WHITEPAPER

Cutting the Cost of Downtime:

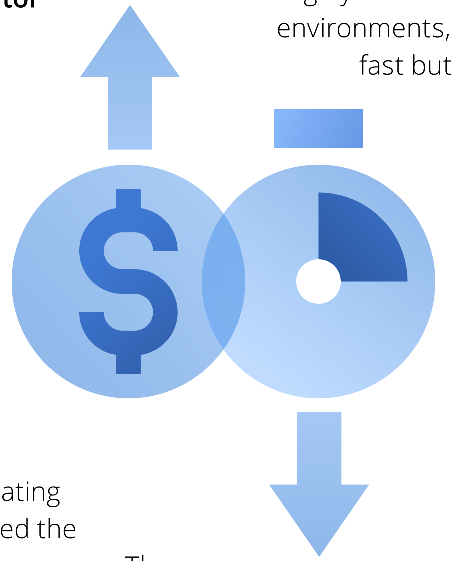
10 Ways Manufacturing IT Can Solve Their Data Protection Problems

How Acronis delivers best-in-class data protection for manufacturers

The Cost of Downtime

The cost of downtime in any industry can be quite high. But for those in manufacturing organizations, where downtime adversely affects hundreds and perhaps thousands of workers, downtime costs are potentially catastrophic.

A recent Aberdeen study puts the average cost of downtime in the manufacturing sector at $260,000 per hour.[1]



Unplanned downtime not only incurs hard dollar costs, but also can slow deliveries to customers and have substantial disruptive effects across the supply chain. When downtime occurs, organizations need to do everything possible to get failed systems back up and running quickly.

Full recovery means the factory gets running again exactly as it was before the outage. Repairing equipment, remediating a cyberattack or fixing the fault that caused the downtime is only one part of the recovery process. The more complex and often more difficult part is accurately and completely restoring failed application servers, virtual machines, cloud workloads and endpoints. Without a strong data protection solution in place, recovering reliably from backup may take longer than fixing the actual fault.

Preventing costly manufacturing downtime requires backup and recovery solutions that are fast, reliable and easy to manage. This includes creating and maintaining backup plans that make business sense given downtime costs, including recovery point objectives (RPOs, a measure of how much data the operation can reasonably afford to lose in the event of an outage) and recovery time objectives (RTOs, a measure of how long the operation can reasonably afford to be offline).

In highly downtime-sensitive manufacturing environments, recovery from backups must not only be fast but also accurate to a foolproof degree. But such solutions are hardly commonplace.

A recent study by Kroll Ontrack Research found 75% of IT managers could not restore all of their lost data from backups.[2]

The issue is exacerbated by widespread malware strains like ransomware that not only render production data inaccessible, but destroy backups as well, thereby greatly increasing data loss, downtime and associated costs.

Losing data like this is a disaster for a manufacturing organization.

With limited IT involvement in manufacturing systems, it’s easy to overlook critical housekeeping activities like data protection. In addition, many digital manufacturing systems run on old, unique, or unusual software environments, making data protection more difficult with IT tools that can only protect relatively recent-vintage operating systems, apps and data formats.

[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.

Acronis delivers best-in-class data protection for manufacturers

There are numerous options for protecting data. But in manufacturing environments with limited or non-existent IT staff and elevated requirements for fast recovery, Acronis Backup stands out. It offers the reliability and data integrity required to protect traditional data centers, edge environments, and addresses the specific needs of the manufacturing sector. Further, Acronis Backup can be administered by a non-expert in data protection, eliminating the need for special training or dedicated staff. Acronis also delivers a fully featured, comprehensive solution that protects a broad range of manufacturing IT systems via a single solution.

Ease of use is a major benefit of Acronis Backup, enabling the simple and flexible creation of backup plans for every device in the organization. Backups can be saved locally, to a remote storage, or to the cloud. Local data backups are often desirable to speed recovery from downtime. Support for 25 languages lets offshore employees work in their native tongue to eliminate translation problems.

Ten critical features to protect manufacturing data

To deliver an optimal solution for data protection in manufacturing environments, Acronis Backup delivers ten critical features:

1. **Fast restoration of data** — Integrated Acronis Instant Restore technology makes it possible for Acronis Backup users to restore any server (whether running on a physical, virtual or cloud platform) to live functionality as a newly created virtual machine, enabling the industry's shortest recovery time objectives (RTOs). For example, it is possible to back up a physical Windows or Linux machine and instantly restore it as VMware or Hyper-V virtual machine (VM) in a matter of seconds.
2. **Scheduled and on-demand backups** — The Acronis management console makes it fast and simple to start backups manually whenever needed, or to create backup plans and automate their execution on a recurring schedule. Plus, it offers the flexibility needed to configure backups of machines disconnected from the corporate network. These capabilities significantly reduce the burden on IT operations to manage the backup process, and allows more skilled staffers to focus on strategic projects and other key tasks.
3. **Support for unique and older server environments** — Many manufacturing IT systems (like process control systems and production line management applications) are highly customized and often run on older hardware and operating system versions. The importance of keeping these systems operating in a stable state means that their operating systems cannot be patched or upgraded to later versions. Image-based backup and bare-metal recovery in Acronis Backup allows these systems to be fully protected and recoverable in the event of a system failure of any kind.
4. **Proactive defenses against the most pervasive malware attacks** — The manufacturing sector is one of the most frequent and profitable targets of criminal malware attacks, and the prioritization of system stability over vulnerability and patch management leaves many manufacturing IT systems open to a wide range of cyber threats, including ransomware and cryptojacking attacks. Acronis Backup with built-in Acronis Active Protection technology uses artificial intelligence and machine learning to automatically detect, terminate and restore any damage from ransomware attacks, as well detect and terminate resource-draining cryptojacking attacks.

5. **Hardened backups** — Many types of modern malware, notably ransomware, are designed not only to infiltrate and compromise production servers, but also to damage or destroy the backup agents and backup archives needed to recover from a malware attack. The tactic is effective: if the victim is unable to find a viable recent backup, it will be more willing to pay the online extortionist for the decryption key necessary to unlock their data. The Acronis Backup agent, backup archives, and cloud infrastructure are hardened specifically to defend against these kind of malware attacks, thus ensuring the ability to recover from any attack on production systems.

6. **Full image backup** — Acronis Backup delivers true image-based backup, creating block-by-block copies of the entire storage medium, providing the most complete protection of the source system. This approach enables the move to new hardware if necessary, and ensures the shortest recovery time without the need to reinstall operating systems, applications and configuration files before returning to production mode.

7. **Off-host backup management** — The manufacturing industry's need for tight RPOs and RTOs can present processing challenges for aging servers running on old hardware. These older systems may struggle to perform their primary duties and also simultaneously run backups, leading to missed backup windows and potentially costly data protection gaps. Acronis Backup offloads backup management process like backup replication or applying retention policies to other machines, freeing up precious CPU cycles and memory on the productions systems. In effect, it takes less time to complete backup cycles and closes data protection gaps.

8. **Bare-metal restore** — The punishing cost of manufacturing downtime places a premium on any feature that can speed up recovery from a production server outage. One way to achieve this is to recover from backup to a "bare-metal" system, i.e. a server with no operating system or other software installed or configured. Acronis Backup enables the recovery of a failed server to a bare-metal target in one very fast operation, including the source system's operating system, applications, configuration settings and data. This avoids the costly, time-consuming process of reinstalling and reconfiguring those components before returning to live production status. It also enables a foolproof way to recover quickly from a malware attack: simply restoring the compromised system using a clean image created before the attack.

9. **Restoral to dissimilar hardware** — Another way to shorten production outages is to recover a failed server to any new hardware that happens to be on hand, which meets the baseline performance specs. But restoring a backup image to dissimilar hardware can cause boot failures due to incompatibilities between the new hardware and the source image (typically of boot media, storage controllers, and network interfaces).

   Acronis Universal Restore is another technology integrated into Acronis Backup — it erases these incompatibilities during the restoral process by automatically inserting the necessary boot image, storage drivers and network drivers. This allows the source system image to very quickly and automatically boot up and run on the new hardware without further reconfiguration or other operator intervention.

10. **Support for virtual environments** — Most manufacturing environments now embrace the use of physical servers as well as VMs running on-premise, in private clouds, and on public cloud services. Manufacturers have to protect all of these different platforms. But there are also distinct advantages in performance and uptime with the ability to move workloads between platform types, e.g. to recover a physical server to a VM for an extremely fast return to live production, or to move a VM server image onto a public cloud service for disaster recovery purposes. Acronis Backup enables the complete protection of physical, virtual and cloud platforms, and makes moving workloads between them easy, fast and reliable.

Conclusion

Unplanned downtime in manufacturing environments is a threat to business profits, customer relationships, company valuation, and the careers of IT professionals charged with protecting systems. Manufacturing IT environments have specific demands that cannot be compromised — namely the need to protect aging legacy systems like specialized process control servers, the high costs of downtime, the growing threat of malware, and the importance of fast, seamless recovery from outages. These demands often present insurmountable problems for data protection vendors.

Fortunately, Acronis Backup delivers an advanced, integrated approach to data protection that ensures the unique combination of performance, breadth of platform support, and ease of operation that manufacturers need to keep their IT operations running reliably.

For more information, please visit www.acronis.com/business.

Acronis Backup

TRY NOW