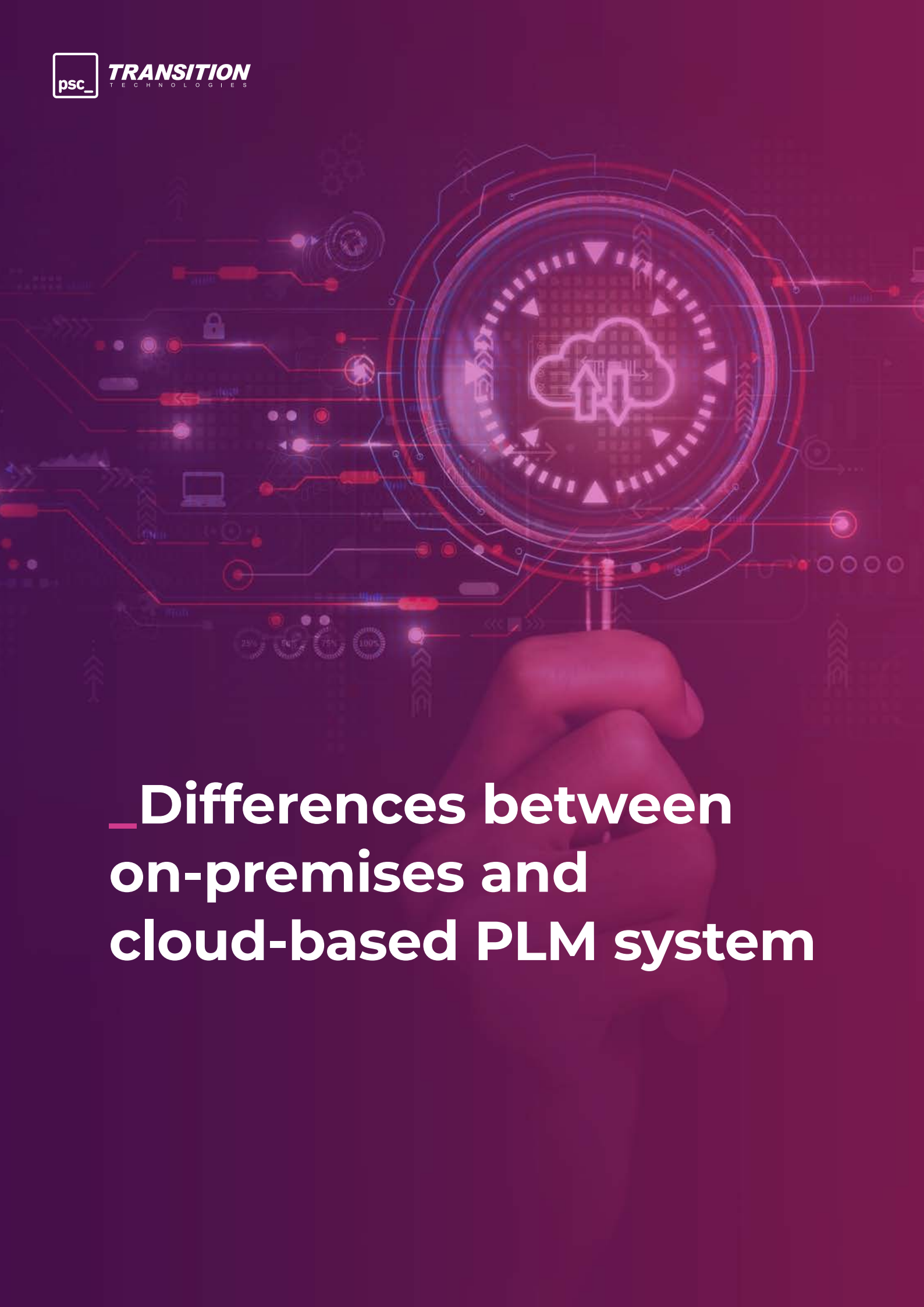




TRANSITION
TECHNOLOGIES

The background of the slide is a dark purple gradient. Overlaid on this is a complex, futuristic digital interface. A hand is visible at the bottom, pointing upwards towards a large, glowing circular hub. This hub is the center of a network of glowing red and white lines that branch out across the screen. Various digital icons are scattered throughout, including a cloud with an upward arrow, a padlock, a laptop, and several circular progress indicators showing percentages like 25%, 50%, 75%, and 100%. The overall aesthetic is high-tech and digital.

Differences between on-premises and cloud-based PLM system

Differences between on-premises and cloud-based PLM systems

Several key differences emerge when comparing on-premises and cloud-based Product Lifecycle Management (PLM) systems. The detailed comparison below reveals how these two approaches compare in various aspects, from setup responsibilities to disaster recovery.

Whether you're considering on-premises solutions or the flexibility of cloud-based systems, this table will guide you through the essential distinctions.

Aspect	On-Premises PLM System	Cloud-Based PLM System
Setup Responsibility	Organizations must set up server rooms, hardware, and software. Train IT internal teams on new technology.	Vendor handles most setup tasks, depending on the service model (IaaS, PaaS, SaaS, FaaS).
Initial Costs	High initial investment in physical infrastructure and software licenses.	Lower initial costs, typically subscription-based pricing.
Maintenance	The organization is responsible for all maintenance, including backups, updates, and patches.	The vendor manages maintenance tasks, reducing the burden on the organization's IT department.
Scalability	Limited by physical hardware, scaling up requires additional investment.	Easily scalable; resources can be adjusted as needed without significant upfront costs.
Customization	A high level of customization is possible, tailored to specific organizational needs.	The vendor's platform capabilities may limit customization options.
Security	Security is managed internally, requiring robust measures and constant monitoring.	Security is managed by the vendor, often with advanced and up-to-date security protocols.
Accessibility	Access is typically limited to on-site or through VPN.	Accessible from anywhere with an internet connection.
Updates and Upgrades	The organization must manually apply updates and upgrades.	The vendor provides automatic updates and upgrades, ensuring the system is always current.
Disaster Recovery	Requires in-house disaster recovery planning and implementation.	Vendor typically offers built-in disaster recovery solutions.