Droplet

DROPLET CONTAINERS

Future-proof your business

Windows Server 2012

Planning for Windows Server 2012 & 2012 R2 end of support?
Deploy your legacy applications on the server architecture (or cloud) of your choice.
No compatibility issues. No code rewrites. Multiple layers of security.

If your IT is running as smoothly as it can, with bespoke and/or proprietary software all working as it should, upgrading your server architecture could lead to disruption and—in the worst case—loss of business. With Windows Server 2012 and 2012 R2 heading for end-of-support this year, you may be faced with a few of the following scenarios:

- Rewriting your software to run on a new operating system.

- Purchasing licenses for newer versions of proprietary apps, or switching to entirely new software systems.

- Upgrading your server hardware to run the newer operating system.

- Installing VMs on new hardware to run your apps as an interim measure while awaiting budget for one of the above 'overhauls'.

- Keeping your system running as is, and sign up with Microsoft for Extended Security Updates (ESUs).

- 'Lift and shift' to a cloud service such as Azure, which offers three more years of extended support.

If these scenarios feel like temporary 'fixes,' fraught with security and operational pitfalls, you're right.

There is an alternative: Droplet.

Droplet lets you keep your legacy apps and servers running as they are currently configured, in a containerised environment. No need for hardware upgrades, as Droplet containers run leaner and cooler. Run more apps on the same system, or run multiple containers on one containerised VM.

Moving to the cloud?

Droplet container apps run equally well on cloud services, such as Azure, AWS and Google Cloud.

SUPPORTED PLATFORMS FOR DROPLET SERVER:

Windows Server 2022, 2019, 2016, 2012, 2008, 2003, 2000, NT

Linux: RHEL 6 and upwards

DROPLET IS SECURE

- Droplet provides complete security for your server estate, whether it is based on modern or legacy systems.
- Droplet's NeverTrust™ model isolates servers, and denies all traffic that is not configured inside the Droplet boundary.
- All transit between client and server is encrypted to prevent man-in-the-middle attacks.
- Allow your server estate to become compliant with Cyber Essentials Plus and NIST.
- Droplet is frequently penetration-tested.

Droplet adds layers of security that dramatically improve your security profile.

DROPLET BENEFITS

Simplicity: No need to refactor, repackage or virtualise apps

No retraining: Upgrading to a modern OS can be disruptive

An out-of-the-box solution: No expensive builds or special skills required

Virtualisation support: Droplet containers complement and enable VDI initiatives

Convenience: Legacy applications delivered without refactoring

Freedom of choice: Supported on any platform (cloud or on-premises) including VMware vSphere and bare metal

No hidden costs: No large-scale data-centre hardware overhead costs, no complex VDI infrastructure

Ease of purchase: Available via simplified licensing, and designed for the subscription generation to exclude unnecessary licenses

Simplify digitalisation and migration initiatives

Compliant to government, military, and public sector standards