Nice to meet you

True Tafeset

Graduate Student at Canisius University in Cybersecurity program

Currently working on a research project

- Synthetic & threat representative environments for education and training of cyber forces, partnered with **USCYBERCOM**

tafeset@canisius.edu & trueyetafese@gmail.com

LinkedIn **Trueye tafese**

WORK FROM HOME AND SECURITY RISKS: SASE SOLUTION

October 10, 2024

Target Audience

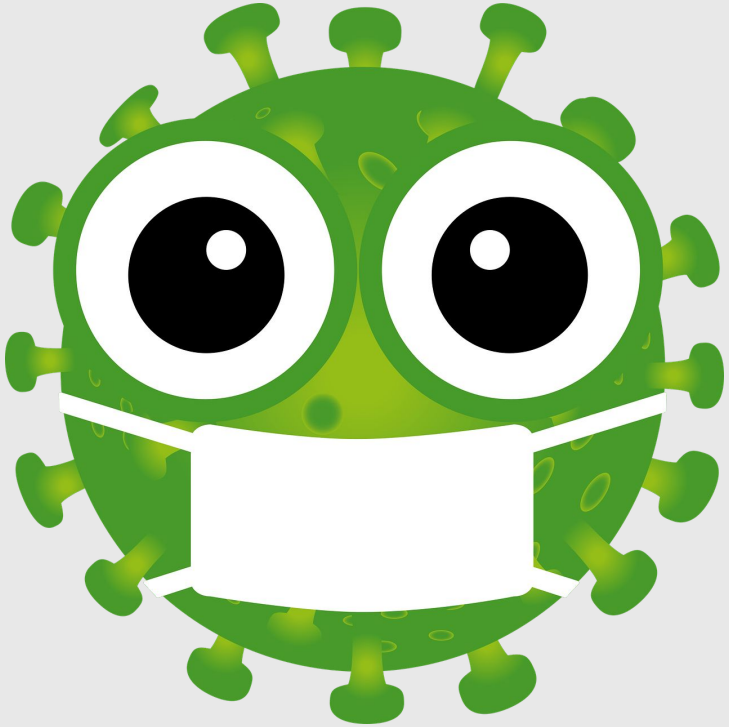
- **IT Consultants and Solution Architects**
- **General Business Audience / Non-Technical**
- **IT and Security Professionals**
- **Compliance and Risk Management Officers**
- **Business Leaders and Decision Makers**

Agenda

- History of work from home.
- Work from home security risks.
- Limitations of Traditional Security Models.
- Security Breach that is linked to remote work vulnerabilities.
- What is SASE?
- Control point of SASE.
- Building blocks of SASE.
- Companies that implemented SASE and How it is implemented?
- How do you Implement SASE Component in your company?
- Company that provide SASE servies's.
- SASE Use Case

History of Work from home

In 1979, five IBM employees were allowed to work from home as an experiment



COVID-19: Gamechanger for WFH

In 2010, the Telework Enhancement Act of 2010 required companies to have work from home policies.

Work from home security risks

- **Network Security:**
  - **Insecure Home Networks**
  - **Unmonitored Access**
  - **Lack of Perimeter Control**
  - **Increased Attack Surface**
  - **Limited Scalability**
- **Data Privacy:**
  - **Phishing and Social Engineering**
  - **Personal Device Vulnerabilities**
- **User Authentication:**
  - **Lack of Multi-Factor Authentication (MFA)**
- **Endpoint Security:**
  - **Outdated Software**
  - **Difficulty in Monitoring and Managing Devices**

Limitations of Traditional Security Models

Static Access Controls

Use rule-based access control like IP address-based, which don't account for dynamic changes in user locations, roles, or contexts.

Perimeter-Based Security

User outside of controlled network environment will be vulnerable that it only focuses on perimeter firewall &IDS

Lack of Visibility and Monitoring

Unable to extend visibility and monitoring remote endpoints or external cloud environments

Inadequate Scalability

VPN can become performance bottlenecks to scale effectively with the growth remote workers.

Limited Threat Intelligence Integration

It rely on predefined signatures and rules

Complexity in Policy Enforcement

Inconsistent security protocol enforcement

Diverse Threat Vectors

The diversity of devices and networks used by remote workers

Enforcement of security protocols can become inconsistent.

Security Breach that is linked to remote work vulnerabilities

- **Twitter Hack (2020): Social Engineering and Weak Access Controls**
  Attackers used spear-phishing techniques to impersonate internal IT staff, tricking employees into revealing credentials. Once inside, they escalated privileges due to insufficient access control measures.
- **Zoom Bombing Incidents (2020) Unprotected Meetings and Weak Authentication**
  Many Zoom users didn't enable basic security settings like meeting passwords or waiting rooms, leaving meetings open t unauthorized participants. The lack of strong authentication mechanisms allowed attackers to easily disrupt meetings, exploiting the default security configuration.
- **Cognizant Ransomware Attack (2020)Unpatched Software and Endpoint Vulnerabilities**
  The attackers used a known vulnerability in an outdated version of the remote desktop protocol (RDP) used by employees working from home. Remote endpoints lacked proper patch management and antivirus protections, making it easy for ransomware to spread.

Cognizant

What is SASE?

Secure Access Service Edge

SASE was introduced by Gartner analysts Neil McDonald and Joe Skorupa in 2019.

SASE IS A NEW ARCHITECTURE STRATEGY FOR SECURITY AND NETWORKING.

THE SASE MODEL ADDRESS THE ISSUE IN CLOUD CENTRIC WORLD.

Control point of SASE

- The aim of SASE is to secure a broader scope in your network real time using these three control points.
    - The **data** which flows in and out of the SAAS applications.
    - The identity of each **user** who's accessing the app.
    - Approval of **access** which is based on how your business interacts with external entities.

SD-WAN

Building blocks of SASE

SASE have 5 main components

SD-WAN

SD-WAN is a network solution that enables dynamic, software-driven management of a wide area network (WAN

Dynamic Traffic Management

- makes real-time decisions about the best route for each data packet.
- optimal performance applications while deprioritizing less essential traffic.

Multiple Connection Types

Supports different connectivity, such as broadband internet, LTE/5G, and MPLS. It automatically selects the best path for data based on the quality and cost of the available connections.

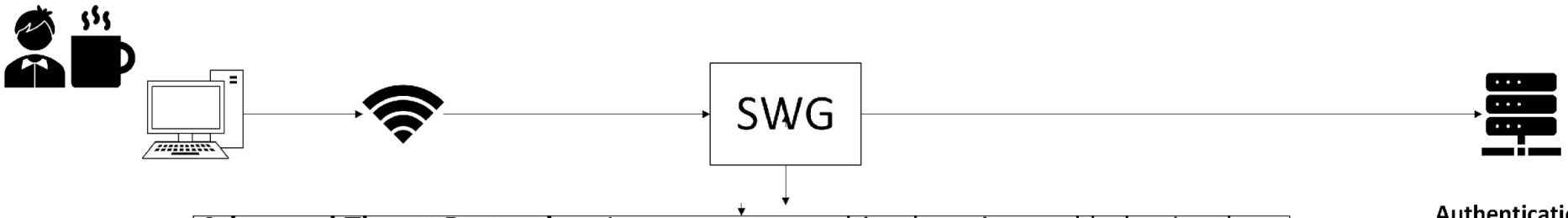
Centralized Control:

network administrators can manage the entire network through a centralized dashboard, which simplifies monitoring, troubleshooting, and policy enforcement across multiple locations

Link Aggregation & Failover:

Can combine multiple internet links into a single virtual connection, ensuring redundancy. If one link fails, the traffic is automatically redirected to another link without disruption.

NG-SWG Next-Generation Secure Web Gateway



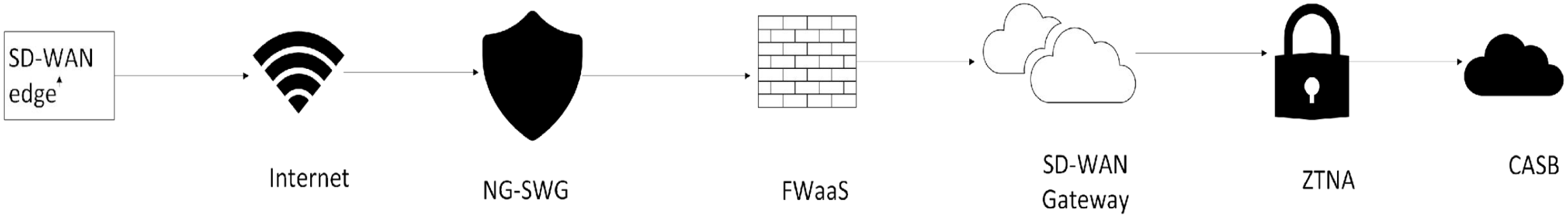
Advanced Threat Protection: Incorporates machine learning and behavioral analysis to detect and block unknown treats.

SSL/TLS Traffic Decryption: fully inspect encrypted web traffic without sacrificing performance.

Inline DLP (Data Loss Prevention): inspect traffic to ensure sensitive data is not leaked or shared with unauthorized sites.

Secure Access for Remote Users: ensuring that **remote users** can connect securely to the internet without needing a VPN.

Zero Trust Integration: enforcing granular access policies that verify the identity and context of each user and device



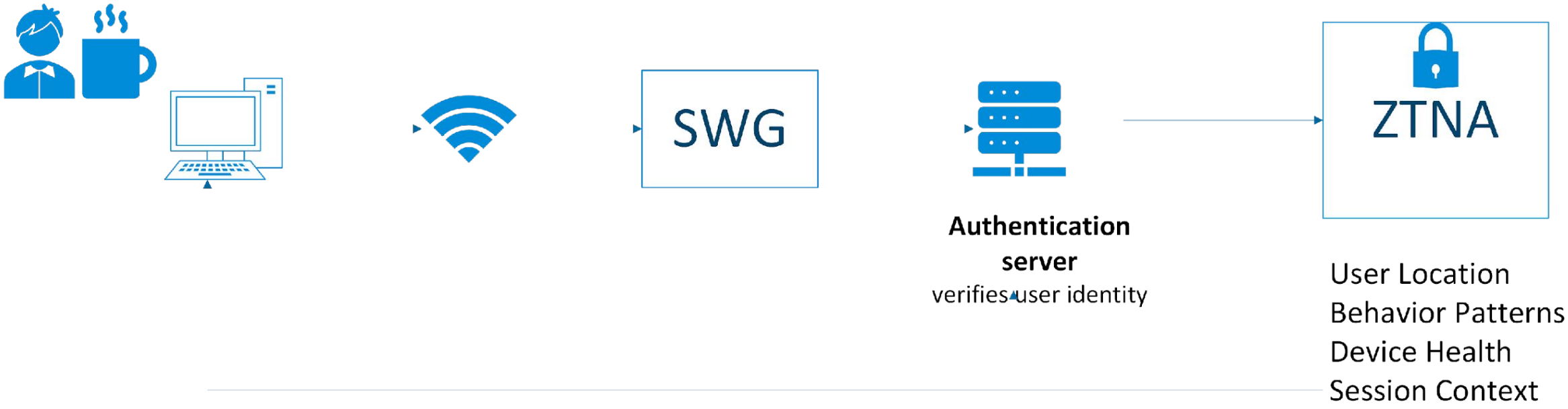
CASB

Cloud Access Security Broker

- Cloud Visibility: Shows unsanctioned app and how they are being accessed.
- Data Security: Encrypted, tokenized and apply DLP for data that are found in cloud app, ensuring it is not improperly shared or accessed.
- Access control: ensuring that only authorized users can access specific cloud resources.
- Compliance and Governance: comply with regulations like GDPR, HIPAA, and PCI DSS by ensuring proper handling of sensitive data in cloud environments.
- Real-Time Threat Detection: monitors unauthorized data downloads, abnormal access times, or suspicious file sharing.
- Policy Enforcement: Organizations can set policies that allow safe use of approved cloud applications while blocking access to unapproved apps.
- Secure Collaboration: By collaborating Microsoft 365 or Google Workspace, CASB enforces encryption of sensitive files before sharing or limiting the

ZTNA

- **Identity-Verification:** It relies on user identity and device verification and provides access to specific services rather than the entire network.
- **Least-Privilege Access**: Instead of granting full network access (like a traditional VPN), ZTNA gives users only the minimum permissions
- **Continuous Authentication**: If suspicious behavior is detected, session will be re-authenticated.
- **Micro-Segmentation**: applications are segmented into small, isolated zones.
- **Policy Enforcement**: user identity, device health (whether the device meets security standards), location, and behavior patterns



FWaaS
Firewall as a Service

- Cloud-Based Architecture
  - Traffic from any location will be filtered.
- Integrated Security Services
  - Integrate Intrusion Prevention System (IPS), anti-virus, URL filtering, and SSL decryption.
- Simplified Deployment
  - Cloud-based, easy to integrate with Microsoft365, Google workspace.
- Elastic Performance
  - Scale its performance based on traffic demands
- Unified Policy Enforcement
  - Uniformly across all users and devices, whether they are in the office or working remotely.
- Scalability
  - Ideal for growing enterprises or businesses with fluctuating traffic volumes.

Challenges

Implementation of SASE

- Zoom-bombing
- Global Performance
- Cloud-Architecture
- User growth

Implementatio of SASE

- Zoom Video Communications using VMware service provider

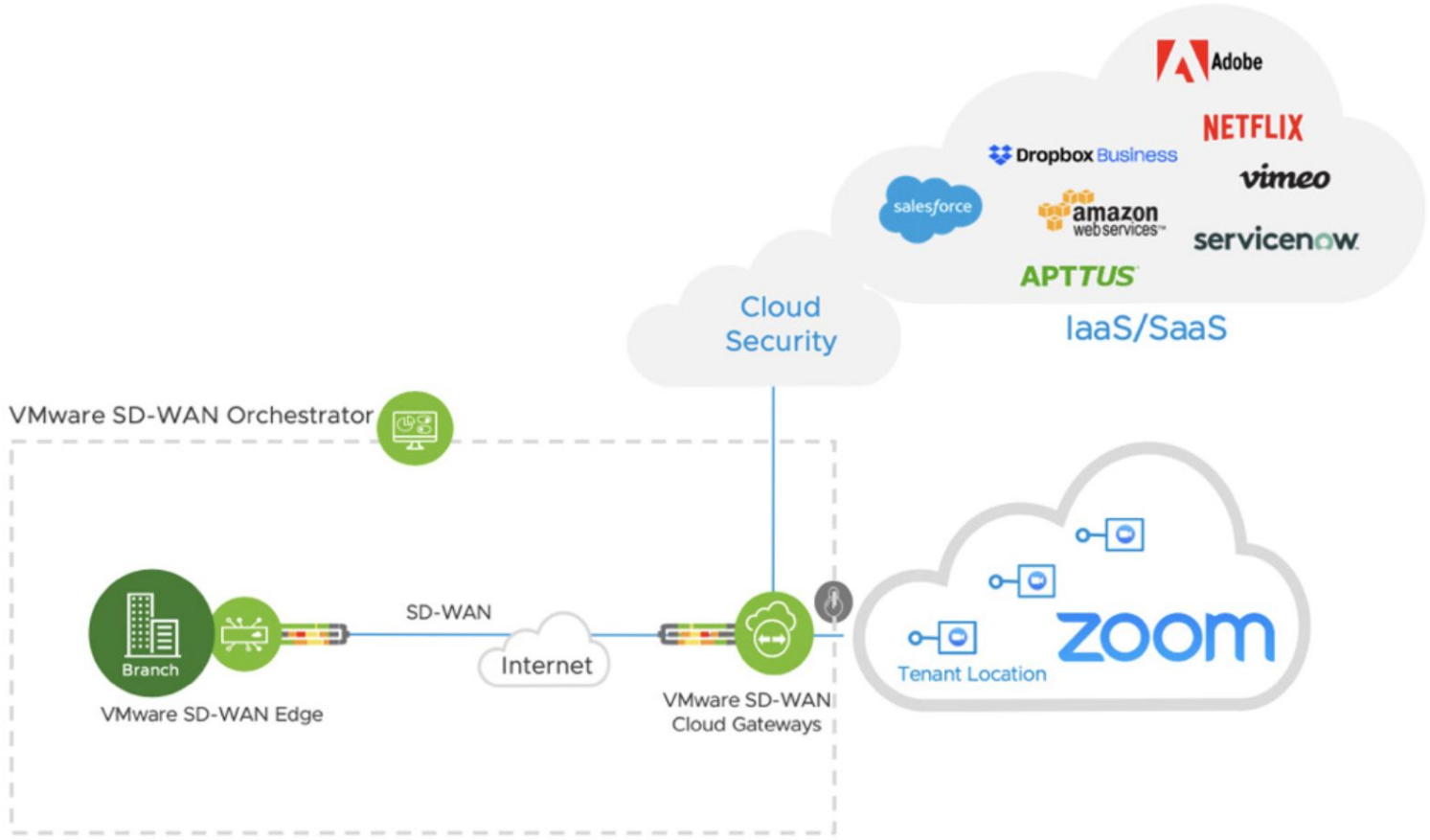


FIGURE 1: VMware SD-WAN for Zoom, the video-first unified communications platform

FIGURE 3: VMware SD-WAN: loss mitigation for better resolution for Zoom video communications

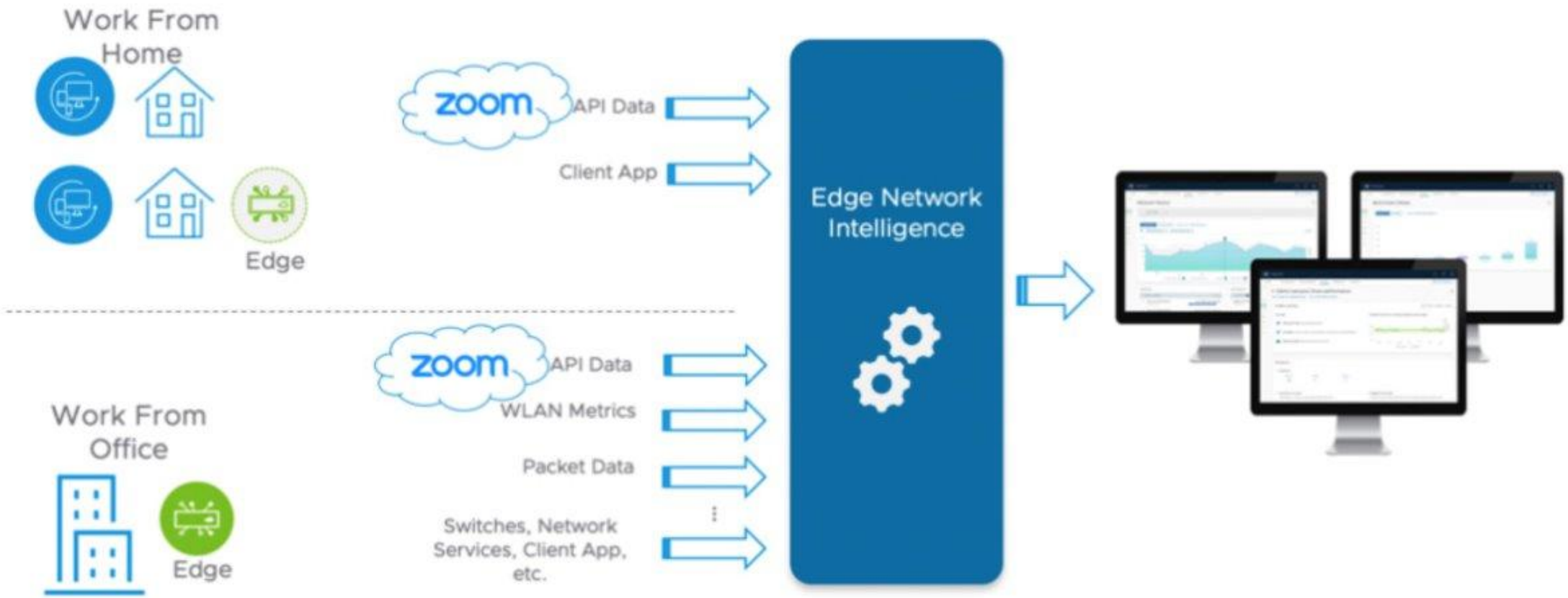


FIGURE 4: Data collection from multiple sources across a distributed enterprise

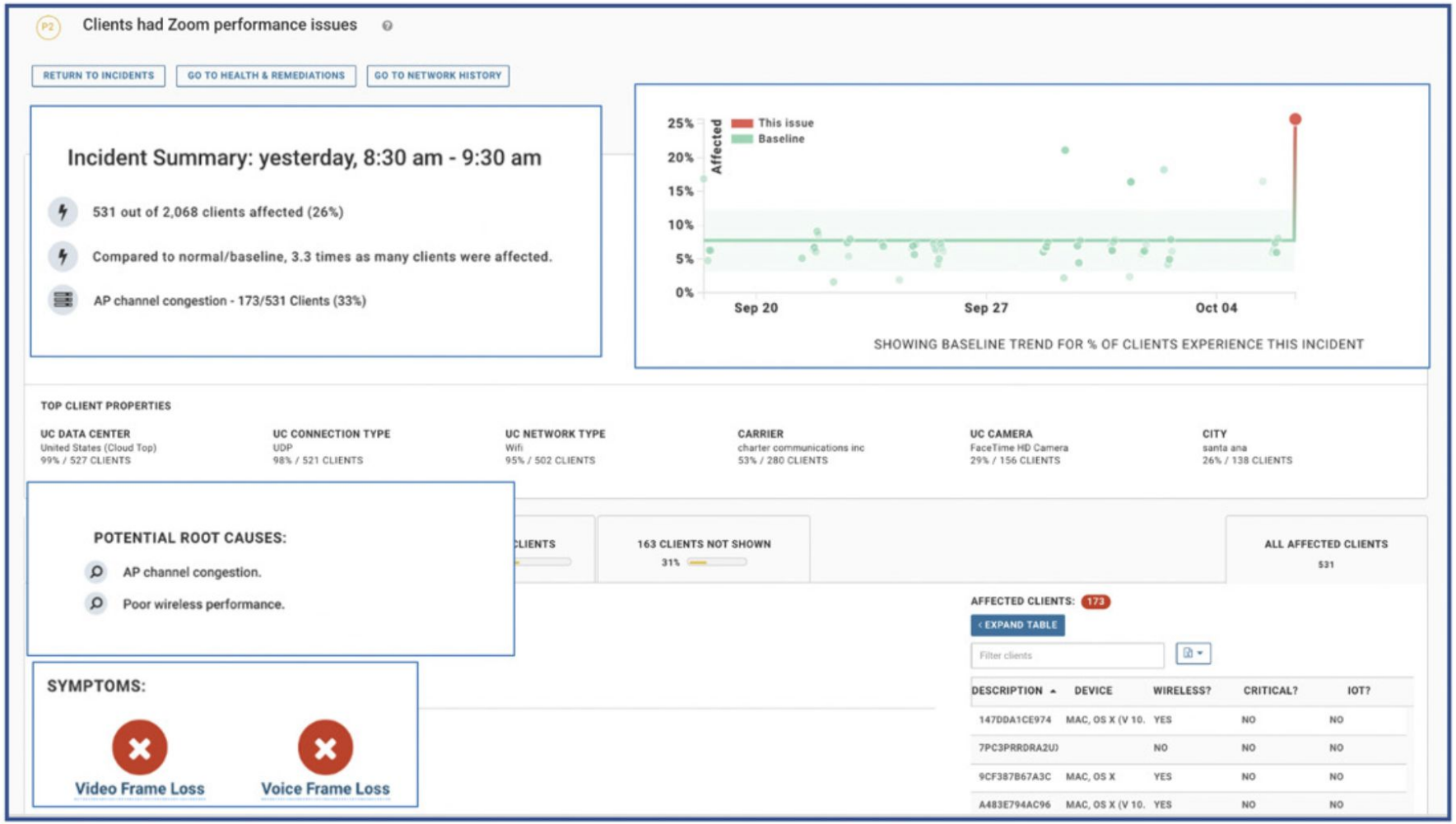


FIGURE 5: Example Client Zoom performance incident summary report from VMware Edge Network Intelligence

Implementation of SASE

AutoNation

Challenges:

- Insufficient bandwidth at retail stores.
- High costs associated with MPLS connections.
- Technological limitations hindering scalability.

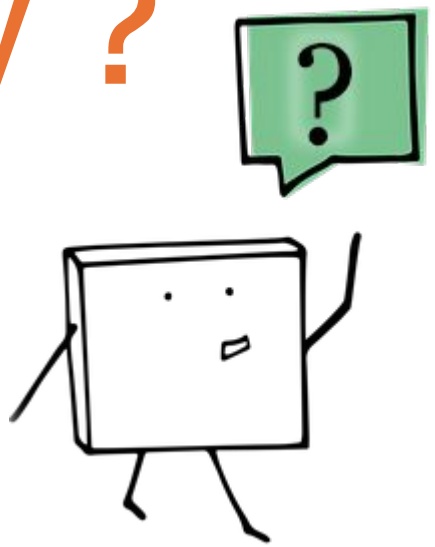
- **SASE Solution**: Implemented Prisma SD-WAN.
  - SD-WAN for enhanced connectivity and network optimization.
  - Centralized policy management to simplify network operations across locations.
- **SASE Components result**:
  - Increased bandwidth by 5x.
  - Reduced network costs by $3 million annually.
  - Improved speed of integrating to new locations by 95%

Implementation of SASE

Jefferies LLC

- **Challenges**:
  - Need for secure, scalable access during sudden shift to remote work.
  - Performance issues due to latency in a dispersed network environment.
- **SASE Solution**: Chose Prisma SD-WAN
  - Enabled a complete shift to remote work within two weeks.
  - Ensured consistent security and performance across global operations.

How do you implement SASE to your Company ?



Implementing SD-WAN to your company

Assess Current Network

Audit the existing WAN infrastructure

Traffic Analysis

Choose an SD-WAN Provider

Cost

Global Coverage

Cloud Integration

Network Configuration

Deploy SD-WAN appliances

Define application policies

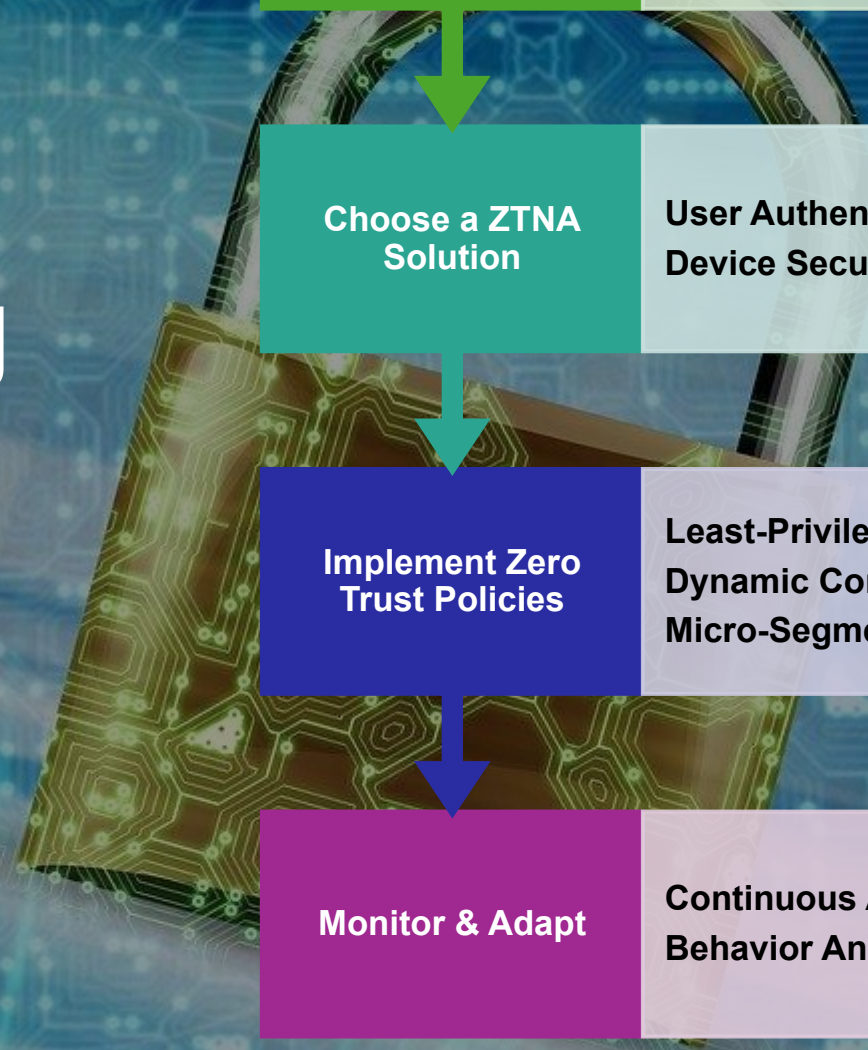
Centralized Management

Test & Roll Out

Pilot Implementation

Full Deployment

Implementing ZTNA to your Company



Audit your current VPN-based access solutions	
Choose a ZTNA Solution	**User Authentication** **Device Security Posture**
Implement Zero Trust Policies	**Least-Privilege Access** **Dynamic Contextual Controls** **Micro-Segmentation**
Monitor & Adapt	**Continuous Authentication** **Behavior Analysis**

Implementing CASB to your company

Discover Cloud Applications

Detect unsanctioned applications used by employees

Define cloud applicaation that needs visibility and control

Data Loss Prevention (DLP) Policies

Configured to inspect traffic for sensitive data like financial records and block or encrypt

Enforce Access Controls

Conditional Access Policies

Configure to enforce access controls based on identity, location, or device.

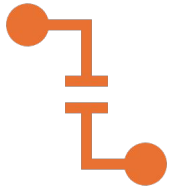
Enforce controls over sharing and downloading data

Monitor Cloud Activity

Enable real-time Monitoring

Set up automated alerts

Implementing FWaaS to your Company



Replace or Supplement On-Premise Firewalls

Evaluate your need.

Define Security Policies

Set policies to segment your network

Enable IDS and IPS

Use FWaaS for deep packet inspection, anti-malware scanning, and protection

Secure Remote Users

Extend firewall policies to remote users without the need for separate VPNs.

Implementing NG-SWG to your company

Identify

Identify Web Security Needs

- User Profiles
- Traffic Patterns

Choose

Choose an NG-SWG Provider

- SSL Inspection
- URL Filtering and Threat Protection

Configure

Configure Web Security Policies

- Content Filtering
- Prevent Data Loss

Protect

Protect Against Web-Based Threats

- Implement Advanced Malware Protection
- Use Real-Time Web Monitoring

What is Left?

Your security and networking policies in a unified platform!!!

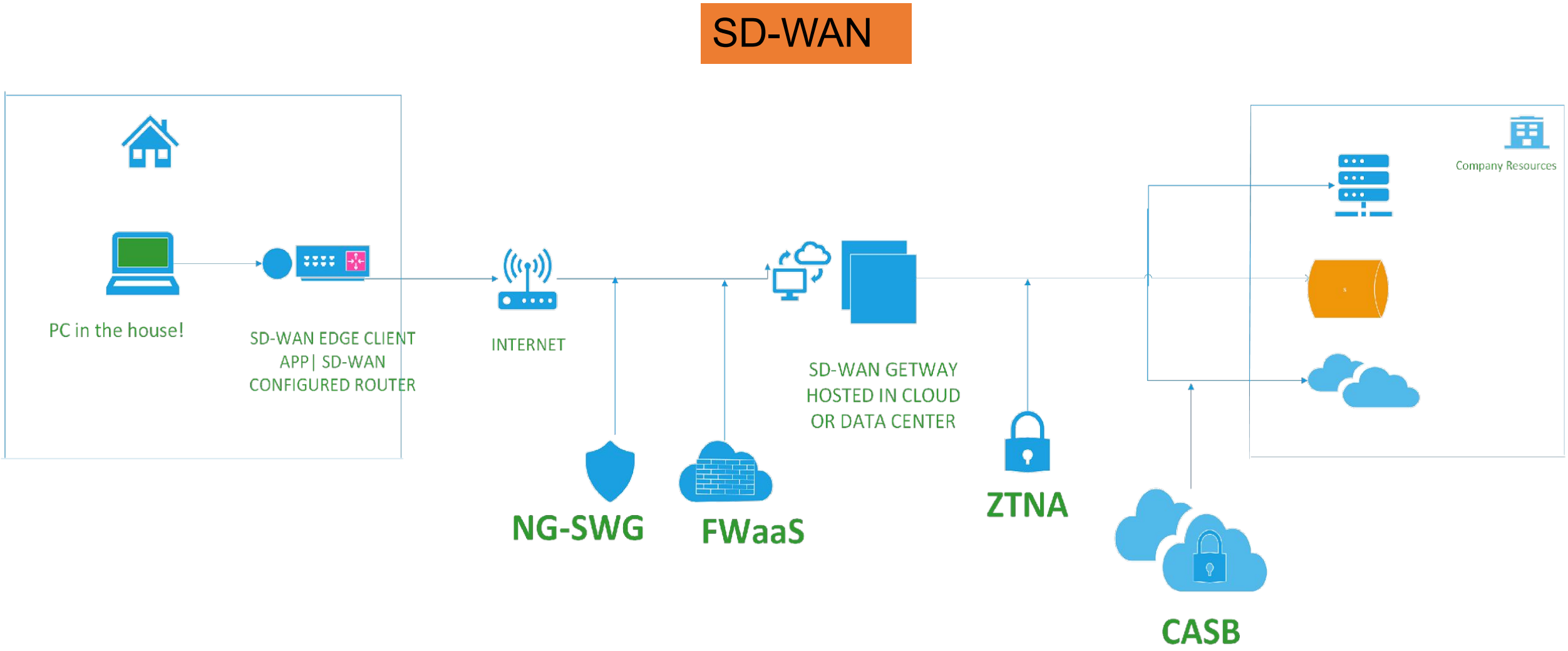
Centralized Management Platform and Reporting and Analytics

- Each SASE platform provides centralized visibility network traffic, user activity, and security policies across the organization.
- Leverage real-time analytics to gain insights into network performance, threat activity, and user behavior.
- SASE can perform automation and orchestration like enables automation for policy enforcement, dynamic network management, and incident response.

Companies That Provide SASE Services

- Cisco Meraki
- VMware VeloCloud
- Fortinet SD-WAN
- Netskope
- McAfee MVISION Cloud
- Microsoft Defender for Cloud Apps
- Zscaler Private Access (ZPA)
- Palo Alto Prisma Access
- Cisco Duo
- Cato Networks
- Cisco Umbrella

Use case


SD-WAN
PC in the house!
SD-WAN EDGE CLIENT APP| SD-WAN CONFIGURED ROUTER
INTERNET
NG-SWG
FWaaS
SD-WAN GETWAY HOSTED IN CLOUD OR DATA CENTER
ZTNA
CASB
Company Resources

How SASE Addresses Work-from-Home Security Risks

1. **Preventing Unauthorized Access with ZTNA**
2. **Improving Network Visibility and Control with SD-WAN**
3. **Protecting Cloud Applications with CASB**
4. **Mitigating Web-Based Threats with NG-SWG**
5. **Replacing Traditional Firewalls with FWaaS**

THANK YOU!

Any Question?