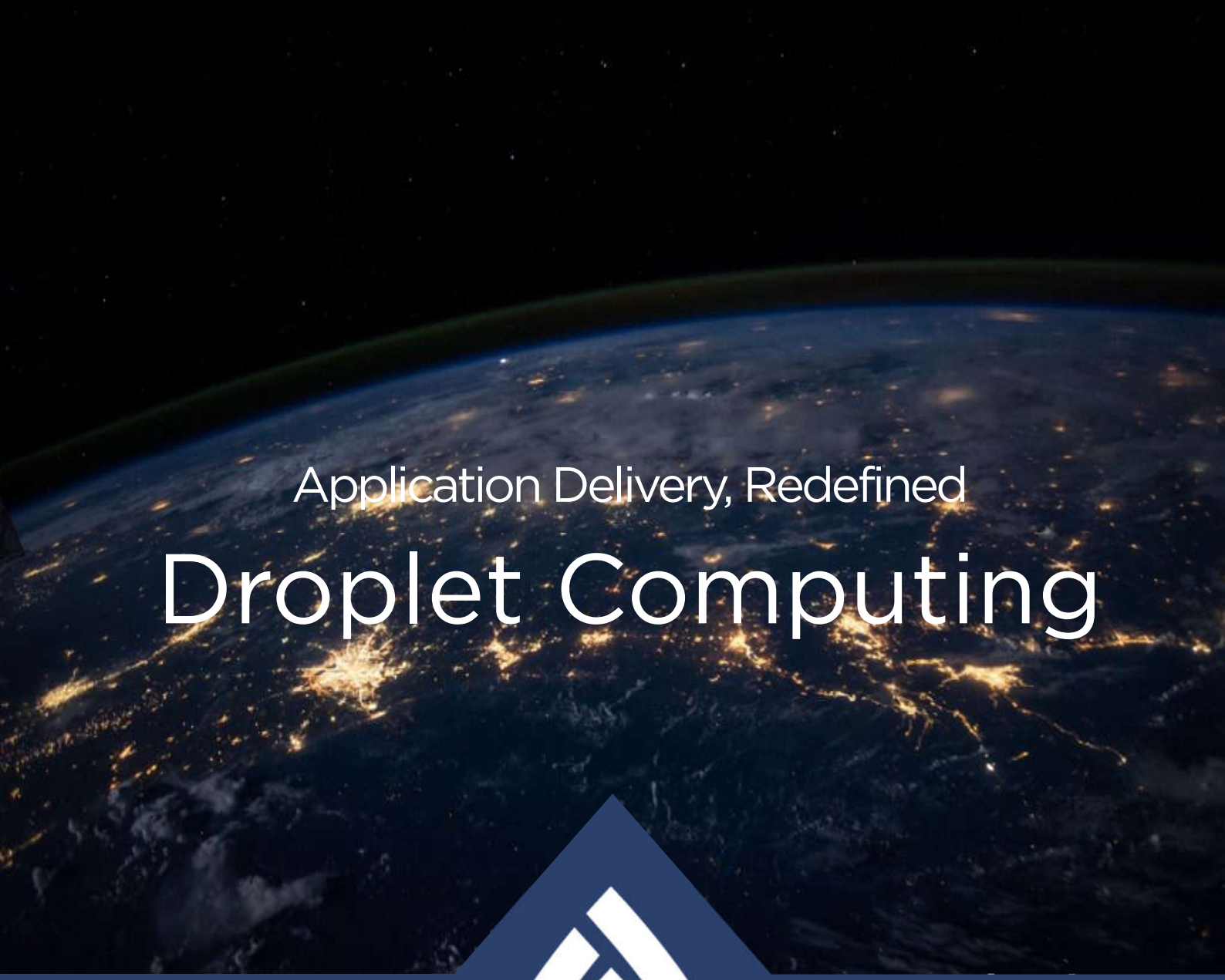


Application Delivery, Redefined

Droplet Computing

Containers:
How Droplet Computing is making an impact

Max Cooter

Freelance Journalist

2019 UK IT INDUSTRY AWARDS computing FINALIST

2018 UK IT INDUSTRY AWARDS computing WINNER UK INNOVATION AND ENTREPRENEURSHIP AWARD

WWW.DROPLETCOMPUTING.COM

About the author

Max is a freelance journalist who has been writing about IT for over 30 years. He was launch editor for two acclaimed publications; Techworld and Cloud Pro, and currently writes for The Register, Computer Weekly and Cloud Pro, amongst others.

Max has also co-authored a book entitled Linux Made Easy, published in 2015, and regularly speaks at IT conferences as a subject matter expert.

Executive Summary

Containers have become a major part of IT infrastructures, solving many issues for IT managers. But they're not a panacea – there are many technological issues that cause headaches. The use of disparate devices to process information; the prevalence of legacy systems and the perennial need to run secure systems will always be top of any CIO's wish list.

This paper looks at how Droplet Computing can solve many of the issues that are hampering technological innovation – such as delivering both legacy and modern applications, and connectivity issues - and how the company can help users get the best of their computer systems.

Introduction

Containers have had a long history. The technology first emerged as a concept within the Unix community in the 1970s but wasn't seen as something technologically viable until this century when various Linux distros started to play around with the idea. Docker took the concept one stage further by offering fully-fledged ecosystems.

The concept has boomed in a way that those early pioneers would not have envisaged. According to 2018 survey from Cloud Foundry, container production usage rose from 22 percent in early 2016 to 38 percent in late 2018. There was a corresponding increase in the number of containers being deployed: three years ago, there were only 37 of organisations deploying 100 or more containers – the current number is just under 50 percent – an example of how quickly the technology has gained favour.

What's the reason for this steady increase? Why are containers capturing the imagination of so many CIOs? First and foremost, containers are a platform in their own right; this means that a container can hold everything that is needed to run an application - all the code and the relevant libraries.

A key element of containers is their portability, something of great interest to many companies who may have a multiplicity of legacy software applications to support. CIOs have wrestled with the problem of trying to integrate one application from one system with another and a ready-made method would save a great deal of development time.

There's another important factor too, the use of containers - with their stripped-down

approach (particularly no operating system) means that there's far less overhead on the system and with companies increasingly opting for faster delivery and real-time information, this is going to be a major factor.

One of the problems facing many CIOs is how to connect individuals who are working in remote offices where there may not be enterprise-grade connectivity. There also may not be dedicated IT teams either, so, if they're to work within the corporate system, there needs to be a simple solution to keep them logged on.

The other headache for CIOs is that there may also be a sub-set of computer users who have very sporadic connection – or even none at all. This presents a challenge for computer administrators who want to make sure that these individuals can work.

Above all, it should be remembered that, despite its provenance, this is a comparatively new technology and that means that there's not a huge base of experienced container experts.

So, companies are looking for ways to roll out containers as efficiently as possible, without putting a strain on IT departments.

The changing face of work

The arrival of cloud computing has changed everything. Companies can implement new initiatives within minutes instead of waiting months to provision servers; indeed, there's less emphasis on the importance of the IT department. This development often goes hand-in-hand with the delivery of apps – something that has been taken as standard on smartphones but is now a major part of how enterprises work.

And talking of smartphones, these now play a major part in commercial life. The last decade has seen a rise in remote working - employees are no longer tied to a single place of employment and could be accessing work applications from home, on trains or even in coffee bars. It's a productive way of working – but only as long as the employee can log on in a secure manner.

Another area where there has been significant change within the enterprise world is the growing acceptance of multi-cloud deployment. In some ways, this is merely an extension of the hybrid cloud set-up, but a more supercharged version.

Here's another manifestation of the importance of containers: when it comes to using components from different cloud providers, the underlying technology that's being used is containerisation: this is an approach that keeps applications working, with their whole runtime environments intact.

By going down this route, organisations can move apps between clouds – even multiple providers – without losing any functionality. This makes sense for enterprises, as they are not limited in the choice of their cloud provider, they can choose the provider that offers the best service for them; not all are the same.

A multiple cloud could also contain private clouds too; indeed, this is an option that many companies choose as they want to keep some highly confidential information in-house. The same criteria applies for mixed private/public clouds as they do for all-public ones; they are very often container-based and there's a need to have a common management platform.

There's another challenge that many businesses will face. Virtually all well-established businesses will have a vast amount of legacy code within their infrastructure. This will be a mixture of custom-written software courtesy of long-departed programmers and firmly established applications, some of which is still being used.

There are issues with legacy code, however. The documentation may be scanty, it may well be written in languages that are not so well known currently and where there may be a shortage of skilled practitioners and many applications may be siloed and easily incorporated in modern infrastructures.

As we have seen, the growing trend is to containerise many applications, and this is an approach that works well when companies have the problem of handling these legacies. It's certainly easier to wrap a container around this code than having to go through the effort of rewriting old software and move to a modern platform, even if you have the requisite staff and ample documentation, such major transformation is still beset with problems.

But once the legacy software has been containerised then the company has a much more manageable deployment to handle.

There is no legacy application that is going to beat the likes of Kubernetes and stop the simplification of the process – once a company has got to grips with the technicalities of containerisation, it will never seek to rewrite legacy code again.
But cloud is not the only technology that has had a transformative effect on the way that organisations manage their computing resources but there are other changes too.

There have been changes in software too. Open source has become a major part of most organisations' infrastructure. And the arrival of virtualisation and containerisation has shattered our thinking on how services can be delivered and sundered the link between the physical and virtual. And, of course, even the most modern business (unless it's newly formed) will have to cope with vast amounts of legacy code.

Navigating all of this is quite a challenge for the CIO. They must make sure that information can be delivered in a timely manner to all employees, wherever they are. And that data could be being delivered to an iPhone, an Android tablet or a Windows PC, a long way from the uniformity of systems that a CIO of 20 or 30 years ago would have expected to see. Most of all, this data must be delivered securely, as security is always going to be top of any CIO's agenda.

The security questions

Given this demand, there's a need to ensure that containers can be rolled out securely. There have been a few issues around containers, particularly with Docker's implementation of them, and all businesses want to know that data can be securely deployed throughout the enterprise.

Containerisation offers a new way of working but the issue of security will always occupy IT departments. The way that the concept could be introduced is not to think of containerisation as a form of technology but as an app, something that users are much more used to. Containerisation should also look to remove, not add, complexity.

And that's the benefit that Droplet Computing, a new contender in the market, can offer. Security is paramount but simplicity is the main element, offering a new way to work.

Droplet Computing tackles containerisation from a completely different angle. Unlike Docker and Kubernetes, the system is endpoint-based – this makes an enormous difference to the way containers are handled. Companies that opt for Docker have a lot of work to do. There's a requirement for skilled staff well versed in Linux to set up the server and by tying the containers to that server, companies are losing a good deal of flexibility. For example, moving containers from one host to another is not a trivial task.

Droplet Computing's approach is based simply on loading a container on a device – there's no complex back-end work today – no knowledge of Linux required: a user could be up and running in just a few minutes.

Furthermore, this approach to containerisation takes into account shifts in business patterns. The enterprise world is changing - something that has a great deal of significance for IT departments. There are other changes afoot that have also shifted the way that people work.

Droplet Computing is looking to tackle these demands by ensuring that applications can be delivered anywhere and to anyone, no matter what that application is or where it's hosted. And most importantly, it delivers all data securely.

That's because Droplet Computing containers are secure entities that are unaffected by any changes within the operating system. This is because the device on which the containers are running is isolated from the host operating system, this means that the host operating system can be updated without any effect on the container or the applications running inside it.

In addition, applications running in Droplet Computing containers are invisible to the host operating system so are less vulnerable to attack from malicious hackers. Furthermore, sysadmins can set policy as to where data is synchronised – whether that's in the cloud or an on-premises server.

A new approach to security

As we've already mentioned, there's a downside to the widespread adoption of containers - at least with the way that they've been deployed by the likes of Docker. They may offer many advantages to companies looking for a streamlined way to deploy to a multitude of different systems, but security isn't one of them: in fact, containers weren't really designed with security in mind, unlike Droplet Computing containers.

There are several reasons why containers have security issues. The most obvious of the vulnerabilities derives from the way that containers work. The reason that the technology works so effectively is that they make use of software images – they are indeed the very foundation of containers. However, there's no guarantee that all images are always absolutely secure – to do so would require them to be signed by an accredited registry.

There has also been a more serious issue and that's the awkward fact that containers are vulnerable to all users because there's no administrator – all users have access to the root kernel. This is in contrast to virtualised environments where access is controlled through a hypervisor.
This flaw has been recognised by container companies and both Docker and RedShift

have tried to address the problem: Docker has created privileged accounts so not everyone has equal access; RedShift has tackled the situation from the other angle and ensures that no containers are root containers so that users can't have any privileged access.

For added security, it's advisable to run containers in public clouds (or a hybrid system that has a public element). This is because AWS, Microsoft and Google all have measures in place to ensure that containers cannot contain malicious code to attack a host computer and, with their experience in multi-tenancy, also ensure that containers from one user cannot infect the containers from another.
But these extra precautions are necessary within server-side containerisation – like Docker – but because the Droplet Computing version abstracts the apps from the underlying OS on a device or virtual desktop, this is not an issue.

It's a system that's been penetration tested by NCC Group, so users can be assured of the security of the system, which is clearly going to be a factor in the minds of CIOs who opt for this way of working.

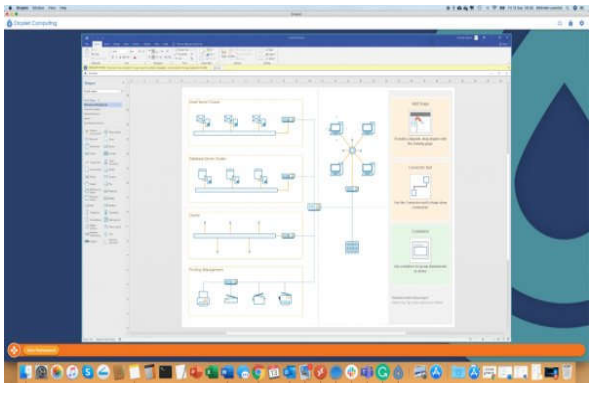
How Droplet Computing containers work

As we've already seen, there's tremendous pressure on IT departments in the modern enterprise. They may have to support legacy apps, on a variety of different platforms and deliver information to employees on a multitude of devices and in various locations, while keeping everything secure. It's quite a challenge – particularly as many IT departments are working under many budgetary constraints.

It's clear that container technology solves many of these problems. As mentioned, it's a cost-effective way of handling software from different platforms and delivering quickly and efficiently but we've also seen that implementing containers can place a strain on IT departments and that there have been worries over security.

What companies need is a way of delivering all the advantages of containers, without any of these concerns: this is where Droplet Computing comes in. This is a way for ensuring that companies can use any number of applications, on any number of devices, in any number of locations, without tying up large volumes of IT support staff. The ability for a company to be able to handle differing devices is a particular boon as there is less of a tendency in the current climate for there to be a single, standardised device.

To give an idea of the sort of benefits that it can bring to a company, take a look at the example of Microsoft Visio, an application that doesn't have a native version for Apple Macs. While there is an online version of the tool, it's neither as powerful nor as fully featured as the native Windows version so Macs have not been able to draw on all the benefits of Visio. By deploying Droplet Computing containers, Mac users can now have access to the same features that Windows users have with the added advantage of being able to run offline.



Microsoft Visio running in a Droplet container on a Mac

Or for enterprises using old versions of products, it becomes easier to make the upgrades without whole systems collapsing. We know that many companies have legacy products going back a number of years; Droplet Computing offers a way of incorporating them without a massive restructuring operation.

To get to this state of affairs, there's no great demand on IT departments. The installation of Droplet Computing containers is especially simple to do and can be carried out in minutes.

One of the main advantages of Droplet Computing containers is that users don't need to dedicate unnecessary resources to run applications as they can assign just the right amount of memory needed. For example, if a text editor requires just 1GB of RAM to run, that's what will be allocated.

Companies can also choose the amount of CPU resource in the same way, by selecting the number of cores to use. Please ensure that you don't over provision the CPU cores and that the underlying devices can deliver the required resources. The required amount of hard disk space is dynamic and will start off at around 1GB, growing to a maximum size of 20GB.

The Droplet Computing container is installed in just two steps: the container app and then the container image file for the operating system. Corporate users can distribute the container app by using a deployment tool such as SCCM.

After loading these, the user can set up a tiling system that offers shortcuts to executables. Because the system is container-based, there's no massive overhead involved, so programs load almost instantaneously. The system not only supports Windows applications but can handle Linux too, particularly useful for development teams who may be looking to sandbox trial applications.

The modern IT world is dependent on connectivity: all the discussion so far has focused on being able to get online and use applications – either through the web or by downloading them. But what happens if applications aren't available online? This is not far-fetched: there will be some situations where users are not permitted to connect to the outside world but still need to do useful work. For example, organisations like the Ministry of Defence have situations where, for security reasons, users aren't permitted to access the Internet.

One of the benefits of the Droplet Computing approach is that it doesn't require users to be online and can allow them to carry out productive work while offline. This is a useful feature when some people could well be working in locations with sporadic (or even no) connections.

Another big advantage of Droplet Computing is that it provides a useful way of providing some a level of disaster recovery to organisations, providing a way to get things working again after any sort of disruption. This doesn't need to an actual disaster, it could be a way of logging on to a corporate system when a user doesn't have his or her computer to hand – Droplet Computing offers a way to use other devices, even if they're not compatible, something that previously would not have been possible. Again, this is a boon for individuals who have to work in different offices, as well as providing help for managers making presentations in unfamiliar environments.

Delivering security, the Droplet Computing way

We talked previously about this new approach to security, but how does it actually work and how does Droplet Computing secure the container?

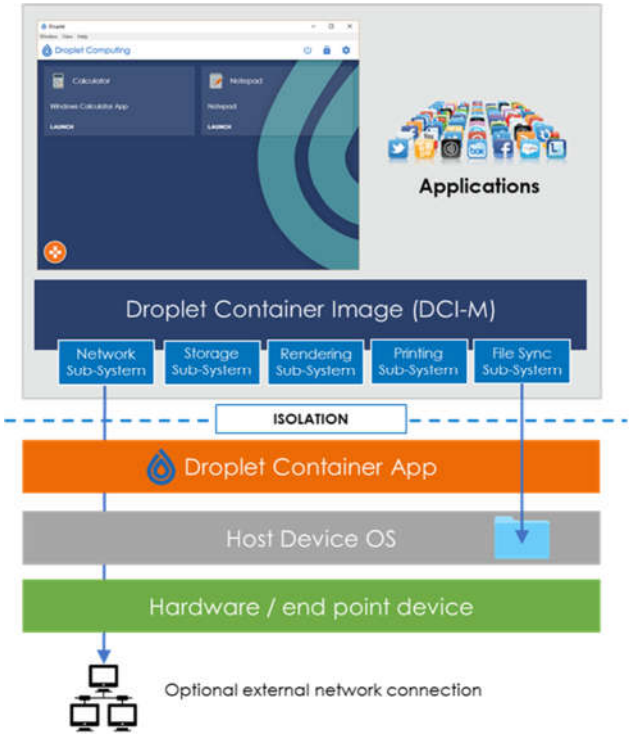
The key word here is isolation. The container runs as an app and runs the container abstracted from the host devices underlying operating system, in a similar way that an OS is abstracted from the hardware in a virtual machine environment using a hypervisor.

This means that the container has no dependencies on that underlying OS and talks directly to the hardware. If the device OS becomes compromised or is attacked, which should not happen as you would have deployed end point protection, there is no way that the container can be accessed.

This can be further demonstrated as if you open the Task Manager on a Windows host for example, the apps are not exposed and therefore not visible to a potential hacker.

The container can also run quite happily without a network connection; however, you can optionally connect it to a network to access centralised docs, files, or network printers.

This is typically a task only undertaken by IT admins to install apps, and once the apps have been installed, the container can then be locked down with no connection to the outside world. It's like building your gold or master image, however this time you are building a gold or master container.



Architecture of the Droplet container

When it comes to saving files and docs, the container has a second private network, shared only with the host device, allowing end users to save documents inside the container while simultaneously being able to still have access to them even when the container is powered off. This shared folder is never exposed externally and as such is not visible on the network.

The biggest risk to any system becoming compromised or data being leaked are the end users. When it comes to end user interaction with their containerised apps, the end users can only launch the apps that appear on the workspace interface. They are unable to access any settings or any other apps, including not being able to delete any existing apps from the workspace. They are effectively locked inside a kiosk style mode inside the container, unable to run any unauthorised software.

Conclusion

The advent of containers has been a boon to many organisations. Virtualisation offered a path to more efficient computing, but the arrival of containers has added another dimension. But, as we have seen, there are limits on what can be achieved by server-side containerisation.

Droplet Computing has taken the concept in a completely different direction, offering huge advantages to corporates grappling with a multiplicity of devices sitting on a goulash of different applications and operating systems. What's more, it does so by simplifying matters so that it doesn't need massive intervention by the IT department.

There have been some fears that the complexity of containers can diminish their effectiveness, Droplet Computing has shown that this doesn't have to be the case. Don't listen to the words of warning – containers don't have to be complicated!

86-90 Paul Street,
London,
England,
EC2A 4NE

Droplet Computing Limited
Registered in England and Wales, Company Number 10536920