PTC Cloud Services: Security Primer

LEARN HOW PTC CLOUD SERVICES CAN PROVIDE YOU PEACE OF MIND FOR YOUR EVER-EVOLVING SECURITY NEEDS

Today, the IT landscape is changing, opening new competitive advantages for early adopting customers. While over 50% of companies are struggling with security concerns, others are wisely focusing on their core business and are becoming market leaders by leveraging all the benefits of new cloud technologies and services.

Security remains the top adoption challenge; with over half of organizations stating that vendors must ensure security measures can meet their compliance requirements. Between cyber-attacks and data leakage, businesses must be diligent in the protection of their data assets.

PTC Cloud Services understands that the availability, integrity and confidentiality of your information are vital to your business operations. Our security posture evolves to meet the ever-changing threat landscape and utilizes a closed-loop process for continual improvement of our security processes and procedures. With over 15 years of cloud services experience and PTC software expertise, PTC Cloud Services provides you with end-to-end security and the peace-of-mind so you can focus on your most important business initiatives.

Did you know?

- 9 out of 10 organizations are using at least one cloud application
- 50% of IT professionals rank security as a top reason for migrating applications to the cloud
- 67% have concerns about the security of cloud computing solutions
- 94% of SMB cloud adopters report that they have experienced security benefits since moving to the cloud


Data Security

PTC Cloud Services is designed and certified to meet many of the compliance requirements of the most demanding environments. PTC’s Information Security Management System (ISMS) is regularly reviewed and audited to ensure that information is current and consistent with global standards. The ISMS consists of a set of policies and procedures documenting our security protocols and ensures a systematic approach to security. All data is encrypted in transit so the Internet communication is secure. Even when data is backed up, it is encrypted and stored within a backup storage library at a remote facility for a period of 90 days. All remote facilities have the same level of physical security as the primary facility to ensure all data is secured from physical access. Below are the security certificates that PTC maintains today.

Certifications include:

- Federal Risk and Authorization Management Program (FedRAMP): U.S. government program to assure standardized approach to security for cloud products and services
- DOD Information Assurance Certification and Accreditation Process (DIACAP): Formal management process to assure security for all DOD information systems
- SSAE-16 (SOC 2 Type 2): Standard annual reporting for U.S. publicly traded companies to ensure physical and environmental security for data centers
- Conform to International Organization for Standardization (ISO) 27001:2013 standards
- ITAR compliant

Physical Security

Worldwide cloud capability

**World-Class, SSAE-16 Audited Data Centers**

- 5 PTC Co-Location Centers with PTC owned computing
- Amazon Web Services’ global infrastructure (AWS)

PTC Cloud Services deploys physical security measures and best-in-class SSAE-16 Audited Data Centers around the world with five PTC Co-Location Centers with PTC owned computing as well leveraging Amazon Web Services (AWS) global infrastructure. Data Center security and operational measures include [see more on AWS site].
• Full time, 24x7 local operations and security guards
• Security cameras
• Perimeter fence
• Locked cage and cabinets
• Diesel generator backup power
• SSAE-16 for US and ISAE 3402 for International
• ISO 27001: Information Security Management System
• ISO 14001: Environmental Management System
• ISO 9001: Quality Management
• Multi-Factor Authentication:
  - Photo identification access cards
  - Man-trap
  - Biometric devices: palm/finger print and retina scan
  - Government issued identification

Infrastructure Security

PTC Cloud Services provides the peace of mind you need for your mission-critical application services with the delivery you can rely on. With proactive monitoring and annual auditing, PTC Cloud Services provides the scalability, reliability and security infrastructure you need including:

• Follow Defense-in-Depth Principles
  - Multiple layers of security to prevent a single weakness from compromising the system
• Intrusion Detection System (IDS)
  - Early warning attacks on the system
  - SOC employed to review alerts for patterns of concern
  - Signatures updated regularly
• Environment Scanning
  - Monthly vulnerability scans
  - Threat-level remediation
• Secure connection for external systems including HTTPS/TLS, encryption and certificates
• Secure authentication through LDAP/LDAPS and AD
• Controlled data center access with VPN and IP filtering
• Multi-layer networks with separate perimeter and application firewalls and each customer segmented onto separate VLANs
• Operating system hardening
• Network traffic limited between sub-nets
• Only necessary ports permitted
• Service access limited to PTC Cloud Services Administrators for limited access to a minimum number of people with separate duties
• Annual data center audits for certifications

Learn more

To learn more, speak to a PTC Cloud Services Expert to discuss your security questions or concerns.