Droplet

ENSURE CYBER ESSENTIALS COMPLIANCE WITH DROPLET CONTAINERS

COMPLIANCE, COMPLIANCE, COMPLIANCE!

It may not be the word of the decade, but, in its various forms and applications, compliance has shaped much of what the IT world revolves around—I think of it as an intense, radioactive and constantly evolving star at the centre of our solar system.

Well, to be fair, the 'radioactivity' is caused by Enemy no. 1: Cyber-crime. Which, as we know, is not some lone dude in a darkened room wearing a hoodie and hacking away at a keyboard, but a group of well-funded, sophisticated, international syndicates. Their target? Your company's data, your users' data, or even your entire data centre.

The threat to public safety makes cybercrime a national concern, which is why the UK government needs to formulate and impose certification standards.

As of January 2021, the National Cyber Security Centre (NCSC) started enforcing the latest version of their Cyber Essentials certification standards, known as v3. These updated standards aim to provide even stronger protection against cyber threats for organisations of all sizes and industries.

NEW DEADLINE

In November last year (2022) the deadline was shifted to provide a grace period, which allows organisations to continue operating under the previous version of the standards until April 2023. This gives businesses and organisations a little more time to implement the necessary changes to comply with the updated standards.

The extension applies to three of the requirements (to quote the NCSC):

- any thin clients included in the scope of certification must be supported and must receive security updates
- all unsupported software is either removed or segregated from scope via a sub-set
- all user accounts on cloud services are protected by multi-factor authentication (MFA)

The other news is that this will coincide with the next, light-touch update to Cyber Essentials' technical requirements, which will focus largely on a series of clarifications. This includes important new guidance on the following issues:

- Clarification on firmware—All firmware is currently included in the definition of 'software', so must be kept up to date and supported. Due to difficulties with information provided by vendors, this is changing to just router and firewall firmware.
- Third party devices—Further information and a new table clarifying how third-party devices, such as contractor or student devices, should be treated in applications.
- Device unlocking—A change in this section to mitigate issues around some default settings in devices being unconfigurable. Where that is the case, it is acceptable for applicants to use those default settings.
- Malware protection—Anti-malware software will no longer need to be signature-based, and clarification has been added around which mechanism is suitable for different types of devices. Sandboxing is being removed as an option.
- Guidance on zero trust architecture in the context of achieving Cyber Essentials and a note on the importance of asset management.

What does it take to comply with these new standards, and how can your organisation ensure you pass certification? Do you replace old, non-compliant apps with a rewritten or updated code version? Do you chuck it all out and sign up for a SaaS solution that promises to keep your data safe? What do you do with your old Windows NT servers that host your critical databases?

REFRAMING THE PROBLEM

Droplet turns conventional thinking on its head.

Instead of rewriting applications, or replacing them, with all the hassle of retraining and bug-squashing this entails—and never mind the cost—we say: "If it ain't broke, don't fix it." If security is the only thing driving an upgrade/crossgrade/code rewrite, it feels like we're overcomplicating matters.

Upgrading to a shiny new server running the latest 64-bit OS is also no reason to go to the added expense of changing software you are otherwise happy with.

Our solution: containerise. Done correctly, containers can ensure cybersecurity and compliance, and Droplet is at the forefront of this technology. As one of our customers put it: "Droplet is a true isolation layer, not sandboxing, and so anything put inside the Droplet container is an instant pass for Cyber Essentials Plus or NIST compliance."

CONTROLS

Droplet provides a set of built-in technical controls that makes it easy to achieve compliance with Cyber Essentials Plus or NIST. These include:

- A firewall that can be configured to block unwanted traffic and protect your systems from external threats. The Droplet firewall is set to "block all incoming packets" by default.
- An intrusion-detection system that can detect and alert you to suspicious activity on your network.
- Built-in encryption capabilities to protect your data from unauthorised access.

We call our approach Nevertrust©, because it is even more robust and locked-down than the industry standard of "zero trust".

Droplet containers can be deployed on multiple architectures, without reconfiguration, including Windows, Linux and Mac. They can also be easily deployed on any cloud platform, including Amazon Web Services, Microsoft Azure, and Google Cloud Platform. This allows businesses to choose the cloud platform that best suits their needs and budget. For ultimate portability, containerised apps can run inside a browser window.

If your company is, as many companies are, still in the position of scrambling to upgrade software and hardware in order to be compliant, take a deep breath: there is a better way. Droplet containers are an easy-to-install, cost-effective and secure option for achieving compliance. With the added benefits of increased security and flexibility, you can start implementing these new standards today and protect your business and personal information.