Cloud computing has offered a wealth of opportunity to every business. There are more applications, more services and more platforms than ever before. Adopting these services can drive business benefits but it does potentially introduce more risk factors. These risk factors include data loss, unauthorised system access or the complexity of network identity management. The broadening of any organisation's network perimeter, along with device mobility, affords greater flexibility and increased efficiency but does increase risk.

This risk needs to be addressed and managed as part of business operations. However it isn't just an aspiration or a need, it is typically a legal or regulatory necessity that carries penalties for failure.

The Problem

Company infrastructures have grown over time. There is a desire to increase the utilisation of internet based services and make greater use of the cloud. This does however increase the perimeter of an organisation's estate and dramatically increase the number of touchpoints. These touchpoints or entry points to the organisation include internet based communications, private cloud communications and business-to-business communications, to name but a few.

A Chief Information and Security Officer (CISO) will look to protect their business and make the appropriate risk based decisions to achieve this goal. These decisions are often made without full and comprehensive data or are based on legacy data which does not afford a timely or accurate picture.
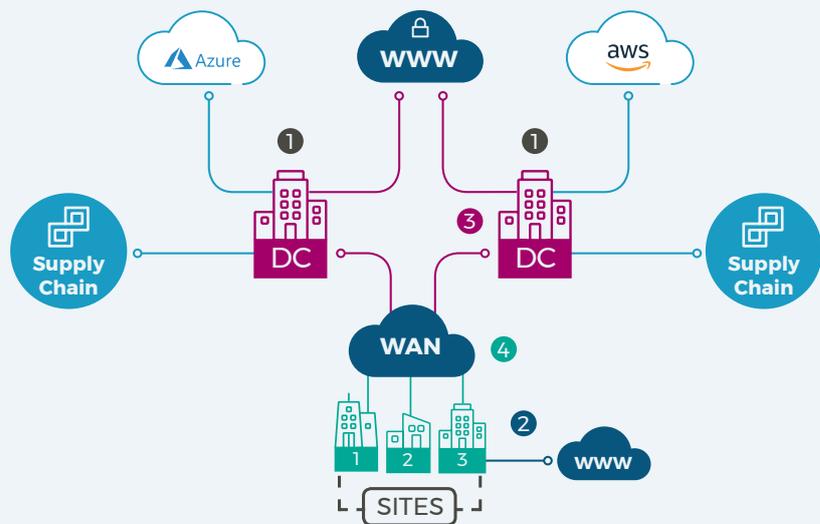
Challenges

1 Multiple egress points with different security policies

2 Shadow IT

3 Incomplete SIEM logs
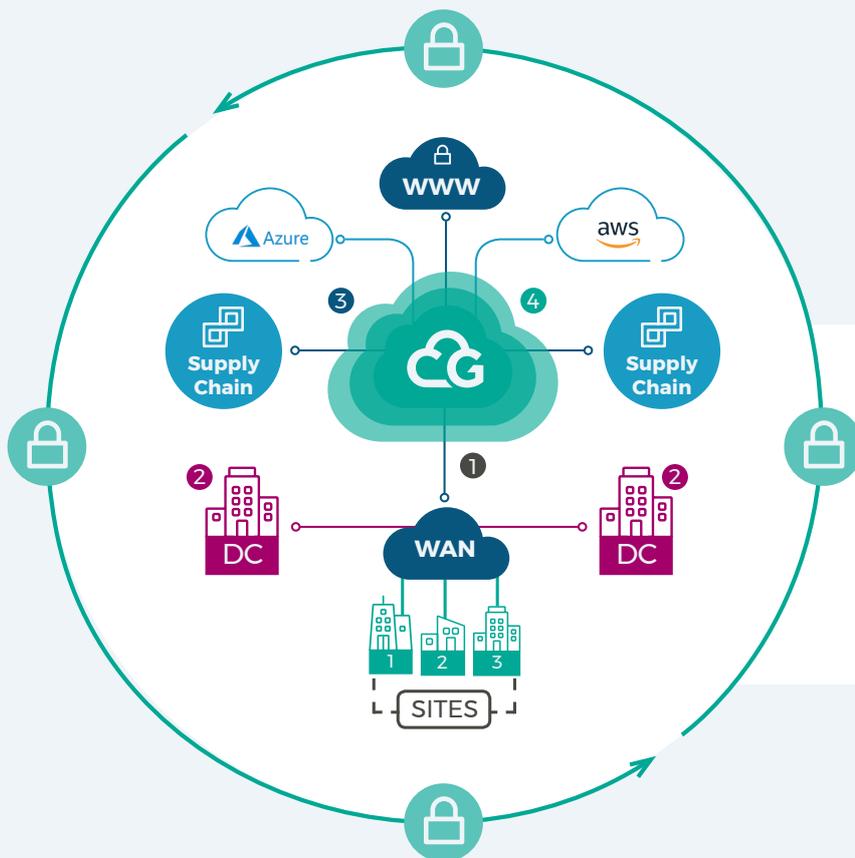
4 No central visibility

Shadow IT has been embedded into the company infrastructure. It isn't malicious and it is often introduced with good intentions as an attempt to keep ahead of the curve and to keep innovating. But at what price? What has been exposed? And why?

Businesses simply don't know what they don't know, and this impacts their ability to make effective decisions that protect their business now and into the future. Data informs but it needs to be accurate, timely and relevant.

The Solution

By centralising your connectivity, businesses have a single, timely and accurate source of truth. Everything is now visible with all data logged and available. The CISO now does know what they don't know and this information allows them to make informed decisions based on empirical evidence.

Cloud Gateway is a hybrid cloud connectivity platform-as-a-service (PaaS) delivering secure connectivity. All of the data flows are visible, logged and can be audited. Not only is the business infrastructure protected, but the power is in the hands of the business to make informed decisions based on facts.

Benefits

1. Centralised ingress
2. No shadow IT or duplicate connectivity
3. Consistent policy and logs
4. Centralised visibility

Get in touch

sales@cloudgateway.co.uk
+44 203 1024 616

About Cloud Gateway

Cloud Gateway is an innovative UK-based startup founded in early 2017. It is pioneering the Agile Network and has developed an award-winning hybrid cloud PaaS solution that provides businesses with both the mechanism and resource support to adopt, develop and operate cloud, hybrid cloud and multicloud environments. Cloud Gateway isn't just a disruptive technology, it is disrupting the entire IT industry.

Visit us at **cloudgateway.co.uk**
Twitter: **@cloudgatewayltd**
LinkedIn: **linkedin.com/company/cloudgateway**

SIX.SIX.107

CLOUD GATEWAY