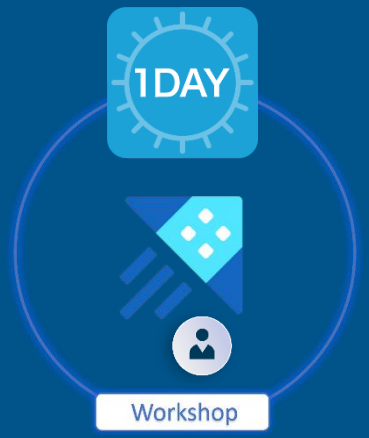
Executive Leadership Series

The Role of CASB and SASE in Cloud Security

TLC Education & Training Services



- CXO's
- Business Executives
- Technology Executives
- Entrepreneurs
- Cybersecurity Professionals
- Cloud Leaders
- Project Managers
- Strategic Planners

The Role of CASB and SASE in Cloud Security

Skills and expertise to help you increase your knowledge in the field of digital technologies

Education & Training Services

About this Workshop

In this one-day workshop, we will take a big-picture look at how SASE and CASB solutions fit into the enterprise security landscape. We will explore the key **differences between SASE and CASB** and explain how each tool helps ensure enterprise security. You will gain an understanding of how SASE and CASB solutions compare and which might be suitable for your organization.

We will discuss in detail how remote work has driven the demand for increased security and networking solutions. How SD-WAN, CASB, and SASE architectures hold the promise of weaving security from the edge to cloud, providing secure access to enterprise applications from wherever they are accessed, and prioritizing traffic that dominates the branch WAN.

Target Audience

- Customers who want to build their knowledge in the space of Zero Trust security technology and are in the process of planning and implementing Zero Trust Security Architecture Framework in their organization.
- CIO/CISO/CTO, CRO, IT Directors/GM IT, Risk and Business Technology Leaders, IT Managers, Application and Development Team Leads, Strategic Technology Planners, Project Managers, Solution/IT/Systems Architects, Enterprise Architects, Network Operation teams , Information Security and Cybersecurity teams, SOC teams and Cloud Leaders.

Cloud adoption has exploded in recent years. Nearly all companies are using cloud solutions, and the vast majority having deployments spanning the platforms of multiple cloud service providers using SD-WAN secure edge computing technology. In this session, we will be exploring CASE, SASE and SD-WAN technologies.

These complex cloud infrastructures can create significant usability and security challenges for an organization. If security settings are misconfigured, an organization's cloud infrastructure, services and applications could be potentially vulnerable to exploitation. SASE (Secure Access Service Edge) and CASB (Cloud Access Security Broker) are two new strategies in the enterprise security landscape. SASE combines network security functions with wide-area network (WAN) capabilities. CASB focuses on securing access to cloud-based applications and services.

CASB and SASE are solutions designed to address complex cybersecurity needs in a growing enterprise cloud environment. The difference between SASE and CASB is that SASE accomplishes this by integrating networking and security into one streamlined solution, whereas CASB uses traditional perimeter-based cloud security architectures.

Unit 1 – The Role of CASB and SASE in Implementing Zero Trust Security

- How to adopt a Cloud Security Risk Management mindset.
- Cloud Security Risk Management Approach.
- Understand 9 Layers of IT Infrastructure Foundation.
- Cloud Security Architecture.
- Cloud Computing Reference Architecture – CCRA.
- NIST Cloud Computing Reference Architecture.
- Cloud Management Components.
- The Top 7 Advanced Cloud Security Challenges.
- Top Cloud Application Security Threats.
- The 6 Pillars of Robust Cloud Security.
- Cloud security features required for Cloud Computing Models.
- Understand Cloud Access Security Broker.
- Security features offered by Cloud Access Security Broker.
- How Cloud Access Security Broker work?
- Requirements of a Cloud Access Security Broker Solution.
- Cloud Access Security Broker solution deployment models.
- Multi-Mode Next-Gen CASB Architecture.
- API-Only CASB Architecture and Multi-Mode First-Generation CASB Architecture.
- Cloud Access Security Broker Vendor Checklist.
- 9 Cloud Security Best Practices any Organization should follow.
- Use cases for Cloud Access Security Broker.
- Understand Secure Access Service Edge (SASE).
- High-Level SASE Architectures.
- SASE Multi-tool Approach.
- Exploring the relationship between SASE and SDP.
- Secure Access Service Edge – In a Nutshell.
- Unit 1 Assessment.

Unit 2 – Exploiting Software Defined WAN Security

- Business Challenges that develop the need for considering an SD-WAN.
- What business problems does SD-WAN solve?
- Software-defined Wide Area Network (SD-WAN) Defined.
- Planning for your SD-WAN solution and SD-WAN Key Characteristics.
- Zero-Touch Provisioning – An impressive capability of SD-WAN.
- Main components that make up the basic structure of an SD-WAN.
- Main types of SD-WAN Architectures.
- MPLS defined and difference between SD-WAN and MPLS.
- MPLS Vs SD-WAN – Pros and Cons.
- SD-WAN Architecture – Flexibility and Scalability.
- How does SD-WAN work and describing SD-WAN Policy Types.
- Build an effective SD-WAN security strategy at the branch.
- Three Models for an SD-WAN Deployment.
- Evaluate where to deploy the SD-WAN controller.
- Assess connectivity choices for SD-WAN deployment.
- SD-WAN and MPLS – Differentiating between the two technologies.
- Common SD-WAN Challenges and strategy when Migrating MPLS to SD-WAN technology.
- Describe SD-WAN Orchestration – Orchestration Vs. Cloud Automation.
- SD-WAN Use-cases and SD-WAN Checkpoints.
- Unit 2 Assessment.

Detailed Information

Course Code	: TN489
Course Duration	: 1 Day Workshop
Course Location	: TLC, Online, and Customer On-site.
Terms & Conditions	:100% payment in advance.
Course Deliverable	: Comprehensive Student Guide and Course Certificate

For additional information:
please write to us at: info@tlcpak.com

Opportunities are made, not found

Executive Leadership Series

The Role of CASB and SASE in Cloud Security

Skills and expertise to help you increase your knowledge in the field of digital technologies

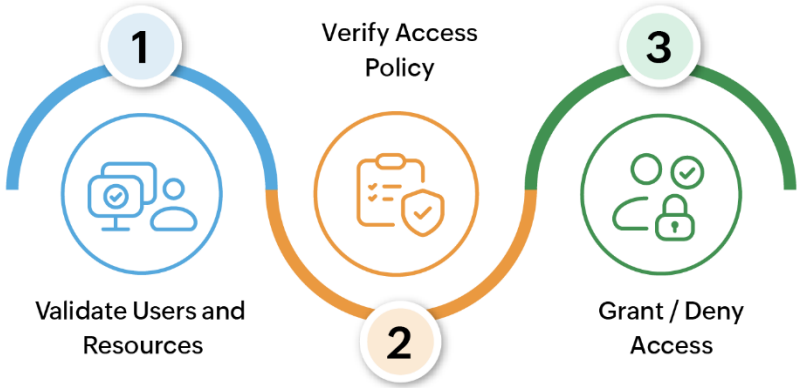
TLC Education & Training Services

Executive Leadership Series

About this Workshop

The enterprise security landscape is complicated and challenging. Understanding how a cybersecurity solution can help specific enterprise needs is key to staying safe in a digital environment.

By knowing the differences between SASE and CASB and understanding which solution fits an organization best, an enterprise can strengthen its network while keeping workflows and costs in mind.



The State of CASB, SD-WAN, CASB, and SASE Architectures

- In this session we will be discussing the **Business Challenges** that develop the need for business and technology executives to consider an SD-WAN .
- Remote work has driven the demand for increased security and networking solutions. Zero Trust, SD-WAN, CASB, and SASE architectures hold the promise of weaving security from the edge to cloud, providing secure access to enterprise applications from wherever they are accessed, and prioritizing traffic that dominates the branch WAN.
- **CASB:** 20% have deployed and 39% plan to deploy | **SASE:** 10 have deployed and 39% plan to deploy | **SD-WAN:** 11% have deployed and 34% plan to deploy.

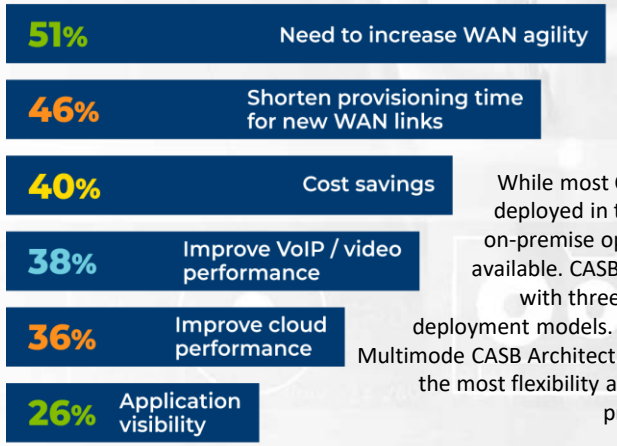
SD-WAN: Thinking of Implementing a new Security Architecture?

When it comes to deploying both SD-WAN and Security Service Edge for their SASE architecture **71% of respondents** would select the best-of-breed vendors for SD-WAN and SASE deployment.

Gartner created a new market category called Security Service Edge (SSE) which refers to the security capabilities required to implement a SASE architecture, unifying CASB, ZTNA, and SWG into a single-vendor, cloud-delivered solution.

What Business problems does SD-WAN Solve?

IT management and security complexities: Monitoring application performance, network activity and troubleshooting is difficult with rigid legacy architecture. Shown below are the SD-WAN investment drivers that solves business challenges.



While most CASBs are deployed in the cloud, on-premise options are available. CASBs operate with three different deployment models. Next-Gen Multimode CASB Architecture offers the most flexibility and robust protection.

SASE provides fully integrated WAN networking and security that connects remote-based users and offices to cloud applications and the public internet.

Business Challenges that organizations should consider when making a business case for opting CASB and SASE Architectures

- At the end of 2023, **50%** of the enterprises unknowingly and mistakenly have exposed some IaaS storage services, network segments, applications, or APIs directly to the public internet, up from 25% in YE22 – Gartner.
- Research shows that more than 60% of incoming alerts are not fully investigated due to high alert volumes and short staff – Splunk.
- By 2023, at least 99% of cloud security failures will be the customer's fault, mainly in the form of cloud resource misconfiguration. – Gartner.
- Insecure APIs will open Doors to Attack.
- Increasing complexity of infrastructure resulting in more time/effort for implementation and maintenance.
- Lack of staff with skills to manage security for a software-defined data center (e.g., virtual compute, network, storage).
- In the end, all these challenges build a strong need to adopt a Cloud Security Risk Management mindset.

80%

of enterprises will have adopted a strategy to unify web, cloud services, and private application access using a SASE/SSE architecture by 2025.

50%

of new SD-WAN purchases will be part of a single-vendor SASE offering by 2025.

48%

say their primary SSE use case is securing access for their remote and hybrid employees distributed across the different geographies.