Acronis

WHITEPAPER

降低宕机成本：

10种方式解决制造业数据保护难题

安克诺斯如何为制造业提供最佳的数据保护。

宕机成本

任何行业的停机成本都可能相当高。但对于那些制造业组织来说，宕机停产会对成百上千的工人产生负面影响，停工成本可能是灾难性的。

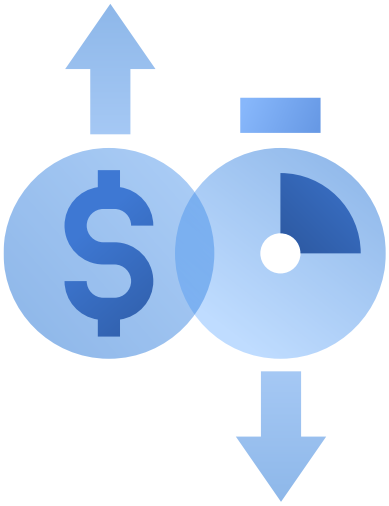
阿伯丁最近的一项研究指出，制造业的平均停工成本为每小时 260，000美元。

计划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重大的破坏性影响。当发生停机时，组织需要尽一切可能让故障系统快速恢复并运行。

完全恢复意味着工厂重新恢复正常运行并与停电前完全一样。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、完全地恢复失败的应用服务器、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需要比修复实际故障更长的时间。

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，包括恢复点目标（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、停机和相关成本，从而加剧停机的问题的严重性。

对于制造组织来说，丢失这样的数据是一场灾难。

由于IT在制造系统中的参与有限，很容易忽略关键的业务管理活动，如数据保护。此外，许多数字制造系统运行在旧的、独特的或不寻常的软件环境中，使得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老式操作系统、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佳的数据保护

数据保护的选择有很多。但在IT人员有限或没有IT人员的制造环境中，对数据保护方案的要求也更高，Acronis Backup是制造环境的最佳选择。它提供了保护传统数据中心、边缘环境所需的可靠性和数据完整性，并满足制造部门的特定需求。此外，Acronis Backup可以由非数据保护专家管理保护，无需特殊培训或专门员工。Acronis还提供功能齐全、全面的解决方案，通过一个解决方案保护各种制造IT系统。

易用性是Acronis Backup的一个主要优点，它可以为组织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、远程存储或云中。本地数据备份通常是为了加快从停机时间恢复的速度。Acronis 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。

保护制造数据的10个关键功能

为了生产环境中的数据保护提供最佳解决方案，Acronis Backup提供了十项关键功能：

1. **快速恢复数据**——集成的Acronis即时恢复技术使Acronis Backup用户能够将任何服务器（无论是在物理、虚拟或云平台上运行）恢复为新创建的虚拟机，从而实现业界最短的恢复时间目标（RTOS）。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为VMWare或Hyper-V虚拟机（VM）。

2. **定时和按需备份**——Acronis Backup控制台使您可以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，它还可以在组织网络断开连接时，配置计算机备份，提供了所需的灵活性。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（如过程控制系统和生产线管理应用程序）是高度定制的，通常在较旧的硬件和操作系统版本上运行。保持这些系统稳定运行的重要的一点意味着它们的操作系统无法修补或升级到更高版本。Acronis Backup中基于映像的备份和裸机恢复允许这些系统在任何类型的系统故障事件。

4. **主动防御可抵制最普遍的恶意软件攻击**——制造业是犯罪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系统面临着各种的网络威胁，包括勒索软件和密码劫持攻击。带有内置Acronis主动保护技术的Acronis 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，以及检测和终止资源消耗的密码劫持攻击。

5. **强化备份**——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，他们将更愿意支付在线勒索者所需的解密密钥，以解锁他们的数据。Acronis Backu代理、备份档案和云基础设施都经过了专门的强化，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. **完整映像备份**——Acronis Backup提供真正的基于映像的备份，创建整个存储介质的逐块级的副本，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，而无需在返回生产模式之前重新安装操作系统、应用程序和配置文件。

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进程上的挑战。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漏洞。Acronis Backup卸载备份管理过程，如备份复制或将保留策略应用于其他计算机，释放生产系统上宝贵的CPU周期和内存。

8. **裸机恢复**——生产宕机带来的巨大成本使任何能够加快生产服务器宕机恢复速度的功能都显得格外重要。实现此目的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 Backup可在一次非常快速的操作中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。这避免了在返回到实际生产状态之前重新安装和重新配置这些组件的高昂、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万无一失的方法——只需使用攻击前创建的干净映像恢复受损系统。

9. **恢复到不同的硬件**——缩短生产中断的另一种方法是将出现故障的服务器恢复到任何新的现有的硬件上，能够满足基本的性能规范。但是，将备份映像还原到不同的硬件可能会由于新硬件和源映像（通常是引导媒体、存储控制器和网络接口）之间的不兼容而导致引导失败。Acronis异机还原（Universal Restore）是另一种集成到Acronis Backup中的技术；它通过自动插入必要的启动映像、存储驱动程序和网络驱动程序，在恢复过程中消除这些不兼容性。这使得源系统映像能够非常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**——大多数制造环境现在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。制造商必须保护所有这些不同的平台。并且，需要能够在性能和运行时间有优势，允许可以在不同平台类型之间移动工作负载，例如将物理服务器恢复到虚拟机以极快速地返回到实际生产，或将虚拟机服务器映像移动到公共云服务以实现灾难恢复。Acronis 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

制造环境中的计划外停机对业务利润、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环境有特定的需求，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 并且及需要快速、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 Backup提供了一种先进的、集成的数据保护方法，确保了性能、广泛的平台支持和保持其IT操作可靠性。