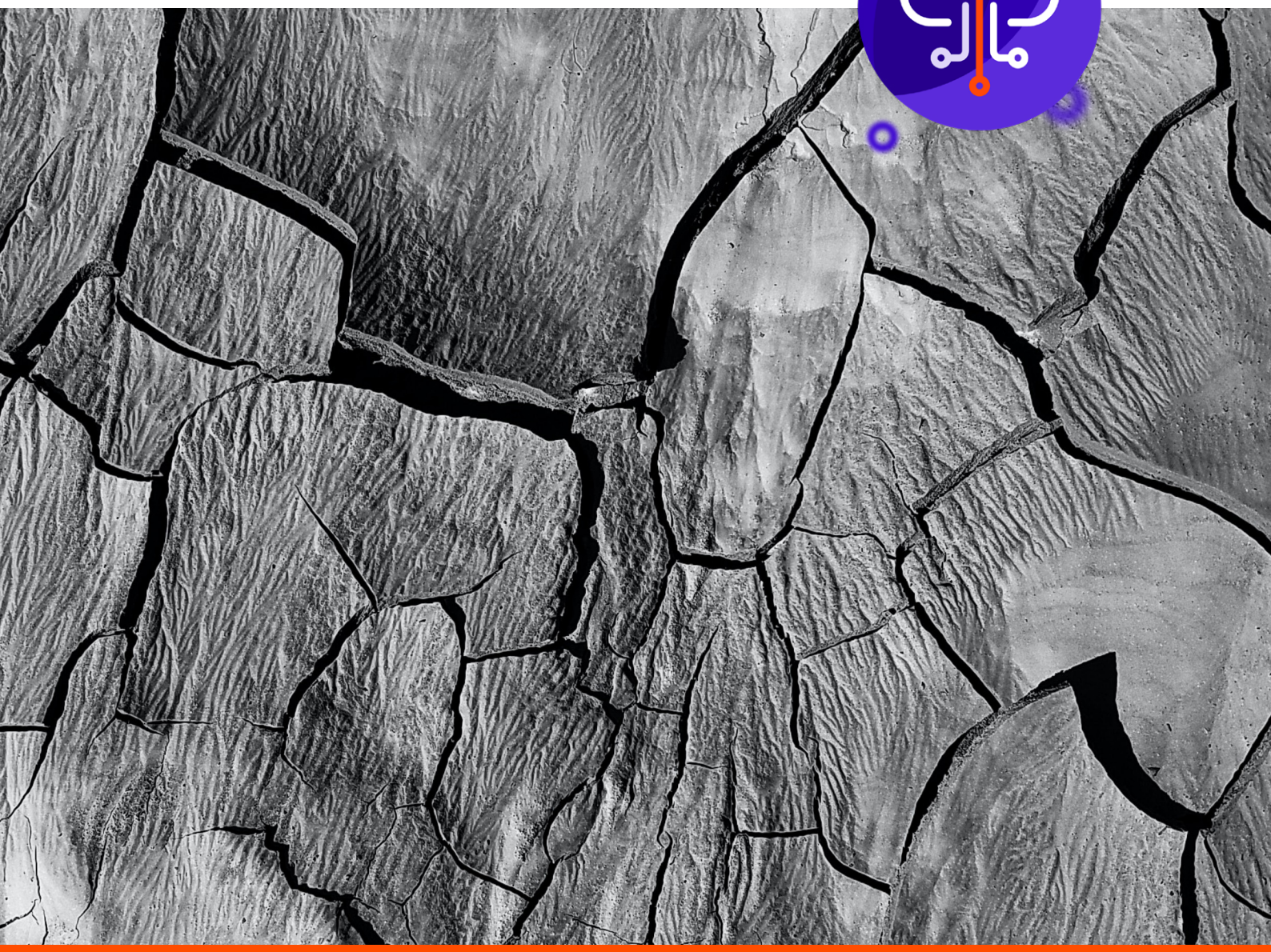
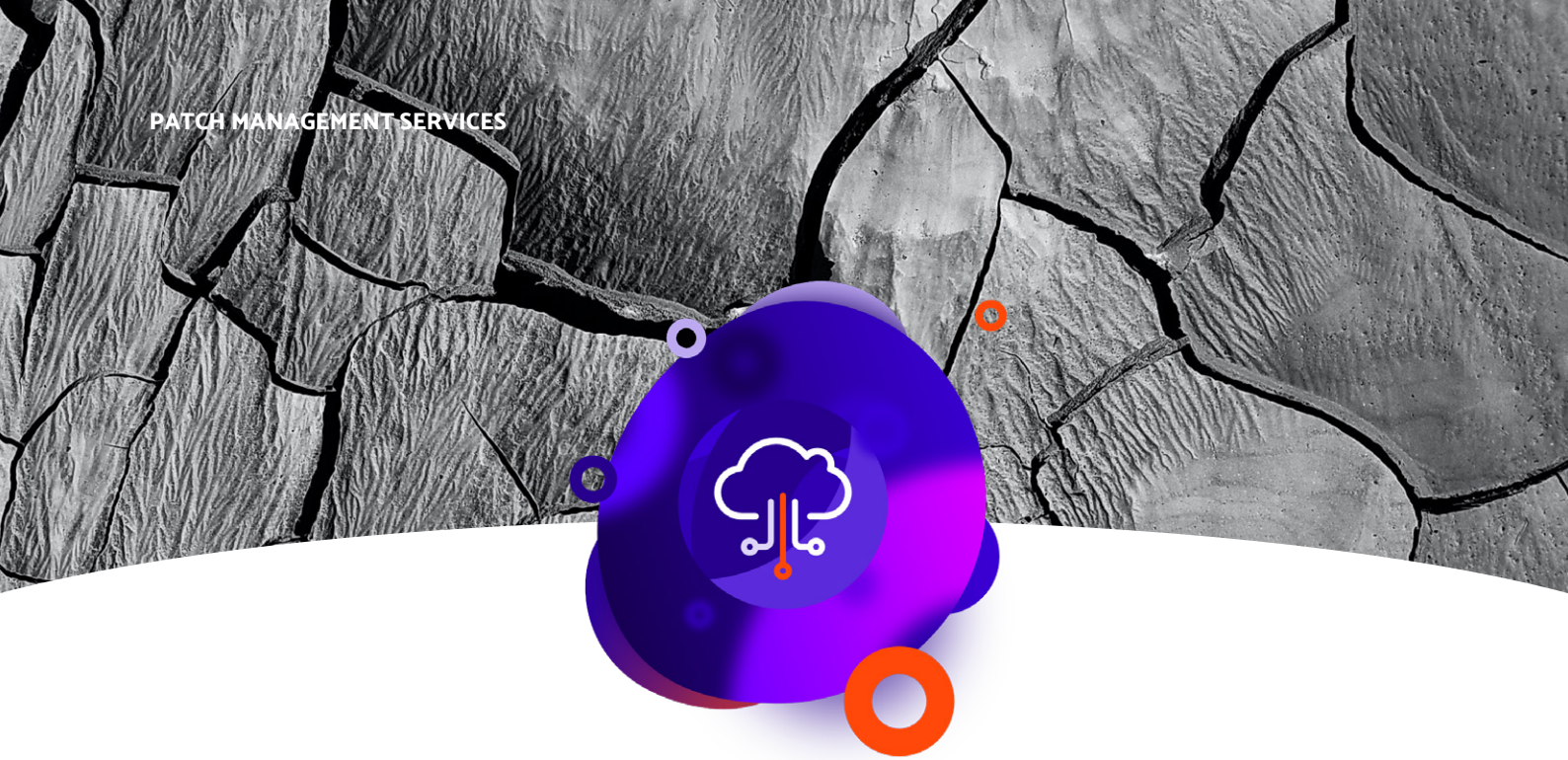
PATCH MANAGEMENT SERVICES (PMS)

EXPLOITATION OF VULNERABILITIES REMAINS THE GREATEST CAUSE OF SECURITY INCIDENTS



METCLOUD

GET CONNECTED • CYBER SAFE



Patch Management Services

A service built to help organisations to reduce down-time and set new standards for efficiency through automation.

Every cyber-attack reminds us of the importance of patching. Cyber-attacks have increased rapidly, and hackers find new and more sophisticated ways to breach your network.

As cybersecurity threats continue to evolve, companies regularly discover new vulnerabilities in their software that can be exploited by hackers. Patches are small updates issued to fix these security gaps. In addition to security fixes, patching can help with an entire array of tasks, such as adding new features or functionalities to your existing software, improving the look and feel of your software, and ensuring the optimal performance of your applications.

WHY YOUR BUSINESS NEEDS PATCH MANAGEMENT

According to surveys conducted by the Ponemon Institute, 57% of cyberattacks were preventable incidents that could have been avoided with a simple patch. Therefore, organisations need a patch management strategy to ensure that their IT network is protected from all vulnerabilities.

The time between a patch release and its installation is crucial to maintain security.

METCLOUD's patch management engine can install, uninstall, and patch your operating systems, 3rd party software and custom software to keep all the endpoints secure.

With the increased frequency that numbers of software patches released every day, and the endpoints added to it, it is increasingly difficult to keep track of your patches manually. Our Patch Management Services gives you the capability to maximize security and maintain compliance.

SETTING PATCH MANAGEMENT INTO ACTION

STEP 1 – INVENTORY MANAGEMENT

- Asset type (laptop, desktop, mobile phone, etc.)
- Asset status (in use or disposed)
- Device location
- Existing software versions in various assets

STEP 2 – CONSOLIDATE SOFTWARE VERSIONS

The next step involves consolidating all the software versions in your IT network. This includes operating systems, third-party software titles and custom software titles. By consolidating your existing software, we can deploy similar patches throughout your network and ensure consistency across your software ecosystem.

STEP 3 – ASSIGN PRIORITY LEVELS

Once we have taken a full inventory of your assets and consolidated your software versions, they need to be categorized based on their risk levels and priority. Patching is equally important for all the assets in your network. However, there might be some critical assets that are more important than other assets. If a particular asset is more exposed to vulnerabilities, it should be patched first. Any weak link in your network can compromise your overall security and put you at immense risk.

STEP 4 – CREATE A PATCH MANAGEMENT POLICY

A patching policy is a generalised set of rules applicable to the end points in a group. With METCLOUD you can create multiple policies based on the diverse types of equipment and tools. Once the policy is created, you will be in total control of your operating system and application updates.

STEP5 – KEEP UP WITH UPDATES AND PATCHES

Scheduling is crucial for patch deployment. You can choose when and how your patches get installed. For example, scheduling patching out of working hours so you will not reduce productivity. This way, technicians are more flexible when updating patches in their vulnerable and non – vulnerable systems.

Third party and custom titles: You can simply define a rule for all the third-party titles and manage their progress (installation, uninstalls etc.) based on your needs. Therefore, all the added custom titles can be added to your policies and specify the equipment for which you need them to.

Why METCLOUD?

Award winning company for cybersecurity, innovation, and excellence. Our vision is to be the global brand of choice for next generation cybersecure cloud services. Our services have been architected with security by design. Ransomware, Cloud vulnerabilities, Phishing attacks Social engineering and vulnerability management are the five top global security threats. METCLOUD's portfolio of cyber security and cloud services will ensure that you protect, defend, and mitigate any potential cyber attack irrespective of how it was carried out.

Let’s get connected.

Call 0121 227 0730
and speak to one
of our experts.

Email the team.
hello@metcloud.com

Visit our website for
more information.
metcloud.com

METCLOUD

GET CONNECTED • CYBER SAFE