

Security Measurements Summary

- Advanced dedicated servers are used for data storage. These servers are hosted by 1-Grid, one of SA's leading hosting companies, whom also host some of the largest companies in South Africa and overseas.
- Server Type: Managed. Data is automatically backed up daily, using specific backup software. Five backups are kept at any given time.
- End-to-end encryption: Comodo security solutions Inc, a U.S based company is used to encrypt and secure our data. Users will notice the s behind the http in the url (https) stands for secure. It indicates that the user is working in a secure environment. Data transmitted from these pages / url's is encrypted and useless to hackers. See below for more information regarding SSL certification.
- Anti-Virus: ESET File Server Security is used to protect the servers from Viruses, Malware and Ransom ware. ESET is famous for being one of the best anti-virus systems and is used by Corporates like Honda, Canon and Allianz. See below for more information on ESET
- Separate data tables for each client: Each profile has its own separate space on the server and only users with the necessary authentication i.e. staff created as users can access these files. There are no shared databases.



COMODO
Creating Trust Online™

A Brief Introduction on how SSL/TLS encryption works

Secure Sockets Layer (SSL) technology protects transactions between your website and visitors. The protocol uses a third party, a Certificate Authority (CA), to identify one end or both ends of the transactions. This is in short how it works.

A browser requests a secure page (usually https ://). Once the secure transaction is initiated, the web server sends its own public key with its own certificate.

The browser checks that the certificate was issued by a trusted party (usually a trusted CA such as COMODO), that the certificate is related to the site contacted and is still valid.

The browser then uses the public key, to encrypt a random symmetric encryption key and sends it to the server with the encrypted URL required as well as other encrypted http data.

The web server decrypts the symmetric encryption key using its private key and uses the symmetric key to decrypt the URL and http data.

The web server sends back the requested html document and the http data encrypted by the symmetric key.

The browser decrypts the http data and html document using the symmetric key and displays the information. In addition to encryption security, SSL certificates give important visual cues to the website's visitor that they are in a secure environment.



- Ransomware prevention
- Zero-day threats detection
- Data breach prevention
- Botnet protection

Multi-layered defense

A single layer of defence isn't sufficient in today's constantly evolving threat landscape. All ESET endpoint products have the ability to detect malware pre-execution, during execution and post-execution. An additional layer is implemented in the form of cloud sandbox analysis with **ESET Dynamic Threat Defense**. By focusing not just on a specific part of the malware lifecycle, this allows ESET to provide the highest level of protection possible.

Server Management

ESET File Security solutions are managed from a single pane of glass that can be installed on Windows or Linux. In addition to installation, ESET has a virtual appliance that you can simply import for quick and easy setup.

Machine learning

All ESET products currently use machine learning in conjunction with all of our other layers of defence and have done so since 1997. Specifically, machine learning is used in the form of consolidated output and neural networks.

Protection of Personal Information Act (POPI)

POPI Act is the Protection of Personal Information Act of South Africa. The Act aims to **regulate** how personal information is processed. The bill broadly defines personal information as anything relating to an "identifiable, living natural person or juristic person" (companies, CC's etc).

We have been meticulous in ensuring our platform is compliant to this act, particularly in relation to the security of data.

Organisations processing a lot of personal information, especially specific personal information like children's information and /or account numbers need to be even more attentive to this act. As accountants in practice, processing personal information is part of our daily routine and as such we are responsible for complying with the conditions set out. There are eight general conditions and three extra conditions summarised here: <http://www.lexisnexis.co.za/pdf/POPI-Infographic.pdf>

Our platform creates the opportunity to easily comply with the POPI Act

