如何使用
安克诺斯备份与恢复系统
保护系统免受勒索病毒的攻击

安装

使用安克诺斯保护系统免受勒索软件非常简单。只需将Acronis Cyber Backup的触控式管理控制台安装在服务器或PC上，并将备份代理部署到您计划保护的机器上即可。完全集中化的管理，您无需关注每个系统。以前安装的任何Acronis Cyber Backup版本都可无缝升级。

启动Acronis Active Protection

部署代理后，启用Acronis Active Protection，它可以检测、停止并反转未授权的加密或文件修改。您可以在单个机器、机器组或整个环境中启用该功能。您可以通过选择设置“仅通知”、“停止进程”和“使用缓存还原”来控制保护级别。您还可以将受信任的应用程序列入白名单并将已知恶意软件列入黑名单。另外，您的备份代理也可以免受勒索软件的攻击。

备份

除了启用Acronis Active Protection之外，还需要备份所有系统以便恢复。只需点击几下，即可将备份排程到本地磁盘、NAS、SAN、集中式重复数据删除存储、磁带或安全的安克诺斯云存储。您可以设置保留策略以便满足任何内部或政府的合规要求。

系统恢复

当谈到数据恢复这项最重要的功能时，安克诺斯可以说是市场上提供最全面解决方案的产品。如果恶意软件让您的数据无法修复，您可以将整个系统镜像恢复到硬件。所有数据被覆盖，没有残留数据、后门程序、恶意软件或其活动的痕迹。

文件恢复

如果只有一个文件受到影响，您可以快速浏览备份以查到并恢复该文件。要查找特定文件，您可以使用搜索功能然后快速扫描备份的内容。

业务现况

47%
的企业在2016年遭到勒索病毒的攻击

20+
平台受Acronis Cyber Backup 12.5支持，包括本地、异地位置、私有云和公有云及移动设备

750,000
的企业信赖安克诺斯保护他们的数据和系统

安克诺斯独有

为各规模的企业提供混合云和本地的数据保护解决方案，通过一个触摸友好的基于Web的控制台备份和恢复所有单独的工作负载。

安克诺斯即时还原功能，只需点击几下鼠标，即可将任意物理或虚拟Windows或Linux系统备份作为VMware或者Hyper-V运行，将恢复时间降至秒级，无需任何备用硬件。

通过使用Acronis Active Protection™主动防御系统，消除了从勒索软件攻击中恢复的需要。

支持20多种平台，包括物理、虚拟、云、终端和移动设备，提供简单、完整及经济实惠的数据保护。

包括Acronis Notary™，可提高合规性、恢复的有效性，并利用区块链验证备份的真实性和完整性。

让您完全掌控数据、系统和备份的位置，提高合规性，确保数据的所有权。

适用于任何场景

防御

Acronis Cyber Backup 12.5是业界首款能够抵御勒索软件的主动防御解决方案。其技术Acronis Active Protection可以主动检测影响数据的可疑行为，通知并停止可疑进程然后还原更改。它已被证明可有效抵制最具破坏性的勒索病毒如WannaCry的攻击，是现有防病毒解决方案的完美补充。

数据恢复

为了进一步保护您的数据，使用Acronis Cyber Backup 12.5执行定期备份。Acronis Cyber Backup 12.5是市场中最完整的解决方案，可以保护超过20个平台，并可以将备份存储在多个不同的存储设备中。另外，Acronis Active Protection可以保护备份文件免受未经授权的修改或删除。使用触摸友好的基于Web的控制台，只需简单的点击，就可以恢复文件夹、文件、数据库甚至各种应用程序项。

裸机恢复

如果您的系统遭受恶意软件损坏而无法修复，使用Acronis Cyber Backup 12.5则可以将完整的磁盘备份恢复到相同或不同的硬件。您甚至可以将物理系统还原到虚拟机，反之亦然。安克诺斯异机还原可以应对不同厂商的不同硬件，调整操作系统设置并注入必要的驱动程序，确保您的Windows或Linux操作系统32位或64位UEFI或BIOS系统在任何受支持的硬件上运行。

Acronis Active Protection™ —设置不同的保护模式

Acronis Active Protection如何运作？

启发式检测方法

Acronis Active Protection使用行为启发式方法来分析由进程执行的文件系统事件，并将其与恶意行为模式数据库进行比较。

白名单和各种程序的黑名单加强了行为启发式的应用。虽然启发式方法能够检测到新的威胁，但由于它是根据经验/行为结果进行操作的，所以可能导致误报。白名单会减少和控制误报，而黑名单则在行为开始前采取早期预防措施。

Acronis Active Protection还包含备份文件和备份代理的自我保护。除安克诺斯软件外，系统中没有任何进程可以修改备份文件。这是另一个强大的自我防御机制，它可以消除对备份代理的任何攻击，并防止备份软件遭受破坏。

此外，Acronis Active Protection会监视系统硬盘的主引导记录（MBR），只有列入白名单的进程才允许更改MBR。

Acronis Active Protection可以保护任何文件吗？

是的，它可以保护您的系统免受三种不同的攻击：

1.攻击任何文件

Acronis Active Protection实时运行，可自动化地将加密的文件恢复到最近的版本。它为您提供了所需的保护，特别是在运行排程备份时。例如，如果系统预定在午夜备份，但是在下午5点时遭受攻击，如果没有Active Protection，您可能会失去长达17个小时的工作数据。Acronis Active Protection避免了这些损失。

2.对本地备份文件的攻击

Acronis Active Protection主动监控本地驱动器并防止修改或删除备份文件。

3.攻击云备份

存储在Acronis Cloud Storage中的文件非常安全，不会受到恶意代码的直接修改。安克诺斯使用强大的端到端加密，只有授权的安克诺斯代理软件才能访问备份文件。

为什么Acronis Active Protecion技术比防病毒加传统备份软件更好？

答案很简单：您的防病毒和备份软件未集成，因此无法保护数据免受勒索病毒的攻击。

Acronis Cyber Cloud配合Acronis Active Protection技术通过一个安克诺斯备份代理可以从本地缓存、本地备份和云备份中恢复原始数据，消除了最危险的威胁勒索。

Acronis Active Protection可以应对将来的威胁

黑客逐渐将备份上的攻击视为增加收入的另一种方式，因此会有更多的勒索病毒变种攻击备份文件。 Acronis Cyber Backup 12.5是目前唯一可以有效阻止对备份文件攻击的数据保护软件。

支持的系统

适合本地控制台的操作系统

- Windows Server® 2019，2016，2012/2012 R2, 2008/2008 R2*
- Windows Small Business Server 2011，2008
- Windows MultiPoint Server 2012, 2011，2010
- Windows Storage Server 2016 2012/2012 R2, 2008/2008 R2
- Windows 10, 8.1, 8, 7
- Linux x86_64内核从2.6.18到4.9和glibc 2.3.4或更高版本

Microsoft Windows

- Windows Server 2019 2016, 2012 R2，2012，2008 R2, 2008, 2003 R2, 2003*
- Windows Small Business Server 2011，2008，2003 R2，2003
- Windows MultiPoint Server 2012, 2011，2010
- Windows Storage Server 2016 2012 R2，2012，2008 R2，2008，2003
- Windows 10，8.1，8，7，Vista，XP SP3

云

- Office 365邮箱
- Amazon Web Services EC2实例
- Microsoft Azure虚拟机

虚拟机

- VMware vSphere ESX(i) 7.0，6.7，6.5，6.0，5.5，5.1，5.0，4.1，包括vSphere Hypervisor (免费ESXi) *
- Microsoft Hyper-V Server 2019，2016，2012 R2，2012，2008 R2，2008
- 带有Hyper-V的Microsoft Windows Server 2019，2016，2012 R2，2012，2008 R2，2008
- 带有Hyper-V的Microsoft Windows 10，8.1，8（x64）
- Citrix XenServer* 4.1.5-7.6*
- Red Hat Virtualization2.2-4.1
- Linux KVM
- Oracle VM Server 3.0-3.4
- Nutanix AHV

应用程序

- Oracle Database 12，11*
- Microsoft Exchange Online
- Microsoft Exchange Server 2019，2016，2013，2010，2007-包括集群配置
- Microsoft SQL Server®2019，2017，2016，2014，2012，2008 R2，2008，2005-包括集群配置
- Microsoft SharePoint 2013，2010 SP1，2007 SP2，3.0 SP2

存储

- 本地磁盘-SATA，SCSI，IDE，RAID
- 网络存储设备-SMB，NFS，iSCSI，FC
- 可移动媒体-ZIP，Rev，RDX等
- 外部HDD和SSD-USB 3.0/2.0/1.1和IEEE1394（火线接口）
- 磁带机，自动加载机和磁带库，包括媒体管理和条形码支持
- Acronis Cloud Storage

文件系统

- FAT16/32
- NTFS
- HFS+ *
- APFS
- ReFS *
- ext2/ext3/ext4
- ReiserFS3, ReiserFS4 *
- XFS *
- JFS *
- Linux SWAP
- exFAT

Web浏览器

- Google Chrome 29或更高版本
- Mozilla Firefox 23或更高版本
- Opera 16或更高版本
- Windows Internet Explorer 10或更高版本
- Microsoft Edge 25或更高版本
- Safari 8或更高版本（运行在Apple OS X和iOS）

注意：标记为*的为有限的支持

安克诺斯®

了解更多详情
www.tieten.cn