Bacula Module for Microsoft 365: Fast, Automated Backup and Recovery

Bacula Enterprise Edition

Microsoft 365 is a cloud-based software solution offered by Microsoft as a service (SaaS). This white paper presents how to correctly and safely back up and protect elements of Microsoft 365 services using Bacula Enterprise.

In addition to the technical capabilities of Bacula Enterprise, it should be noted that Bacula's Microsoft 365 module comes with a disruptive licensing model specifically for MSPs and large organizations, allowing them to deploy Bacula's technology for a fraction of the cost of other vendors.

Version 1.0, June 1, 2021

Companies across industries are modernizing their data platforms, and an important part of this trend includes the ongoing adoption of SaaS solutions. Microsoft 365 is a cloud-based software solution offered by Microsoft, as a service (SaaS). It is one of the most used SaaS solutions for providing services such as mailboxes and collaboration solutions among many others, and is intended to be used by customers who want to externalize their businesses services such as email, collaboration, video conferencing, file sharing, and others.

The misconception about Microsoft 365 capabilities

Unfortunately, even though Microsoft 365 is widely used in business, the problem of information security – especially data backup and recovery strategies – is as relevant as ever. It's not uncommon for a lot of companies to have few or poorly defined plans in regards to data protection for their Microsoft 365 and other SaaS-related systems. Many users find themselves relying upon Microsoft's built-in capabilities, despite operating in an enterprise environment. Some users simply hope for the best, or blindly trust the SaaS provider to deliver advanced backup and recovery services if needed. Still others confuse Microsoft's Service Level Agreement with backup strategies.

What's the problem with Microsoft's existing backup and recovery services?

Microsoft 365 is not in itself an enterprise-grade data backup and recovery solution. As such, it may likely fall short in adequately safeguarding data created and used in common enterprise circumstances. These enterprise-typical circumstances nearly always create the need to address certain challenges, for example:

- Internal organization accidents or mistakes
- External security threats such as ransomware
- Compliance and other legal requirements
- Retention policy requirements
- Accidental deletion of 365 data
- API lock-in, or API changes by the SaaS provider

The difference in responsibilities

To know the correct approach to backing up an organization's cloud data (especially when it comes to Microsoft 365), it is important to understand the difference between Microsoft's responsibilities and a user organization's responsibilites when using Microsoft 365. Here is a general overview of the responsibilities of Microsoft towards the Microsoft 365 user:

- Microsoft 365's main responsibility is to provide an uptime-related cloud infrastructure and SLAs for higher availability.
- Microsoft 365's data replication capabilities are basic, at best – including both Recycle Bin for short-term data recovery and geo-redundancy feature.
- Microsoft 365 handles the role of a data processor when it comes to interacting with the client – handling industry compliance certifications, data privacy, regulatory controls, etc.
- Microsoft 365's security responsibilities exist only at the physical infrastructure level, as well as logical security, app-level security, and various controls for both administrators and regular employees/customers.

One can further discern the differences between the responsibilities of Microsoft and the responsibilities of a customer in question, based on the framework above:

- Accessing data that resides inside Microsoft 365 and controlling it is the ultimate responsibility of a customer since it is that customers' business data.
- It is a customers responsibility to ensure the enterprise-level data retention and backup capability for their data, as Microsoft's capabilities in this field are severely limited. This includes point-in-time recovery, granular recovery, and many other features.
- A customer has the role of a data owner in their interactions with Microsoft 365 – meaning their data is their own responsibility, both in terms of various external regulations, as well as for internal legal and/or compliance requirements.
- Protecting business data from both internal (insider threat, accidental deletion, etc.) and external (ransomware, malware, and more) threats is the sole responsibility of a customer, not Microsoft.
- It is the enterprise's responsibility to manage risk mitigation from having – or not having – a dedicated, independent backup strategy.

Organizations that do not address the above points are exposing themselves to a number of potential risks and/or threats by not having a third-party backup system.

There are three main types of risks that can be identified:

- Regulatory compliance and retention. While Microsoft does offer its own form of retention policy (90 days), this is often not enough for some industries with more stringent rules, including healthcare, finance, government, etc. It is also important to have a third-party backup system to be compliant with some of the more strict European data regulations, such as GDPR.
- Little to no data control in mixed deployments. Having no independent backup system means that the organization is likely in a SaaS lock-in situation and has limited control over its own data, and with no exit strategy from a single SaaS in the first place.

- Security breaches and data loss as a whole. Both internal and external threats still exist for Microsoft 365, despite the fact that it is a well established cloud platform. Internal threats are always present, for example accidental or even malicious data deletion, corruption or loss. External threats, on the other hand, may come from direct network attack, ransomware and other malware. Unfortunately, the high growth in cloud use by the enterprise sector has partly led to a similar rise in the number of companies that are exposed to some sort of malware or ransomware event, and the ever-increasing amount of unrecoverable data incidents is alarmingly high.

Another problematic point in this context is the dual existence of on-premise and SaaS data and applications in some companies. There are also cases of mergers and acquisitions, with different teams not using a unified version of collaboration or email suite, making it harder to work without a unified backup system in place. Often, Microsoft 365 adoption can be greatly simplified by having a unified backup system in place.

Reasons to back up Microsoft 365 data

Despite the fact that Microsoft 365 as a whole is a broad and capable platform, it typically does not offer enough to fully cover many problems and threats that arise in a large enterprise that needs constant access to its data at all times.

Below are six of the most prominent problems, and why they are critically important to most enterprises:

External threats to an organization's security

Some decade-old security threats are still as common today as they were ten years ago, with both malware and ransomware increasingly capable of bringing severe problems to a company that does not have high enough levels of security. There are many ways that external threats can penetrate a company's network, applications and data. In this case, a dedicated comprehensive backup solution can act as a safeguard in case of a resulting scenario where an organization has to restore all or a some of its data from scratch.

Internal threats to an organization's security

While the majority of people perceive external hackers as the main problem for an organization's security, there are a significant number of incidents that happen due to a company's own employees, either on purpose or accidentally.

In a large company, it can be hard to keep track of everyone's permissions and capabilities, which may create opportunities for people with dishonorable intentions. Microsoft does not necessarily discern between a regular employee and a terminated one, which can leave a lot of back doors inside the system for ex-employees.

At the same time, it's not uncommon for users to create significant problems for its company unintentionally; by either downloading an infected file or leaking credentials that can be used to access the company's internal network. This can be somewhat mitigated by attaining a certain level of education of the employees, but it is better

to not leave anything to chance by having a number of safeguards in place, including a dedicated backup system.

Deletion by accident

Geo redundancy can be both a blessing and a curse. Even unintentional deletion of a single user can be quickly replicated throughout an entire network, effectively damaging the ability to restore them. While there is an option that Microsoft 365 offers called 'recycle bin', as well as limited versioning, it still won't help an organization to restore something that was permanently deleted by accident. On the technical side, there are two types of deletion that exist inside of Microsoft 365 as a system – hard deletion and soft deletion. As the name suggests, soft delete implies at least some way of restoring deleted files, even if inconvenient. On the other hand, hard delete purges the file in question entirely from the system, with no way to reverse it. There is no real built-in point-in-time recovery for Exchange 365, and recoveries of partially deleted files are limited to 30 days. Point in time recovery for OneDrive/Sharepoint is limited to 30 days from deletion. It is important to know that only a third-party backup solution can work as a safeguard to someone hard-deleting an important document by accident.

Compliance and legality

Legal action is something that can bring unusual or unexpected requests that a business might not be capable of meeting; the same goes for compliance requirements. Having a third-party backup system typically makes it much easier to retrieve such data, even if the original copy was already deleted for some reason. Unfortunately, Microsoft's capabilities in this area are severely limited, despite a few safety nets such as 'Litigation Hold', or 'In-Place Hold'.

Retention policies

As a consequence of a quickly-developing digital age, various retention policies tend to develop remarkably fast too, and it is sometimes problematic to keep up with them. Microsoft 365's capabilities in this field are also limited and would not replace a comprehensive backup solution's capabilities in this respect.

Microsoft's own capabilities in terms of data retention are represented by their 90-day data storage policy and little more – which is more than problematic for some specific fields of work with strict data compliance requirements. It is not possible to align data protection of Microsoft 365 services to general retention periods or policies longer than 30 days. There is no automated way to extract any data from the cloud to save it in external places (this could lead to eventual compliance problems). A dedicated backup solution is clearly one of the best ways of keeping an organization from breaching policy or compliance requirements.

Hybrid deployment management

Microsoft 365 adoption itself is also a notable topic in this context, since this kind of adoption usually requires some sort of a transition window and process to transfer all of the data from the on-premise storage to an online one. There are even cases

of companies leaving part of their legacy physical data to have more flexibility and control – which is a challenge to handle from a management standpoint. One of the safest ways to work around that is by using a flexible backup solution that treats both data forms the same way.

Choosing a third-party backup solution

Data protection as a whole is capable of solving a number of potential issues and threats to Microsoft 365 data, from compliance issues and business continuity threats to security vulnerabilities and data loss. Having a basic backup system in place is typically no longer enough for a medium or large enterprise, and that includes SaaS.

Nowadays it's not uncommon for data protection vendors to extend their services towards Microsoft 365. However, there are several important features that should be checked before opting for a solution intended to be an organization's primary source of data protection and backup:

Specific features . Granular recovery, policy-based retention, incremental backup, and automation capabilities all should be included in the solution.

Additional security . Multifactor authentification, access control, and SaaS usage statistics go a long way towards improving the overall security of a company.

Flexibility . The solution must provide the freedom to choose between using another or multiple clouds or existing on-premise capacity for backups and restores.

Scalability . Capability to scale both up and down to meet future business demands and the potential to roll out SaaS throughout the company.

The breadth of capabilities . Hybrid deployment management is also strongly recommended to make SaaS adoption easier.

Integration with Microsoft 365 . The solution should be capable of deeply integrating into both Microsoft 365 and the organizations' other existing IT technologies and environment(s).

Bacula's backup and recovery module for Microsoft 365 is very easy to deploy and configure, and supports the following M365 services:

- OneDrive
- Emails
- Mailbox settings
- Sharepoint Online
- Calendars
- Contacts
- OneNote

Bacula ships with advanced parallelization, resiliency, automation and flexibility features and is designed to cover practically all possible M365 use case scenarios. Below is a full feature list:

Common features:

- Microsoft Graph API-based backups
- Multi-service backup in the same task
- Multi-service parallelization capabilities
- Multi-thread single service processes
- Generation of user-friendly report for restore operations
- Network resiliency mechanisms
- Latest Microsoft Authentication mechanisms
- Discovery/List/Query capabilities
- Restore objects to Microsoft 365
  - To original entity
  - To any other entity
- Restore any object to filesystem
- Incremental & Differential backup
  - Advanced delta function for improved performance (for selected services)
- Backup and Restore of Exchange Online Mailboxes[1]
  - Mailfolder, message and attachment granularity for restore
  - Email addresses and mailfolders selection capabilities for backup
  - Mailbox settings protection
  - Folder rules protection
  - Restore objects to Microsoft 365 or to any file-system
  - Restore MIME messages to any filesystem
  - Incremental & Differential backup
  - Support for user mailboxes and shared mailboxes
- Backup and Restore of OneDrive for Business & Sharepoint Document libraries
  - Backup and Restore of User drives
  - Backup and Restore of Groups drives
  - Backup and Restore of Sharepoint document libraries

[1]Email/Mailboxes module is currently provided only on request. It will be fully supported in future versions of Bacula Enterprise Edition Microsoft 365 Plugin where new features will be also added around this module.

        - Include/Exclude system libraries
        - Include/Exclude hidden libraries
    - Backup main entity drive unit, but also any other unit
    - Advanced selection capabilities
        - Target entities (Users/Groups/Sites)
            - List Include/ List Exclude/Regex include/Regex Exclude...
        - Folders selection capabilities for backup
            - List Include/ List Exclude
        - File selection capabilities for backup
            - Regex include/Regex Exclude...
        - Drive unit selection capabilities
    - Folder and file granularity for restore
    - Computed hash check at backup and restore time
    - Backup and restore of permissions shares
    - Backup and restore of shared elements to each entity
    - Backup and restore of OneDrive file versions
- Backup and Restore of Sharepoint Sites
    - Backup of Site Objects (MS Graph Object)
        - Backup Site Sharing permissions
    - Backup of full Site Templates (PnP Powershell Provisioning):
        - Site metadata
        - Lists metadata
        - ListItems metadata
        - WebPages metadata
        - DocumentLibraries metadata
        - Support for Sub-Sites
    - Restore backed up sites as new sites using Site Template (PnP Powershell Provisioning)
    - Backup/Restore Lists Objects (MS Graph Object)
    - Backup/Restore ListItems (MS Graph Object)
    - Backup/Restore Document Libraries Drive Items
- Backup and Restore of Contacts/People
    - Backup/restore groups of contacts
    - Backup/restore Contacts
    - Backup Organizational contacts (Read-only)
- Backup and Restore of Calendars
    - Backup/Restore Calendar groups
    - Backup/Restore Calendars

        - Calendar permissions
    - Backup/Restore Events
        - Support for Attachments
            - File Attachments
            - Reference Attachments
            - Item Attachments including MIME objects
- Backup and Restore of Onenote
    - Backup/Restore of Notebooks
        - User notebooks
        - Site notebooks
        - Group notebooks
    - Backup/Restore of SectionGroups/Sections
    - Backup/Restore of Pages
        - Support for Page resources: images and files

Below is shown a simplified vision of the architecture of Bacula Microsoft 365 module inside a generic Bacula Enterprise deployment:

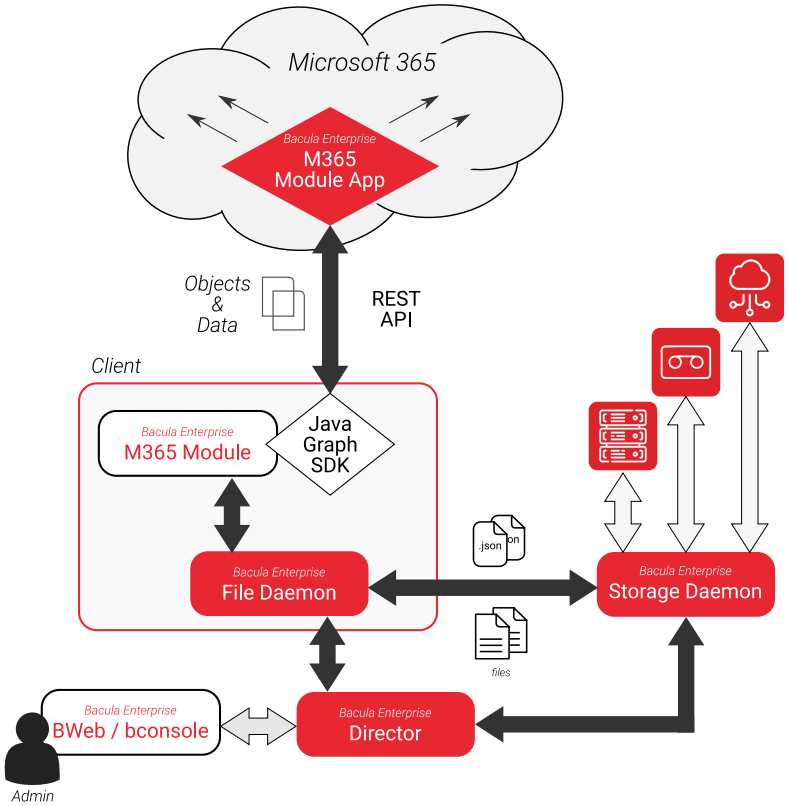

Figure 1: Microsoft 365 module architecture

Please contact Bacula Systems for an exhaustive list of all information types that can be protected using Bacula's module. When the module works with objects containing additional data (MIME files for messages, data for attachments and files of OneDrive, etc), that data is also backed up. Bacula can also provide precise details on the module's services and special features for each of Microsoft 365's separate services.

Technical and Demanding IT Environments

Bacula is unique in its combination of functionality, scalability and reliability. Its broader technology includes Snapshots, advanced deduplication, single file restores, single mailbox restores and data verification, all in one cloud-agnostic platform effortlessly spanning both physical, virtual, container and Cloud environments. Organizations using Bacula's Microsoft 365 module can also use Bacula's broader tools and features to further exploit and improve Microsoft 365 backup and recovery where possible, helping to maximize efficiency, speed and security across the entire organization.

Bacula Enterprise is enhanced by a constantly growing number of modules that delivers faster data recovery and minimal downtime to an IT infrastructure. These modules include PostgreSQL, MSSQL, MySQL, Oracle, SAP HANA, Sybase, Hadoop, NDMP, NetApp, Delta, SAN Shared Storage, VMware, KVM, Hyper-V, Xen, Proxmox, Docker, Kubernetes, Bare Metal Recovery, VSS, Active Directory and of course high performance Deduplication. It also offers native hybrid cloud integration, via S3, S3-IA, Azure, Google Cloud, Oracle Cloud and Glacier interfaces. Despite integrating with such varied and large environments, Bacula automates security to protect the overall environment and data. Its tight access control and centralized authentication mechanisms are essential for the larger, more demanding IT environments of today and tomorrow.

Some of the additional features available with Bacula Enterprise are:

- Centralized data control
- Highly configurable, especially for clusters, multiple OS's, disk, tape, virtual tape, robotic libraries and Cloud
- Scalable from a few machines to many thousands
- Simple onsite and off-site replication
- Bare Metal Recovery for both Linux and Windows platforms
- Deduplication at both the client and storage levels
- Integrated Snapshots and Virtual Full
- VM Performance Backup Suite for integration with many different types of hypervisors
- Natively integrated support for Docker (and its external volumes) and Kubernetes, including persistent data
- Continuous Data Protection

- Client behind NAT (for backing up remote devices)
- Especially broad compatibility with tape technologies

The diagram below gives a broad overview of some of the many technologies for which Bacula offers native integration

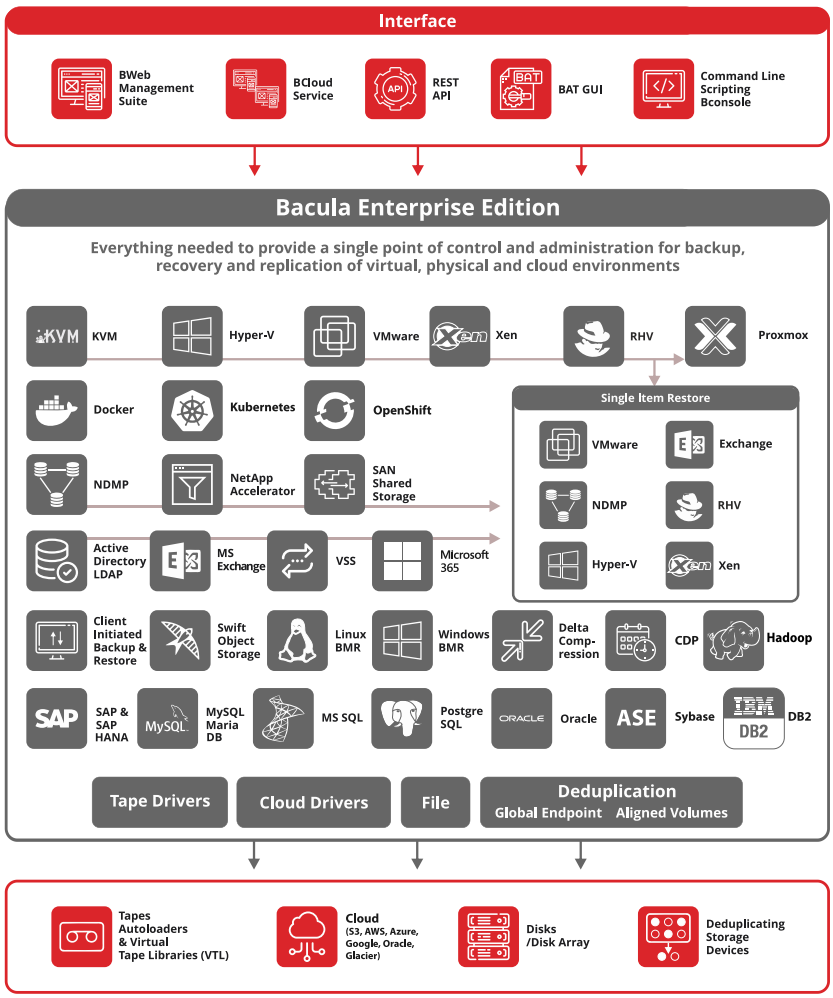

Figure 2: Bacula Enterprise's Feature Set

Ransomware

Backup and recovery is an IT department's last and most critical line of defense. Bacula anticipates the number of Ransomware attacks to increase dramatically. Where criminals extort money from companies is by encrypting their data so the

company can't use it – and avoiding this situation is so much easier if the company under attack has effectively protected backups it can access and restore easily.

It may be initially difficult for an IT department to detect a Ransomware attack; first incursions can be, in practice, nearly undetectable. But once the malware starts encrypting, a good backup software should know, via detectable changes such as increase in File Change Rates, backup size increases, many file name changes, files vanishing and new ones appearing. All of this is tracked by Bacula and can easily be detected and reported. **Bacula offers an especially robust architecture and feature set to protect against Ransomware**, however, there are also some basic best practices that should be observed by any IT department:

- Use Different Credentials; User context for accessing the backup storage should be completely confidential.
- Access permissions are essential – don't rely on user accounts of file system access control, use dedicated services
- Make offline storage part of your strategy; This is one of the best defenses against propagation of ransomware
- Be sure to use the 3-2-1-1 rule.
- Do not rely on different file systems to protect backup storage; more sophisticated types of Ransomware are coming. **Please contact Bacula Systems for its ransomware white paper**.

Deduplication

IT organizations are constantly being challenged to deliver high quality solutions with reduced total cost of ownership. One of those challenges is the growing amount of data to be backed up, together with limited time to run backup jobs (backup window restictions).

Bacula Enterprise offers several successful ways to tackle these challenges, one of them being Global Endpoint Deduplication, which minimizes network transfer and Bacula Volume size using unique deduplication technology. Certain types of data structure can present the opportunity for immense savings in time and disk space. Certainly with Microsoft 365, and its clear emphasis towards text-based data, there are opportunities to make huge space and time savings using Bacula's patented deduplication technology. Bacula offers two different approaches to deduplication:

Aligned Volumes

Bacula Systems' first step in deduplication technology was to take advantage of underlying deduplicating filesystems by offering an alternative (additional) Volume format that is aligned on specific chunk boundaries. This permits an underlying file system that does deduplication to efficiently deduplicate the data. This new Bacula Enterprise Deduplication Optimized Volume format is often called "Aligned" Volume format. Another way of describing this is that we have filtered out all the metadata and record headers and put them in the Metadata Volume (same as existing Volume format) and put only file data that can be easily deduplicated into the Aligned

Volume. Since there are a number of deduplicating file systems available on Linux or Unix systems (ZFS, lessfs, ddumbfs, SDFS (OpenDedup), LiveDFS, ScaleDFS, NetApp (via NFS), Epitome (OpenBSD), Quantum (in their appliance),..., this Bacula Aligned Volume implementation is designed to enable users to choose the deduplication engine they want to use. More information about Deduplication Optimized Volume Format can be found in Bacula Systems' DedupVolumes whitepaper, available on request.

Global Endpoint Deduplication

Bacula Systems' latest step in deduplication technology is to offer the Global Endpoint Deduplication feature. With Global Endpoint Deduplication, Bacula analyzes data at the block level, then Bacula will store only new chunks in the deduplication engine, and use references in standard Bacula volumes to chunks stored in the deduplication engine. The deduplication can take place at the File Daemon side (saving network and storage resources), and/or at the Storage Daemon side (saving storage resources).

Clearly, the benefits of Bacula's native deduplication technology – which typically equate to very important and significant savings when applied to large M365 environments (due to the typical nature and structure of its data) should be taken into account by large organizations seeking to significantly improve the efficiency of their storage and data management.

Conclusion

Making use of Bacula's module for backup and recovery of Microsoft 365 brings high-end enterprise-level backup and recovery features to organizations that need enterprise-grade protection; not only of its Microsoft 365 data, but its entire IT infrastructure. Bacula's wide range of features, together with its broad compatibility with IT environments makes an organization far less vulnerable to data loss, significantly reduces Business Continuity threats, and significantly helps towards an organization having complete and unrestricted control of its own business data. Bacula Enterprise is designed to facilitate positive change within an IT infrastructure. Its especially broad compatibility with other technologies helps remove barriers, while its modularity and flexibility help improve agility, and speeds new capabilities into the IT environment.

In an organization's IT departments(s) where new policies, processes and culture change are planned – or even in process – Bacula's flexibility and resilience enable IT leaders to future-proof the backup and recovery aspect of their strategy, while at the same time exploit the overall significantly lower risk that Bacula's architecture represents for new deployments.

Bacula's Microsoft 365 module comes with a disruptive licensing model specifically for MSPs and large organizations, allowing them to deploy Bacula's technology for a fraction of the cost of other vendors. Bacula's game-changing pricing model for Microsoft 365 allows large organizations and MSPs to make enormous savings, and means every MSP now has a new opportunity to enhance its product portfolio and profitability. Contact Bacula now for more information.

Bacula's approach allows organizations to protect more environments, with more security, much faster and with lower risk than they ever have before.

For More Information

For more information on Bacula Enterprise Edition, or any part of the broad Bacula Systems services portfolio, visit www.baculasystems.com.

Rev : 299 V. 1.0
Author(s): J