Securing the Cloud - Solution Brief

Secure Cloud Computing

A Cloud Access Security Broker (CASB) solution enables your enterprise to safely adopt cloud applications, enforce compliance and ensure data security at the point of access and on any device.

Major concerns for organisations using public cloud include secure user access, data visibility, control and compliance and additional threats from the increased cloud attack surface. Organisations must enable employees to safely use cloud apps on a range of devices, both corporate supplied and BYOD from wherever they might be located.

A Cloud Access Security Broker (CASB) is a policy enforcement point that delivers secure connectivity, data monitoring and threat protection in the cloud, on any device, anywhere.

Our CASB solution with integrated identity management, includes native SAML Single Sign-on, Active Directory synchronisation and authentication, contextual multi-factor authentication, and more - without the hassles of budgeting for and deploying a third party identity system.

Incorporated, high-performance Data Loss Prevention and access control engines identify and control the context by which applications are being accessed, as well as the data being accessed. Contextual access control tracks numerous contextual variables, including location, user group, access method, managed vs unmanaged device, time-of-day and more. Fine-grained control allows your organisation to vary the level of access within and across cloud applications.

Integrated Zero-Day Malware Threat protection, powered by Cylance, to analyse and block known and unknown threats either at rest or in the cloud, known and unknown malware threats are blocked even on unmanaged devices without agents.

The CASB management system learns user behaviour while collecting detailed reporting on every user and admin transaction. Increased control, such as step-up authentication, and suspicious activity alerting provide visibility and mitigation to minimise risk.

Key Features

Protect data on managed and unmanaged devices
Enable employees to use cloud apps on a range of devices whilst monitoring and securing sensitive data.

Detect and respond to suspicious activity
Detect and block irregular user behaviour.

Mission critical visibility and analytics
Single pane, cross app views into employee cloud usage.
Customisable alerts that provide instant visibility of emerging threats

Identify threats from unauthorised shadow IT
Establish what SaaS applications are being used by employees and asses the threats they present to your network.

Identity Management
On-board multifactor authentication, AD integration and support for major IAM vendors.

Contact

t: +44 (0)330 2233915
e: webenq@ng-it.co.uk
w: www.ng-it.co.uk

Registered Office 4 Oxford
Court
Manchester
United Kingdom
M2 3WQ

About NG-IT

NG-IT Limited is a privately held IT Solutions partner providing next generation cloud infrastructure and cloud security. Our aim is to provide peace of mind for our customers so they remain focussed on managing and growing their business.

Specifications within are subject to change without notice.