WHITE PAPER

SECURITY AND RELIABILITY

POWERPLAN®

PowerPlan is dedicated to safeguarding your information

To protect the privacy of its customers and the safety of their information, PowerPlan maintains high standards of data security. PowerPlan relies upon state-of-the-art secure data centers, enforces strict internal product controls, and regularly audits its policies and procedures using third party auditors.

Some of the key tenets of PowerPlan's security program are:

- Security designed from the ground-up in the application, network, hardware, and operational procedures
- Use of SSAE 18 SOC 2 Type 2 audited and ISO-27001:2013 certified data centers
- PowerPlan conducts SSAE 18 SOC 1 Type 2 and SOC 2 Type 2 audits on the hosting services and environments
- Adherence to best practices for code development, testing and operations
- Regular vulnerability testing and penetration testing by third parties for the application, network, and infrastructure
- Consistent monitoring of the environments for availability, anti-virus & malware threats, unauthorized access and more
- Annual security awareness training for all employees and contractors, and annual security reviews of our vendors and data center providers

PowerPlan data centers have passed the rigorous security audits of leading financial services companies and corporations in the Global 1000.

The following sections of this document cover the key areas of PowerPlan security in detail, including: Physical Security, System Security, Operational Security, Reliability and Application and Data Security.

Physical Security

A key aspect of security is the physical security of the hardware containing the customer data. PowerPlan uses the leading hosting providers Amazon Web Services (US, EU and APAC) and Microsoft Azure (US) for its data centers.

PowerPlan data centers have the following physical safeguards:

- Data center staffed 24 hours a day, 7 days a week
- Each data center access is limited to Amazon Web Services technicians and Microsoft Azure data center technicians only
- Entry to the data centers is regulated by photographic identification, biometric scans, man traps and secured shipping/receiving areas isolated from data center floor

- Interior and external security camera surveillance monitoring, with the video stored for review
- Unmarked facilities to maintain a low profile
- Physical security audits by third parties

Further information about PowerPlan data center operations, security policies, and procedures are available at https://aws.amazon.com/compliance/, https://aws.amazon.com/security/, https://azure.microsoft.com/en-us/overview-trusted-cloud/compliance/, and https://azure.microsoft.com/en-us/overview/security/.

In addition to making sure that the infrastructure containing customer data is physically secure, PowerPlan makes sure the networks and hardware containing customer data are hardened and tested against attack.

Hardware security requirements include:

- New hardware and VM's are provisioned with a hardened operating system following documented procedures (for example: only necessary programs and services, default accounts disabled, default passwords changed, and all security patches and security monitoring agents applied)
- Security patches are applied on a regular basis
- All systems are firewall protected
- All public-facing machines are in a Demilitarized Zone (DMZ), in which a firewall separates public-facing from internal hardware
- Intrusion Prevention Systems and host-based Intrusion Detection Systems constantly monitor the internal network providing alerts to operations staff
- Next-gen anti-virus scanning and detection on all machines, with signatures updated every 24 hours and 24x7x365 monitoring and remediation for advanced threats
- Quarterly and on-demand penetration testing is conducted by an Approved Scanning Vendor
- All machines can only be accessed by named accounts, so that a detailed log of activities is available

In addition to securing your data, PowerPlan ensures that it will be available when you need it.

Operational Security

It is not enough to have a secure physical and network environment, they must be operated in a secure manner. PowerPlan and its data center providers work as a team and have the following operational security provisions:

Data center operational security includes:

- Policies and procedures that are SOC 2 Type 2 audited and ISO-27001:2013 certified
- Access to confidential information is limited to authorized personnel only, in accordance with documented processes
- All employees are trained on documented information security and privacy procedures
- Multiple and thorough background security checks are conducted for all data center personnel
- Systems access is logged and tracked for auditing purposes
- Secure document destruction policies and procedures are followed
- Change management procedures are fully documented
- Independently reviewed and regularly tested Disaster Recovery and Business Continuity plans

PowerPlan Corporate operational security includes:

- PowerPlan has fully documented policies and procedures
- Background checks are performed on all employees
- Access to the production network is limited to authorized personnel, who access it using a secure, site-to-site Virtual Private Network (VPN) with multifactor authentication
- Access to customer data is restricted to authorized personnel only, according to documented processes
- Documented and regularly tested Disaster Recovery and Business Continuity plans

Reliability

In addition to securing your data, PowerPlan ensures that it will be available.

- PowerPlan data centers provide a very reliable infrastructure for the hosting of the PowerPlan application
- System redundancy is provided at all levels, to ensure that your data is still available even in those rare situations when the first line of defense falters. This includes:
  - o N+1 redundant HVAC (i.e., there is at least one independent backup component to ensure system functionality continues in the event of a system failure)
  - o Advanced fire suppression

- Power
    - N+1 redundant Uninterruptable Power Supply
    - Onsite and regularly tested diesel generators for utility outages, with onsite fuel storage
- Network
    - Multiple Internet Service Providers (ISPs)
    - Fully redundant, enterprise-class routing equipment

- Intentional network underutilization, so that spikes are easily managed
    - Distributed Denial Of Service (DDOS) mitigation
- Support 24 hours a day, 7 days a week
- Regular backup of critical customer data is provided. Backups are encrypted using industry standard strong encryption and stored in an alternate data center region.
- All devices within the PowerPlan production infrastructure are fully redundant, highly available (HA) configurations. All devices are hot swappable, requiring no down time for hardware failure and replacement

PowerPlan solutions have been designed from the ground up to protect the security of your information.

Application and Data Security

A secure infrastructure cannot protect your data if the applications providing access to your data are not secure. PowerPlan solutions have been designed from the ground-up to protect the security of your information.

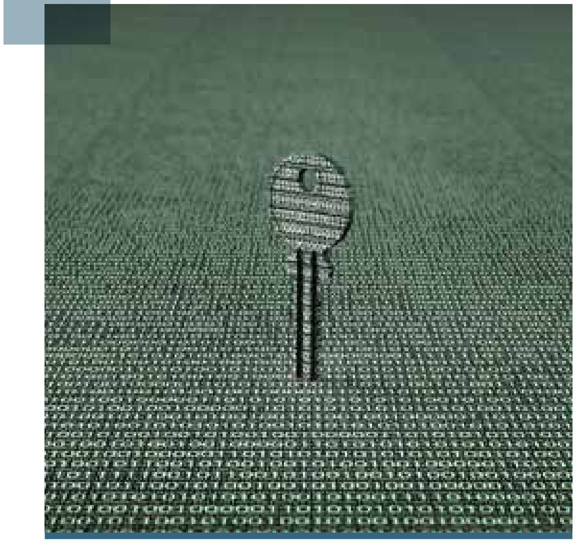
Application Security

User access to PowerPlan and your data is controlled by Authentication and Authorization.

Authentication

Authentication controls whether or not you can access PowerPlan. This generally involves checking credentials, determining if the user is enabled, and if they are logged in from an allowed network.

- PowerPlan applications integrate with customer's IdP using SAML 2.0 which provides a secure authentication method to the PowerPlan software and enables immediate termination of access at offboarding.
- PowerPlan personnel authenticate to hosting environments using 15-character passwords and multi-factor authentication
- When PowerPlan maintains credentials, they are encrypted and never stored in clear text
- Passwords maintained by PowerPlan solutions can only be reset, never recovered
- PowerPlan solutions automatically lock account access after a number of failed login attempts
- PowerPlan solutions support idle timeouts



Authorization

Authorization controls how the user can use the system and what they can view.

- PowerPlan solutions contain access controls that administrators can use to control and manage the breadth of functions and features available to their end users
- PowerPlan administrators can define security permissions by modules, configuration tables, and companies to allow end users to only see the information and utilize the functionality that they are allowed to access

Data Security

- Customer data is fully encrypted during transit via TLS channels. The status of the PowerPlan TLS support can be checked at any time via Qualys SSL Labs
- Customer data is AES-256 encrypted at rest using self-encrypting storage
- All customer data remains in the primary data center, with encrypted backups at the designated BC/DR location in an alternate region within the data center.
- PowerPlan solutions log authentications (login success and failure) and all administration operations.
- When a customer cancels their account with PowerPlan, their data and backups are permanently deleted from the PowerPlan data center and is no longer accessible.

Certifications

PowerPlan solutions maintain a number of independent security-related audits and certifications.

- PowerPlan's solutions are SOC 1 Type 2 and SOC 2 Type 2 audited every 6 months (PowerPlan's SOC reports are provided upon request)
- PowerPlan's data centers are SOC 1 Type 2 and SOC 2 Type 2 audited
- PowerPlan data centers are ISO-27001:2013 certified

Security Reporting

PowerPlan security policies and procedures are designed to minimize the risk of the breach of customer data. However, in the rare event of a breach of customer data, PowerPlan has a documented and annually tested Incident Response Plan for investigating the breach and reporting it to customers, working with the customers to mitigate the risk, and if necessary, reporting to regulators and legal authorities.

POWERPLAN®

PowerPlan.com
confidence@powerplan.com

Confidential & Proprietary – Copyright © 2021 PowerPlan, Inc.
REV21_04A