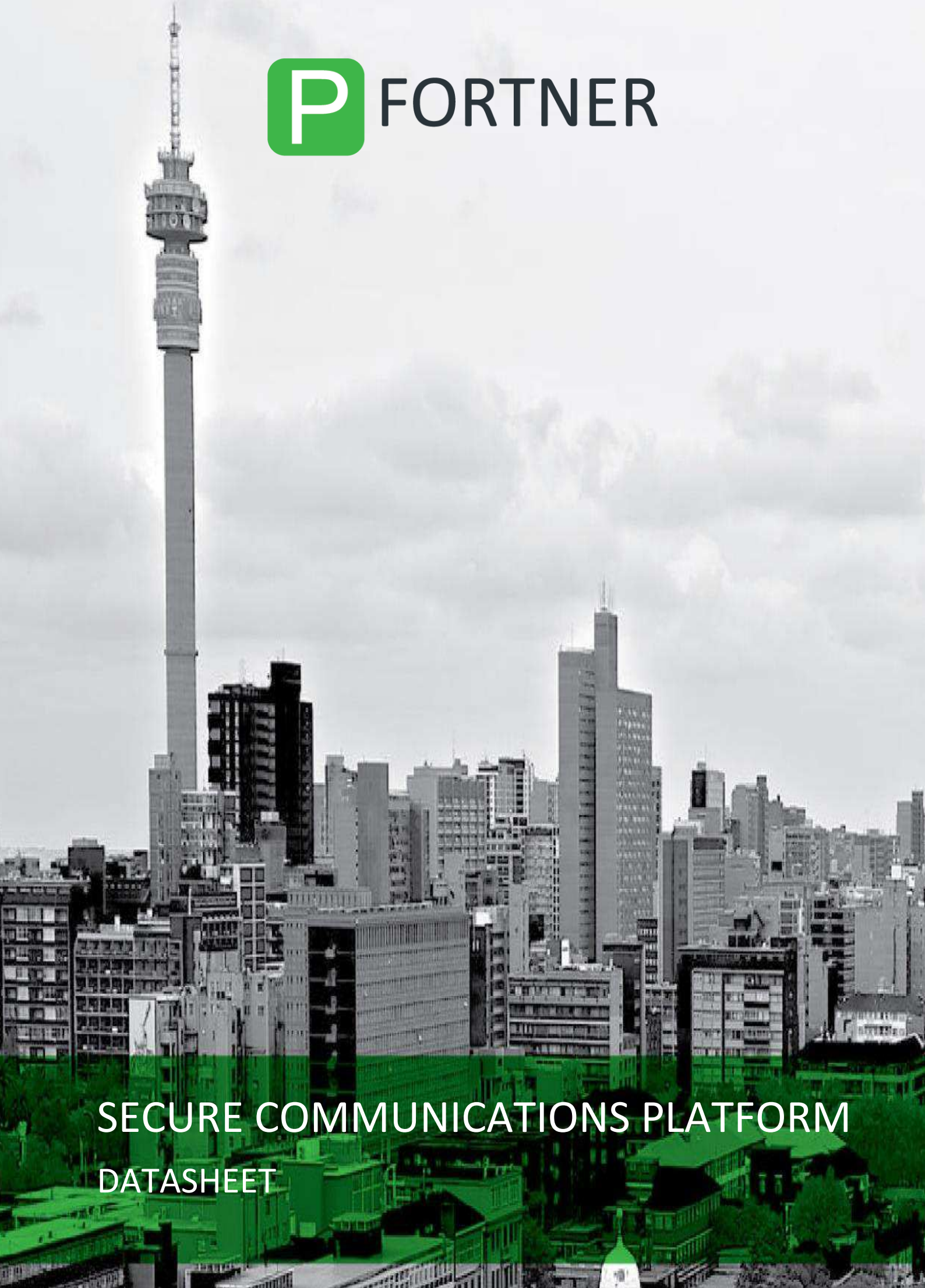
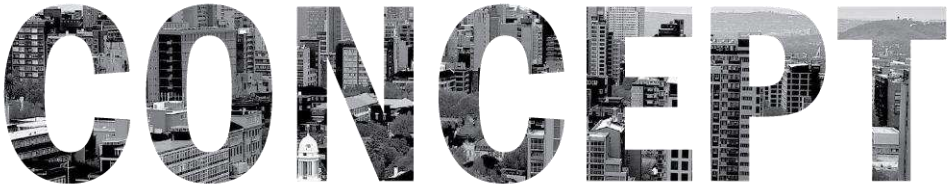
FORTNER



SECURE COMMUNICATIONS PLATFORM

DATASHEET



What is SCP?

PFORTNER SCP (Secure Communications Platform) is a person to person communications solution that protects confidential information flowing between employees, business partners and clients.

It could also be defined as a data sovereign OUT OF BAND communications platform that allows for governance and oversight.

The system provides interaction via browser, smartphone app or Outlook plugin and can be hosted in the cloud or on premise.

"Data sovereign OUT OF BAND communications platform"

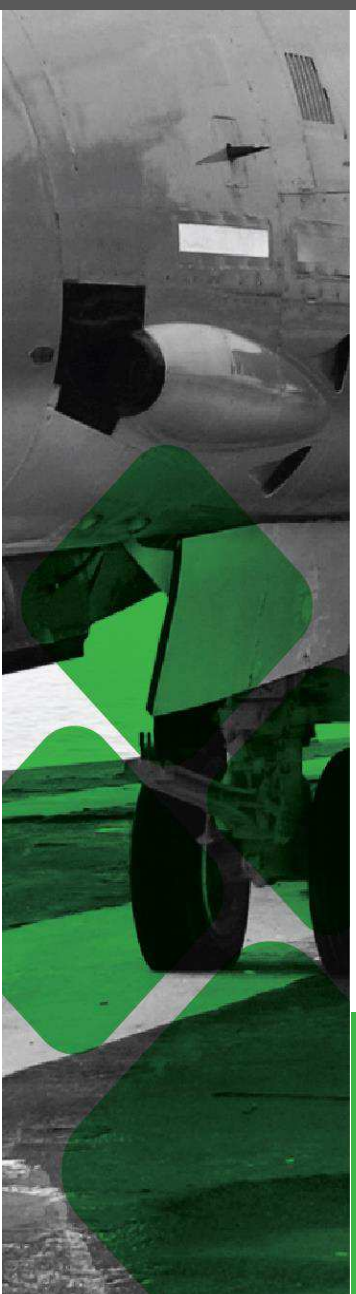
What are the benefits of SCP?

- Comply with data protection laws
- Reduce risk of unauthorised dissemination of information
- Structured data trail with reporting for audit purposes
- Simple on boarding process
- Seamless integration into current business processes

What are the main features of SCP?

- Secure instant messaging
- Secure file sharing
- Subject-based conversations
- Cross-platform
- Active Directory integration
- Searchable
- Customisable

What makes SCP different?



Data Sovereignty

Data ownership and control of all secure communications makes SCP stand out from its competition.

Competitive products offer either secure end-to-end encryption without any storage / management capabilities or the users' data is stored on the provider's servers making the data vulnerable to exploitation by the host. Neither of these approaches are suited for everyday business requirements.

SCP's approach gives users the security and privacy needed while giving business the control of that communication data whilst never loosening security standards.

Simplicity

SCP is designed to be accessible and easy to adopt. Because SCP is accessible through any browser anywhere in the world, adoption is made easy and workflow is seamless.

Microsoft Outlook users can enjoy the security of SCP from within that familiar email environment.

Users on the move can access all their SCP discussions straight from their mobile phones through the app or even the mobile browser.

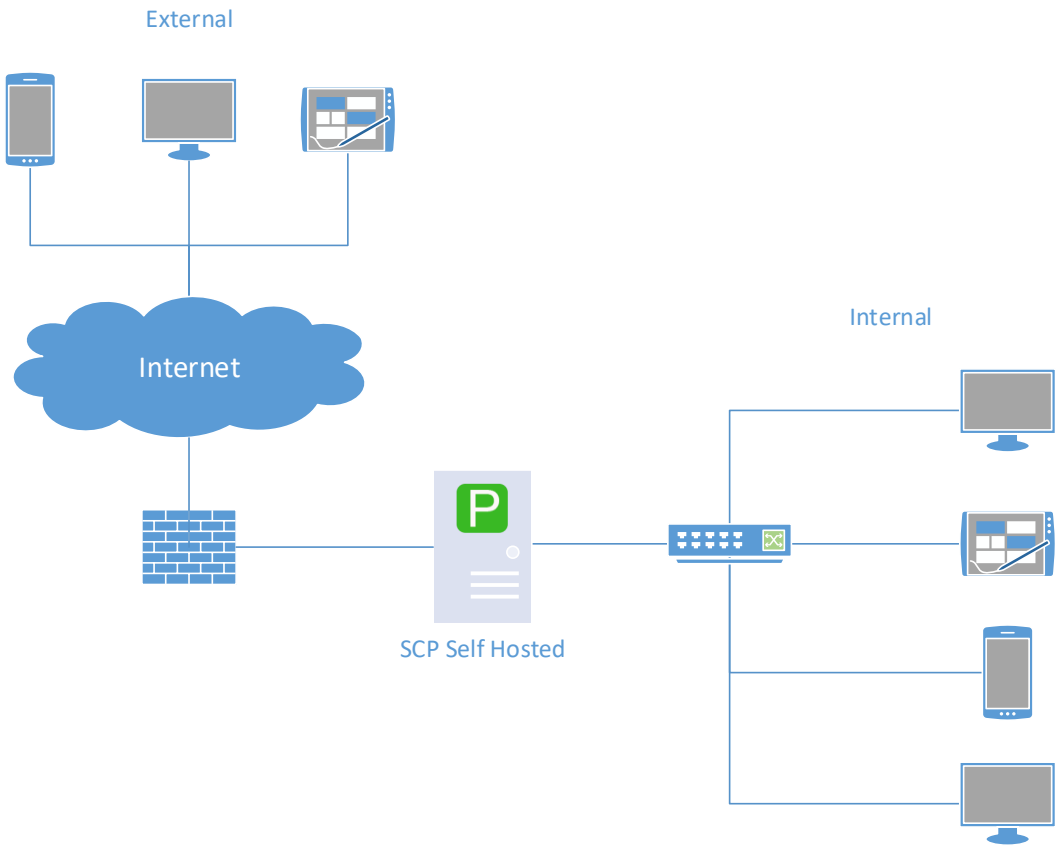
"OUT OF BAND" communication is the data transferred through an independent data stream contrary to the normal data flow. This mechanism provides an alternative encrypted channel, which allows any data sent via that mechanism to be secure.

How does SCP work?

Architecture

SCP servers are built with a hardened Linux OS deployable on cloud/organisation's data centre. On the application level, SCP has a Service Oriented Architecture (SOA). Client-server communication is protected by TLS/SSL.

Communication is handled by a REST API and push messaging (both Google Cloud Messaging (GCM) and Apple Push Notification Service (APN)). This makes it easy to integrate into SCP from third party tools.



Encryption

SCP uses TLS 1.2. The security of this algorithms has been tested over many years of use in hundreds of different applications. Organisations can therefore rest assured that all communications are secure while in transit.

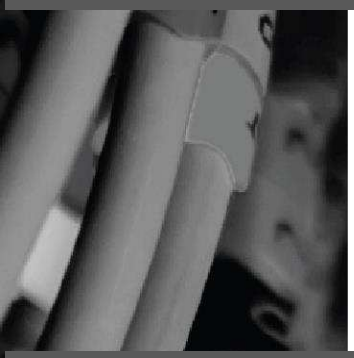
Messages are furthermore segregated per conversation based on the participants, resulting in only intended recipients being able to see the messages within their conversations.

Distribution

The outlook plugin is distributed through the web client as a download from within the client. The iOS and Android apps are distributed via private or public app stores. The SCP system can be distributed as a virtual machine or a hard install for any of the following formats:

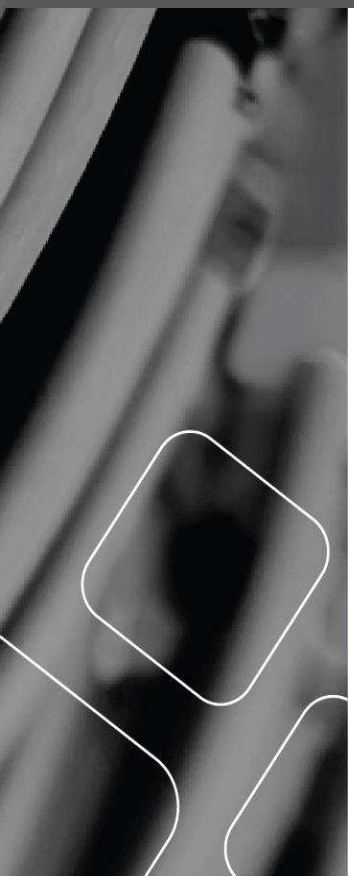
- Amazon EC2 image
- DASD (.raw)
- Live CD/DVD (.iso)
- OVF Virtual machine
- Preload ISO (.iso)
- VMware / VirtualBox / KVM (.vmdk)
- Xen guest

Can SCP's security be trusted?



SCP goes through rigorous penetration testing to ensure our security implementations are up to standard. The penetration tests are done annually by SensePost (www.sensepost.com), an internationally renowned penetration testing company.

Some use cases include



Board & Executive communications
Large file transfers
Staff and Group communication
Collaboration with regulators / auditors
Secure person to person communications
Healthcare providers sharing patient information
Card data handling and taking Exchange out of PCI DSS scope
Dealing with 3rd parties
Private wealth individuals communicating with bankers
One Time Pin
Sharing of Personally Identifiable Data


SECURE | COMMUNICATIONS PLATFORM