Cloud Security

Prioritizing data protection

As more and more companies are adopting cloud-based hosting strategies, the complexity of Cloud Security becomes a growing concern. To avoid security complications in the cloud, companies must choose a cloud provider that not only prioritizes security, but also understands the role security plays across the entire enterprise.

Introduction

With the proliferation of cloud offerings in today's marketplace, many companies are leveraging cloud-based business applications. Research shows that up to 50% of IT professionals* rank security as a top reason for migrating applications to the Cloud – whether this is a Software as a Service (SaaS) application like Office 365, Infrastructure as a Service (IaaS) like Amazon Web Services, or a Platform as a Service (Paas) as offered by Salesforce.com. While immediate value is seen when moving to the Cloud, including client agility, improved collaboration, and simplified processes for software updates, two challenges still remain:

- How does an organization develop a strong and robust security program in an ever-changing threat landscape?
- How does one stay on top of internal and external threats, product and application risks, business risks, and regulatory and industry compliance requirements?

We at PTC understand the core requirement of all PTC Cloud offerings is ensuring the confidentiality, integrity, and availability of customer data is not violated. As a part of designing the PTC Cloud hosting infrastructure, a best practices Information Security Management System (ISMS) was implemented to minimize risk, ensure service continuity, and provide governance over policies and procedures.

* 2015 IDG Cloud Computing Study

Organizational Security and Personnel

PTC instills a strong security culture amongst staff and management; beginning with onboarding and continued with role-based security training. Roles and responsibilities are defined in written job descriptions and communicated to employees and managers. Background investigations are conducted as a pre-requisite for newly hired PTC Cloud employees.

PTC Cloud utilizes experienced information security professionals in the Cloud Security organization. Security Architects are responsible for developing, documenting, and implementing security relevant components. Dedicated Compliance Architects are responsible for policies and standards and reviewing all system related security plans throughout the hosting environment's internal and production networks from cradle to grave.

Documented policies and procedures are used to help ensure the security, performance, and availability of all networks, systems, services, and applications for Cloud solutions. All of these policies meet or exceed industry standards and best practices. Organizational security is one of the pillars of PTC Cloud's security architecture, designed to define and maintain the effectiveness of the network, application, system, operational, and service components.

Change Management

PTC Cloud has established a systematic methodology to managing changes so that changes to any system or service are reviewed, approved, and well communicated. Our change management process is designed to prevent unintended service disruptions and maintain the integrity of the services provided to customers. A change is any addition or modification in the PTC Cloud hosting environment or the systems, applications, and services used to deliver Cloud Solutions.

- PTC Cloud has been audited by third-parties and strives to maintain a rigorous security program
- PTC Cloud operations are ISO 27001 audited and certified
- PTC Cloud Data Centers are ISO 27001 certified and have met the stringent audits of ISO 14001 and ISO 9001
- Our government offerings/data centers meet the required security approach for security assessment, authorization, and continuous monitoring for products and services and FedRAMP
- All data centers are SSAE16 SOC 2 Type II Security & Availabilty Trust Principles audited for the US and ISAE 3402 internationally
- ITAR Data Centers

View PTC Cloud FedRAMP Authorization page

https://marketplace.fedramp.gov/#/product/ptccloud-services?sort=productName&productNameSearch=ptc

PTC Cloud Security Monitoring

PTC Cloud uses an Intrusion Detection System (IDS) for continuous security/compliance monitoring and log analysis across all our environments through our Software-as-a-Service offerings, coupled with 24x7 monitoring services from our third party security operations center.

Leveraging a wide variety of monitoring services, PTC Cloud provides a high level of service performance, awareness, and availability. These monitoring services are implemented to detect unusual, unauthorized, or unanticipated activities and conditions at inbound/outbound communication points, on systems/servers, and within the applications operating within the hosting environments. These services monitor server, network, and application usage, unauthorized intrusion attempts, system and application events, and system and application metrics. The monitoring services are configured to oversee key operational metrics and telemetry, and alerts are configured to automatically notify operations and management personnel when defined thresholds levels are reached.

Risk Assessment

As part of our business planning process, PTC Cloud evaluates the infrastructure, data, software, and procedures and needs for additional tools and resources as part of our ongoing risk assessment process. A formal risk assessment that specifies risk tolerances and processes for evaluating security risks based on threats and specified tolerances is performed on a perpetual basis. Controls and mitigation strategies for risks identified and rated during the risk assessment are evaluated for effectiveness and recommendations for improvements are reviewed and approved by management. In addition to the annual risk assessment, PTC Cloud personnel proactively subscribe to security informational services to monitor industry trends, regulatory changes, and the security impact of emerging technologies.

Configuration Management

All configuration changes to PTC solutions or services managed by PTC Cloud are within the scope of the PTC Cloud Configuration Management Procedure. The Configuration Management Procedure helps to ensure that a baseline standard exists and is adhered to in order to maintain consistency of the product's performance, functionality and physical attributes with its requirements, design, and operational information throughout its life for solutions and services managed by PTC Cloud.

Application software patches and updates are applied to hosted cloud solutions and supporting systems. Prior to applying patches, IT Administrators are responsible for reviewing operating system and software security updates. Review of high risk database and application security patches occurs at least on a monthly basis and at least quarterly for operating systems. Monthly, a system-generated baseline report is distributed and reviewed by IT Administrators. Results of the review including assessment of patches not applied are recorded within the support desk ticketing system.

Identity & Access Management

PTC Cloud has established and administers all accounts in accordance with a role-based scheme that organizes information system and network privileges into roles. Logical access to the network, systems, services, and applications is protected through the use of native operatin system and/or application level access control mechanisms and restricted through the use of identification and authentication mechanisms, including the use of unique account IDs ("UID") and passwords. Where possible, all infrastructure components applications, and services are configured to use a single sign-on functionality leveraging an identity directory service. Access to all administrative systems, services, and interfaces is limited to segmented, secured networks that may only be reached by means of PTC Cloud managed bastion hosts that are only reachable over a dedicated hosting environment Virtual Private Network (VPN). VPN software is configured with multi-factor authentication that leverages an out-of-band authentication ("OOBA") technique to identify and authenticate users and privileged users to the PTC Cloud network, infrastructure devices, systems and environments.

Incident and Vulnerability Management Process

PTC Cloud has documented an Incident and Response Management Policy and Plan to provide employees a process for informing the Company and Customers of potential security breaches. PTC's Incident & Response Policy and Plan are based on NIST Computer Security Incident Handling Guide – Special Publication 800-61. PTC Cloud Intrusion Detection system (IDS), is configured to provide continuous monitoring of PTC Cloud's hosting environments, early identification of potential security threats and vulnerabilities, and detect unusual system activity and non-compliance with regulations and standards across the PTC Cloud's hosting environments.

Reducing risk starts with the identification of vulnerabilities. PTC Cloud does this through periodic scheduled scans, ad hoc scans, penetration test initiatives, vulnerability tracking, and remediation.

Certifications and Audits

Over the years, PTC Cloud has worked with third-party auditors to test and benchmark the security program and as a result, are ISO 27001: 2013 certified and maintain SSAE16 SOC 2 Type II Security & Availability Trust Principles.

By being audited by third-parties, PTC Cloud maintains a rigorous Security and Compliance program in alignment with the ISO framework, the SSAE16 SOC 2 Type II Security & Availability Trust Principles and the Federal Risk, and Authorization Management Program (FedRAMP).

Additionally, PTC Cloud has implemented various risk reduction controls, including administrative and physical assets to manage access to computing systems and physical facilities.

Data Centers Security

PTC Cloud's data centers are able to meet the stringent audits of ISO 14001 and ISO 9001, and are SSAE 16 audited for the United States, and ISAE 3402 internationally. These data centers have multi-layered security that includes full-time 24/7 location operations and security guards, security cameras, alarms, vehicle barriers, locked cages, and multifactor access like photo-identification access cards, trap doors, and biometric devices.

Data Security

Data is encrypted in transit using HTTPS/TLS (Transport Layer Security). TLS 1.2 is default for communication with customers. For most connections, the content of the messages is further secured using Advanced Encryption Standard (AES) 128 algorithm, and the RSA 2048 algorithm is used for key exchanges. Data uploads are also encrypted through SSH tunnels or VPN.

Because PTC Cloud recognizes the need for data separation, each customers' data is held separately either through total physical hardware separation or separation of databases, schemas, and networking resources. Virtual Machine segregation and isolation reinforce our IaaS offerings. Network traffic is directed to specific hosts ensuring that customers' communications remain private and isolated.

Learn More

PTC Cloud understands the needs of enterprise businesses and provides the peace of mind you need for your mission-critical application services with the delivery you can rely on.

To learn more, speak to a PTC Cloud Expert to discuss your security questions or concerns or visit PTC.com/services/cloud/security to learn more.