paramount

ZERO TRUST WEBINAR

AHLAN CYBER اهلا سايبر

appgate

paramount

ZERO TRUST WEBINAR

Zero Trust is the sharpest tool to fight cyber threats. Learn from the experts how to safeguard your organization.

Jason Garbis
Chief Product Officer, Appgate

Rajesh Vikraman
Head IT infra, Cloud & Cybersecurity

James Tolfree
VP Sales, Appgate

Amit Kumar Sharma
BU Manager, Paramount

Premchand Kurup
CEO ,Paramount

What is **Zero Trust?**

AHLAN CYBER أهلاً سايبر

appgate

paramount

Zero Trust

- “Zero Trust is an information security model that denies access to applications and data by default. Threat prevention is achieved by only granting access to networks and workloads utilizing policy informed by continuous, contextual, risk-based verification across users and their associated devices.”
- All entities are untrusted by default
- Least privilege access is enforced
- Comprehensive security monitoring

“The Definition of Modern Zero Trust,” Forrester, 2022

TCP/IP is a Weak Security Foundation (Implicit Trust)

TCP/IP Connect First, Authenticate Second

All resources are visible

Connect

Authenticate

AHLAN CYBER أهلاً سايبر appgate paramount

TCP/IP has a poor policy language

Should 192.168.4.11 have access to 10.5.0.3?

Yes or No?

The End Result?

Too often:

Wide open, flat networks

Users with broad access to hundreds or thousands of resources

Network security teams “give up” and rely on authentication only for access control

AHLAN CYBER أهلاً سايبر appgate paramount

TCP/IP
Connect First, Authenticate Second

All resources are visible

Connect

Authenticate

Zero Trust
Authenticate First, Connect Second

Authenticate

Connect

All resources are visible

Zero Trust Enables a Rich Policy Language

Should Jim have access to the production SAP® server?

Jim

It Depends!

SAP Production Server

What project is Jim working on?

Is Jim's machine patched?

What time is it?

What's our current security posture?

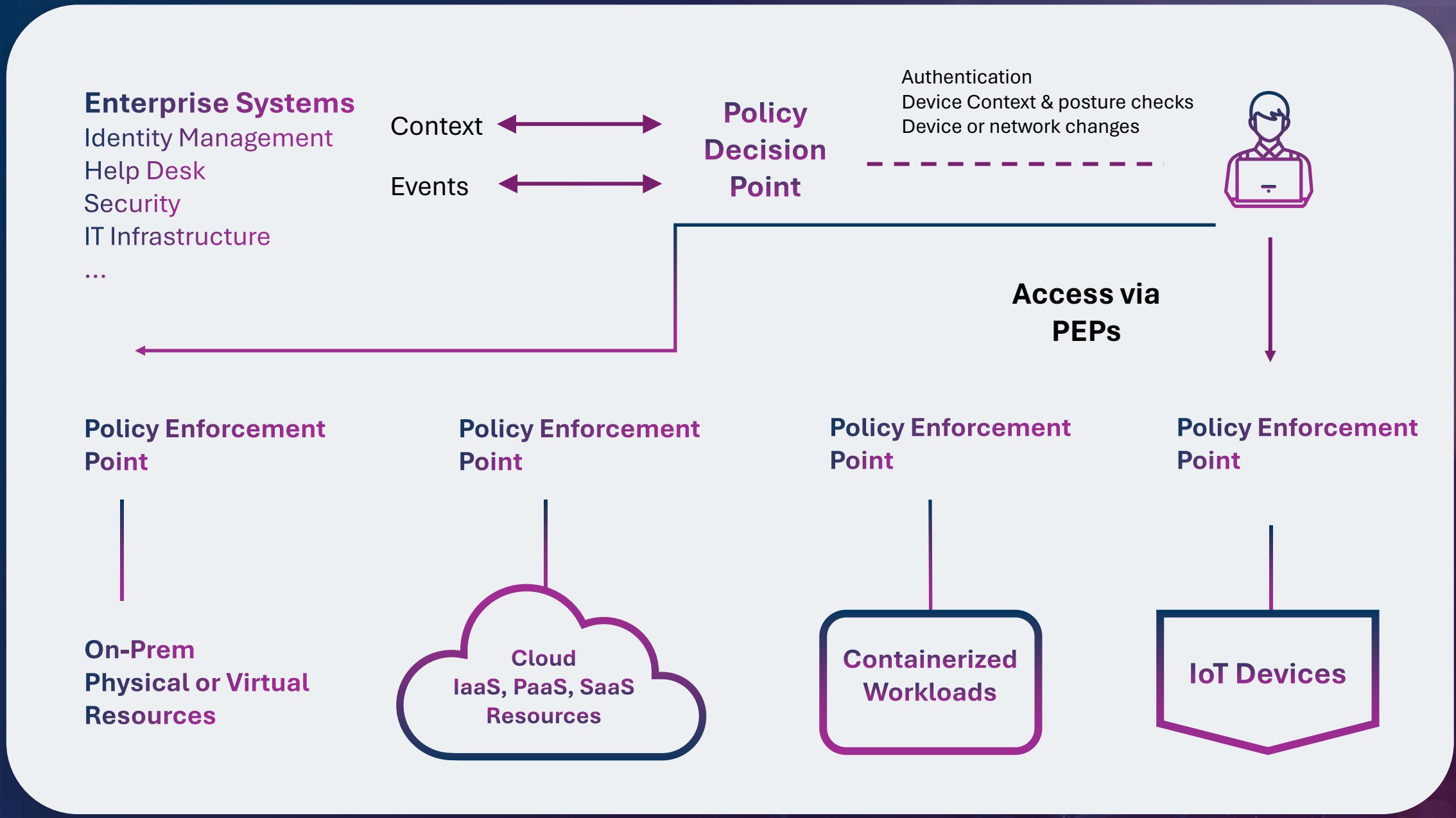
Jim

SAP Production Server

It Depends!

Where is Jim connecting from?

Is there an open Service Desk Ticket?


Enterprise Systems
Identity Management
Help Desk
Security
IT Infrastructure
...
Context
Events
Policy Decision Point
Authentication
Device Context & posture checks
Device or network changes
Access via PEPs
Policy Enforcement Point
On-Prem
Physical or Virtual Resources
Policy Enforcement Point
Cloud
IaaS, PaaS, SaaS Resources
Policy Enforcement Point
Containerized Workloads
Policy Enforcement Point
IoT Devices

Why Start with **Zero Trust** Network Access?

AHLAN CYBER أهلاً سايبر

appgate

paramount

Zero Trust

- “Zero Trust is an information security model that denies access to applications and data by default. Threat prevention is achieved by only granting access to networks and workloads utilizing policy informed by continuous, contextual, risk-based verification across users and their associated devices.”

- All entities are untrusted by default
- Least privilege access is enforced
- Comprehensive security monitoring

- ” The Definition of Modern Zero Trust,” Forrester, 2022

Zero Trust Network Access

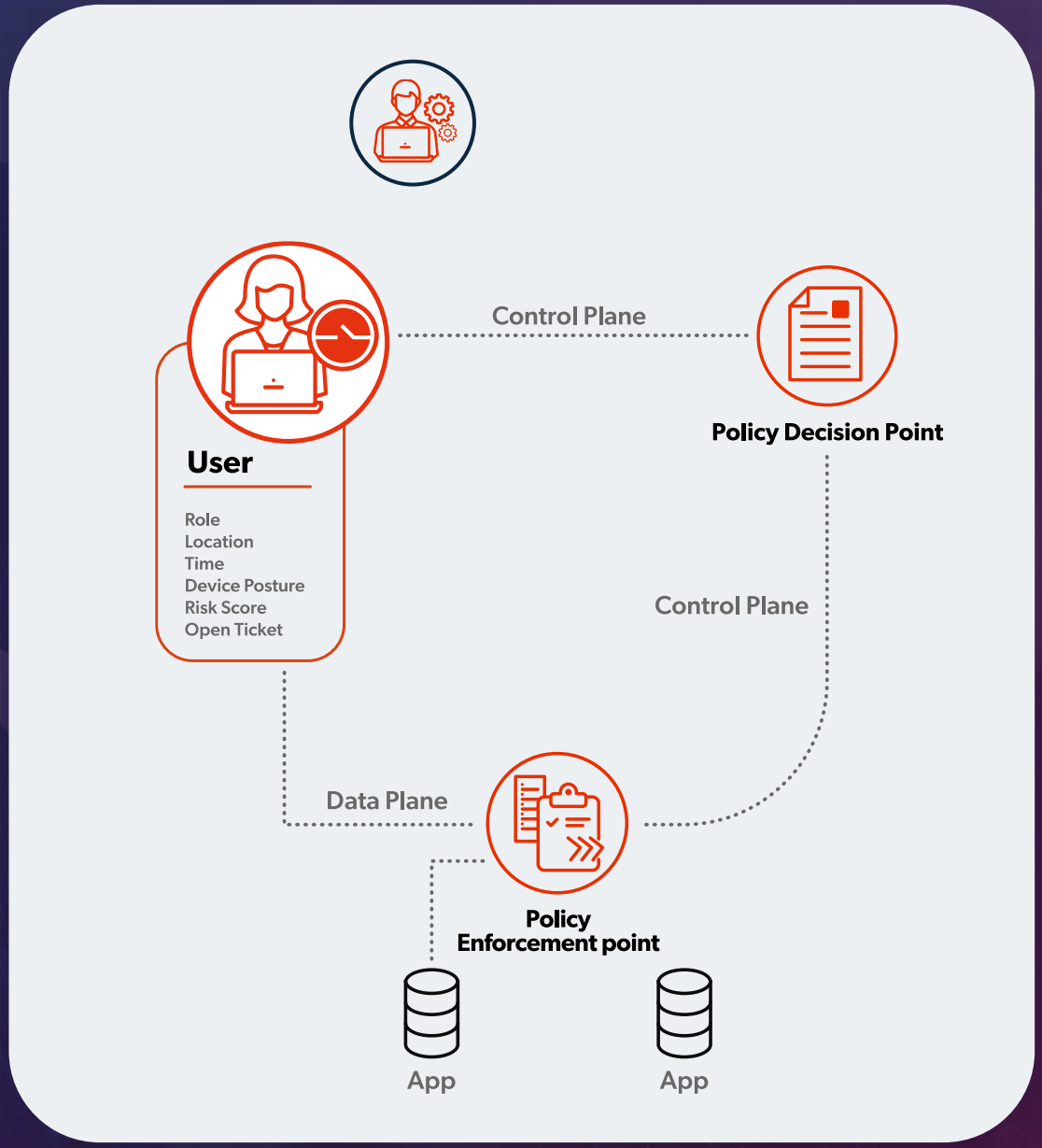
Zero Trust Network Access is a security solution that helps organizations take a significant leap in achieving their Zero Trust goals. Originally termed as a software-defined perimeter, ZTNA delivers a modern architecture that replaces legacy, failing hardware solutions like VPN and NAC with a unified policy engine for all users, workloads, and devices.

Cloak all resources and make the attack surface invisible
Use context and risk cues to deliver just in time, just right access for everyone and everything
Simplify access management with a unified policy engine
Scale and interoperate easier with a software-defined, API-
driven architecture

Contextual access to workloads

The bread and butter of Zero Trust Network Access

- Cloak all infrastructure and enforce “default deny”
- Unify access policies across all heterogenous workloads
- Enrich policies using context and threat cues
- Automate policies for dynamic entitlement adjustments when context and/or risk changes
- Choose the right deployment model
- Don’t forget to secure resource-to-resource connections



Zero Trust Network Access: The Right Way Forward

Zero Trust Access

Phase Out Legacy Technology

Replace and reduce outdated, insecure legacy access and network technologies

Transform Enterprise Networks

Replace legacy enterprise security controls and simplify network architecture

Modernize Secure Access

Deliver the latest in secure access solutions for all users and resources across complex hybrid infrastructure, regardless of location

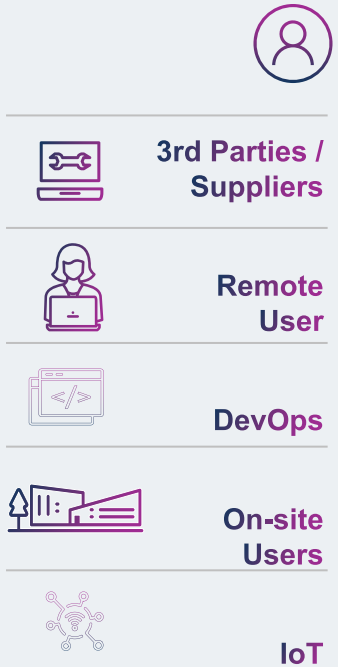
Reduce Operational Overhead

Decrease security admin overhead, delivery times and operational challenges, while increasing cost savings and business ROI

Universal ZTNA: Secure Access For All

Appgate SDP Zero Trust Network Access

User-to-Resource | Resource-to-Resource



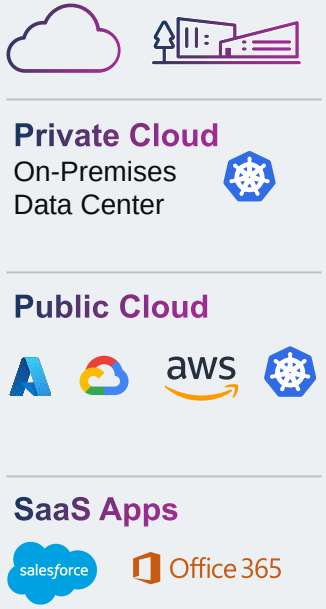
Identity-Centric
Multi-dimensional profile
User and device attributes
SSO, SAML, LDAP, Radius

Least Privilege Access
Microsegmentation
Concurrent encrypted access
Dynamic and continuous

Cloud Native
Cloud engineered
Operate natively in cloud
Distributed and scalable

Cloaked Infrastructure
Single packet authorization (SPA)
Can't hack what they can't see
Trusted user, trusted device, risk & context

Flexible and Agile
API integrations and automation
Cohesive security ecosystem
Automation/secure access as code



Unified Policy Engine

Centralized management | Consistent policies, monitoring and logging

Practical Considerations for Zero Trust Implementation

Identity and Access Management

→

Compliance requirement

Who should access?
When to access?
What to access?

→

Technology integrations

Think big, start small, scale fast

Understand the business value

Challenges

Challenges

Design Principle

- Agile, Consolidate, Simplify, Optimize.

Security Requirements

- Need to fortify security at branches.
- Looking for a cloud-based control plane for better visibility and management.

New Acquisitions and Mergers

- Need for cross-business application access.
- Addressing gaps in security controls.

Tech Refresh

- Approaching tech refresh of WAN solution.
- Evaluation of SD-WAN solutions.

Hybrid Cloud & Hybrid users

- Changing perimeter with hybrid cloud adoption.
- Integration with multiple data centers and IaaS.
- Need for backend integration, and developer access for partners and in-house teams (DevOps and content teams).

Local Services Challenges

- Local services like file servers for subsidiaries are not consolidated due to latency, bandwidth, and capacity challenges.

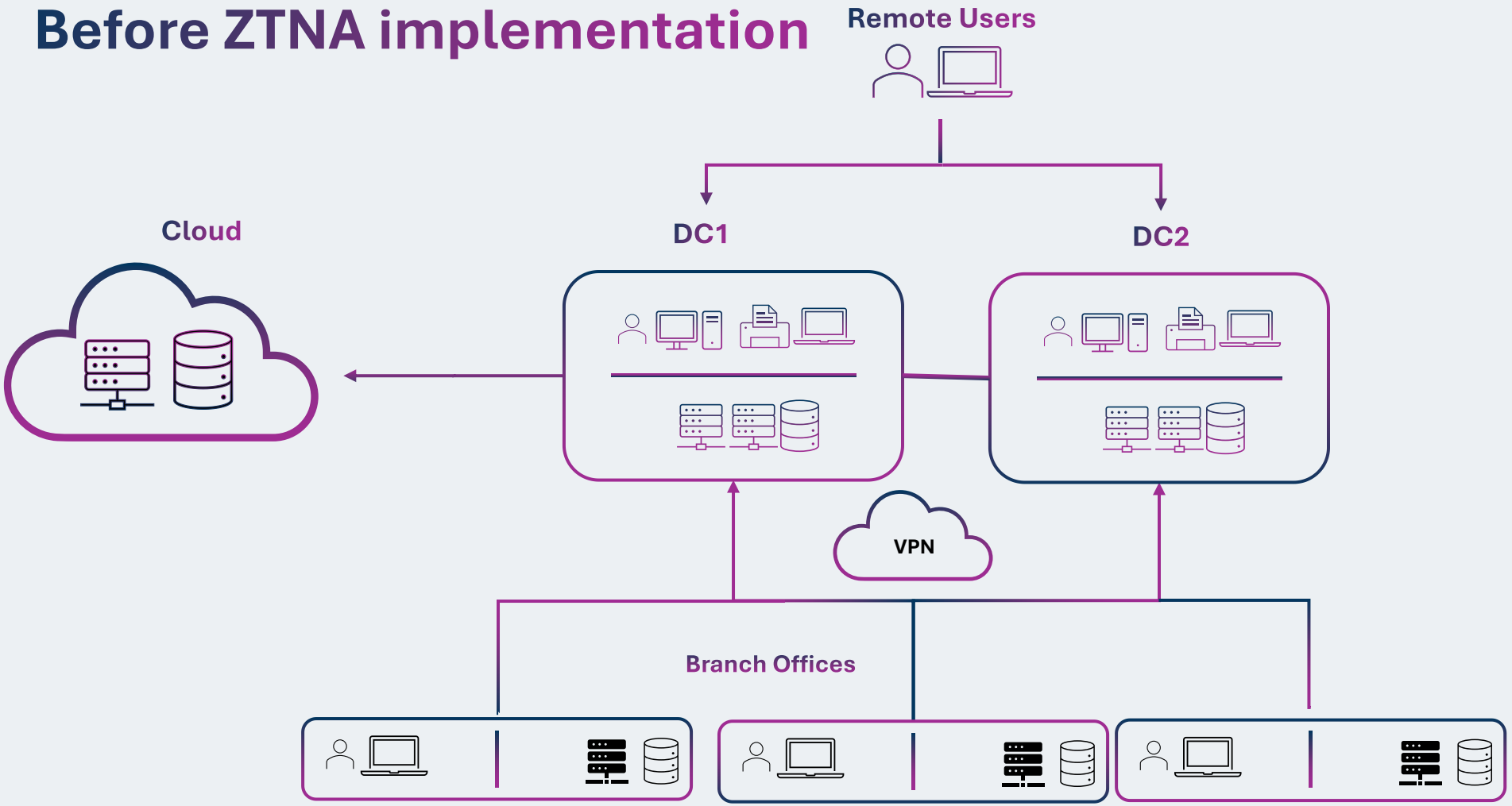
- Hub-spoke multi-point VPN architecture is used to avoid hits on costly leased lines at data centers.

Approach & Solution

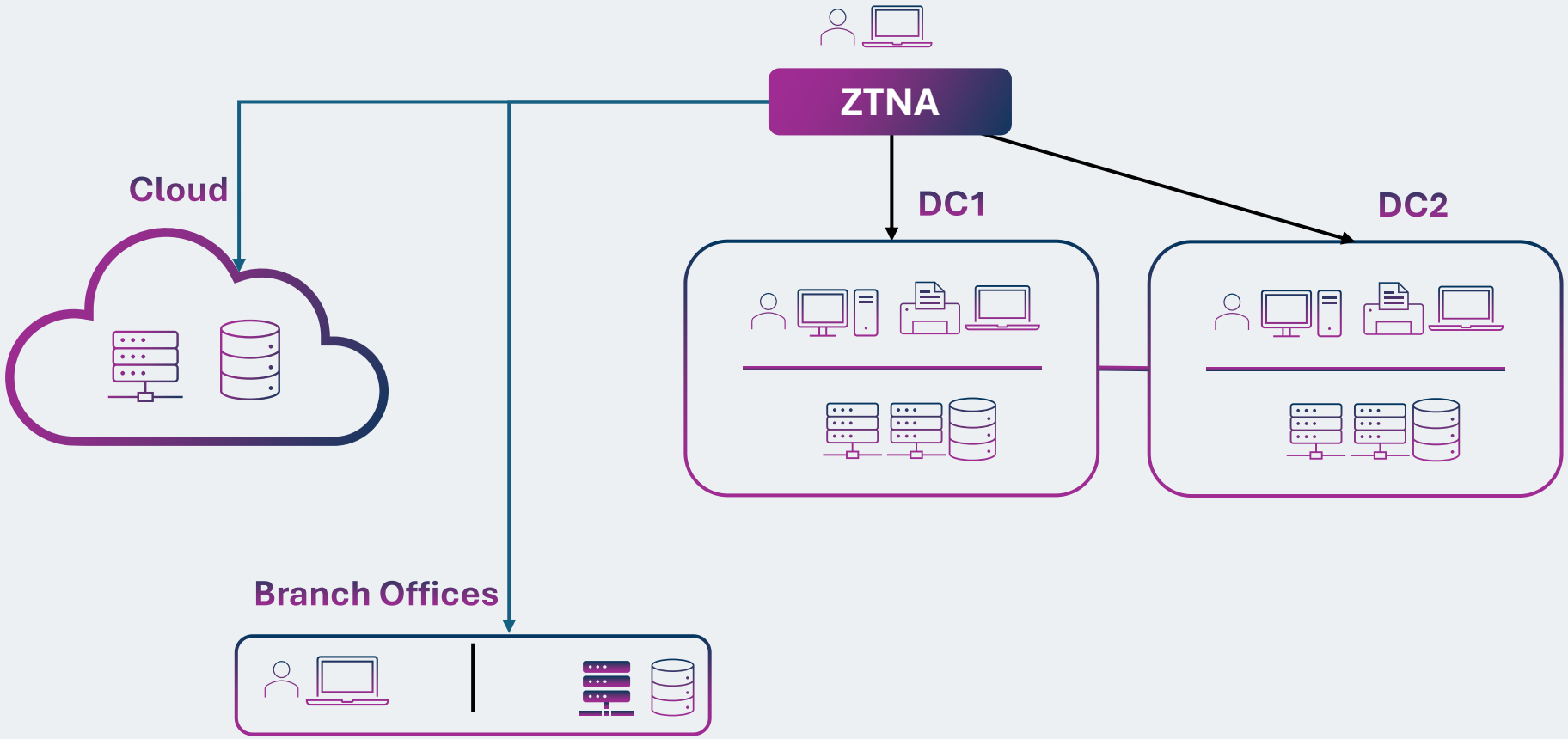
Approach & Solution

- Evaluation of **SD-WAN** and cloud-based **SDWAN/SASE solutions.**
- POCs conducted; high TCO due to variable costs as data flows through the service provider cloud (egress charges) and lack of support for hybrid or on-premise deployments.
- Sometimes we felt our requirement for a client-based multipoint connectivity is an unrealistic dream.

Before ZTNA implementation



After ZTNA implementation



Remote Users / Branch / Office users / Third-party

Increased Agility, Better Consolidation, and Simplified network!

Results

Operation costs Efficiency

- Eliminated SDWAN investment, achieving significant network cost savings.
- Simplified operations and reduced overhead, enhanced agility.
- Same level of security anywhere.

Network

- Moved to cafe model networks with Internet and local services.

Enhanced Security with improved user Experience

Hybrid identity, MFA, and posture verification.
Micro-segmentation
Dynamic granular access
Continuous validation
Centralized policy engine
Quick onboarding of new acquisitions.
Unified and better user experience.
Predictable cost due to direct routed ZTNA.

Our Engagement Approach – Embarking a ZERO TRUST journey

Plan

- Assessment charter & business priorities
- Stakeholder mapping
- Access to systems and data
- Workshop planning
- Pre requisites and dependencies
- **Kick-off**

Collate

- Security tool inventory and collecting organization policies procedures, standards & frameworks
- Identify infrastructure, roles and privileges.
- Configuration Documents
- Operational documents

Analyze / Review

- Review of
  - Policy documents
  - Procedures and frameworks
  - Operational documents
  - Risk Registers and documents
- Conduct Risk Assessment
- Configuration review of implemented Microsoft security solutions

Report

- Updating Customer ISMS policy with ZT principles
- Modified change management template reflecting ZT principles
- Delivering Zero Trust artifacts
- Gap Assessment report
- Risk Assessment report and Risk Register

Recommend

- Detailed report of assessment & maturity
- Content for business case
- Benefits of ZT approach
- Road map to achieve complete zero trust
- Sign-off and Closure

Ask us anything

Thank You

AHLAN CYBER أهلاً سايبر

appgate

paramount