BACKONLINE: VEEAM BACKUP

ONLINE DATA BACKUP AND RECOVERY: RANSOMWARE PROTECTION

ONSITE BACKUP PROTECTION:

Local backup files are often the first target of recent ransomware, ensuring the attacked company cannot simply recover their encrypted data from local disk-based backups. There are several strategies to mitigate this attack vector locally:

Isolate the backup server and storage:

In the event domain administrator credentials or other privileged account credentials on the domain are compromised, having the backup server off the domain and as logically isolated as practically possible, allows for a fast recovery from local backup files. Whilst this approach is not fool proof, it is the first line of defence against backup compromise. The storage the backups reside on should be similarly isolated, with write access only available from the backup server.

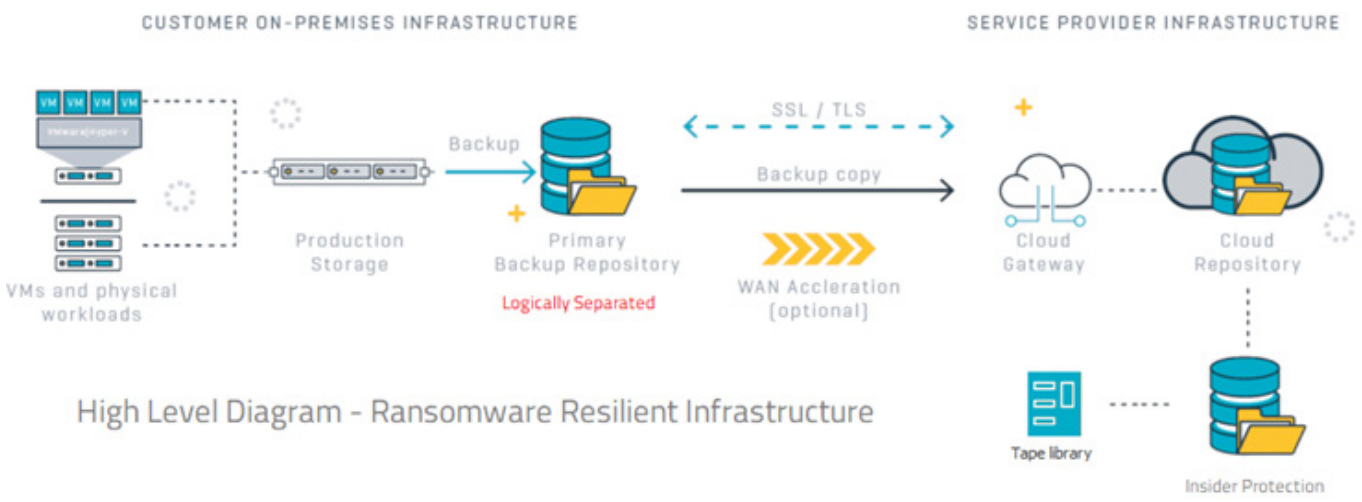
User Rights Assignment:

Domain Admin rights should be restricted, with Role Based Access Controls (RBAC) implemented across the organisation, utilising least privilege principles. Similar policies should be applied to the backup server operating system and the backup software. RBAC can be implemented via Veeam Backup and Replication, with the Veeam Backup Administrator role limited to as few users as possible.

OFFSITE BACKUP PROTECTION:

The sophistication of modern crypto malware means the 3-2-1 rule is more important than ever.

An air-gapped backup is the most effective defence – an attacker cannot access a tape or USB HDD sitting offsite in a vault. However, in most instances where company data and local backups have been compromised, every hour data isn't available is extremely costly & recovery from offsite media can be time consuming.



Cloud based offsite backups can help mitigate this immensely, allowing fast access to critical files, servers & databases. There are instances where these backups can also become compromised however, such as an attacker gaining access to the backup console and deleting cloud-based backups before executing the main attack.

TIMG takes a hybrid approach to mitigate these issues and ensure client data is secure, uncompromised and quickly available in times of crisis. Veeam Insider Protection is implemented on all Cloud Connect accounts, ensuring cloud backups that have been accidentally or maliciously deleted, can be immediately recovered by our support team & transferred to external media (or imported to a TIMG restore only VBR server for fast recovery of critical files/VMs). This functionality is not visible to the end user and 100% segregated from the client network, meaning even a compromised local backup console doesn't affect client recoverability.

timg.co.nz
0800 SECURITY
contact@timg.co.nz

THE INFORMATION MANAGEMENT GROUP