Acronis

Acronis Cyber Protect

AI 支持的数据保护和网络安全集成解决方案

发现可防御现代威胁的颠覆性安全防护解决方案

传统安全工具并不是为当今网络威胁而设计的。使用各种保护工具拼凑而成的传统方法（用于备份、修补程序自动化、反恶意软件，配置管理等）不仅复杂、昂贵，而且效率低下。

通过将数据保护与网络安全集成在一起，Acronis Cyber Protect 提供了一种革命性的网络安全保护方法。这种集成的方法解决了复杂性难题，针对当今存在的各种威胁提供了更完善的防护，并且通过节省时间和资金最大限度地提高效率。

凭借全栈反恶意软件防护和全面的端点管理，Acronis Cyber Protect 利用独特集成的保护技术应对高级网络攻击，同时简化日常 IT 运营、端点部署和管理以及报告。现在，您可以通过一个页面管理网络安全保护的所有方面。

网络安全和端点保护

端点保护管理：漏洞评估和修补程序管理、远程桌面和驱动器运行状况

反恶意软件针对恶意软件的新一代基于 AI 的全栈防护，包括 URL 过滤和自动备份扫描

备份和恢复在任何设备上，从任何事故中快速且可靠地恢复应用程序、系统和数据

降低复杂性	效率最大化	提供更好的安全保护
使用单个工具解决所有问题，以此来简化您的安全保护工作： • 一个许可证 • 一个代理 • 一个管理控制台 • 一个供应商支持热线 • 一个有关受保护系统的共享信息来源	去除不必要的开支，并利用现有资源提供更完善的保护： • 简化管理 • 无需新硬件 • 无需其他 IT 人员 • 无需培训 • 无需花费时间和资金来管理多个供应商	使用可提供所有三层防护的单个解决方案消除防御中的漏洞： • 主动性：漏洞评估和修补程序管理、从备份中删除恶意软件，驱动器运行状况监控 • 活动性：持续的数据保护、实时恶意软件防御、自我防御能力。 • 反应性：集成的灾难恢复、取证备份，以及与其他安全解决方案共存的能力
简单	**高效**	**安全**
✓ 通过一个页面轻松管理网络安全保护的所有方面 ✓ 解决了性能和兼容性问题 ✓ 快速、轻松地发现并解决问题 ✓ 减少管理多个供应商的时间以及与之相关的麻烦	✓ 提高工作效率 ✓ 减少不必要的管理时间 ✓ 避免新的开销 ✓ 轻松管理网络安全保护的所有方面 ✓ 减少 TCO	✓ 主动避免代价高昂的停机时间 ✓ 保持系统正常运行 ✓ 快速、有效地响应事故 ✓ 将勒索软件攻击扼杀在摇篮里 ✓ 保障员工在安全环境下工作 ✓ 激发客户的信心和信任

ACRONIS CYBER PROTECT 的功能

识别	保护	检测	响应	恢复
自动发现新设备	远程代理安装	防御恶意软件和漏洞	集成备份的修补程序管理	备份和灾难恢复
漏洞评估	备份和灾难恢复	硬盘驱动器运行状况控制	恶意软件隔离	备份中的取证信息
数据保护地图	统一保护策略管理	信息显示板和报告	利用可引导介质进行急救	远程桌面

功能区域根据 NIST 网络安全框架进行分组

创新型数据保护方案

数据保护和网络安全的集成带来了一些独特的功能，借助这些功能，Acronis Cyber Protect 成为了唯一能够提供前所未有的网络安全保护的解决方案

- **持续的数据保护**：避免关键应用程序中的任何数据丢失
- **故障安全补丁**：在安装任何支持立即回滚的修补程序之前自动备份端点
- **使用更少的资源提供更完善的保护**：将负载转移到中央存储（包括云）中，并启用更积极的扫描和漏洞评估
- **取证备份**：包含备份中有价值的数字证据以简化和加速调查
- **数据保护地图**：通过分类、报告和非结构化数据分析，监控文件的保护状态
- **安全端点恢复**：将反恶意软件更新和修补程序集成到恢复过程中
- **智能保护计划**：自动调整修补、扫描，并备份到当前 CPOC 警报
- **全局和本地白名单**：通过防止错误检测来支持更积极的启发式方法

Acronis

在 www.acronis.com 注册 30 天试用 Acronis Cyber Protect