SOLUTION BRIEF

Ransomware proof your backups

Nutanix Mine *with HYCU*

HIGHLIGHTS

Backups to WORM enabled target:
Combat ransomware and other malicious attacks with HYCU's detailed support to Nutanix Mine's WORM enabled object storage.

Security without performance penalty:
Securely protect Nutanix led datacenter components - AHV, ESX, Volume Groups, Nutanix Files, ROBO with zero impact to production.

WHAT HAPPENS WHEN AN INEVITABLE RANSOMWARE MEETS AN IMMUTABLE BACKUP?

Ransomware attacks have become increasingly prevalent and pose a significant threat to businesses in all verticals. Imagine a healthcare organization unable to access their patient records and appointment schedules or a bank unable to access their customer's financial records. Well, you don't have to imagine it because ransomware attacks have increased by 238% taking advantage of the COVID 19 crisis, as if things can't get any worse. More than a quarter of attacks this year have targeted either the financial or healthcare verticals.

A company of any size should have several safeguards and policies in place, such as an antivirus and antispam solutions, disabling macros, keep all systems updated and provide a highly restrictive internet access. However, cyber perpetrators have become increasingly sophisticated and are extremely perseverant. They always find a way to break into the system and all it takes is for a single user to take the bait. This means, it's not a matter of whether your organization will be attacked, it's simply a matter of when.

With that being said, an inevitable ransomware attack doesn't mean its game over. You can check out our Nutanix technical brief that showcases how customers can detect, prevent and recover from a ransomware attack. One can architect a robust backup strategy to recover from any form of (locker or crypto) ransomware attacks. HYCU paired with Nutanix Mine can help to secure your backups using three simple techniques:

1. Immutable storage
2. Isolated backups
3. Inhibited access

Immutable storage:
What if a user or a malware, even with admin rights, couldn't delete or modify any of the backups? This is only possible by writing primary backups to WORM enabled S3 Object storage in the most efficient manner. WORM (Write Once Read Many) enabled S3 Objects, ensures 100% data immutability until its expiration time. This means even administrators won't be able to modify or delete any backups until its retention time is up.

NUTANIX

End-to-end encryption:
Achieve native encryption during data-transit and encryption at-rest of all data backed up to Nutanix Mine secondary storage.

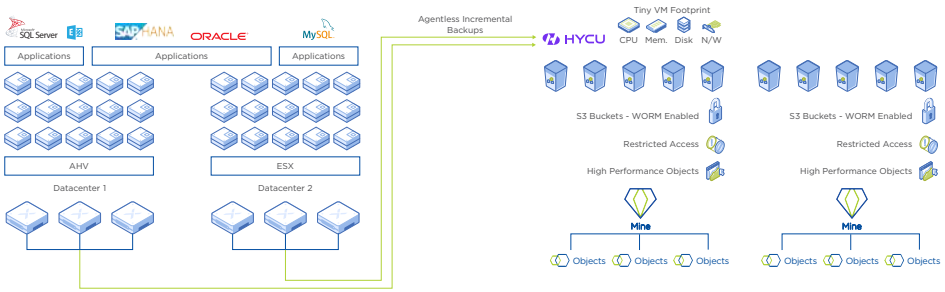
Air-gapped at every level:
From detailed network segmentation of management and data paths to restricted access to Nutanix Mine buckets.

Robust Access Control:
Empower end-users and applications owners with task-delegation, while maintaining strict rules to access their authorized resources.

The ultimate cost-efficient combo:
When Nutanix Mine and HYCU are combined together, you get a high-performance, simple, scalable and secure data protection solution.

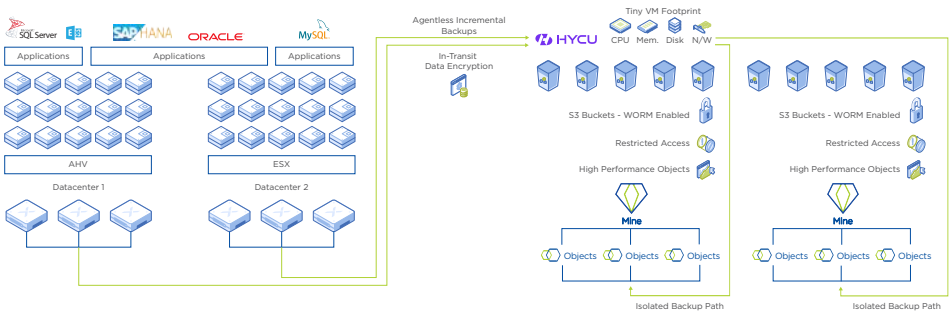
While, the security features of S3 Object storage are indeed promising, most of the backup vendors in the market today treat Object storage as a secondary or tertiary backup target as a cheaper alternative. These vendors can't perform regular incremental backups to Object Storage and only restrict them to secondary copies or archives. This is due to the common misconception of Object storage's inability to deliver satisfactory backup performance as a primary backup target.

This is where the Nutanix Mine *with HYCU* comes into picture. Nutanix Mine (powered by Nutanix Objects) is known for its cost-efficiency, simplicity, scalability, high performance and WORM support. With HYCU's proprietary write optimization of incremental backups, copies and archives to Object Storage and its built-in backup security features (described further below), the cost-efficient combo of Nutanix Mine and HYCU hits into ultimate overdrive. This ensures instant recovery of files, VMs, file shares and applications from the most recent uncorrupted backup version, with a minimum backup RPO of one hour.



Isolated backups:
As the name implies, you simply isolate the backups from your regular production environment, also known by the term air-gapped backups. This means, no user, process, application or server should have access to the network and the data-storage device storing the backups, except for your HYCU backup server. The HYCU virtual appliance is treated as a black box, as it is based on a security-hardened CentOS Linux image with no root access, and an option to disable SSH access.

You need a data-protection solution that's simple (i.e. without any complex architecture of media/repository and proxy servers) while at the same time easily provision logical networks to dedicated backup targets, with in-transit encryption that's siloed totally from your production environment. This will ensure backups from ever being discovered by any malware when a production environment is compromised.



NUTANIX™

SUMMARY:

Nutanix Mine *with HYCU* isn't just a cost-efficient solution, but also the most robust and secure data protection solution offered at a fraction of the cost compared to its competitive counterparts.

To summarize, Nutanix Mine *with HYCU* can deliver:

- Backups to WORM-enabled S3 storage with no performance penalty
- Provide network segmentation between desired sources and backup targets
- Deliver robust RBAC, multi-tenancy and more for software-level backup security

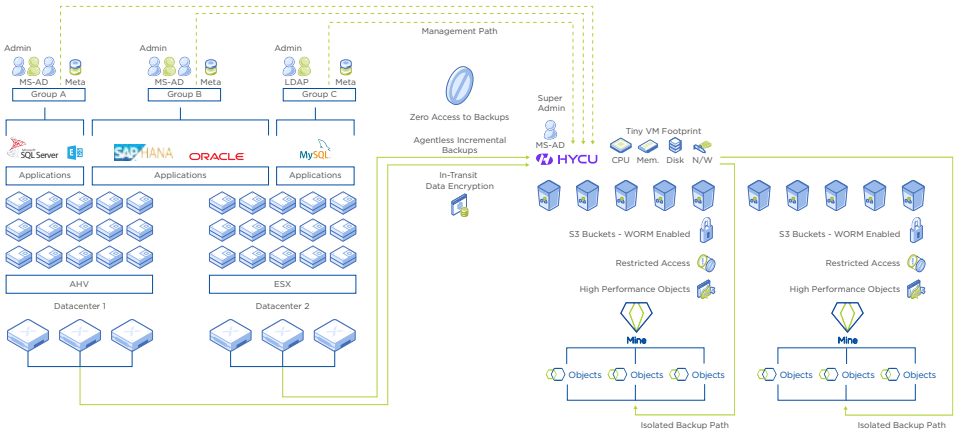
If you'd like to find out more on how Nutanix Mine *with HYCU* can meet your data protection needs, please contact Nutanix at mine@nutanix.com and HYCU at info@hycu.com

Inhibited access:

The access to the backups, network and backup storage should at least be restricted and at best for end users be denied outright. This can only be achieved by a solution that has robust RBAC policies with secure multi-tenancy, that includes seamless integration with multiple AD, LDAP/s domains. Also, care must be taken to ensure that even administrators have no rights to manually delete backups.

With HYCU's self-service and RBAC capabilities, organizations can host multiple groups in a shared environment. Every group's backup metadata, such as restore-points, VM details, application inventory and user-data are stored in secure databases where unauthorized users, even super-admins, cannot access them. This also includes events, alerts and backup reports, that are filtered down to the specific group's authorized resources within the multi-tenant environment.

HYCU disables manual backup deletion to prevent any forms of malicious intent from within an organization. HYCU can also allow administrators to easily pause backup expiration based on policy retention time, to serve during ad-hoc compliance audits or emergencies.



NUTANIX™
YOUR ENTERPRISE CLOUD

T. 855.NUTANIX (855.688.2649) | F. 408.916.4039
info@nutanix.com | www.nutanix.com | @nutanix