Petri IT Knowledgebase Resource
A BWW Media Group Brand

Petri IT Knowledgebase

解决制造业可用性的7个痛点

Sponsored by
Acronis

目录

在工厂车间运行的流程对制造企业至关重要，任何停机都会立即导致生产力和收入的损失。这意味着，保护关键制造应用程序（如过程控制服务器）并保持它们的高可用性一直应该是首要任务。

但是，这种对高可用性的需求也带来了一些制造行业特有的IT挑战。例如，应用程序通常高度专用于不同的离散进程，但它们通常在过时的操作系统（如 Windows XP）上运行。软件大多非常稳定，很少（如果有的话）更新。

本白皮书讨论了制造停机的成本，探讨了维护正常运行时间的主要挑战，并考虑了能够支持制造业IT基础架构的数据保护解决方案。

制造业宕机成本很昂贵

制造业依赖于可靠、连续的生产过程，每一分钟的停工都是极其昂贵的。即便如此，对于该行业来说，宕机也频频发生。行业研究表明，几乎每一家工厂都会因停工而损失至少5%的生产能力，而许多工厂损失高达20%。

> 制造商每年要应对多达800小时的停机时间

根据阿伯丁研究公司的数据，82%的公司经历了计划外停机。过去三年， 来自Arimo的研究表明，制造商平均每年要处理多达800小时的停机时间。工厂停机会对几个主要领域的业务造成不利影响：

- **生产损失**——可靠的制造流程直接等同于利润。生产时间损失直接影响企业的盈利，降低利润。
- **产能损失**——工厂停机会降低整体生产产出。
- **增加的直接人工成本**——无论工厂是否生产，直接的固定的人工成本保持不变。停机意味着每生产一款商品的人工成本增加。
- **声誉受损**——停机会降低订单履行和产品交付，从而损害客户关系，降低公司的品牌和价值。
- **网络攻击造成的经济损失**——除了造成停机外，勒索软件等有针对性的网络攻击可能迫使企业向网络犯罪分子支付费用，以便可以恢复基本服务，防止损坏公司的声誉。

阿伯丁最近的一份报告估计，非计划停机每年给该行业造成50亿美元的损失，其中系统故障占总损失的42%。按照阿伯丁的说法，“非计划停工的成本可能是毁灭性的，工业厂房的成本估计在每小时10000美元到260000美元之间。”

虽然企业可能已经意识到这些报告（或已经直接感受到了这些影响），但提高可靠性面临着一些必须要解决的挑战。幸运的是，有的解决方案不仅可以解决可靠性的问题，而且可以非常高效且简单的实现。

1 传统的数据保护解决方案缓慢，复杂且不完整。

工厂车间IT部署通常包括多个服务器，它们执行独立的专门任务，每个服务器有不同的备份。许多应用程序运行在较旧的操作系统上，如windows xp。多个备份带来了操作复杂性和增加的手动干预，延长了恢复时间。

解决方案

使用能够支持各种平台（物理、虚拟、云）、操作系统和应用程序工作负载的数据保护解决方案，这些平台可能具有或可能不具有对集中管理控制台的网络访问权限。优先考虑能够创建高度自动化备份计划的解决方案，该解决方案的管理界面直观到足以让非IT人员操作。

> "...宕机可能是毁灭性的，制造业宕机损失大约是每小时10000到260000美元。"

2 勒索软件和加密劫持恶意软件都会影响正常运行时间和性能

勒索软件是对制造业最普遍的恶意软件威胁之一，它对目标服务器的文件进行加密，勒索赎金以获取解锁和恢复服务的密钥。许多勒索软件变体包括蠕虫组件，它们可以通过网络扩散到其他目标，包括备份服务器。

例如，2019年，挪威铝业制造商Norsk　Hydro在勒索软件攻击后被迫关闭内部网络。这种情况并非例外——根据NTT安全公司2019年全球威胁情报报告，制造业是网络犯罪攻击最常见的目标之一：

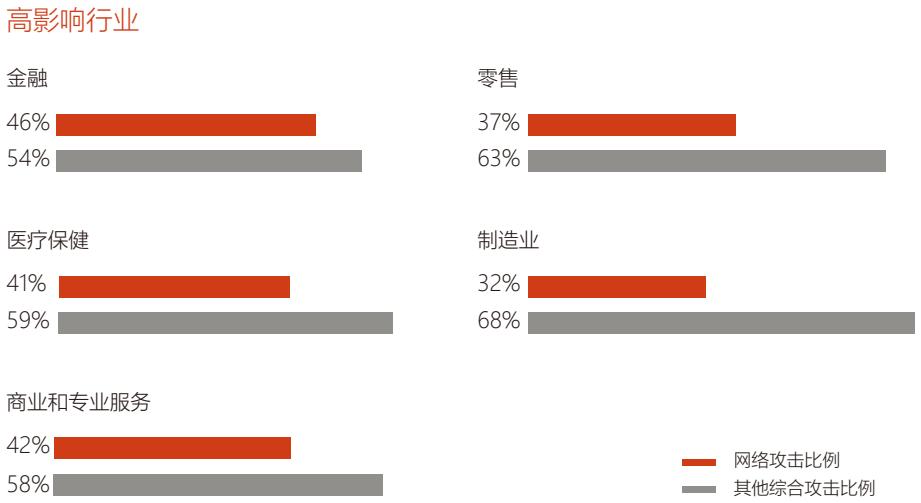

Figure 1 - Threat Impact by Industry

根据IBM2019的X-Force威胁情报指数，加密劫持是另一种普遍存在的恶意软件威胁，在2018年激增了450%。感染加密劫持恶意软件的服务器和工作站被用来秘密挖掘加密货币。远程网络罪犯会窃取系统资源（CPU周期、内存、电源和散热系统），降低了系统性能和可用性，由于消耗增加而缩短了硬件操作寿命，以及更高的电力和暖通空调成本。

解决方案

部署一个数据保护解决方案，其中包括基于人工智能和机器学习的行为反恶意软件功能。这些先进技术可用于识别和终止勒索软件（包括零日攻击）和加密劫持等高优先级的威胁。

3 工厂缺乏熟练的IT支持员工

2018年企业战略小组（Enterprise Strategy Group）的一项调查报告显示，26%的受访企业认为，备份和恢复是其组织中因IT技能短缺而受到阻碍的一个领域：制造业也不例外。具有有限IT技能的工厂IT工程师在从备份中恢复故障机器只能依靠纸面的说明。

> 部署数据保护解决方案...为整个工厂环境启用按钮式备份和恢复。

解决方案

部署一个数据保护解决方案，使任何管理员或员工都可以轻松管理，该解决方案具有自动化功能，可以为整个工厂IT环境启用按钮式备份和恢复。

4 制造环境包括老化的操作系统和应用程序

许多制造应用都是老旧而稳定的。它们很少更新，通常运行在过时的硬件和操作系统上。根据ARC咨询集团的数据，"当今全球自动化系统的安装数字中，有相当一部分至少有20年的历史，并且越来越难以妥善维护，成本也越来越高。"企业战略集团（enterprise strategy group）2018年的一项调查显示，31%的企业SSE，数据备份和恢复现代化是他们打算投资最多的领域。

使这些应用程序及其底层操作系统和硬件保持稳定状态的必要性使数据保护复杂化。有意识地选择不安装新的操作系统修订版或应用修补程序会打开各种恶意软件攻击可利用的安全漏洞。

解决方案

部署一个数据保护解决方案，可以在必要时将任何物理、虚拟或云平台（运行任何操作系统和应用程序工作负载）恢复到不同的硬件。

5 缓慢的数据保护是劳动密集型的，会产生不完整的备份。

制造业中使用的传统数据保护解决方案通常需要大量的人工干预和大量的工时来操作。停电直接减少了生产时间，增加了直接的劳动力成本。缓慢、劳动密集型的备份操作可能会导致备份周期和数据保护方面的漏洞。当组织确实遇到系统故障时，恢复过程通常是复杂的、多步骤的、易出错的，并且可能会充满数据漏洞。

> 有意识地选择不安装新的操作系统修订版或应用修补程序会打开安全漏洞。

解决方案

部署一个高性能数据保护解决方案，其速度足以满足组织的恢复时间和恢复点目标，并具有自动计划的备份计划和快速恢复操作。

6 从备份中恢复太慢

根据infonetics的一项研究，大多数企业平均每月经历两次停电，每次停电持续约6小时。与此同时，《工业周刊》报道称，从传统备份中恢复数据是一个漫长、高度手动的过程，需要数小时甚至数天才能完成。

> 部署高性能数据保护解决方案可以在几分钟内而不是几小时内恢复故障系统，并可执行裸机和自动恢复操作。

虽然诊断问题和确定是否需要恢复系统需要花费时间，但由于恢复过程本身很长，通常会导致大量额外的停机时间。在某些情况下，较旧的备份和恢复技术可能需要数小时才能恢复单个出现故障的系统。

解决方案

部署一个高性能的数据保护解决方案，该解决方案可以从备份中快速恢复出现故障的系统（最好在几分钟内，而不是几小时），包括执行裸机和自动恢复操作的能力。

7 备份操作太慢，无法满足允许的备份窗口

在工厂环境中，找到执行备份操作的合适时间段是另一个挑战。这是因为许多生产系统需要全天候运行，因此很难安排备份时间。这些生产环境是严格的管理和他们的计算资源往往是有限的。随着数据量的增长，缓慢的备份操作可能会变得更慢，这使得在计划开始下一次备份之前无法完成当前备份。如果无法适应备份窗口，可能会导致数据保护出现重大漏洞。

解决方案

部署一个数据保护解决方案，该解决方案具有足够的速度在分配的窗口内完成备份，可以与生产应用程序同时运行，对性能的影响最小，如果需要，还可以向辅助服务器或虚拟机卸载备份管理开销。为了减少数据量和执行备份所需的时间，该解决方案还应支持差异备份和增量备份。

Acronis解决制造业的数据保护挑战

Acronis是制造业数据保护产品和服务的领先供应商。其旗舰解决方案Acronis Backup提供了广泛的平台支持、可靠性和简单性的独特组合，可以为制造IT基础架构提供完整的数据保护。

它被全球50多万家公司采用，为21多个平台（包括Windows XP、Linux、Mac、Windows 7、Windows 8、Windows 10和Windows Server）以及虚拟化平台（如VMWare vSphere、Microsoft Hyper-V、Red Hat Virtual）提供了方便、高效、安全的备份。它可以将故障系统恢复到不同的硬件，包括裸机物理服务器及Oracle虚拟机服务器，以及虚拟和云环境。

Acronis Backup包括多个功能，可解决制造业的难题。Acronis Instant Restore通过确保在几分钟内从备份中快速恢复整个系统，减少了停机时间。此外，内置的Acronis主动保护检测并终止勒索软件和密码劫持等高优先级恶意软件威胁，提供基于人工智能的行为反恶意软件防御，补充基于签名的反病毒解决方案。

案例研究： 马夸特使用安克诺斯实现快速恢复

马夸特集团是一家领先的机电和电子开关及开关系统制造商，在美国、中国和印度等四大洲的19个地方经营制造业务。其制造过程的可用性至关重要——任何数据丢失或系统故障都可能导致成本高昂的生产延迟和交付瓶颈。生产数据的快速可用性和较低的恢复时间是高优先级。

> "Acronis Backup是一个安全、简单且快速的备份，可以让我们公司向前迈进一步"
>
> Catalin Dragoman, System Administrator at Marquardt

Marquardt的数据保护负载目前是40兆字节的数据，运行在各种各样的操作系统上的1600个端点上。该公司选择Acronis Backup作为其数据保护，因为它能够快速、可靠地备份和恢复各种系统。它还发现Acronis Bakcup易于部署和使用，节省了系统和网络资源的消耗，并且能够根据需要精确地恢复整个系统或单个文件。

Marquardt的系统管理员Catalin Dragoman说："Acronis Backup是一种安全、简单和快速的备份，自从我们的生产系统的可用性大大提高以来，它使我们的公司向前迈进了一步。"

案例研究：领先的欧洲汽车制造商使用Acronis改进过程控制恢复

一家领先的欧洲汽车制造商希望提高其备份、恢复和数据保护能力，因此采用了Acronis Backup。

先前的解决方案，这家汽车制造商只能在30至60分钟内恢复其系统，这是一个耗时的过程，需要大量的人工干预。每个工厂平均有100个控制系统，每年需要数千个工时才能恢复。生产线维护窗口也有时间限制——有很多时候系统备份无法完成。马夸特还想保护生产过程免受勒索软件日益增长的威胁。

Acronis使这家汽车制造商能够通过备份代理集中备份其所有系统，而不会中断生产操作，所需时间仅为以前解决方案的一半。Acronis Backup提供自动备份，并在出现任何错误时通知IT部门。在几分钟内，操作人员可以恢复任何失败的系统，重新启动它，并使生产线再次运行。如果进程控制服务器损坏无法修复、集成的异机还原（Acronis Universal Restore）可以将其还原到新的替换服务器，甚至是具有不同硬件配置的服务器。同时，内置的Acronis主动保护会自动检测并终止勒索软件攻击，即使系统没有运行最新补丁。

Acronis安克诺斯®

有关其他信息，请访问 www.tieten.cn