Open source software (OSS) is emerging as a core part of IT infrastructure and applications, largely due to the growing popularity of agile development methodologies and DevOps practices. With a substantial number of commercial and bespoke applications incorporating OSS, it cannot, and should not, be ignored. So how can organisations effectively manage the challenges of using OSS, while maximising its benefits and reaping the rewards?

OPEN SOURCE SOFTWARE: IT’S HERE TO STAY
After a slow start within the corporate environment, OSS is now on an upward trend and will quickly become an important part of business operations. Awareness of OSS will grow as organisations recognise where OSS already exists and begin to incorporate it within their IT infrastructure.

With OSS becoming commonplace within organisations, it brings a different set of risks and perceived challenges compared to closed source (proprietary) software. Establishing the difference between the myth and the reality will be critical to securing OSS.

As it becomes the mainstay within application development and infrastructure, security professionals will need to understand OSS and manage the challenges associated with its components.

ABOUT THIS BRIEFING PAPER
This briefing paper introduces the topic of OSS and debunks some of the related myths. It helps security leaders to:
- understand what OSS is
- recognise the challenges and appreciate the benefits of using OSS
- set up a programme of protective measures to effectively manage OSS.

OSS is often perceived as being insecure and unsupported. As these negative connotations continue to taint its reputation, some organisations officially prohibit it, even though they may unknowingly be using OSS. Others wholeheartedly adopt OSS, harnessing its advantages, such as aiding flexible and rapid development. OSS will continue to divide opinion for some time to come.

This paper demonstrates that OSS is here to stay and that it can be a positive influence on software development, if used and managed responsibly.

Deploying Open Source Software: Challenges and rewards
May 2020

AUTHOR
Paul Holland

REVIEW AND QUALITY ASSURANCE
Andy Jones
Eleanor Thrower
Emma Bickerstaffe
Mark Ward

DESIGN AND ILLUSTRATION
Vijay Mistry

INFORMATION SECURITY FORUM
Founded in 1989, the ISF is an independent, not-for-profit association of leading organisations from around the world. The organisation is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management and developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organisations and developed through an extensive research and work programme. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions.

By working together, ISF Members avoid the major expenditure required to reach the same goals on their own.

Consultancy services are available to support the implementation of ISF Products.

WARNING
This document is confidential and is intended for the attention of and use by either organisations that are Members of the Information Security Forum (ISF) or by persons who have purchased it from the ISF direct. If you are not a Member of the ISF or have received this document in error, please destroy it or contact the ISF on info@securityforum.org. Any storage or use of this document by organisations which are not Members of the ISF or who have not validly acquired the report directly from the ISF is not permitted and strictly prohibited. This document has been produced with care and to the best of our ability. However, both the Information Security Forum and the Information Security Forum Limited accept no responsibility for any problems or incidents arising from its use.

CLASSIFICATION
Restricted to ISF Members, ISF Service Providers and non-Members who have acquired the report from the ISF.