proofpoint
365 TOTAL PROTECTION

FACTSHEET
AI POWERED

VM BACKUP

BACKUP AND RESTORE YOUR COMPANY DATA WITH EASE: AT ANY TIME, WITH SPEED AND MASSIVE STORAGE SAVINGS

Hornetsecurity's VM Backup is a powerful, reliable and easy-to-use backup and replication solution for Microsoft Hyper-V, PROXMOX, Physical Windows Servers, and VMware virtual machines (VMs) to protect against enterprise data loss. The award-winning solution provides robust, streamlined and enterprise-level functionality.

HOW DOES **VM BACKUP** HELP YOU?

Immutable Storage – All data is protected from ransomware attacks by leveraging immutable storage.

Augmented Inline Deduplication – Reduces backup storage requirements leading to higher back-up speed and cost savings.

Reliable business continuity – WAN-optimized replication guarantees business continuity.

Your data is secured and protected from ransomware

Reduce downtime and data loss: Thanks to Continuous Data Protection (CDP) and WAN-optimized replication, **your backup files are available in just minutes in the event of a data loss scenario**, and your organization can continue working as usual. Storing **immutable backups** leveraging object locking on **cloud storage locations** gives you additional peace of mind as your backups are protected from ransomware attacks and other malicious actors. The **unique Augmented Inline Deduplication** also results in massive storage savings for your backups and **reduces unnecessary costs**.

KEY FUNCTIONALITY INCLUDES:

Ransomware Protection leveraging Immutable Cloud Storage: Backups are protected using immutable cloud storage, meaning it is impossible for data to be erased or modified by anyone for a set duration. This provides an additional layer of security to your existing backups.

Massive storage savings by using Augmented Inline Deduplication: Common data is only transferred to the backup or offsite location ONCE. Unlike most competitors, the service does not handle this post-process so it immediately ensures that only changed data is sent to the customer's backup repository (rather than removing the identical data after the transfer).

VM BACKUP

KEY FUNCTIONALITY INCLUDES:

Seamless cloud backup to Microsoft Azure, BackBlaze B2, Amazon S3 or Wasabi: Users can simply enter their account details and store their offsite backup copies with their provider of choice. This way, customers can easily make a backup copy of their data direct to Azure, BackBlaze B2, S3 or Wasabi, as well as to a local disk, network path or a Hornetsecurity Offsite Backup Server.

Continuous Data Protection (CDP): Continuous Data Protection (CDP) allows users to back up virtual Windows machines (VMs) as frequently as every 5 minutes ensuring that, should a data loss scenario occur, only a few minutes of data are lost. This dramatic reduction in data loss saves companies time and money while minimalizing hassle.

WAN-Optimized Replication: Replication enables users to be back up and running in minimal time should disaster strike. It enables administrators to replicate ongoing changes on their VMs to a remote site and to seamlessly continue working from the replicated VMs should something go wrong with the live VMs.

Various restore options: Granular restore options are supported for full VM or individual files or emails, enabling file retrieval with a few clicks. It is also possible to restore one or more VMs to a different host and from multiple points in time. Fast OnePass restores and clone restores are also supported.

Instant boot from backup: Users can boot any VM version directly from the backup location without affecting backup integrity.

Backup Health Monitor: Backup Health Monitor proactively monitors the health of the backup storage from the customer to detect any integrity issues with the customers' backup data. If it finds any issues, it will attempt to repair them automatically by backing up the affected data again during the next backup job.

Cross Platform Restore: Allows backups taken for Virtual Machines hosted on VMware to be restored to a Hyper-V host and vice-versa, facilitating migration from one platform to another.

Automatic Configuration of Newly Discovered VMs: A simple way to automatically protect newly discovered Virtual Machines without the need for manual intervention. Users have control over what settings are automatically applied and which VMs are excluded from this configuration. Any manual intervention afterwards will override the automatic configuration.