Secure Service Edge (SSE)

Protecting Users, Cloud, Applications, and Data Everywhere with SSE

Prepared and present by
Makara MEAS(Mr.)
Network and Cybersecurity Manager @Proseth Solutions

KHNOG

Agenda

01	Security Challenges
02	What is Secure Service Edge?
03	Why is Secure Service Edge Important?
04	SSE Components
05	SSE Use Cases
06	RECAP

KHNOG

Security Challenges

Security Challenges

Trends in Digital Transformation and Gen-AI

Hybrid Workforce

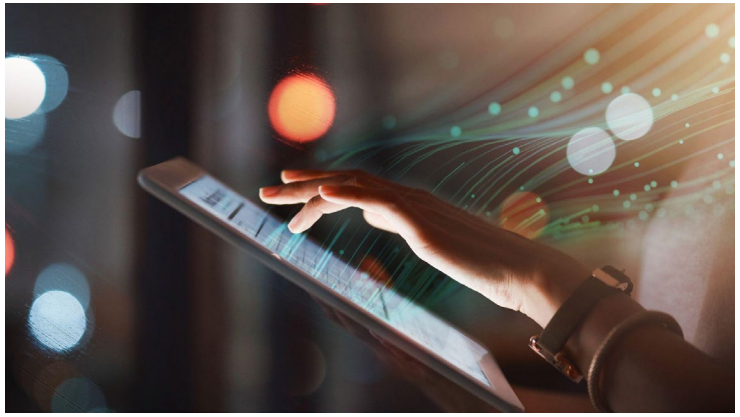
84%

Source 1: 2023 Forbes Remote Work Statistics & trends.

Businesses have a permanent hybrid work model

Avg SaaS Applications

125+



Source 2: 2022 Gartner: Market Guide for SaaS Management Platforms

Digital Transformation is Accelerating + AI/ML

Spending Growth 2024

14.3%

$215 billion in Sep-2024, increase from 2023

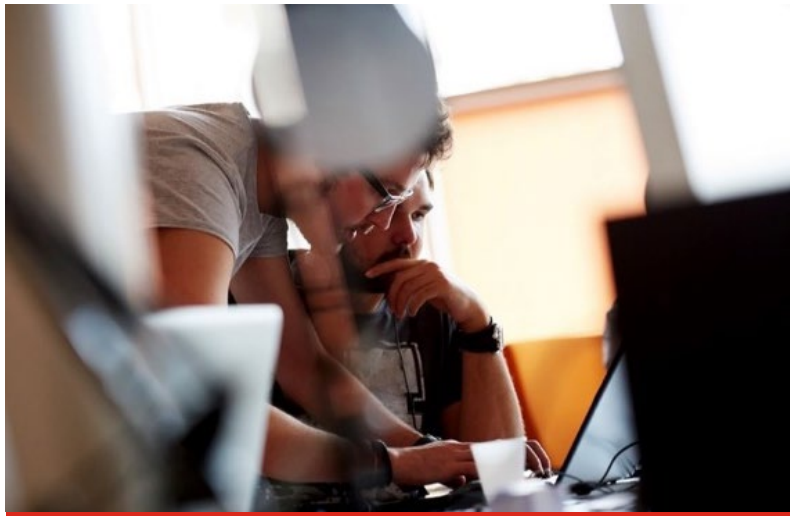
Source 3: 2024 Gartner 2024 Global Security and Risk Management

Gartner report of Cloud Services, Hybrid Workforce, and Rapid emergence of Gen-AI

KHNOG

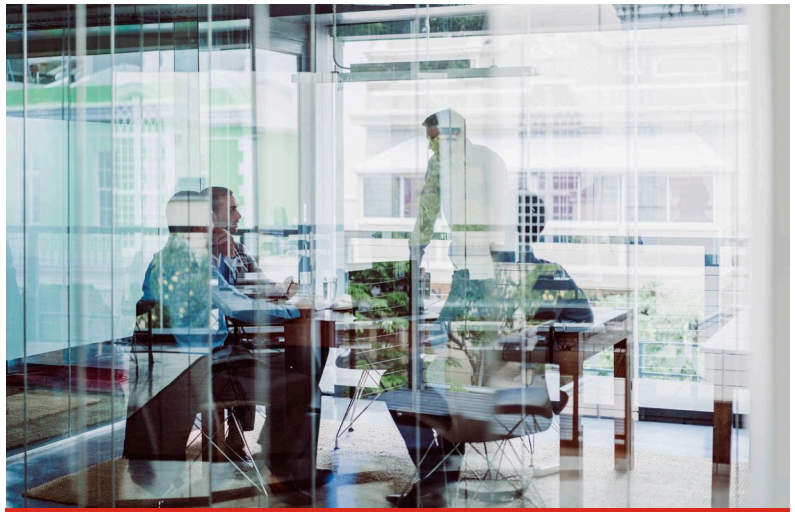
Security Challenges

IT and Security Challenges



Inconsistent security and security gaps

82% of security leaders have been surprised by a security event, incident, or breach which evaded a control they thought was in place.



Lack of visibility

60% of companies admitted to not being confident in their ability to measure security controls designed to mitigate ransomware continuously.

Impact to NetOps/SecOps.

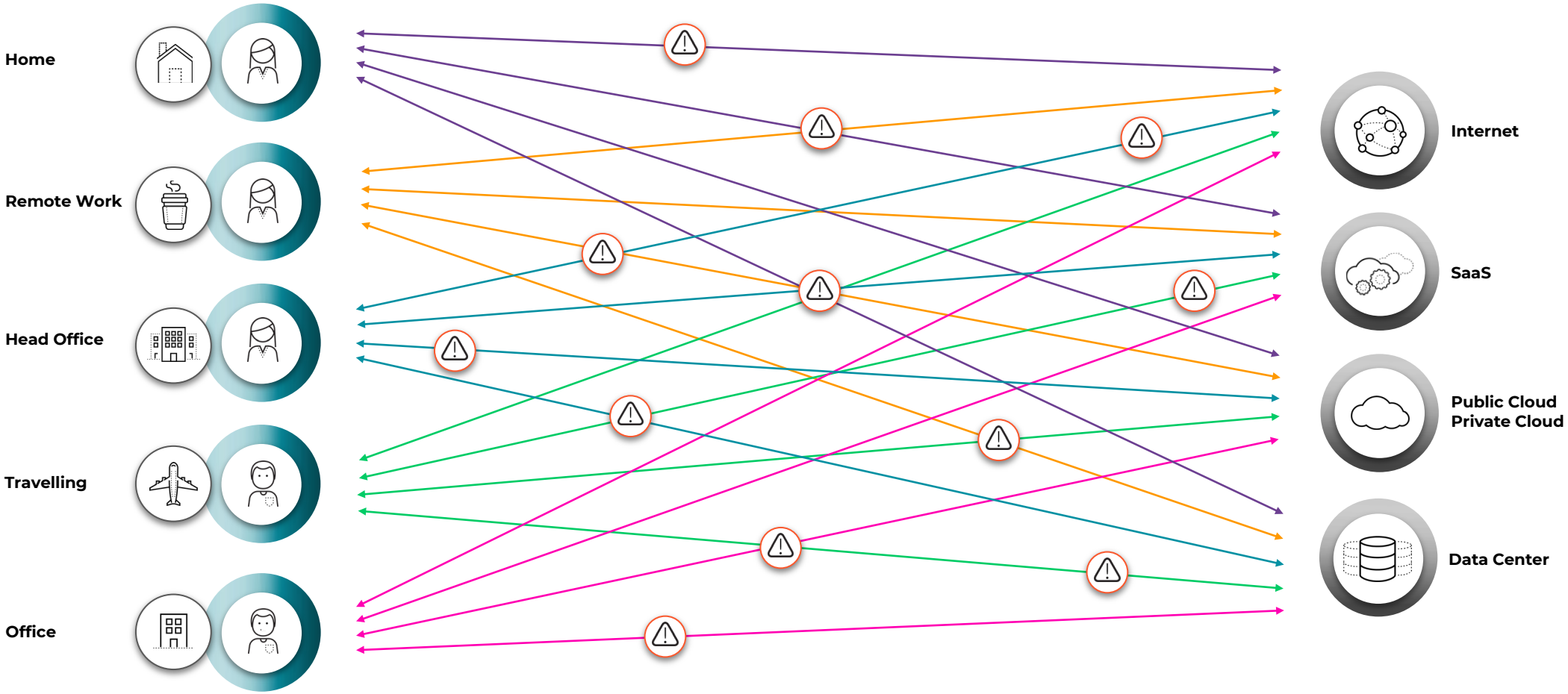
Growth of shadow IT

83% of IT professionals reported that employees stored company data on unsanctioned cloud services and the average company has 975 unknown cloud services.

https://panaseer.com/reports-papers/report/2022-security-leaders-peer-report/
https://www.smartfile.com/blog/shadow-it-risks/

Security Challenges

The Attack Surface Look Like ☺



KHNOG


What is SSE?
Why is SSE Important?
SYSTEM
HACKED

What is Secure Service Edge?

- Security service edge (SSE), as defined by Gartner, is a concept of convergence of network and security services delivered from a purpose-built cloud platform.
- SSE is primarily delivered as a Cloud-based service and may include on-premises or agent-based components.
- Security Service Edge (SSE), concepts introduced by Gartner in 2021, focuses on the Security Components of the Secure Access Service Edge (SASE) framework, which was introduced by Gartner in 2019.
- Who is Gartner?
    - Gartner, Inc. is a leading American company, research and consulting firm that provides insights and advice on technology and business strategies.
      Founded in 1979

Source Gartner: https://www.gartner.com/en/information-technology/glossary/security-service-edge-sse

KHNOG

Why is Secure Service Edge Important?

- As a growing industry trend, fundamental challenges of organizations face relating to remote work, the Cloud, Secure edge computing, and Digital transformation in Gen-AI.
- AI/ML enhances SSE components by providing advanced threat detection, real-time analysis, and automated responses, making it easier to secure digital transformation initiatives.

Hybrid Workforce

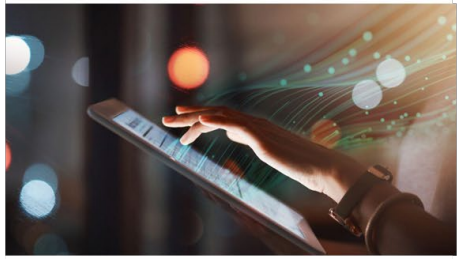
84%

Source 1: 2023 Forbes Remote Work Statistics & trends.

Businesses have a permanent hybrid work model

Avg SaaS Applications

125+



Source 2: 2022 Gartner: Market Guide for SaaS Management Platforms

Digital Transformation is Accelerating + AI/ML

Spending Growth 2024

14.3%

$215 billion in Sep-2024, increase from 2023

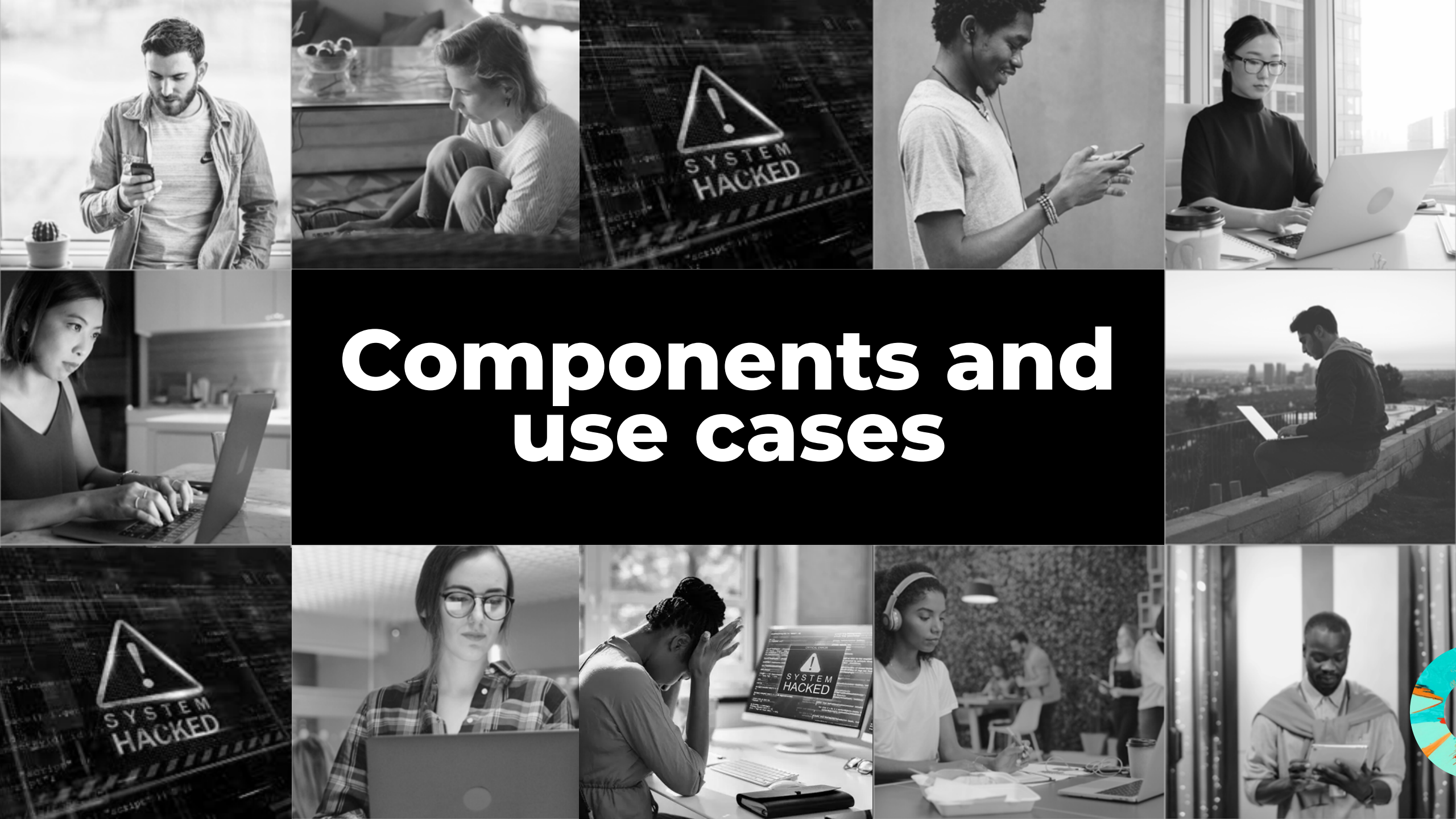
Source 3: 2024 Gartner 2024 Global Security and Risk Management

Gartner report of Cloud Services, Hybrid Workforce, and Rapid emergence of Gen-AI

KHNOG

Why is Secure Service Edge Important?

- **Stronger, consistent cloud-based security** that extends protection across HQ and out to branch offices and remote/mobile users
- **Optimized, low-latency network and security performance**, because traffic isn't hairpinned to a central data center for enforcement
- **Scalability to adapt to an organization's shifting needs**, such as adoption of new cloud services and growth or movement of the workforce
- **Streamlined security and networking management** through a centralized, cloud-delivered platform for critical security services
- **More predictable costs and reduced operational overhead** through minimizing the need for on-premises hardware deployments



Components and use cases

SSE Components

WAN EDGE

SD-WAN

A virtual WAN architecture that allows enterprises to leverage any combination of transport services, including MPLS, LTE, and broadband internet services, to securely connect users to applications everywhere.

NGFW

Advanced type of Firewall that that providing features such as, Deep Inspection, IPS/IDS, Apps Control, TI, Web Filtering, File Filter, etc.

SSE

SWG

A security solution that filters unwanted software/malware from user-initiated web traffic and enforces corporate and regulatory policy compliance.

ZTNA

A security model that requires strict verification for every user and device trying to access resources on a private network, ensuring no implicit trust.

CASB

A security policy enforcement point between cloud service consumers and providers, offering visibility, compliance, data security, and threat protection.

FWaaS

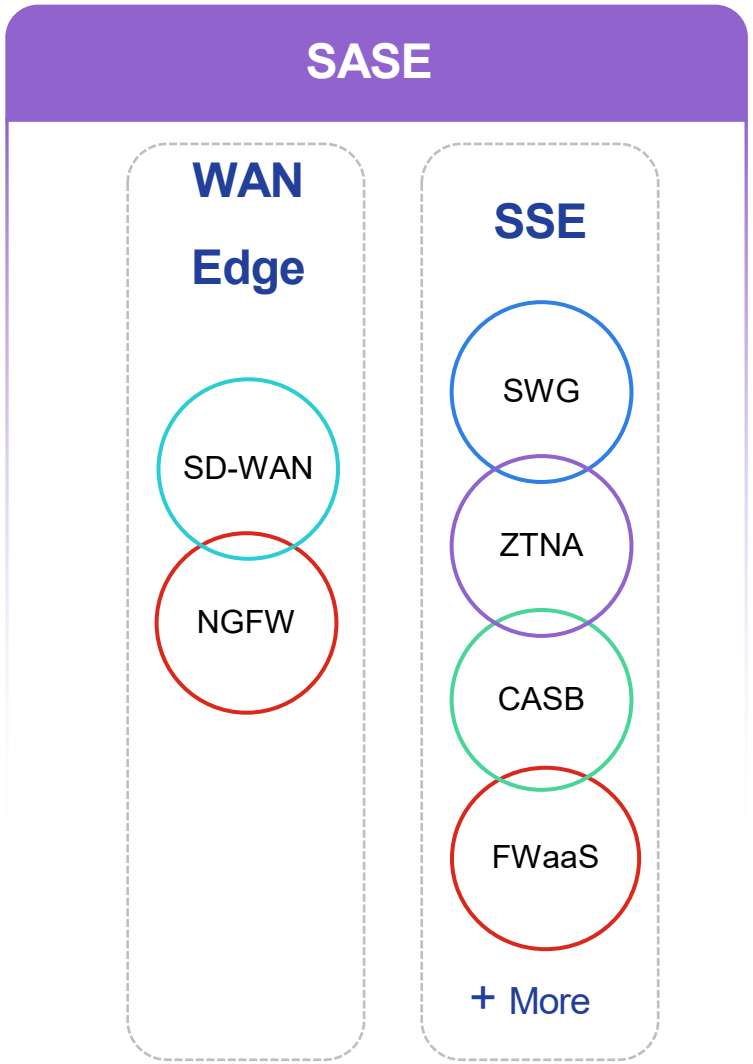
A cloud-based firewall solution that provides advanced threat protection, intrusion prevention, and web filtering without the need for on-premises hardware.

+ More

KHNOG

SSE Components

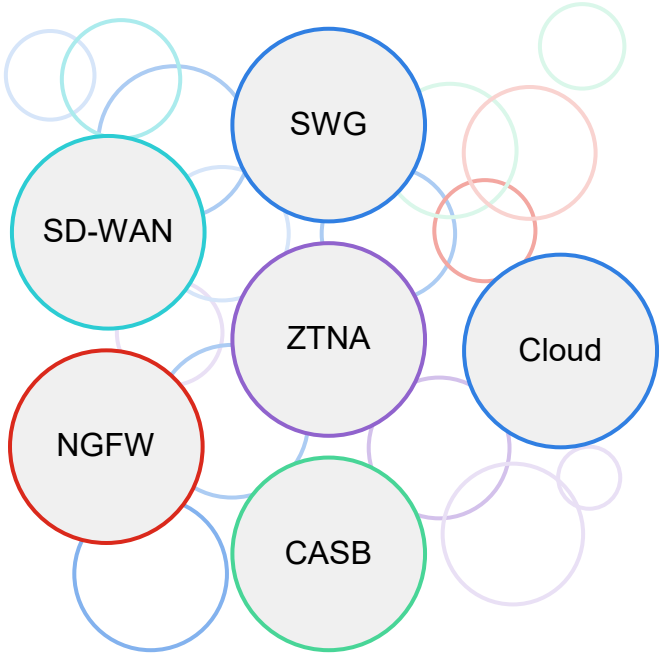
Key Point
Adopting SSE before SASE



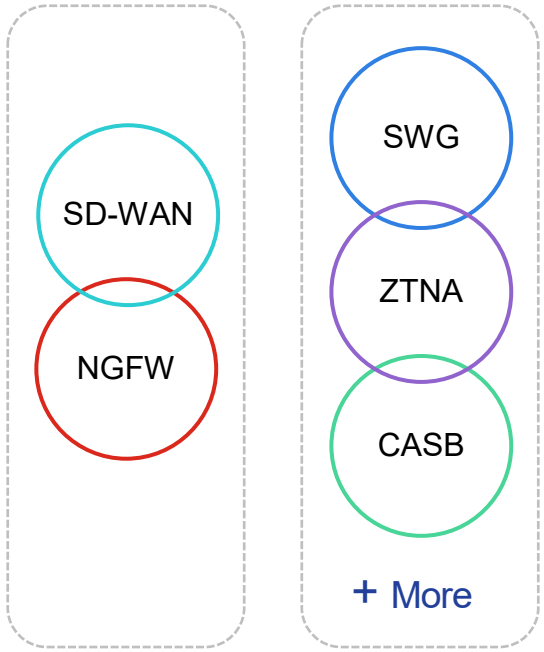
 |

Evaluation of Single-vendor SSE/SASE

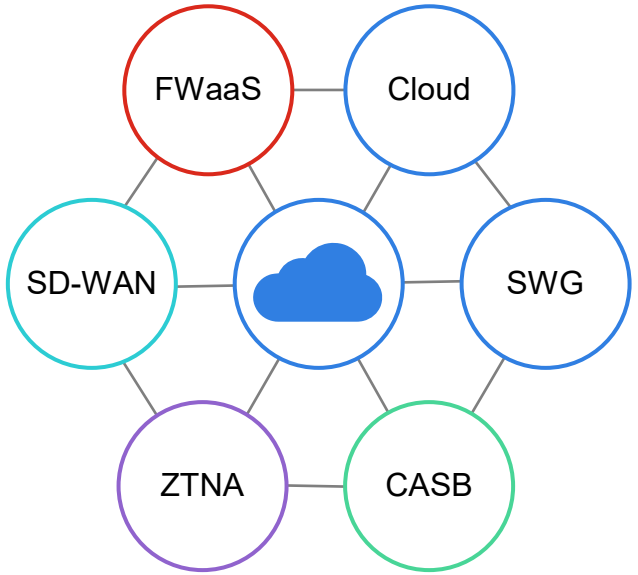
Point Product Vendors



Dual-Vendor SASE



Single-vendor SASE



50 Vendors

20 Vendors

Single Vendors

Source Gartner: https://www.gartner.com/en/documents/5556895

KHNOG

SSE Use Cases

Secure Internet Access

Secure Private Access

ZTNA

FWaaS

SWG

Challenge: Ensuring secure internet and private application access for remote employees.

Solution: SIA and SPA provide secure, controlled access to internet and private applications, enhanced by AI/ML for real-time threat detection and adaptive access control.

SSE Use Cases

Secure SaaS Access

CASB

Challenge: Protecting data and applications across multiple cloud environments.

Solution: SSA ensures secure access to SaaS applications, with AI/ML-driven data protection and threat intelligence to safeguard cloud resources.

RECAP

- Security service edge (SSE), as defined by Gartner, is a concept of convergence of network and security services delivered from a purpose-built cloud platform.
- SSE is primarily delivered as a Cloud-based service and may include on-premises or agent-based components.
- Security Service Edge (SSE) is a subset Components of the Secure Access Service Edge (SASE) framework, which was introduced by Gartner in 2019.

SSE Components

SWG

A security solution that filters unwanted software/malware from user-initiated web traffic and enforces corporate and regulatory policy compliance.

ZTNA

A security model that requires strict verification for every user and device trying to access resources on a private network, ensuring no implicit trust.

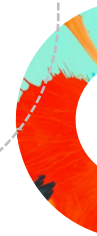
CASB

A security policy enforcement point between cloud service consumers and providers, offering visibility, compliance, data security, and threat protection.

FWaaS

A cloud-based firewall solution that provides advanced threat protection, intrusion prevention, and web filtering without the need for on-premises hardware.

+ More



Thank You

Prepared and present by
Makara MEAS(Mr.)
Network and Cybersecurity Manager @Proseth Solutions

 |

KHNOG