5 STEPS TO CONTROL CLOUD USAGE

Better the cloud you control (than the one you don't)

The cloud exists in every modern enterprise

But what about the Shadow IT infrastructure in your organisation?

33% of UK companies have a secure BYOD mobile strategy

69% think employees working outside the office is a security risk

60% admit employees use unsanctioned file-sharing or productivity apps

40% say the primary concern about millennials is their use of unapproved apps and devices

(Source: Ponemon 2017)

The average enterprise has over 1,000 cloud services in operation – more than 90% are not 'enterprise ready'.[1]

The business relies on those services

You need the right balance: Enabling services without impacting security or compliance

Blocking those cloud applications is not the answer

Cloud access security brokers help enterprises shine a light on their Shadow IT infrastructure in five steps

A cloud access security broker (CASB) is on-premises or cloud-based software that sits between cloud service users and cloud applications to monitor all activity and enforce security policies. (Wikipedia)

5 Steps to Control Cloud Usage

1 Get full visibility of cloud usage

- Understand all the cloud services used in your enterprise
- Assess enterprise readiness by evaluating risk scores based on your usage
- Identify traffic from sanctioned and unsanctioned cloud services
- Determine whether access is from on premises or remote users

2 Take granular control of cloud services

- Don't 'block everything' – cloud services are being used for valid business reasons
- Set security policies based on identity, service, activity and data
- Protect sensitive data with advanced cloud data loss prevention
- Mix and match policy elements to reduce risk without blocking services

3 Protect your valuable data

- Enable easy sharing via cloud services, without risking sensitive company data
- Detect sensitive data as it moves to and from sanctioned (and unsanctioned) cloud services
- Protect sensitive data with strong encryption
- Stop data exfiltration to unsanctioned cloud destinations

4 Keep your enterprise compliant

- Understand activity-level usage of your cloud services
- Detect non-compliant behaviour and anomalies
- Maintain detailed audit trails of all cloud activities
- Govern access to your cloud services to ensure compliance

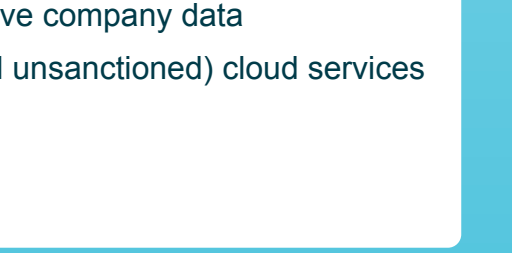
5 Run due diligence on cloud services

- Run checks on new and requested apps and cloud services
- Check appropriate security controls can be applied
- Ensure that usage of services can be audited for compliance purposes
- Assess whether the services will compromise business continuity plans

Get in touch to find out how to identify your Shadow IT infrastructure

www.netskope.com | 020 3962 1800

1 February 2018 Netskope Cloud Report



netskope