FourNet®

Quick Guide to

Cloud Access Security Brokers (CASB)

Welcome to our Quick Guides to Cyber Security .

These guides have been created to give you an overview of the key pillars and solutions needed to overcome the challenges arising from Cyber threats.

Other guides in our security series:

- **Secure Infrastructure |** Quick Guide on Edge/Perimeter Security
- **Secure Infrastructure | Quick Guide to CASB**
- **Secure Infrastructure |** Quick Guide to ZTNA
- **Secure Infrastructure |** Quick Guide to SIEM
- **Secure Infrastructure |** Quick Guide to Socially Engineered
- **Secure Infrastructure |** Quick Guide to Endpoint Security

In these guides, we outline all the major risks and threats, security trends, common challenges, and impacts. Finally, we consider the best ways to calculate and mitigate the risks to your organisation, the key measures which should be introduced, and outline how FourNet's best-in-class security solutions can help.

If you take one concept from this series, it is that effective cyber security requires a layered approach to be successful. Also be mindful that compliance does not make an organisation secure and relying solely on technology to provide the solution won't combat the inherent risks humans pose.

Building the right security culture and strategy is like Lego, needing many pieces to intersect and interplay to help mitigate the increasing level of risk our organisations face.

This guide focus on Security Incident and Event Management otherwise known as SIEM and how this solution is helping to shape the cyber security landscape, providing organisations with visibility, Threat intelligence and the tools needed to combat and respond to threats in the new digital landscape.

Contents

01 Overview of CASB and Background to the Technology

02 Security Challenges That Have led to CASB

03 What Security Benefits does CASB Offer

04 Considerations When Looking to Implement CASB

05 The Benefits of CASB and SASE Integration

06 How FourNet can Help

01 Overview of CASB

02 Security challenges that have led to CASB

03 What security benefits does CASB offer?

04 Considerations when looking to implement CASB

05 The Benefits of CASB and SASE integration

06 How FourNet can Help

Overview of CASB and Background to the Technology

Cloud Access Security Brokers (CASBs) are an increasingly essential technology for organisations seeking to strengthen their cyber security posture. As businesses continue to embrace cloud services, safeguarding sensitive data and ensuring compliance have become critical concerns. This guide provides an overview of CASBs, explores the security challenges that drive their adoption, and highlights key considerations when implementing this technology. It also discusses the benefits of CASBs and their integration with Secure Access Service Edge (SASE).

Overview of CASB and Background to the Technology

A Cloud Access Security Broker (CASB) acts as an intermediary between cloud service users and cloud applications, enforcing security policies and ensuring that data and applications in the cloud remain secure. CASBs address the unique security requirements of cloud environments, enabling organisations to extend their security controls beyond traditional on-premises infrastructure.

The rise of CASBs emerged in response to the rapid adoption of cloud computing, where traditional security measures, such as firewalls and VPNs, proved inadequate. CASBs provide visibility into cloud usage, protect sensitive data, ensure regulatory compliance, and help prevent data breaches. They do this by offering services such as data loss prevention (DLP), encryption, access control, and threat detection for cloud services.

81% of organisations that use SIEM say that it has helped them enhance their threat detection abilities

Security challenges that have led to CASB

The widespread adoption of cloud services has introduced several security challenges, necessitating the deployment of CASB solutions

Shadow IT

Employees often adopt cloud applications without the knowledge or approval of IT departments. This can lead to unauthorised use of potentially insecure apps, which increases the risk of data breaches and compliance violations. CASBs help organisations discover and manage shadow IT by providing visibility and control over unsanctioned cloud applications.

Data Leakage and Loss

Cloud environments introduce the risk of accidental or malicious data leakage. Data stored or processed in the cloud is often beyond the control of traditional security mechanisms, making it more vulnerable to unauthorised access. CASBs help prevent data leakage by applying DLP policies, encrypting data, and monitoring access.

Complex Cloud Environments

Modern organisations often rely on a mix of public, private, and hybrid cloud environments, each with its own security requirements. Managing security across this diverse landscape can be challenging. CASBs offer a unified security solution that spans multiple cloud environments, reducing complexity and ensuring consistent policy enforcement.

Compliance and Regulatory Requirements

IOrganisations operating in regulated industries must comply with strict data protection standards such as GDPR, HIPAA, or PCI-DSS. Ensuring compliance across multiple cloud services can be complex. CASBs assist in maintaining compliance by enforcing security policies, monitoring for policy violations, and providing audit logs.

What security benefits does CASB offer?

CASBs provide a range of security benefits, helping organisations protect their cloud environments from threats while maintaining compliance. Key benefits include:

Visibility and Control

CASBs offer detailed visibility into cloud usage, providing insights into which services are being used, by whom, and for what purposes. This visibility enables organisations to identify and manage risks more effectively, including the use of shadow IT.

Data Protection

Through features like data loss prevention, encryption, and tokenisation, CASBs help safeguard sensitive data in the cloud. They can prevent unauthorised sharing, access, and storage of critical information

Threat Protection

CASBs provide advanced threat protection by detecting and mitigating cyber threats, including malware, ransomware, and unauthorised access attempts. They utilise behavioural analytics, anomaly detection, and machine learning to identify suspicious activities.

Compliance and Governance

CASBs ensure that organisations meet regulatory requirements by enforcing security policies and providing auditing and reporting capabilities. This helps organisations avoid costly penalties and fines associated with non-compliance.

User Authentication and Access Control

CASBs enhance identity and access management by enforcing multi-factor authentication (MFA) and role-based access control (RBAC). This ensures that only authorised users can access cloud resources.

01 Overview of CASB

02 Security challenges that have led to CASB

03 What security benefits does CASB offer?

04 Considerations when looking to implement CASB

05 The Benefits of CASB and SASE integration

06 How FourNet can Help

Considerations when looking to implement CASB

When implementing a CASB solution, organisations must consider several factors to ensure a successful deployment

Cloud Deployment Model

Different CASBs offer varying levels of support for different cloud deployment models (e.g., public, private, hybrid). Organisations should choose a CASB solution that aligns with their cloud strategy and integrates seamlessly with their existing infrastructure.

Integration with Existing Security Tools

It is essential to ensure that the CASB integrates well with the organisation's existing security tools and platforms, such as identity and access management (IAM), endpoint security, and security information and event management (SIEM) systems.

Data Security and Privacy Requirements

Organisations should assess their specific data security and privacy requirements, particularly if they operate in regulated industries. They should choose a CASB that provides the necessary data encryption, DLP, and compliance features.

User Experience and Adoption

The CASB should not hinder user productivity. Solutions that offer a seamless user experience with minimal disruption to business operations are more likely to be adopted by employees.

Cost and Scalability

The cost of implementing and maintaining a CASB solution is a key consideration. Organisations should choose a solution that is not only cost-effective but also scalable to accommodate future growth and evolving security needs.

Vendor Reputation and Support

Selecting a CASB vendor with a strong reputation for reliability, security, and customer support is crucial. A well-established vendor will offer ongoing support and updates to address emerging security threats.

01 Overview of CASB

02 Security challenges that have led to CASB

03 What security benefits does CASB offer?

04 Considerations when looking to implement CASB

05 The Benefits of CASB and SASE integration

06 How FourNet can Help

The Benefits of CASB and Integration with SASE

SIEM solutions provide a range of benefits that can help organisations strengthen their cybersecurity posture

The integration of CASB with Secure Access Service Edge (SASE) architectures offers significant advantages for organisations seeking to enhance their security posture. SASE combines network security functions (such as secure web gateways, firewall-as-a-service, and zero-trust network access) with wide-area networking capabilities. When integrated with CASB, SASE creates a holistic security solution that spans both cloud and on-premises environments.

Unified Security Architecture

Integrating CASB with SASE provides a single security framework that covers cloud services, remote users, and corporate networks. This unified approach simplifies security management and reduces the complexity of managing multiple security solutions.

Consistent Policy Enforcement

CASB and SASE integration ensures that security policies are consistently enforced across all cloud services, endpoints, and network connections, regardless of user location. This enhances overall security and ensures compliance with organisational policies.

Improved Performance and Scalability

SASE architecture is designed to be cloud-native, which improves network performance and scalability. CASB services benefit from this architecture, ensuring that security is delivered with minimal impact on performance, even as the organisation grows.

Enhanced Threat Detection and Response

SASE's built-in threat intelligence capabilities, combined with CASB's advanced threat protection, provide comprehensive threat detection and response capabilities across the entire network. This reduces the risk of data breaches and helps organisations respond to threats in real time.

.

Simplified Management and Visibility

IBy consolidating security services into a single platform, SASE and CASB integration simplifies the management of security policies, providing better visibility into both network and cloud security.

In Conclusion

Cloud Access Security Brokers (CASBs) have become essential for organisations looking to secure their cloud environments. By providing visibility, data protection, and compliance capabilities, CASBs address many of the security challenges introduced by cloud adoption. When integrated with SASE, CASBs further enhance security, delivering a unified solution that ensures consistent protection across all environments. By carefully considering their needs and selecting the right CASB solution, organisations can strengthen their cyber security posture while supporting business growth and innovation

01 Overview of CASB

02 Security challenges that have led to CASB

03 What security benefits does CASB offer?

04 Considerations when looking to implement CASB

05 The Benefits of CASB and SASE integration

06 How FourNet can Help

How FourNet Can Help

Our clients benefit from our experience working with some of the biggest names in government, healthcare, and finance. We have delivered solutions that have been recognised as Best of Breed by industry bodies such as Government Digital Service (GDS).

At FourNet, our solutions are designed to always protect your organisation from downtime - whether it's network failure or an attack on your infrastructure - so you can concentrate on what matters most: keeping people safe.

Trusted by Mission Critical Organisations

FourNet are trusted by some of the most secure and mission critical organisations in the UK including Whitehall, Downing Street, Cheshire Fire and Rescue, South Coast Ambulance Service, and others. Offering a diverse portfolio of solutions for both public sector and private enterprise with cloud solutions like ANTENNA and Agile Cloud.

We also provide highly available contact centre solutions delivering 999 & 111 services to the public and back-office solutions to support a flexible, agile workforce and have highly accredited and security cleared engineers and consultants.

Helping You to Understand Security Posture

FourNet's security specialists are here to help your organisation detect, defend, and repel threats from whatever threat vector they emerge. Our team of experts will work alongside you to identify and remediate areas of concern or risk. We work with you to build a business case to demonstrate ROI and payback periods based on your current costs and KPIs. Get in touch to schedule an initial discovery call.

Managed Security to Remove the Worries

We offer a range of managed solutions from the world's leading security vendors all underpinned by SC and DV level security cleared engineers and consultants. Our best-in-class security cleared service management from our dedicated secure Service Desk, FourNet provides a fully managed service desk and Security Operations Centre (SOC) with 24/7 phone support and multi-factor authenticated ITSM access.

Whether you are looking to secure and control access to critical systems or wanting to outsource security to a managed SOC we can help. We work with you to create an understand your organisation and provide the help, solutions, and support where it is needed most.

Discover if your Network is Ready for Emerging Threats

Discover whether your security solutions are keeping pace with the threat landscape with a FourNet Cyber Assessment.

Get in touch to arrange your assessment

Check out our Other Guides to Cybersecurity

Click Here >>

FourNet®

Manchester Office (HQ)
3 Scholar Green Road,
Cobra Court,
Manchester. M32 0TR
Tel: 0845 055 6366

hello@fournet.co.uk
fournet.co.uk

FourNet PR & Media Office
Tim Reid
e-mail: treid@fournet.co.uk