PLATAINE®
people-smart automation

How Plataine keeps your data

Safe & Secure?

The Industrial Internet of Things (IIoT) delivers a step-change in manufacturing productivity. Factories are increasingly using cloud-based, AI-enabled software to ensure all people, systems and machines are constantly connected. The benefits are huge, yet there are precautions that must be taken to make sure they are protected against cyber-security threats.

Explore this introductory walk-through, to learn which measures Plataine takes to keep your cloud-based data safe and protected.

Multi-tenant architecture

A multi-tenant solution allows multiple customers to use the same software and runtime environment. Multi-tenancy is a core benefit of SaaS because it reduces costs by sharing core infrastructure, yet at the same time is highly configurable to the needs of individual customers. Total data security is guaranteed because all files are stored in industry-leading protected environments (such as a dedicated AWS S3 bucket). Meanwhile, IIoT providers are able to efficiently offer ongoing updates, in a way that would be impossible for completely bespoke software.

Communication on secured channels

All API communication should be conducted over a secured HTTPS channel, which uses an encryption protocol to encrypt standard HTTP communications.

Authentication & authorization

Secure authentication and authorization procedures mean more than just having a username and password. Industry leading IIoT systems hold multiple levels of information about individual users so that they can enforce strict rules for access on an individual level.

Password cryptographic hashing

The most secure way to store passwords is to use cryptographic hashing, which means the passwords themselves are not stored – instead, only the password's digest is stored. Therefore, even if the database which contains the digests is broken into, the data is useless.

Separate accounts for production and development personnel

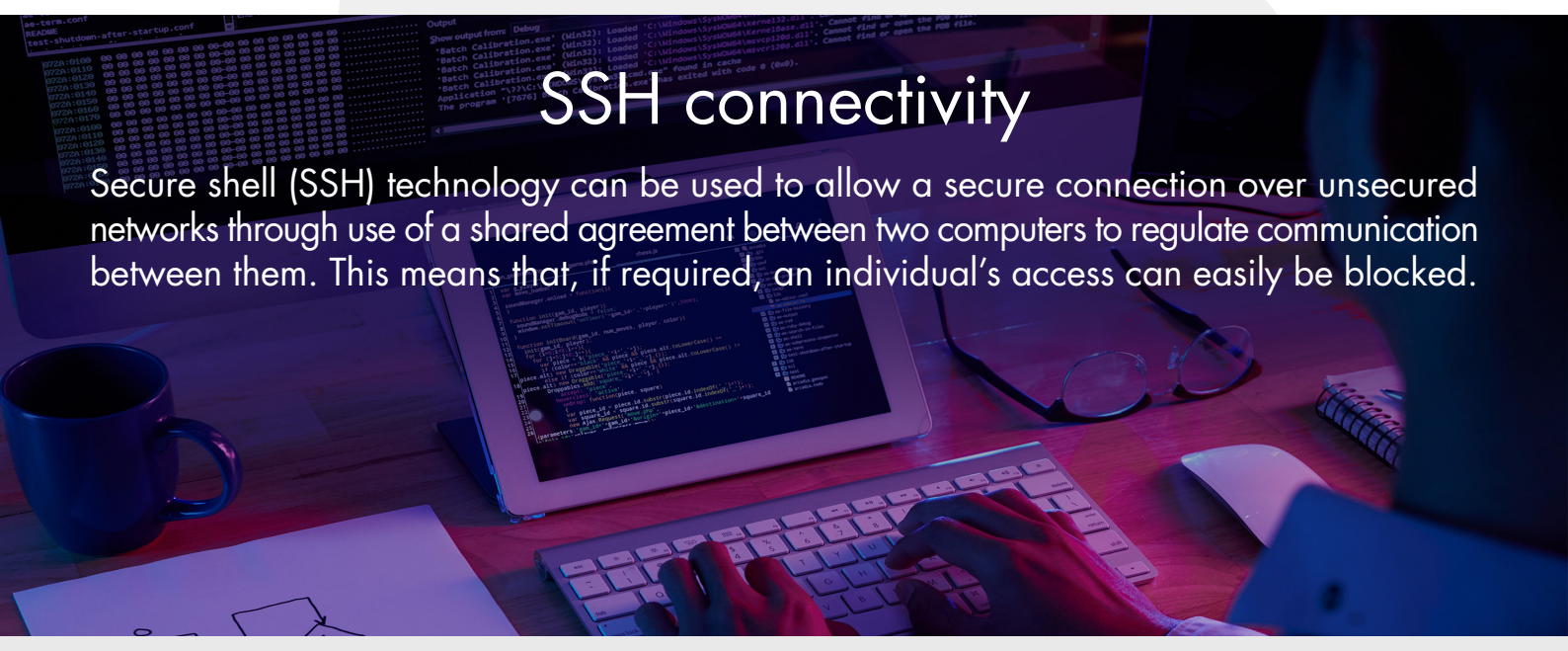
Different levels of user access ensure IIoT system users can only access the data they need to perform their own specific roles.

Data encryption

IIoT solutions rely on encryption for security because data and applications are stored in the cloud – outside company firewalls. According to recent research , most companies prefer to manage their own security keys, ensuring only they control access to their cloud-based information. The best IIoT solution providers always invest heavily in the latest encryption technology.

Most accessibility is restricted to a VPN

Highly secure IIoT systems restrict entrance for APIs to a single API gateway. All other components can be restricted so that access is only possible via a virtual private network (VPN) – creating a totally secure channel between the user and the cloud.



SSH connectivity

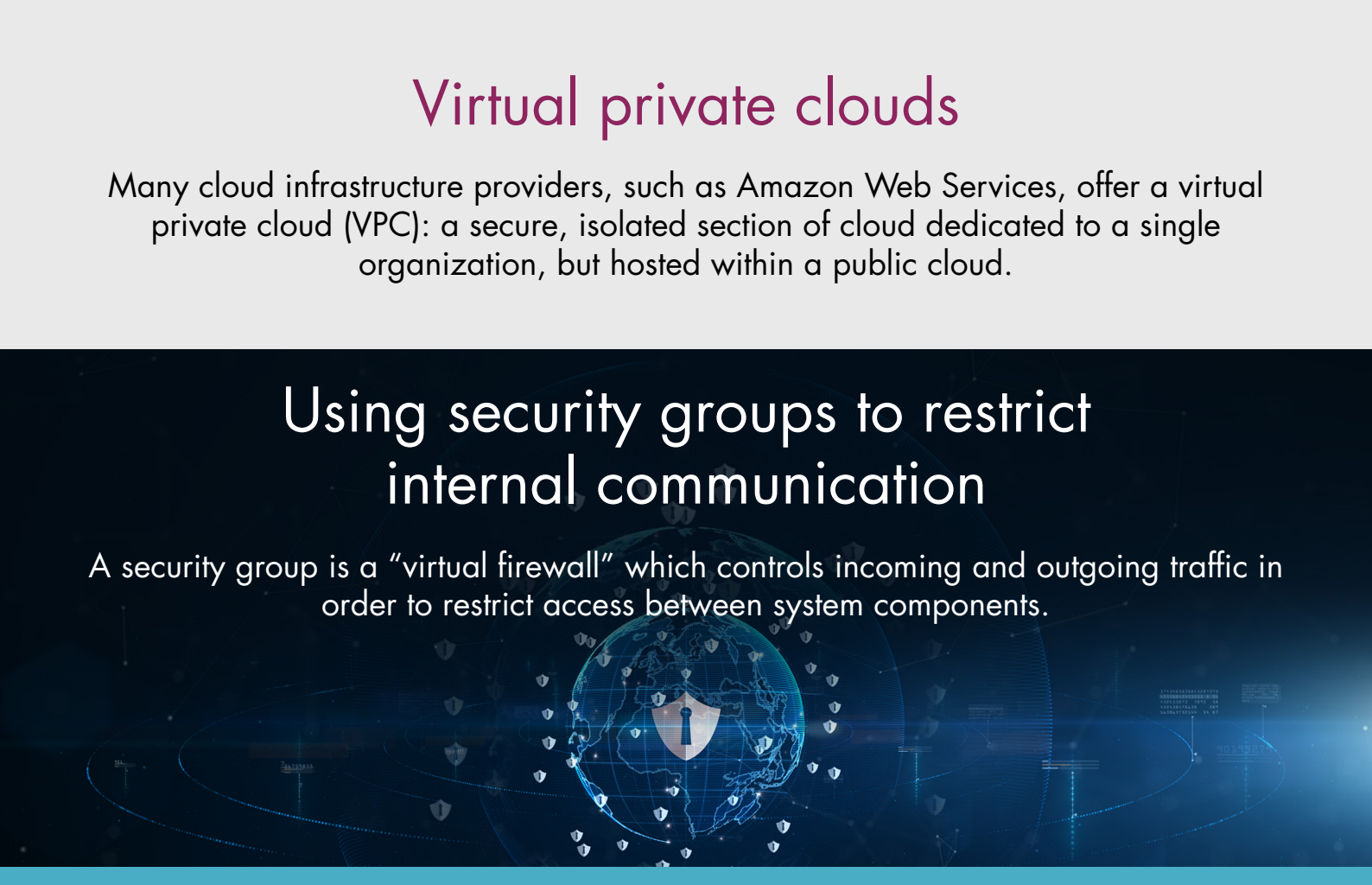
Secure shell (SSH) technology can be used to allow a secure connection over unsecured networks through use of a shared agreement between two computers to regulate communication between them. This means that, if required, an individual's access can easily be blocked.

Virtual private clouds

Many cloud infrastructure providers, such as Amazon Web Services, offer a virtual private cloud (VPC): a secure, isolated section of cloud dedicated to a single organization, but hosted within a public cloud.

Using security groups to restrict internal communication

A security group is a "virtual firewall" which controls incoming and outgoing traffic in order to restrict access between system components.



Time to take the next step

At Plataine, we provide IIoT solutions to some of the world's largest OEMs, Tier 1 & 2 discrete manufacturers. contact us to learn more: www.plataine.com

PLATAINE®
people-smart automation