Security and Infrastructure Overview

Paymaster is hosted *at* Microsoft Azure facilities in South Africa . *Paymaster resides on a combination of our own physical servers and Azure's virtual hosting infrastructure.*

Unlike a typical corporate network, due to Paymaster's cloud based model, no clients are able to log onto our network in the hosted environment.

Protection at the Application Level

Paymaster protects your data by ensuring that only authorized users can access it.

- *Paymaster is powered by a single instance, multi-tenant architecture, in which all users and applications share a single, common infrastructure i.e. database, and code base but is logically unique for each customer. Authorization and security policies ensure that each customer's data is kept separate from that of other customers through the use of a TenantID field which associates each record, across multiple tables, with an individual tenant.*
- *Paymaster provides each user in an organisation with a unique email address and password that must be entered each time a user logs on. This user record is associated with a TenantID.*
- *All access to Paymaster is governed by strict password security policies and all passwords are stored in encrypted format within the encrypted database providing a double layer of security.*
  Further to the passwords being encrypted, the entire database is encrypted at rest.
- *Users are required to select a strong password based on the following criteria:*
- - *be a minimum of 8 characters.*
  - *contain a minimum of 1 numeric characters.*
  - *contain a minimum of 1 Uppercase character.*
  - *contain a minimum of 1 lowercase character.*
  - *not contain the word 'password' (i.e. password1)*
  - *not contain space(s) between characters (i.e. pass 1word)*

  Users accounts are locked after there have been more than 5 unsuccessful login attempts
- *128 bit SSL encryption is present on every form within the system – this means your information is encrypted during transmission between our servers and your browser.*
- *Administrators can define security roles and attach users to these roles. Roles can be defined to restrict or allow users to any form within the system.*
- *Administrators can give users access to view specific employees that are in turn attached to organisation units defined on company level. This restricts users to only see employees' details in specific units.*
- *All employee self-service users are only able to view their own profiles.*
  Reports that are emailed to users are sent in a password protected zip file.
- *An audit trail exists on every screen for traceability purposes.*

Protection at the Facilities Level

Paymaster utilises one of the most modern data centres in South Africa. The security in the data centre consists of visible and invisible physical measures and other facilities to guarantee an uninterrupted service.

- Paymaster is backed up every 15 mins to an offsite disaster recovery site and every evening a full backup is also done and stored in encrypted format.
- No public access - Public access to the hosting facilities is strictly forbidden.
- Video surveillance - Live video surveillance of the entire data centre is in place 24 hours a day. All entrances are monitored to the data centres to ensure that only authorized personnel enter them.
- Access cards – A data-centre access proximity card system represents the second layer of security for entering the data centre. Access to the data centre itself is restricted to Certified Technical Points of Contact. Biometric security - Biometric security systems are the third layer of security for entering the data center.
- Biometric hand scanners are used to restrict access to the data centre and only Certified Technical Points of Contact have use of the biometric hand scanner system to enter the data centre.

In addition, the following safety and redundancy measures are in place to ensure continuity and stability at the data centre:

- Redundancy - All critical systems in the hosting centre are redundant. (N+N redundancy indicates having a complete replica of the system in place, as backup should the primary system fail.)
- Environmental monitoring - The data centres have N+N redundant heating, ventilation, and air conditioning systems to ensure that, even in the event of a system failure, the hosting environment will not be affected. The data centre also has an advanced fire-suppression system in place to contain fire.
- UPS (uninterrupted power supply) systems – The power systems are designed to run uninterrupted even in the event of a total power outage. All production systems in your hosting environment are fed with conditioned UPS power that will run whenever utility power fails. The UPS power subsystem is N+N redundant, with instantaneous fail-over to generators to ensure continuity.
- Diesel generator systems – Onsite diesel generators automatically start up in the event of a power surge or interruption in the power supply.

Protection at the Network Level

Paymaster uses proven security practices to ensure network security.

- Paymaster utilises a perimeter firewall that protects our network from malicious or unwanted behaviour from traffic entering our network as well as keeping our network safe from Zero Day attacks, DOS (denial of service) and DDOS (distributed denial of service) attacks, spoofing attacks and malicious code.
- Our Intrusion Prevention Systems (IPS) is a network security service that monitors network and/or system activities for malicious or unwanted behaviour and can react, in real-time, to block or prevent those activities.

McAfee Vulnerability Scanning Process

Paymaster uses McAfee vulnerability scanning process on a daily basis to crawl our website for any vulnerabilities.

Audit - Port Scan

The first audit phase is a thorough, interactive port scan. Accurately determining which ports on an IP address are open is the crucial first step to a comprehensive security audit. The McAfee Secure proprietary firewall and IDS/IPS aware network discovery technology is designed to accurately map out any size or complexity of network topology. This is often not a simple process. Unlike most scanning solutions based on Nmap, McAfee advanced dynamic port scanning can handle all targets, from desktop PCs to the most aggressive firewalls, IDS and IPS systems.

Audit - Network Services Scan

During this second audit phase of the audit process, McAfee thoroughly interrogate each service running on every available port to determine exactly what software is running and how it is configured. Once this information is acquired it is matched to their Knowledge Base of vulnerabilities in order to launch additional application specific and generic tests of each available service. These tests are based on their extensive knowledge base of over 10,000 vulnerabilities, which is updated every 15 minutes.

Audit - Web Application Scan

Web application testing is the third audit phase of the McAfee Secure daily security audit, and perhaps the most important. According to analyst firm Gartner Group, an estimated 70% of all security breaches today are due to vulnerabilities within the web application layer. Traditional security mechanisms such as firewalls and IDS' provide little or no protection against attacks on your web applications. During this testing phase, all HTTP services and virtual domains are checked for the existence of potentially dangerous modules, configurations settings, CGIs and other scripts, and default installed files. The web site is then deep crawled, including flash embedded links and password protected pages, to find forms and other potentially dangerous interactive elements. These are then exercised in specific ways to disclose any application-level vulnerabilities such as code revelation, cross-site scripting and SQL injection. Both generic and software specific tests are performed in order to uncover misconfigurations and coding error vulnerabilities.