出的互联网 IP，以免影响体检任务。然后点击立即降配按钮即可完成降配操作，并等待退款到账。

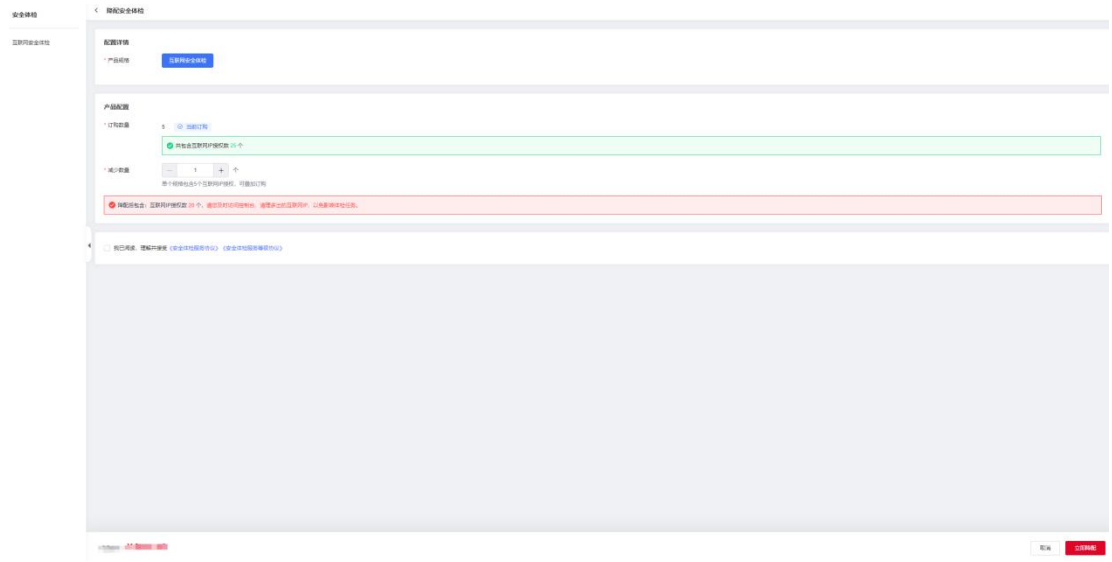
操作步骤

登录产品控制台。

点击控制台增加按钮，跳转到安全体检产品增项页面。



在降配页面，输入减少数量，并点击“立即降配“按钮，跳转到退款页面。



在“退款”页面，核对退款金额，并及时查看账单信息。

降配成功后，返回产品控制台，及时清理超出授权数量的体检 IP，否则无法正常开启体检任务。

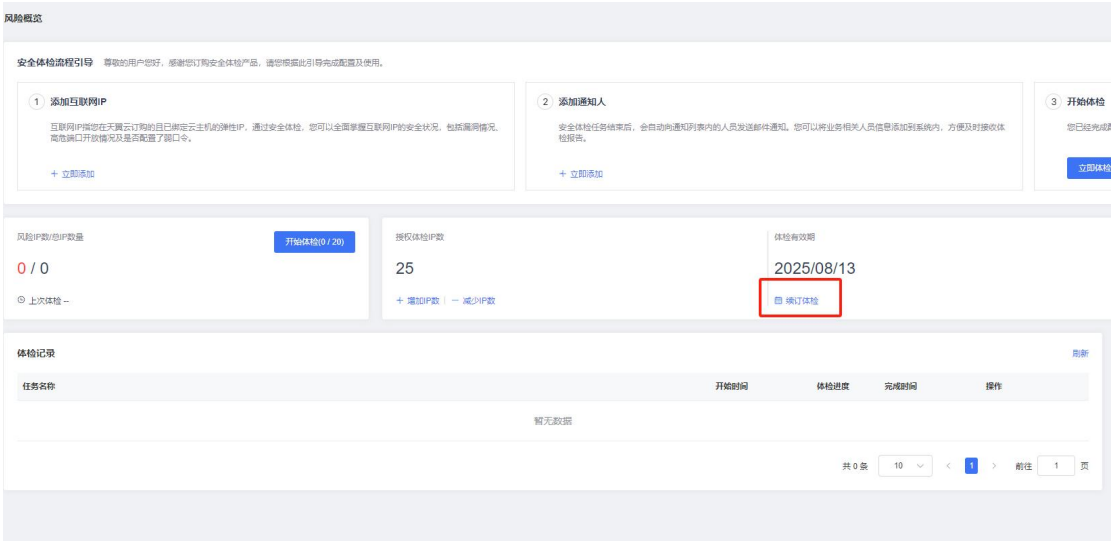
2.5. 产品续订

安全体检产品当前支持按年订购，您可在产品服务到期前，选择续费，或者开通自动续费，服务到期前，将为您自动续费 1 年。

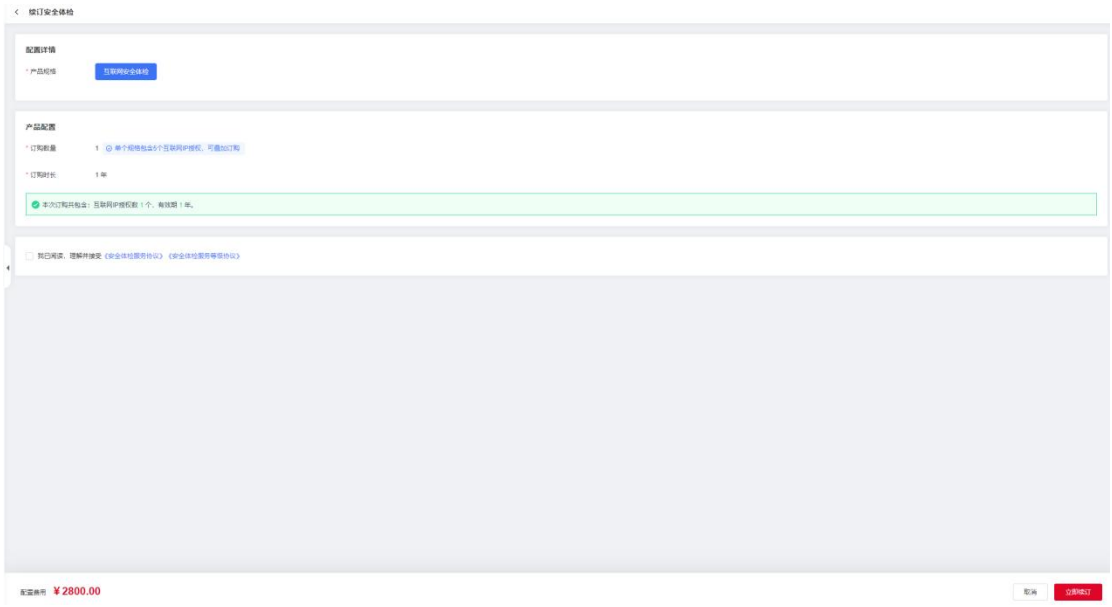
安全体检续费操作步骤

登录产品控制台。

点击“续订体检”按钮，跳转到安全体检续订界面。



在续订页面，点击“立即续订“按钮，跳转到支付页面。



在“支付”页面，请选择付款方式进行付款。

付款成功后，返回产品控制台，查看续订结果。

2.6. 产品到期

安全体检产品到期后，如您未开通自动续订，产品将自动冻结，

届时您将无法操作体检 IP、通知信息、启动体检、下载或预览报告等操作，产品将持续冻结 15 天，15 天后，如您仍未完成续订操作，产品将销毁，您的所有数据将被清除并无法恢复。

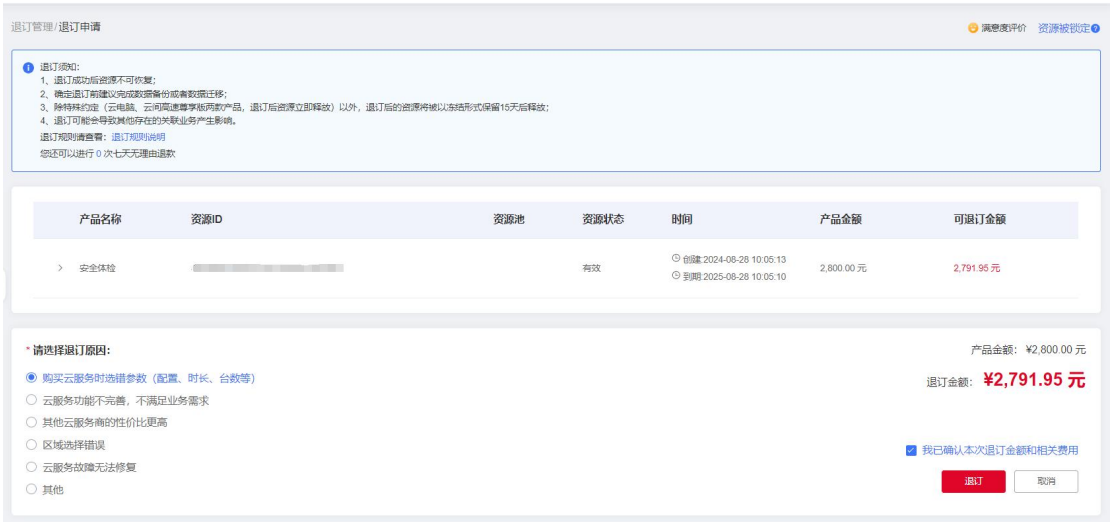
2.7. 产品退订

如安全体检产品无法满足您的业务需求，您可通过邮件反馈使用建议，反馈邮箱：ctyun-mdr@chinatelecom.cn。

如您确实需要退订，请按照以下流程操作。

登录天翼云账号，并进入“费用中心”，选择“订单管理”后进入“退订管理”，找到产品订单后，选择“退订”按钮。

点击退订按钮后，即可进入退订申请页面。



选择退订原因并勾选“我已确认本次退订金额和相关费用”后，点击“退订”按钮，即可完成退订。

退订须知：

1、退订成功后资源不可恢复；

2、确定退订前建议完成数据备份或者数据迁移；

3、除特殊约定（云电脑、云间高速尊享版两款产品，退订后资源立即释放）以外，退订后的资源将被以冻结形式保留 15 天后释放；

4、退订可能会导致其他存在的关联业务产生影响。

3. 快速入门

3.1. 首次执行

为了帮助您更好地理解和使用安全体检，我们准备以下快速入门操作指导，当您完成产品订购并开通后，您也可以在控制台上查看此操作指导，并通过右上角按钮展示/隐藏此引导。

请按照以下步骤进行操作：

第一步：添加互联网 IP

进入安全体检产品控制台。

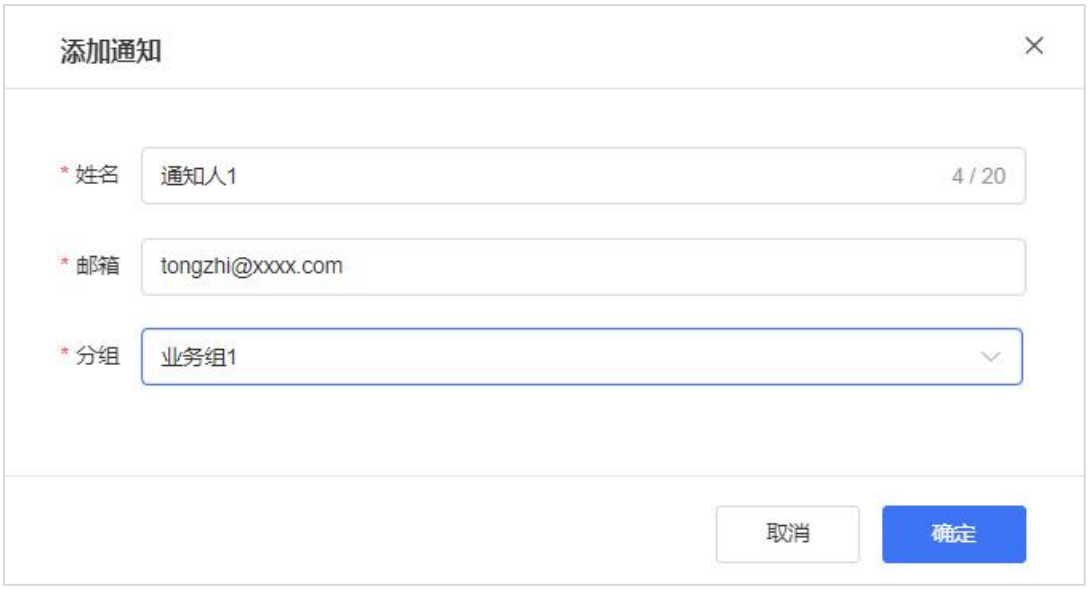
点击“安全体检流程引导”第一步的“立即添加”按钮，打开添加体检 IP 对话框。

选择已开通弹性 IP 的资源池，产品将自动获取 IP 地址列表。

勾选 IP 地址，点击确定后，体检 IP 将被添加至体检 IP 列表。

第二步：添加通知人

点击“安全体检流程引导”第二步的“立即添加”按钮，打开添加通知对话框。



输入姓名、邮箱、分组信息后，点击确定，通知信息将被添加至通知列表，体检报告生成后，将自动发送至通知列表内的邮箱地址。

第三步：开始体检

点击“安全体检流程引导”第三步的“立即体检”按钮，弹出体检提示对话框。

体检提示

安全体检包含互联网 IP 漏洞检测、高危端口开放检测、弱口令检测等内容，开始体检前，您需要关注以下内容：

1、建议您选择低业务影响时段进行体检，以减少对用户正常访问

的影响。

2、提前通知 IT 团队、业务负责人以及可能受影响的第三方，避免体检期间产生不必要的告警或混淆。

3、体检前对重要系统及关键数据做备份，以防万一发生问题时可以快速恢复。

4、体检期间，请您持续关注系统性能，确保体检活动不会导致服务中断，此外，您应准备好应急响应计划，以便快速开展遇到问题时的快速恢复流程

5、您需确保有权对目标系统进行扫描，并确保扫描活动符合当地法律和组织的内部政策，您需承担因未授权导致的法律问题。

点击“我已明确上述内容，开始体检”按钮，将开启安全体检。

请遵循以上步骤，开启您的安全体检之旅。如有任何疑问或需要进一步的帮助，请随时联系我们的客服团队。祝您使用愉快！

4. 用户指南

4.1. 体检 IP 管理

体检 IP 是您在天翼云上订购的，且已绑定云主机的弹性 IP（EIP），您可以根据资源池选择弹性 IP，并添加到体检 IP 列表，后续每次体检任务，将检测体检 IP 列表的所有 IP 的安全状况。

添加体检 IP

点击“添加”按钮，打开添加体检 IP 对话框，并选择资源池，等待系统自动获取 EIP 信息，请注意：已在体检 IP 列表中且未完成绑定的 EIP 信息不在此显示。

选择资源池时，如您通过下拉无法快速选择到目标资源池，您可通过输入资源池名称，快速检索所有资源池。比如您希望选择北京 1 资源池，则输入“北”，则可快速检索出“北 XXX”资源池。

如您所选资源池内含有大量 EIP 信息，无法快速定位，同样可通过搜索功能快速检索 EIP 信息，搜索功能支持模糊搜索。

点击“刷新”按钮，可立即刷新当前选定资源池下的 EIP 信息。

您根据业务需求，选择需要添加至体检 IP 列表内的 IP 地址，点击确定，即可完成添加。

删除体检 IP

您可以点击每条 IP 地址操作列的删除图标，删除一条体检 IP，也可以多选 IP 地址后，选择右上角“批量删除”按钮，快速删除多条

体检 IP。删除多条 IP 地址时，需要二次确认，点击确定后，即可完成删除操作。

搜索体检 IP

您可在体检 IP 列表内搜索框输入想要搜索的 IP 地址，点击搜索按钮完成搜索。搜索框支持模糊搜索。

刷新体检 IP 列表

点击体检 IP 列表右上角刷新按钮，您可以主动刷新体检 IP 列表数据。在您执行连通性测试时，方便主动获取检测结果。

4.2. 通知信息管理

每次安全体检任务结束后，将自动生成体检报告，如您已经在体检列表内配置通知信息，报告生成后，将自动发送至通知人邮箱内。因报告数据汇总及报告渲染原因，体检结束至报告发送至邮箱，可能会有一定延迟，请您耐心等待报告发送。

添加通知信息

点击通知列表右侧“添加”按钮，打开“添加通知”对话框，并输入姓名、邮箱、分组信息，点击“确定”，即可完成添加。

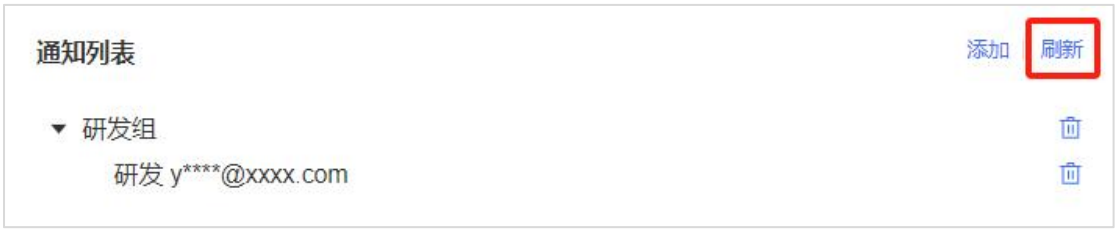
分组支持选择当前已有分组，直接输入代表新建分组，您可以根据实际业务情况，创建不同部门分组，实现体检报告快速分发至相关责任人员。

添加分组

添加通知信息时，您可以直接输入分组名称，并选择下方弹出的分组名称，如当前分组已存在，则自动加入已有分组，如当前分组不存在，选择并点击确定后，将自动新建分组。

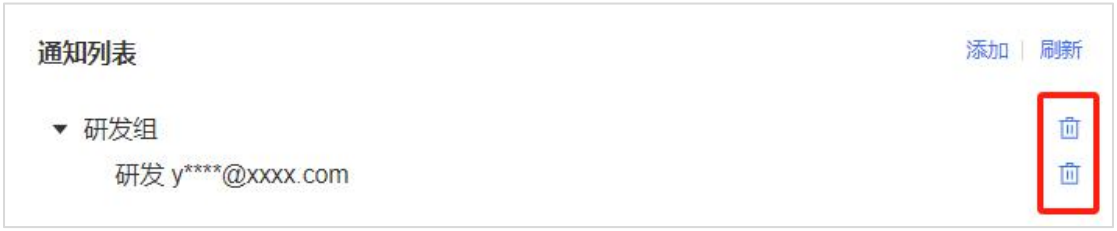
刷新分组

如果您添加通知信息后，通知列表内没有正确显示，请您点击右上角“刷新”按钮，手动刷新数据。



删除通知信息

您可以通过点击通知列表右侧“删除”图标，删除已经添加的通知人员信息及分组信息，删除后数据无法恢复，请您谨慎操作。



如点击单个通知信息的删除图标，信息将自动删除，如删除后分组内无其他通知人员信息，则此分组自动删除。

点击分组删除按钮时，系统将弹窗再次确认是否删除，点击确定后，此分组及分组下的所有通知信息都将被删除。

删除分组

以上是通知列表管理的所有功能，请根据实际业务情况，维护通知信息。

4.3. 开始体检

您完成添加体检 IP 后，即可开始体检。点击“开始体检”按钮，产品弹出体检提示信息：

点击“我已明确上述内容，开始体检”按钮，即可创建体检任务，并在体检记录中，生成一条体检记录。

等待体检完成后，您可以预览或下载体检报告。如果您已经配置通知信息，则会向您配置的邮箱内自动发送 PDF 版体检报告及漏洞详单附件。

刷新体检状态

体检进度受体检 IP 数量、体检任务总数影响，任务完成时间可能存在差异，您可以点击体检记录右上角“刷新”按钮，刷新当前体检任务进度，或者等待体检完成后，自动发送报告邮件。

4.4. 连通性检测

体检 IP 连通性检测是开始体检任务前的一项重要工作。体检 IP 与体检引擎互联网 IP 网络不通将会导致体检失败。

您可以点击体检 IP 列表右上角“测试连通性”，检测所有体检 IP 与体检引擎互联网 IP 的网络连通性。当单个体检 IP 网络不可达时，您可以点击此体检 IP 的刷新按钮，完成单个 IP 的检测。

当前体检引擎 IP 到此 IP 地址网络不可达，建议您检查：

1、安全组策略是否限此 IP 访问；

2、防火墙配置是否限制此 IP 访问；

3、体检引擎互联网 IP 是否添加至白名单；

4、此弹性 IP 是否正确绑定云主机；

5、云主机是否正常开机。

4.5. 报告解读

体检任务完成后，产品将根据本次体检结果，自动生成 PDF 格式体检报告以及 Excel 版本漏洞详单。您可以通过控制台预览或下载报告及漏洞详单，如果您已经配置通知信息，将自动向指定邮箱发送报告及详单内容。体检报告共包含体检概述、体检结果概述、急需处理的高危端口、急需处理的弱口令、急需处理的高危漏洞、漏洞详单、报告说明等 7 大块内容。安全体检报告内包含详细的处置建议，您可以根据报告内容快速开展修复工作。

4.6. 体检后的处置建议

体检完成后，您可以根据体检报告及漏洞详单查看互联网业务的漏洞开放、弱口令、高危端口开放等安全问题。体检报告包含推荐的处置建议，产线可根据这些建议，完成漏洞修复并及时更新线上系统，防止被攻击人员利用，造成损失。

通用处置建议

安全体检建议对存在漏洞的主机参考附件中提出的解决方案进行漏洞修补、安全增强。

建议所有 Windows 系统使用"Windows Update"进行更新。

对于大量终端用户而言，可以采用 WSUS 进行自动补丁更新，也可以采用补丁分发系统及时对终端用户进行补丁更新。

对于存在弱口令的系统，需在加强使用者安全意识的前提下，督促其修改密码，或者使用策略来强制限制密码长度和复杂性。

对于存在弱口令或是空口令的服务，在一些关键服务上，应加强口令强度，同时需使用加密传输方式，对于一些可关闭的服务来说，建议关闭该服务以达到安全目的。

对于 UNIX 系统订阅厂商的安全公告，与厂商技术人员确认后进行漏洞修补、补丁安装、停止服务等。

由于其他原因不能及时安装补丁的系统，考虑在网络边界、路由器、防火墙上设置严格的访问控制策略，以保证网络的动态安全。

建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的严重漏洞，攻与防的循环，伴随每个主流操作系统、应用服务的生命周期。

建议采用安全体检系统定期对网络进行评估，真正做到未雨绸缪。

远程安全评估系统建议对存在不合规检查项的主机参考对应的检查点详情中提出的调整方案和标准值进行修正。

5. 常见问题

5.1. 产品类

1、什么是安全体检产品

天翼云安全体检产品是一款面向具备互联网业务的用户，提供周期性、精准、全面的互联网 IP 安全检查的产品，帮助用户监测、发现业务风险，生成体检报告，实时掌握业务安全状况。

安全体检产品采用黑盒扫描方法，检验互联网 IP 高危端口开放、弱口令、漏洞开放情况，并对所检测系统的整体安全状况作出具体分析和加固建议。

2、安全体检包含哪些体检内容？

安全体检主要包含以下内容：

- 针对全量体检 IP 进行高危端口开放探测。
- 针对全量体检 IP 互联网开放服务进行弱口令探测。
- 针对全量体检 IP 的操作系统漏洞、中间件漏洞进行探测和发现，提供修复建议及加固参考。

3、高危端口处置建议有什么？

1) 对于不使用的高危端口，应立即关闭或禁用，以减少攻击面。
2) 使用安全组限制特定 IP 地址或子网对这些端口的访问。
3) 通过配置防火墙策略阻止对高危端口的未授权访问。
4) 对于远程管理端口（如 SSH、RDP），实施多因子身份验证，增加访问安全性。
5) 制定应急响应计划，在检测到高危端口的攻击时迅速反应。

4、弱口令常见的处置建议有哪些？

个性化密码

用户不应在其密码中包含任何与他们自己或系统相关的明显信息，例如用户名、系统名、生日等。

更改默认密码

初次登录时应强制用户更改默认密码。

不应使用出厂预设的默认密码。

避免密码重复使用

不同系统和服务应使用不同的密码。

避免部门或团队内部使用相同的密码。

密码存储安全

对存储的密码进行加密处理，避免以明文形式存储。

使用安全的哈希算法，并考虑加入盐值（salt）来增加破解难度。

定期更改密码

定期更新密码，但也要考虑到频繁更改可能带来的用户体验问题。

多因素认证

在可能的情况下启用多因素认证（MFA），以增加额外的安全层。

5、为什么企业需要定期进行安全体检？

企业定期进行安全体检至关重要，因为这有助于及时发现可能被黑客利用的安全漏洞。随着网络安全威胁的不断演变，新的漏洞和攻击手段层出不穷。定期的安全体检可以帮助企业保持最新的安全态势，确保关键数据和资产免受侵害。此外，定期的安全体检还能帮助企业

满足合规性和监管要求，从而避免因不合规而产生的损失。

6、安全体检能发现哪些类型的问题？

安全体检能够发现多种类型的安全问题，包括但不限于：

- 操作系统漏洞：未打补丁的操作系统可能导致攻击者利用已知漏洞。
- 配置错误：不当的系统配置可能暴露不必要的端口和服务，增加被攻击的风险。
- 弱密码：使用容易猜测的密码会增加账户被破解的可能性。
- 软件缺陷：第三方应用程序中的漏洞可能会被恶意利用。
- 恶意软件感染：安全体检还可以帮助检测是否存在已知的恶意软件。

7、安全体检的结果应该如何处理？

一旦安全体检完成，组织需要采取以下步骤：

- 优先级排序：根据漏洞的严重程度和潜在影响为每个漏洞分配优先级。
- 制定计划：创建一个具体的行动计划来修复漏洞，包括分配资源和设定修复期限。
- 修复验证：修复后重新进行扫描，确保漏洞已被成功解决。
- 持续监测：建立持续的安全监测机制，确保系统的安全状态。

8、安全体检会对业务运营产生影响吗？

大多数现代的安全体检工具设计为尽量减少对业务运营的影响。然而，在进行安全体检时，仍然需要注意以下几点：

计划时间：选择非高峰时段进行体检，以减少对正常业务的影响。

性能考量：确保工具的使用不会导致网络拥塞或系统性能下降。

资源调配：合理安排人力资源，确保体检过程中出现问题时能够迅速响应。

9、安全体检可以完全防止数据泄露吗？

虽然安全体检是预防数据泄露的重要步骤之一，但它并不能保证完全防止数据泄露。这是因为新的漏洞可能随时出现，而且安全体检工具只能检测到已知的安全问题。为了进一步增强安全性，组织还需要结合其他安全措施，例如员工培训、访问控制策略、加密技术和事件响应计划等。

10、安全体检的频率应该是多久一次？

安全体检的频率取决于组织的具体需求和安全政策。一般而言，建议至少每月进行一次安全体检，特别是在重大系统变更、新项目上线或发现重大安全事件之后。对于关键系统或高风险环境，可能需要更频繁地进行安全体检。

11、企业内部团队是否可以自己执行安全体检？

企业内部团队完全可以执行安全体检，但前提是他们具备必要的技能和经验。如果内部团队缺乏相关知识或资源，可以考虑购买专业的安全服务，如托管检测与响应服务。专业团队不仅拥有专业的工具，还具备丰富的经验和专业知识，能够更有效地识别和解决问题。

5.2. 计费类

1、安全体检计费模式是什么？

安全体检产品采用预付费，默认购买周期为一年，用户可自订单生效之日起享受购买期限内的服务，当购买的服务到期后，服务自动停止。服务为按照 IP 数量定价，单个互联网安全体检规格包含 5 个互联网 IP 授权，详细价格参考如下表格（以下表格中的月价格仅方便您参考，本服务当前仅支持按年购买、不支持按月付费）：

产品规格	产品描述	年付价格(元/年)
互联网安全体检	提供 5 个及以内互联网 IP 安全体检服务，发现 IP 风险暴露情况、漏洞开放情况，推送安全体检报告。	2800

2、安全体检如何升配？

安全体检支持增加授权体检 IP 数量，在控制台页面，点击“增加 IP 数”按钮，进入安全体检升配页面，用户可根据自身需求输入要增加的规格数量（请注意单个规格包含 5 个互联网 IP 授权，如果您需要增加 6 个互联网 IP，仅购买 2 个互联网安全体检体检即可）。然后点击立即升配并支付。

3、安全体检支持的体检次数是多少？

安全体检订购后，支持 20 次/年的体检次数授权，请您合理安排体检。安全体检本身是为了发现和修复系统中的安全漏洞，从而提高系统的安全性。然而在某些情况下，漏洞扫描也可能带来一定的危害性或负面影响，包括可能造成目标系统负载上升、目标系统瘫痪及合规性问

题。建议您每次扫描前跟业务方确认好体检时间及体检频率。