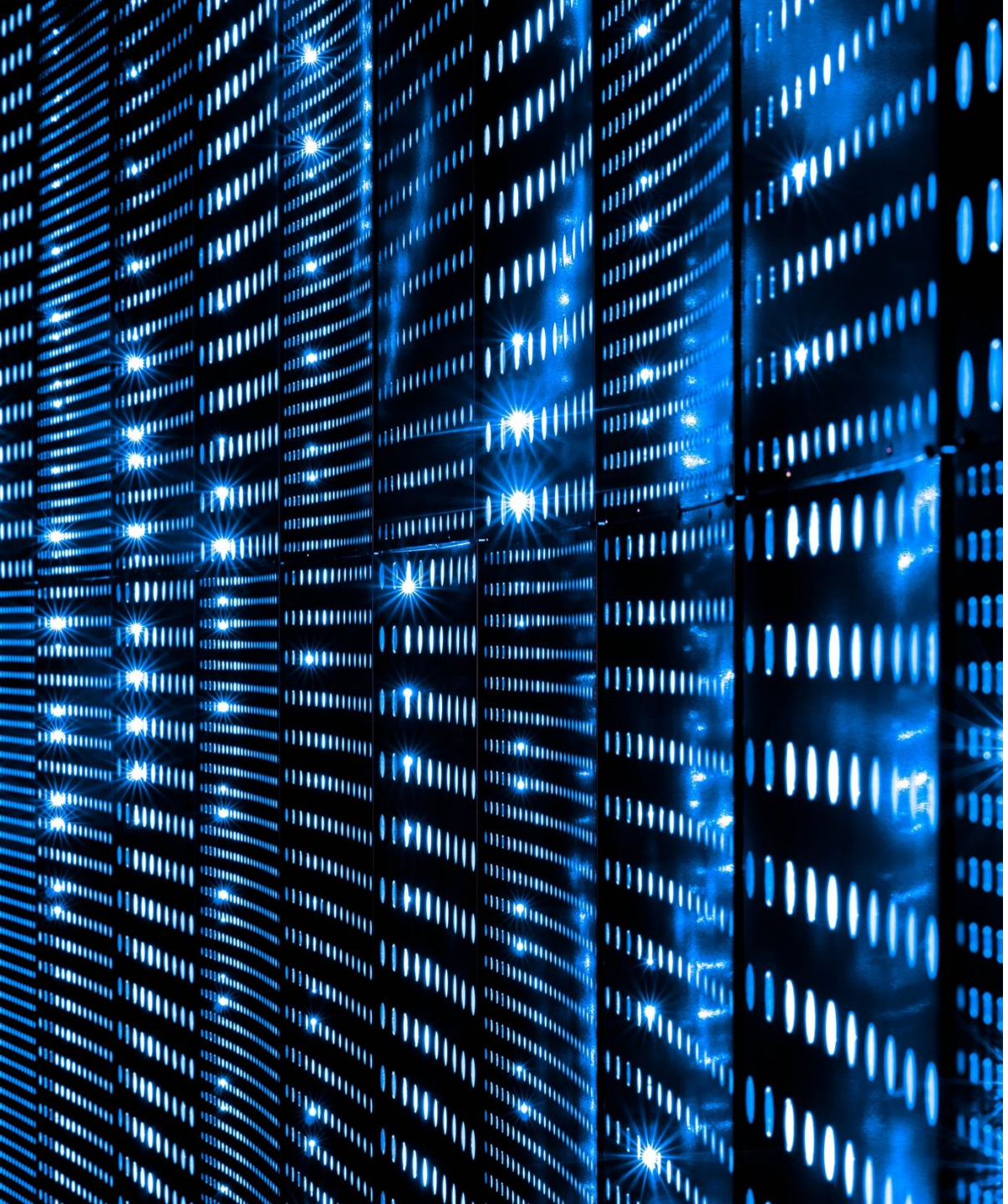


Secure Access Service Edge (SASE): Modernizing Enterprise Security and Networking

This slide provides an introductory overview of the Secure Access Service Edge (SASE) framework, a cloud-based security and networking solution that converges network security and wide-area networking capabilities to address the evolving needs of modern enterprises.

Introduction to SASE

CLOUD ADOPTION TRENDS

Organizations are increasingly migrating workloads and services to the cloud, creating a distributed and dynamic IT environment.

REMOTE WORK EXPANSION

The COVID-19 pandemic has accelerated the shift towards a remote and mobile workforce, leading to a decentralized network perimeter.

LIMITATIONS OF TRADITIONAL SECURITY

Traditional network security models, such as VPNs and centralized data centers, are no longer effective in managing the complexities of cloud-based and distributed environments.

SASE WAS INTRODUCED BY GARTNER IN 2019 AS A MODERN SECURITY FRAMEWORK TO ADDRESS THE CHALLENGES POSED BY THE EVOLVING IT LANDSCAPE, PROVIDING SECURE AND OPTIMIZED ACCESS TO CLOUD-BASED RESOURCES FOR REMOTE AND MOBILE USERS.

Key Principles of SASE

- **CLOUD-NATIVE ARCHITECTURE**

  SASE is built on a cloud-native model, allowing organizations to deploy security and networking solutions without relying on physical infrastructure. This eliminates traditional network bottlenecks and provides scalability, flexibility, and cost efficiency.

- **IDENTITY-DRIVEN ACCESS CONTROL**

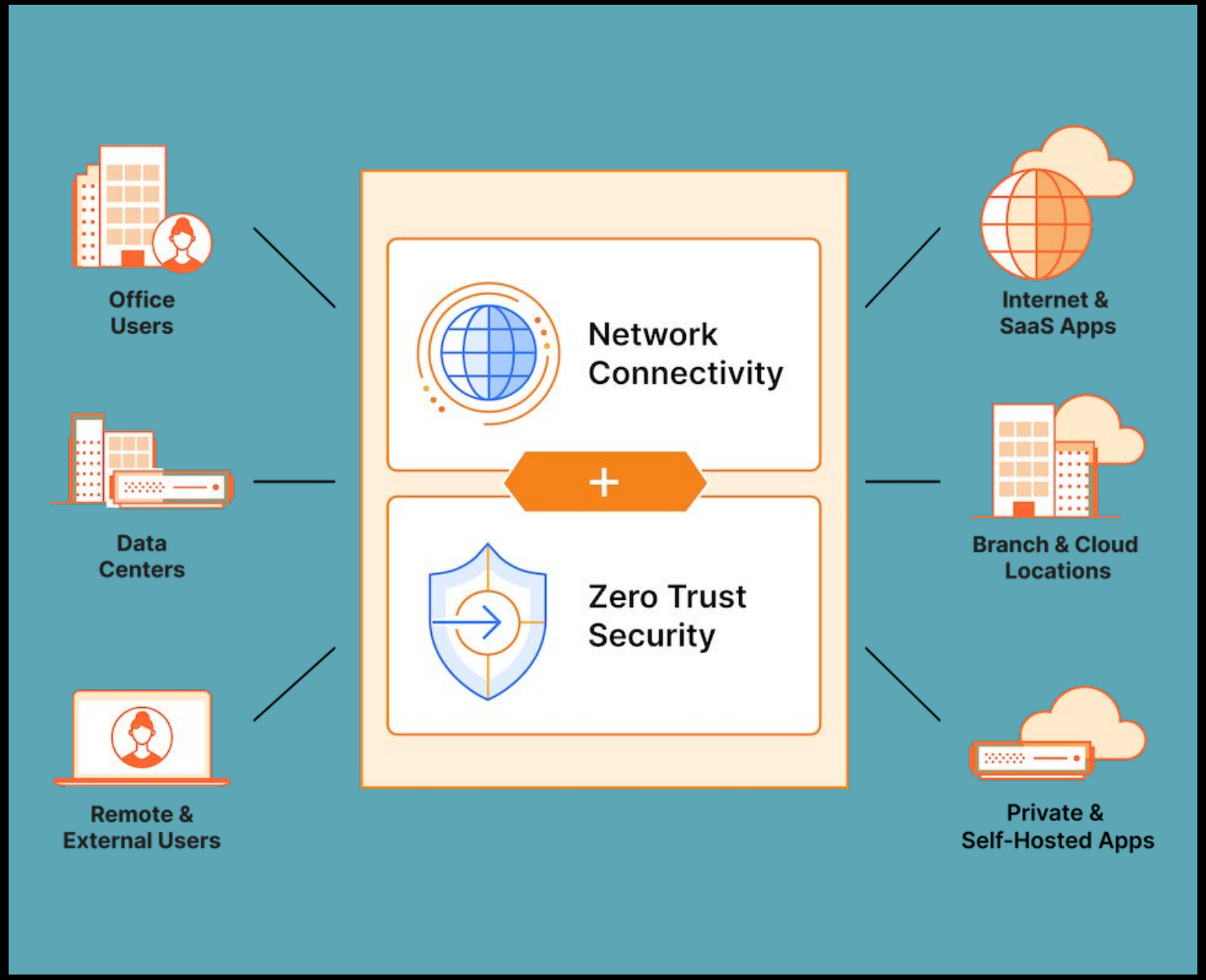
  Instead of relying on network perimeter-based security, SASE enforces policies based on user identity, device security posture, and contextual factors. Access is dynamically granted based on real-time risk assessments, ensuring Zero Trust principles are upheld.

- **GLOBALLY DISTRIBUTED SECURITY ENFORCEMENT**

  SASE delivers security functions closer to users and applications by leveraging globally distributed cloud edge locations. This reduces latency, optimizes performance, and ensures security enforcement happens at the network edge rather than relying on centralized data centers.

- **INTEGRATION OF NETWORKING & SECURITY**

  Traditional security architectures treat networking and security as separate domains, often leading to performance degradation and security gaps. SASE unifies both domains, integrating secure networking (SD-WAN) with security services (ZTNA, FWaaS, CASB, and DLP) to create a holistic security framework.



Cloud-Native Architecture

SASE is built on a cloud-native model, allowing organizations to deploy security and networking solutions without relying on physical infrastructure. This eliminates traditional network bottlenecks and provides scalability, flexibility, and cost efficiency.

Identity-Driven Access Control

USER IDENTITY

SASE enforces access policies based on the user's identity, including their role, privileges, and authentication status.

DEVICE SECURITY POSTURE

SASE evaluates the security configuration and health of the user's device, such as operating system, installed applications, and security settings, to determine the level of access.

CONTEXTUAL FACTORS

SASE considers contextual factors, such as user location, time of access, and network connection, to assess the risk and dynamically adjust access permissions.

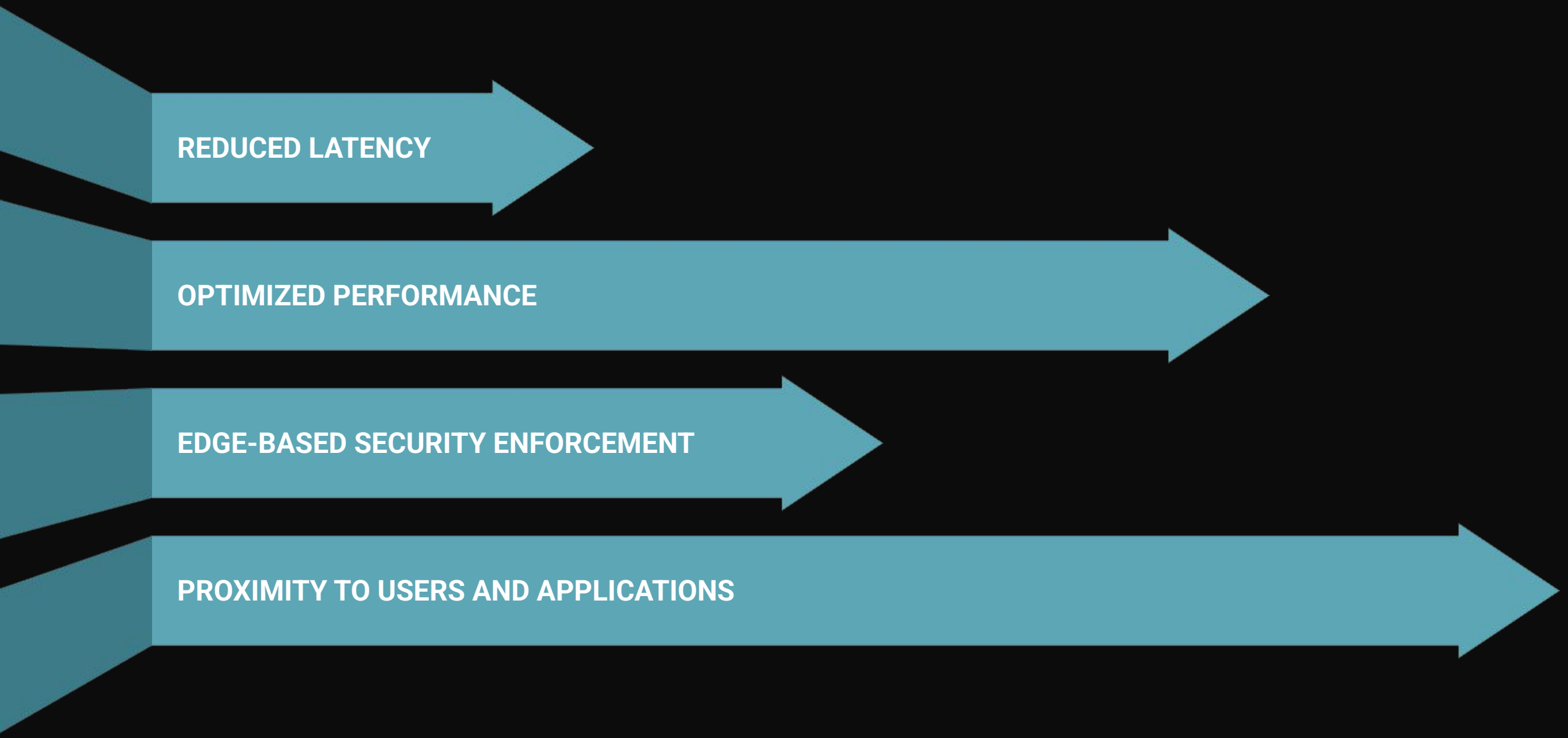
REAL-TIME RISK ASSESSMENT

SASE continuously monitors user activities and network traffic, performing real-time risk assessments to ensure that access is granted or revoked based on the current security posture.

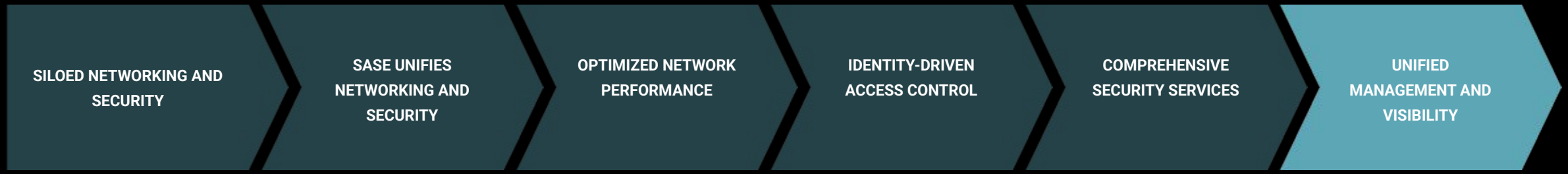
ZERO TRUST PRINCIPLES

By basing access decisions on identity, device security, and contextual factors, SASE upholds the principles of Zero Trust, where trust is never assumed and access is continuously validated.

Globally Distributed Security Enforcement



Integration of Networking & Security



Traditional network and security architectures treat these domains as separate, leading to performance degradation, security gaps, and operational complexities.

SASE integrates secure networking (SD-WAN) and security services (ZTNA, FWaaS, CASB, DLP) into a single, cohesive framework, providing a holistic approach to secure access and data protection.

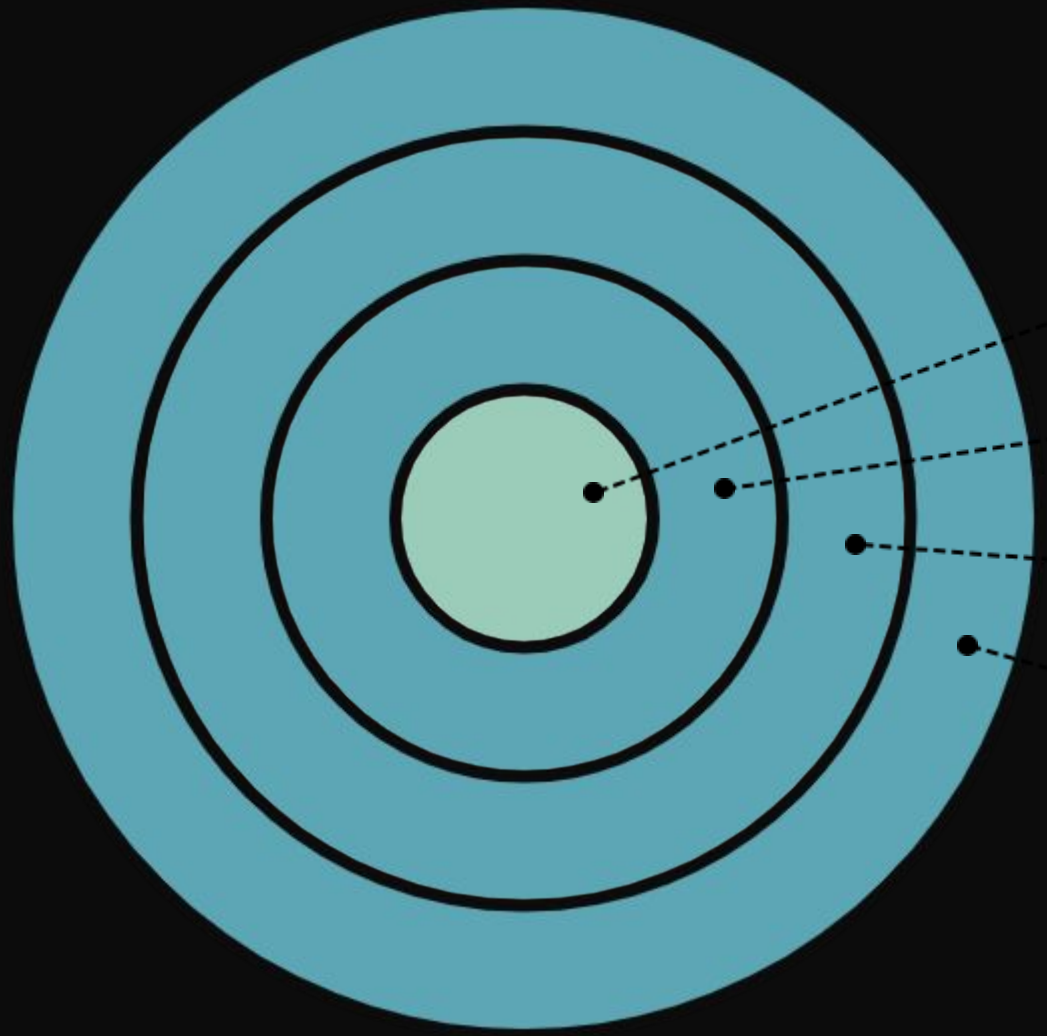
By integrating SD-WAN, SASE ensures secure, high-performance connectivity for cloud and SaaS applications, reducing latency and improving user experience.

SASE leverages ZTNA to enforce access policies based on user identity, device security posture, and contextual factors, ensuring only authorized users can access approved resources.

SASE integrates FWaaS, CASB, and DLP to provide a complete set of security capabilities, including web filtering, cloud app security, and data protection, all delivered from the cloud.

SASE offers a centralized management and visibility platform, allowing organizations to monitor and control their entire networking and security infrastructure from a single pane of glass.

Continuous Threat Monitoring & Risk Adaptation



TRAFFIC MONITORING

Continuous analysis of network traffic patterns

BEHAVIORAL ANALYTICS

Identifying and profiling user activity anomalies

POLICY ADAPTATION

Dynamic adjustment of security policies in real-time

PROACTIVE MITIGATION

Rapid detection and neutralization of security threats

Core Components of SASE

ZERO TRUST NETWORK ACCESS (ZTNA)

Replaces traditional VPNs by enforcing identity-based access control. Grants access to applications and services based on user identity, device health, and location to reduce the risk of unauthorized access.

SOFTWARE-DEFINED WIDE AREA NETWORKING (SD-WAN)

Optimizes network performance by intelligently routing traffic across multiple network connections, including MPLS, broadband, and LTE. Ensures secure, high-performance connectivity for cloud and SaaS applications.

CLOUD ACCESS SECURITY BROKER (CASB)

Provides visibility and security controls for cloud applications by enforcing policies for data protection, access control, and shadow IT detection. Prevents data leakage, unauthorized sharing, and insider threats in cloud environments.

SECURE WEB GATEWAY (SWG)

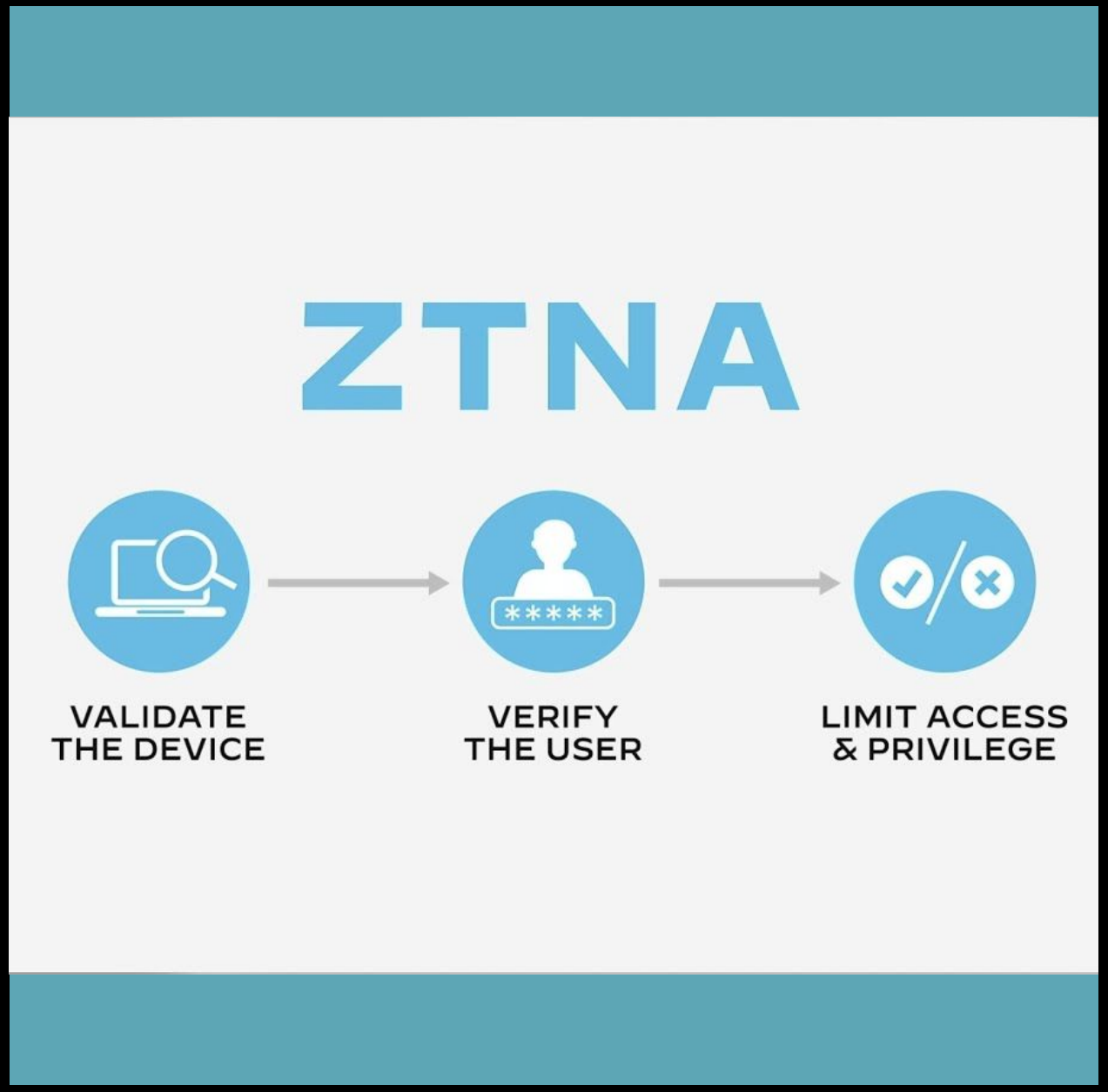
Protects users from malicious web traffic, phishing attacks, and malware by filtering web access and enforcing security policies. Ensures safe browsing and prevents access to risky or compromised websites.

FIREWALL AS A SERVICE (FWAAS)

Delivers next-generation firewall capabilities from the cloud, providing intrusion prevention, deep packet inspection, and traffic filtering to protect cloud workloads and remote users.

DATA LOSS PREVENTION (DLP)

Enforces policies to prevent data exfiltration and unauthorized data sharing. Inspects email, cloud storage, and file transfers to block sensitive data from being exposed or misused.



Zero Trust Network Access (ZTNA)

Zero Trust Network Access (ZTNA) is a security model that replaces traditional VPNs by enforcing identity-based access control. Instead of relying on a network perimeter, ZTNA grants users access to specific applications and services based on their verified identity, device health, and location, reducing the risk of unauthorized access.

Software-Defined Wide Area Networking (SD-WAN)

INTELLIGENT TRAFFIC ROUTING

SD-WAN optimizes network performance by dynamically routing traffic across multiple network connections, including MPLS, broadband, and LTE. It analyzes real-time network conditions and intelligently selects the best available path to ensure optimal performance.

MULTI-LINK CONNECTIVITY

SD-WAN leverages a mix of network connections, such as MPLS, broadband, and LTE, to provide redundancy and failover capabilities. If one connection experiences degradation or failure, SD-WAN automatically reroutes traffic to the next available and most suitable link, ensuring uninterrupted connectivity.

SECURE CLOUD CONNECTIVITY

By optimizing network performance, SD-WAN ensures secure, high-performance connectivity for cloud and SaaS applications. This improves user experience, application responsiveness, and overall productivity for remote and distributed workforce accessing cloud-based resources.

Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), Firewall as a Service (FWaaS), and Data Loss Prevention (DLP)

Comparing the security coverage of CASB, SWG, FWaaS, and DLP

Conclusion

HOLISTIC SECURITY AND NETWORKING CONVERGENCE

SASE integrates security and networking functions into a unified, cloud-native platform, addressing the challenges of distributed and cloud-based environments.

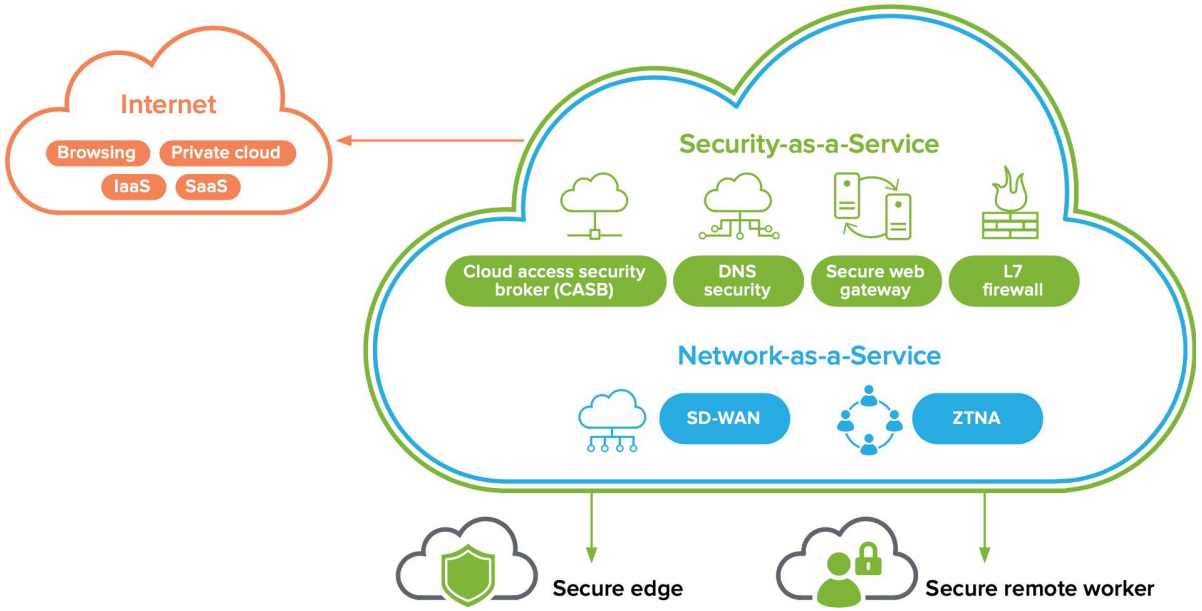
SECURE ACCESS ANYWHERE, ANYTIME

SASE enables secure, high-performance access to critical applications and data, regardless of user location or device, through identity-driven access controls and cloud-native architecture.

ADAPTABLE AND SCALABLE SECURITY

The cloud-native design of SASE provides flexibility, scalability, and cost efficiency, allowing organizations to quickly adapt to changing business and security requirements.

SASE REPRESENTS A TRANSFORMATIVE APPROACH TO ENTERPRISE SECURITY AND NETWORKING, EMPOWERING ORGANIZATIONS TO MAINTAIN SECURE AND HIGH-PERFORMING ACCESS TO CRITICAL APPLICATIONS AND DATA IN THE AGE OF CLOUD-BASED AND DISTRIBUTED BUSINESS MODELS.



Empowering the Future: Secure and Seamless Enterprise Connectivity with SASE

Explore the transformative power of SASE to empower your organization's future through enhanced security, performance, and simplified management.

SASE Deployment Models

CLOUD-NATIVE SASE

A fully cloud-delivered SASE solution where all security functions are hosted by the provider. This model is ideal for organizations with remote workforces and cloud-first strategies.

HYBRID SASE

A mix of on-premises and cloud-based security enforcement. This model is suitable for organizations with data center dependencies and legacy infrastructure that require gradual cloud adoption.

PRIVATE SASE

For industries with strict regulatory compliance (e.g., banking, healthcare), private SASE solutions host security functions within private cloud environments to ensure data sovereignty and compliance.

ORGANIZATIONS CAN CHOOSE THE SASE DEPLOYMENT MODEL THAT BEST ALIGNS WITH THEIR SPECIFIC SECURITY AND NETWORKING REQUIREMENTS, CONSIDERING FACTORS SUCH AS CLOUD ADOPTION, LEGACY INFRASTRUCTURE, AND COMPLIANCE NEEDS.

Benefits of SASE

IMPROVED SECURITY & ZERO TRUST ENFORCEMENT

SASE eliminates traditional perimeter-based security gaps by enforcing identity-centric policies, preventing unauthorized access, lateral movement of threats, and data breaches.

ENHANCED PERFORMANCE & LOW LATENCY

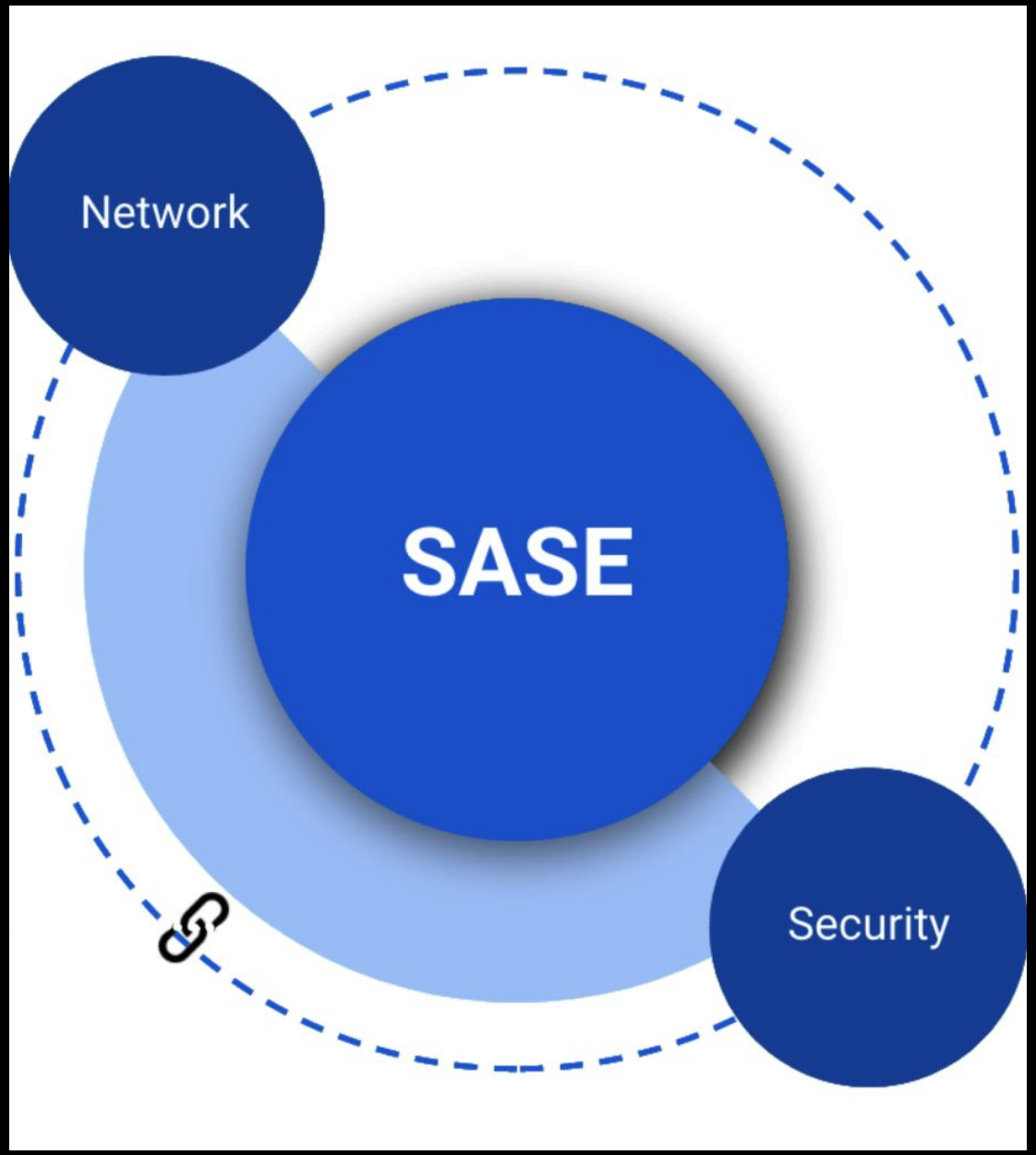
By leveraging distributed cloud edge locations, SASE reduces latency and network congestion, allowing users to experience faster access to applications and improved overall performance.

SIMPLIFIED SECURITY & NETWORK MANAGEMENT

SASE consolidates multiple security and networking functions into a single, unified platform, reducing the complexity of managing disparate point solutions.

COST EFFICIENCY & SCALABILITY

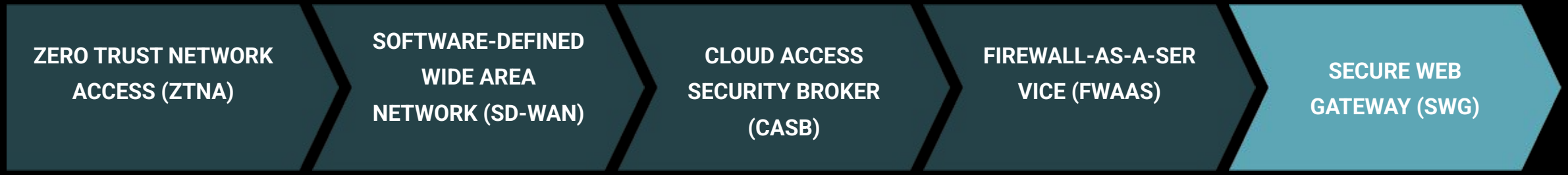
By eliminating traditional hardware dependencies, SASE reduces capital expenditures (CapEx) and operational costs. Organizations can scale security and networking resources dynamically based on demand.



Case Study: Implementing SASE for a Global Enterprise

A leading multinational technology company faced security and performance challenges in managing its remote workforce and multi-cloud infrastructure. Traditional VPN-based security models resulted in high latency, performance bottlenecks, and increased attack surfaces. The company required a cloud-native security solution that could provide secure, optimized access to applications for remote users across the globe.

SASE Architecture Components



ZTNA enforces identity-based access controls to securely connect remote users to applications, regardless of location or network. It verifies user identity, device posture, and security context before granting access, ensuring only authorized entities can access resources.

SD-WAN optimizes network connectivity by intelligently routing traffic through the best available network paths, reducing latency and improving application performance. It leverages dynamic path selection, traffic prioritization, and WAN link aggregation to provide a seamless user experience.

CASB provides visibility and control over cloud application usage, mitigating data leakage and compliance risks. It monitors user activities, detects anomalies, and enforces security policies to prevent unauthorized access and data sharing across SaaS applications.

FWaaS delivers enterprise-grade firewall capabilities as a cloud-hosted service, providing advanced threat protection, application-level controls, and granular policy enforcement at the network edge. It protects users and resources against known and emerging threats without the need for on-premises hardware.

SWG inspects and filters web traffic to protect users from web-based threats, such as malware, phishing, and inappropriate content. It enforces granular access policies, URL filtering, and SSL/TLS inspection to ensure secure and compliant web browsing, even for remote users.

SASE Deployment Outcomes

Percentage reduction in security incidents, improvement in application performance, and cost savings