安克诺斯®

白皮书

降低停机成本：

10大特色功能为制造业数据安全保驾护航

安克诺斯如何为制造业
提供一流的数据保护方案

停机成本

所有行业的停机成本都非常高昂。但对于那些制造业企业来说，停机停产会对成百上千的工人产生负面影响，停工成本是灾难性的。

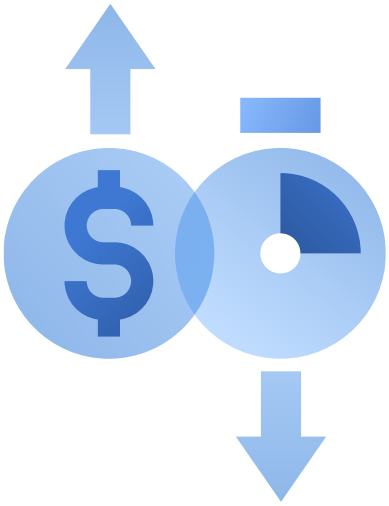
阿伯丁（Aberdeen）最近的一项研究指出，制造业的平均停工成本为每小时 260，000美元。

意外停机不仅会带来高昂的成本，而且会减慢向客户的交付速度，并对整个供应链产生毁灭性影响。当发生停机时，企业需要尽一切可能让故障系统快速恢复并运行。

完全恢复意味着企业重新恢复正常运行并与停机前完全一样。修复设备、修复网络攻击或修复导致停机的故障只是恢复过程的一部分。更复杂、更困难的部分是准确、完全地恢复故障的应用服务器、虚拟机、云工作负载和端点。如果没有强大的数据保护解决方案，可靠地从备份中恢复可能比修复实际故障需要更长的时间。

防止代价高昂的生产停机需要快速、可靠且易于管理的备份和恢复解决方案。这包括创建和维护备份计划、业务可承受的停机成本、恢复点目标（RPO——衡量业务在中断情况下能够承受损失的合理数据量）和恢复时间目标（RTO——衡量业务能够承受的合理离线时间的指标）。

在对停机时间高度敏感的制造环境中，从备份中恢复不仅速度要很快，而且必须精确到万无一失的程度。但这样的解决方案并不常见。



Kroll Ontrack Research最近的一项研究发现，75%的IT经理无法从备份中恢复所有丢失的数据。

并且，勒索软件等广泛传播的恶意软件不仅使生产数据无法访问，而且还会破坏备份，从而大大增加数据丢失、停机时间和相关成本，从而加剧停机问题的严重性。

对于制造企业来说，丢失这样的数据是一场灾难。

由于IT在制造业系统中的参与度有限，很容易忽略关键的业务管理事务，如数据保护。此外，许多数字化制造业系统仍运行在老旧的或不常见的软件环境中，这使得IT执行数据保护的工作更加困难，现有的IT工具只能保护相对较新的操作系统、应用程序和数据格式。

[1] "Manufacturing Downtime: Causes, Impact, and Mitigating Risk，" BlackBerry AtHoc, August 2018.

[2] "Kroll Ontrack Research: One-Third of Companies Experience Data Loss When Moving Data，" Kroll Ontrack, March 2018.

安克诺斯为制造业提供最一流的数据保护方案

虽然市面上有很多种数据保护方案，但在IT人员有限或没有IT人员的制造业环境中，加上其对数据保护方案的要求也很高，那么，Acronis Cyber Backup 就成为制造业的首选。

Acronis Cyber Backup提供了保护制造业信息安全所需的可靠性、完整性、安全性，并满足制造业企业的特定需求。此外，无需特殊培训或专门员工，可由普通操作员管理数据保护的备份和恢复。Acronis Cyber Backup是一款快速、可靠且易于管理的备份、恢复和安全保护解决方案。

易用性是 Acronis Cyber Backup 的一个主要优势，它可以为企业中的每个设备简单而灵活地创建备份计划。备份可以保存在本地、远端存储或云中。本地数据备份通常是为了加快从停机时间恢复的速度。同时，Acronis Cyber Backup 支持 25 种语言，使海外员工能够用母语工作，避免了翻译问题。

10大特色功能保护制造业数据安全

为了给生产环境中的数据保护提供最佳解决方案，Acronis Cyber Backup提供了10个特色功能：

1. **快速恢复数据**——集成的Acronis即时恢复技术使用户能够将任何服务器恢复为新的虚拟机，无论是在物理、虚拟或云平台上，从而实现业界一流的恢复时间目标（RTO）。例如，可以备份物理Windows或Linux计算机，并在几秒钟内立即将其还原成VMware或Hyper-V虚拟机。

2. **定时和按需备份**——利用Acronis Cyber Backup控制台，可以使用户在需要时手动启动备份，或创建备份计划并按定期计划自动执行备份，操作变得快速而简单。此外，还可以灵活地备份没有和公司网络连接的计算机。这些能力大大减轻了IT运营部门管理备份过程的负担，并允许更熟练的员工专注于战略项目和其他关键任务。

3. **支持独特和较旧的服务器环境**——许多制造业IT系统是高度定制化的，例如过程控制系统和生产线管理应用程序。通常在较旧的硬件和操作系统版本上运行。为了保持这些系统稳定运行，通常不会对它们的操作系统打补丁或升级更新。Acronis Cyber Backup中基于镜像的备份和裸机恢复可以允许这些系统在任何类型的系统故障事件中快速恢复。

4. **主动防御可抵制最普遍的恶意软件攻击**——制造业是恶意软件攻击最频繁和最有利可图的目标之一，因其系统稳定性优先于漏洞和补丁管理，所以使许多制造业 IT 系统面临着各种网络威胁，包括勒索软件和隐蔽挖矿攻击。带有内置主动保护技术的 Acronis Cyber Backup 使用人工智能和机器学习自动检测、终止和恢复勒索软件攻击造成的任何损坏，以及检测和终止消耗资源的隐蔽挖矿攻击。

5. **强固备份**——许多类型的现代恶意软件，特别是勒索软件，不仅是为了渗透和危害生产服务器，而且还用于破坏或销毁从恶意软件攻击中恢复的备份代理和备份归档，这种策略是有效的：如果受害者无法找到一个可用的的近期备份，他们将更愿意支付赎金给勒索者，获取解密密钥以解锁他们的数据。Acronis Cyber Backup代理、备份存档和云基础设施都经过了专门的加固，以抵御此类恶意软件攻击，从而确保能够从对生产系统的任何攻击中恢复。

6. **完整镜像备份**——Acronis Cyber Backup提供真正的基于镜像的备份，创建整个存储介质的逐个数据块的副本，为源系统提供最完整的保护。此方法允许在必要时迁移到新硬件，并确保最短的恢复时间，而无需重新安装操作系统、应用程序和配置文件，即可轻松返回到生产模式。

7. **脱主机备份管理**——制造业对严格的RPO和RTO的需求可能会给运行在旧硬件上的老化服务器带来性能上的挑战。这些较旧的系统可能难以执行其主要业务的同时运行备份，从而导致错过备份窗口进而可能导致代价高昂的数据保护缺失。Acronis Cyber Backup转移备份管理任务，如备份复制或将清理任务转移到其他计算机上执行，释放生产系统上宝贵的CPU和内存资源。

8. **裸机恢复**——和生产停机带来的巨大成本相比，任何能够加快生产服务器恢复速度的功能都显得格外重要。实现此目标的一种方法是从备份恢复到"裸机"系统，即没有安装或配置操作系统或其他软件的服务器。Acronis Cyber Backup可在一次操作中非常快速地将故障服务器恢复到裸机目标，包括源系统的操作系统、应用程序、配置设置和数据。这避免了重新安装和重新配置这些组件所需的高昂成本和耗时的过程。它还提供了一种从恶意软件攻击中快速恢复的方法，只需使用攻击前创建的干净镜像恢复受损系统即可。

9. **恢复到不同的硬件**——缩短生产中断时间另一种方法是将出现故障的服务器恢复到任何新的现有硬件上，能够满足基本的性能要求。但是，将备份镜像还原到不同的硬件可能会由于新硬件和源镜像之间的不兼容而导致启动失败，通常是启动分区、存储控制器和网络接口。Acronis异机还原是另一种集成到Acronis Cyber Backup中的技术。它通过自动插入必要的启动镜像、存储驱动程序和网卡驱动程序，在恢复过程中消除这些不兼容性。这使得源系统镜像能够快速地自动启动并在新硬件上运行，而无需进一步重新配置或其他操作员干预。

10. **对虚拟环境的支持**——大多数制造业环境都支持使用物理服务器以及在本地、私有云和公共云服务上运行的虚拟机。制造业企业必须保护所有这些不同的平台，要保持性能和运行时间的优势，就需要能够在不同平台类型之间移动工作负载，例如为了能够快速恢复实际生产，而将物理服务器恢复到虚拟机中，或将虚拟服务器的镜像移动到公共云以实现灾难恢复。Acronis Cyber Backup支持对物理、虚拟和云平台的完全保护，并使在它们之间移动工作负载变得简单、快速和可靠。

总结

制造业环境中的意外停机对企业利润、客户关系、公司估值以及负责保护系统的IT专业人员的职业生涯构成威胁。制造业IT环境有其特定的需求，既需要保护老化的传统系统如专用的过程控制服务器、避免高成本的停机时间、日益增长的恶意软件威胁，还及需要快速、无缝地从停机中恢复。这些要求常常给数据保护供应商带来无法克服的问题。

幸运的是，Acronis Cyber Backup提供了一种先进的、集成的数据保护方法，同时将性能、广泛的支持平台和易用性完美的结合在一起，为制造业提供了保持良好运行所必需的一切。