Droplet

DROPLET VS APP PACKAGING–WHAT'S THE DIFFERENCE?

ARCHITECTURE

DROPLET CONTAINERS	APP PACKAGING
EASE OF DEPLOYMENT Droplet container images are self-contained, including dependencies, and are isolated away from the underlying OS.	**OS-SPECIFIC DEPLOYMENT** Packaged apps are factored and locked to a specific host OS. App-V apps require a complex architecture comprising management server, publishing server, reporting server and client. Load balancing can be achieved by installing on multiple servers behind a load balancer. MSIX (appx) packaging only contains the app itself, without dependencies.
COMPATIBLE Droplet containers can run on any architecture that supports the container runtime, including Linux, MacOS and Windows/Windows Server, as well as cloud platforms.	**LIMITED COMPATABILITY** MSIX is only compatible with Windows 10. App-V packages must be configured for specific Windows hosts
Droplet containers run without additional hypervisors or VM layers.	Packaged apps require all the resources of their host OS—or may require a VM to run.
PORTABLE Containers don't require a complete VM as they are self-contained. This results in minimum performance overhead.	**BESPOKE** Major OS upgrades require apps to be reconfigured and repackaged. Apps must also be repackaged for different architectures.
CLOUD-READY Run Droplet container apps on Microsoft Azure or VMware vSphere.	**CLOUD-SPECIFIC** Packaged apps must be custom-built for cloud deployment and often require a VDI platform.

SECURITY

DROPLET CONTAINERS	APP PACKAGING
ISOLATED Droplet containers provide isolation between the app and the host system.	**INTEGRATED** Each packaged application requires its own user space, VM or platform.
Droplet containers are locked down by the NeverTrust™ model.	Packaged apps have the same privileges as other apps on the system.
As Droplet containers are isolated from the OS, one can run multiple instances of the same application on the same host, each in its own container with its own resources.	MSIX packaging includes features such as code signing and runtime attestation to ensure the integrity and authenticity of the package and its contents.
All inbound and outbound traffic is blocked by default: only required traffic is explicitly opened.	Malformed apps can potentially create security holes. Apps are subject to the same vulnerabilities as native apps.
NeverTrust™ model places containerised apps in an isolated environment that is invisible to intruders.	Zero-trust networks, such as Citrix. require authentication-protected access and ongoing intrusion detection.
Regulatory compliance made easy.	Compliance requires additional safeguards to be put in place.

USAGE

DROPLET CONTAINERS	APP PACKAGING
SIMPLIFIED LICENSING Droplet licenses are per container—unlimited apps.	**COMPLEX LICENSING** App packages may require multiple licenses for OS, VM and apps.
SIMPLE SETUP Apps work out of the box—no complex setup required; no special skills required.	**COMPLEX SETUP** Specialised skills to deploy: • App-V packaged apps require isolation groups within a Citrix environment • MSIX/MSIX app attach packaged apps require Microsoft App-V Desktop Client on user devices, which must be enabled on VDA machines
REMOTE WORK FREED Droplet containers can run independently on a device and do not require being logged in to a server.	**REMOTE WORK TETHERED** App packages are delivered by the server, much like VDI, therefore remote users must have a secure internet connection to the server.