

# Acronis SP Protection

(免费获取)

## 服务提供商是网络攻击的热门目标

MSP 是网络攻击的目标，这些网络攻击旨在访问客户的终端以及有价值的信息。服务提供商所依赖的平台正在遭受愈来愈多诸如 [SolarWinds](#)、[ConnectWise](#) 和 [Kaseya](#) 漏洞之类的供应链攻击。

Acronis 致力于为服务提供商合作伙伴提供支持，不仅帮助他们改进实践方法，还最大限度地帮他们降低网络攻击的风险并减少其业务的停机时间。Acronis 向其合作伙伴提供的免费 SP Protect 计划包括用于实现企业自身安全防护的 Acronis Cyber Protect Cloud NFR 许可证、以安全为中心的开发实践，以及用于提高企业服务技术人员效率的网络安全培训模块。在 Acronis 的帮助下，您将比以往任何时候都更有能力防范各种威胁和供应链攻击。



## 81% 的服务 提供商

都担心其组织可能会遭受网络安全漏洞的侵害，从而导致客户的 IT 系统遭到破坏\*

## 管理网络风险所需的一切资源都是免费的

软件： 改善您的安全状况	培训： 拓展企业团队的网络安全专业知识	方法： 成为经过认证且以安全为中心的合作伙伴
<ul style="list-style-type: none"> <li>利用 Acronis Cyber Protect Cloud NFR 计划，无需额外成本<b>即可保护自身业务</b></li> <li>在现代威胁对企业业务造成损害或横向传播到企业客户之前，<b>自动阻止这些威胁</b></li> <li>降低企业基础架构中的<b>数据丢失风险并消除漏洞</b></li> <li><b>启用安全调查和审核</b></li> </ul>	<ul style="list-style-type: none"> <li>利用由 Acronis #CyberFit 学院提供的安全意识和网络安全保护培训模块，培养“安全第一”的文化意识</li> <li>借助专为服务提供商量身定制的内容，提供更好的服务</li> <li>拓展专业知识并轻松销售网络安全服务</li> </ul>	<ul style="list-style-type: none"> <li>确保您提供的服务能够防御漏洞，并防止攻击通过企业渗透客户的防御系统</li> <li>确保企业及其客户的数据只有企业自身可以访问，并且在任何既定的时间内都可访问</li> <li>选择经过认证的 MSP 合作伙伴并享有以安全为中心的方法</li> </ul>

## 并非只有客户存在风险 - 保护企业自身的终端免遭其他“漏网之鱼”的攻击

通过 [NFR 计划](#) 免费利用 Acronis Cyber Protect Cloud 来保护企业自身的基础架构。利用一体化网络安全保护解决方案，提高企业业务弹性，防止遭受现代网络威胁的侵害，并降低漏洞和技术问题所造成的影响。

\*来源：“MSP 的心声：网络安全和 MSP 未来的角色”，2021 年，Acronis 和 Vanson Bourne。

防范现代威胁	有限的攻击面	降低数据丢失和停机风险
借助新一代防恶意软件、URL 过滤和电子邮件安全解决方案，防范现代各种形式的恶意软件和勒索软件，包括零日威胁。利用内置的漏洞利用防范功能，降低供应链风险。	借助适用于 270 多个应用程序的自动化补丁管理，识别并消除整个组织的安全漏洞。	凭借以下功能，降低安全事件和技术问题对企业业务的影响，进而减少财务和声誉损失： <ul style="list-style-type: none"> <li>• 一流的备份和灾难恢复</li> <li>• 自动化的勒索软件回滚</li> <li>• HDD 运行状况监控</li> <li>• 故障安全修补</li> </ul>

开始保护您的业务

请求

## 为客户提供更全面的网络安全专业知识

为了有效抵御当今的威胁，客户不仅需要拥有技术，还需要具备专业知识。Acronis #CyberFit 学院能够为我们的合作伙伴提供更好的服务，持续更新以服务提供商为中心的安全培训模块集，并重点关注网络安全保护、威胁态势、合规性和基本网络安全实践，包括：

- 恶意软件的定义、攻击防御方式以及从漏洞恢复的方式
- 移动安全性
- 多重身份验证 (MFA)
- 密码安全性
- 隐私和个人身份信息 (PII)
- 云安全性
- 物理安全性
- 远程监控和管理 (RMM)
- 数据丢失防护 (DLP)
- 无线网络安全性
- 权限升级
- 网络钓鱼
- 分布式拒绝服务 (DDoS) 攻击
- 社会工程
- 其他

开始培训计划

启动

## Acronis 为企业合作伙伴量身定制的以安全为中心的方法



**2020 年 AV-TEST 参与者和测试获胜者**



**通过 2020 年 VB100 认证**



**通过 2020 年 ICSA Labs 终端防恶意软件认证**



**2020 年 MRG-Effitas 参与者和测试获胜者**



**2020 年 AV-Comparatives 参与者和测试获胜者**

Acronis 的产品可确保企业的所有数据在每个阶段都经过端到端的加密，只有企业自身能够访问。我们采用透明的、以安全为中心的开发惯例，并确保工程师定期接受安全培训，以保护客户数据免遭最新威胁的侵害。Acronis 通过独立的测试实验室（如 VB100、SE Labs、AV Test 和 AV Comparatives），对其代理程序进行测试。自 2018 年以来，我们在 HackerOne 上设立了一个 Bug Bounty Program（漏洞赏金计划），以确保我们的产品具有最高级别的安全性。

- AES-256 客户数据加密
- 以安全为中心的开发
- 独立评估技术
- 漏洞赏金计划