SWG AND CASB

Endida's Secure Web Gateway (SWG) and Cloud Access Security Broker (CASB) are built from the ground up to fit with todays hybrid working environment, ensuring your corporate devices are secure and adhearing to policy no matter where they are.

WHAT DOES SWG AND CASB PROVIDE?

Secure Web Gateway

Enforce strict browsing policy for any website

Browser Isolation

Only safe content is delivered to users

Hybrid Enforcement

Policy enforced in office, at home or anywhere

Cloud Access Security Broker

Direct and secure access to SaaS platforms

Data Loss Prevention

Erase the risk of data leaks or data copying

Greater Productivity

Increase productivity on corporate devices

GET IN TOUCH TO FIND OUT HOW WE CAN HELP YOU TODAY

endida.com | 0238 2180 428 | info@endida.com

THE FOUR CORNERSTONE FOUNDATIONS OF SWG AND CASB

VISIBILITY

Companies need visibility and control across both managed and unmanaged cloud services

COMPLIANCE & POLICY

Regulatory, local and governmental compliance regulations are increasing for cloud-based applications

DATA SECURITY

Endida's service will protect any data that is travelling to, within and stored in the cloud reducing the risks of costly data leaks.

THREAT PROTECTION

We use the data from typical user patterns to identify malicious behaviour and activities as well as negligent behaviour.

HOW DOES SWG AND CASB WORK?

With our service in place we can detect & prevent cyber threats and enforce security policies to prevent unauthorised access and data leakage. Additionally, Endida provides analytics and reporting which helps to identify security risks and compliance gaps, and provides actionable insights into how you can improve your security posture.

ENFORCING SECURITY POLICY

Be sure it is your employees and known devices accessing your cloud-based applications.

ADAPTIVE ACCESS CONTROL

Give access to the right data by the right people in you organisation rather than blanket access to everyone.

DATA LOSS PREVENTION

Put in place measures to ensure your data is not at risk from outside attackers or insider threats (disgruntled employees).

BEHAVIOUR ANALYTICS

Is an employee accessing data or a cloud-based application they don't normally have access too?

AUTOMATED REMEDIATION

If any of the rules are violated or compromised, automatically shutdown access and investigate.

PRODUCTIVITY GAINS

Prevent access to non-productive sites and applications, including personal Gmail, social media and even job sites.

GET IN TOUCH TO FIND OUT HOW WE CAN HELP YOU TODAY

endida.com | 0238 2180 428 | info@endida.com