P.A.S.S.

Pro-Active Seamless Support

Simple, Reliable, Secure

1. What is it?

PASS is a full-featured, automated solution for monitoring your environment. It is easy to install and setup, and it works in the background. PASS constantly monitors your environment for any changes that may constitute an issue with the equipment's functionality. Once triggered, it opens a service ticket and sends error reports to System Engineers who can then troubleshoot and resolve the issue proactively before it becomes a problem or an interruption to the business.

2. How does it work?

With Storage; PASS utilizes the array's Service Processor's own monitoring capabilities, as well as PASS's own protocols, to detect changes or errors in the state of the array. It then saves those changes in a log. Every 10 minutes, PASS compares the new log to the old, hashes and saves any log changes. It zips, encrypts and sends the log changes to the 'Central Diagnostic Center' where the package is unzipped, un-encrypted and un-hashed. The codes in the log are compared to and deciphered from the relevant databases in the Central Diagnostic Center. If there is an error, the Central Diagnostic Center then notifies all related parties (eg. engineers, customer, etc..) and immediately opens up a service ticket in our Response Ticketing system. Engineers can then investigate issues via a secure connection to the 'interface'. With Systems; PASS is loaded to a local workstation and monitors devices for triggered events which are severe in nature and passes a notification to the PASS software. The error log is compared in the same manner as storage to the Central Diagnostic Center and notifies all parties accordingly.

4-part Platform:

The PASS System is broken up into 4 parts. This is done to increase efficiency, reliability and security. The 4 parts are:

1. **Array API** -- independent client-side software package installed on the Storage Array's Service Processor which monitors the array and communicates to the Central Diagnostic Center.
2. **Workstation API** – similar to the Array API, but installed onto a workstation and monitors other devices and communicates to the Central Diagnostic Center.
3. **Central Diagnostic Center** -- the main data-center side server cluster where info is sent from the API, interpreted and the needed actions are initiated.
4. **Interface** -- The connection platform for System Engineers to securely connect to the Central Diagnostic Center in order to further investigate API communique and possible array issues.

Multi-part Service Method:

The PASS workload is broken into 4 parts. This is done to improve compatibility, modularity and security. The 4 stages are:

1. Monitor & Detection
2. Encryption & Transport
3. Decipher & Identify
4. Alert

Health-checks:

Heartbeats -- Several times per day, an API will send a 'heartbeat' to the Central Diagnostic Center. This heartbeat is little more than a time-stamp, letting the Central Diagnostic Center know that the device is alive and healthy. The Central Diagnostic Center expects a heartbeat from each API at a specific time. If the Central Diagnostic Center doesn't receive a heartbeat from a specific device from a determined length of time, it sends an alert to engineers to investigate the situation.

3. What are its features?

One-time Install:

PASS installs quickly and easily onto any Storage Array's Service Processor or Workstation. Once it is configured for the device, it just works, and it works well. There is no need to 'ping', initiate, reconfigure or "tweak" a PASS installation. “It just works”.

Smart-Design:

We live in a world without the perfect platform. Software crashes and operating systems "blue-screen". This is a constant and consistent reality. To combat these difficulties, PASS was built to be aware of its environment. PASS monitors its platform constantly and is able to actively and independently restart dead and zombie processes and services or even reboot the Service Processor / Workstation, if needed, to ensure proper functioning of the device and of PASS.

Compatibility:

In the world of IT Infrastructures, you'll rarely (if ever) see a homogeneous network. Every company utilizes a patchwork of machines with different manufacturers, models, from different eras, and with different features. An all-encompassing solution is needed to simplify the already too complex task of ensuring the health of a corporate environment. To this end, PASS was designed to function on ANY Storage Array or Workstation utilizing a Windows or Linux based Service processor, regardless of make or model. It's a one-stop shop for data integrity.

Security:

1. PASS resides in the Central Diagnostic Center in our highly secure, hardened data-center, in a DMZ, and behind a double firewall; this configuration is nearly impervious to various network scans attacks.

2. Client initiated connections -- All PASS communications start at the API and are sent to the Central Diagnostic Center. This ensures that connections can't be 'spoofed' by 3rd parties or used to control PASS or the array.

3. 256-bit AES encryption -- All communications within PASS are encrypted to ensure data security throughout the transmission.

4. Secure, triple-authenticated point-to-point protocols -- All PASS transmissions are initiated through highly authenticated protocols which ensure that only PASS is on the line.

Constant Upgrades and Improvements:

PASS is constantly being upgraded and improved. New security protocols and feature sets are being added daily, with mass roll-outs performed quarterly. PASS always keeps one step ahead of the game.

4. FAQ

Is PASS PCI Compliant??

-- PASS was built with the PCI compliance needs of our customers in mind. Not only does PASS meet these standards, but exceeds requirements several-fold.

Is PASS Hackable (i.e. vulnerable to spoofing, man-in-the-middle, etc.)?

-- In reality NO software or hardware on earth is 100% impervious to attack. Even the U.S. military's newest unmanned APIs have been hacked by university students. We are very aware of this. Hackers are thwarted by PASS in 2 ways: 1. Over-the-top and even unnecessary security protocols are used. 2. Very little information (which is actually quite useless info to hackers) is transferred from client machine to the 'Central Diagnostic Center'.

What info does PASS transfer?

-- PASS ONLY transfers an encrypted, hashed version of the specific info regarding the current hardware or software ERROR which has occurred... ONLY the ERROR. NO other info concerning machine type, configuration, or use is included. If a hacker tried to intercept a PASS communication and, was able to decrypt the message (assuming the hacker already possessed the manufacturer's proprietary database of codes identifying specific errors), they would ONLY know that an error has occurred on a machine (eg. drive failure, etc...). All info regarding the identity and configuration of the machine is stored on the PASS 'Central Diagnostic Center'.

Does PASS access data stored on the storage array?

-- PASS only transfers information from the storage array's service processor. NO DATA in any shape or form stored on the array's Hard Drives can be accessed by the service processor; therefore, no customer data can be gleaned or sent off-premises by PASS.

How does the PASS client communicate with the 'Central Diagnostic Center'?

-- Each PASS client can connect with the 'Central Diagnostic Center' via either modem or network, all using proprietary encrypted point-to-point protocols based on ssh2 with multi-key authentication. PASS uses a proprietary, fully-encrypted transmission method similar to sftp (i.e. ftp over ssh) to send the encrypted log from the API to the Central Diagnostic Center. This transmission is a one-way street. The Central Diagnostic Center cannot send communication to an API during this 'call'. If it did, the API would not respond and the connection would be closed.

Does PASS access information on servers or other devices?

-- PASS only transfers information from the event logs on a system or device. Most event logs are passed through triggers; therefore, no customer data can be gleaned or sent off-premises by PASS.

Could a hacker use PASS to hack my network?

-- PASS is a client-to-host protocol and cannot work the other way around. All communiques are client initiated and cannot be initiated from an external source. A hacker would have to already have physical access to the array's service processor to find, or change PASS in any way. However, by this point, they've already hacked the machine without using PASS.

For more information, please call Sherlock Services at (866) 827-6804.