Why VPN losing its relevance

in the world of
sophisticated Cyber Attacks ?

# VPN vs ZTNA

Outcome based Approach

SWIPE RIGHT

Problems with VPNs & Traditional Network Access

Vulnerable to Data Breaches due to lack of fine-grained Access and micro-segmentation

Easily Susceptible to Phishing Attacks despite Multi-Factor Authentication

Highly Error Prone in ever-changing VMs/ Containers setup: Dependencies on Manual and IP-based configurations

Ransomware attacks on workloads due to Lateral Movements across networks

Poor User Experience
Higher Latencies due to VPN Gateway Traffic Hairpinning and Login fatigues

VPN gateway dependencies -
Constraints due to the need for High available service with adequate capacity

Zero Trust Network Access - Use cases

Secure and **granular Remote Access** of Apps

Zero Trust Access to Data in SaaS such as like OneDrive, AWS S3 etc and Data Protection

Secure Infra Access, DevOps and **Multi-Cloud Ops**

Simple **Cloud Workload protection**

Compliance Enablement - Auditable Access Logs and micro-segmentation for PCI DSS, HIPPA

Third party / Contractor **Access control**

VPN Vs ZTNA

Outcome Parameters	VPN	ZTNA
Risk of Data breaches and ransomware attacks	**High** - Due to higher attack surface due to Perimeter based trust model	**Very Low -** Hugely Reduced Attack surface due to Granular Access based on Zero Trust
Staff User Experience	**Poor** - Higher latency due to traffic hair pinning at the VPN Gateway Datacenter or HQ | Frequent Sign-ons leads to Staff Fatigue	**Improved Experience** - Lower latency traffic & packet loss due to Direct, Peer to Peer & mesh connectivity | Single Sign On and adaptive authentication delights Staff users
Availability & Scalability	**Challenging** - Lower Scalability and Redundancy VPN gateway setup constraints	**Built in Scalability and Redundancy** - Cloud based auto scaling and redundancy Not dependent on central VPN gateways
Ease of Deployment & Management	**Time consuming, Manual & Error Prone -** Based on expensive Hardware Appliances - Not software defined approach	**Deployment in Minutes with full automation -** Easy REST API Orchestration, custom workflows - No need for Gateway Hardware deployment
Compliance to Cybersecurity Framework	**Not Compliant** - Provides basic secure remote access	**Supports ISO 27001** and similar certification audits through deeper audit logs and optional forensics
Cost-effectiveness	**Higher cost -**Considering the need to deploy central VPN gateway, backhaul bandwidth and Opex	**Lower TCO** Simple per user license subscription on-demand

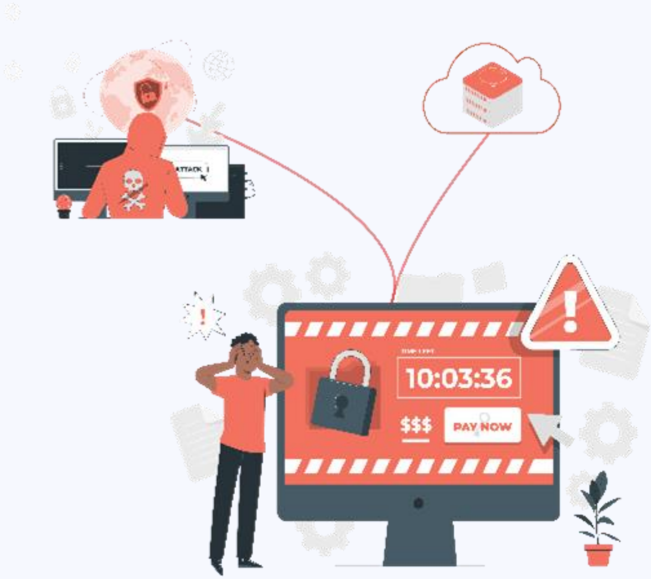
SWIPE RIGHT

1. Risk of Data breaches and ransomware attacks

Up to 90% reduction in the critical network-based attack surface & Risk

VPN

✗



Higher attack surface due to Perimeter based trust mode

- Macro-segmentation - **Network-level access**
- Lack of Device Trust availability
- User Authentication failures through Phishing attacks

ZTNA

✓

Hugely Reduced Attack surface due to Granular Access based Zero Trust

- Micro-segmentation - **Application-level access**
- Continuous User, Device, Location verification
- Flexible, Fine grained Resource Access Policy

How ZTNA lowers Attack Surface up to 90% over VPN

Each of the vulnerability multiplies leading to a larger attack surface

	WHO	WHAT	WHEN	WHERE	WHY	HOW
VPN	◒	✕	✕	◒	✕	✕
	• User Role • MFA • Device Trust	• App Identity • App role • Endpoint Location	• Time • Day • Duration	• Workload Tags • Group Memberships	• Meta data • Security Groups	• IDS/Deep Packet Inspection
ZTNA	✓	✓	✓	✓	✓	✓

Kipley Policy Method

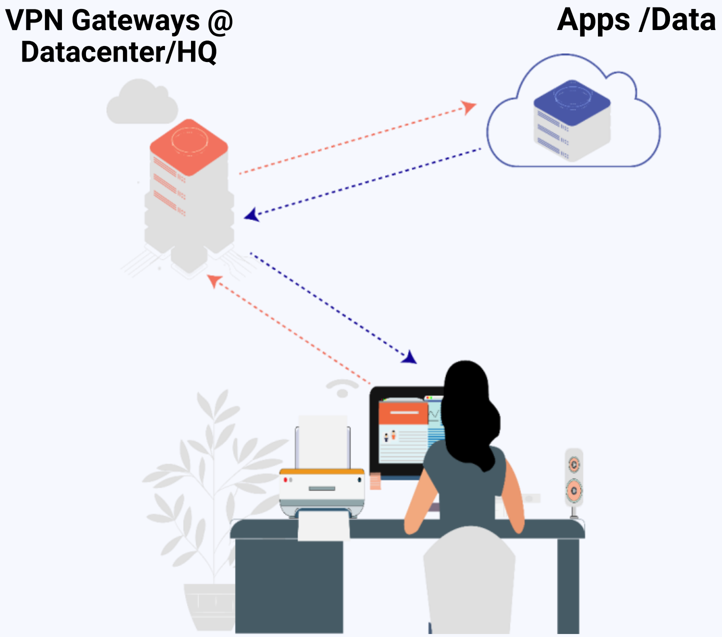
Describes the Who, What, When, Where, Why, and How of access of Data, Applications, Assets, and Services (DAAS)

- **Who** should be allowed to access a resource?
- **What** application is the asserted identity allowed to use to access the resource?
- **When** is the asserted identity allowed to access the resource?
- **Where** is the resource located?
- **Why** is the user (the Who) allowed to access the resource?
- **How** should traffic be processed as it accesses a resource?

2. Staff User Experience

VPN

✗

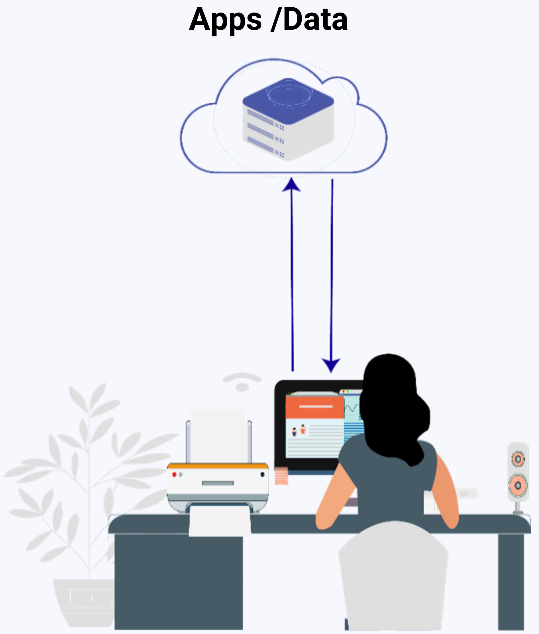


Poor

- Higher latency and some **data losses or leakage** happens due to **traffic hair pinning at the Datacenter or HQ** and congestion over VPN Gateway
- **Frequent Sign ons** leads to Staff Fatigue

ZTNA

✓



Highly Improved

- Lower latency traffic & packet loss due to Direct, Peer to Peer & mesh Communications; leads to **faster response time** and improved productivity
- **Single Sign On** and adaptive authentication delights Staff users

3. Remote Access Service - Availability & Scalability

VPN

✗

Lower Scalability and Redundancy setup burdens

- Needs Redundant gateways to be setup
- **Not flexible with Scaling** the capacity with existing hardware

ZTNA

✓

Built in Scalability and Redundancy

- **Cloud based auto scaling** and redundancy
- Not dependent on central VPN gateways

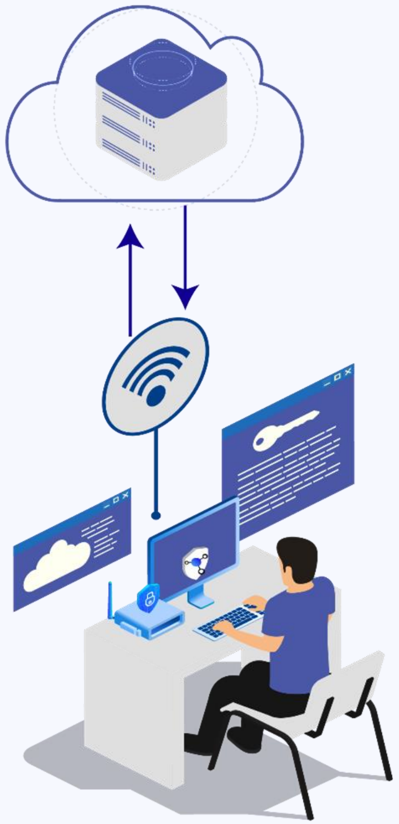
4. Ease of Deployment & Management

VPN

✗

Time consuming, Manual and Error Prone

- Based on **expensive Hardware** Appliances.
- Hub and Spoke based on On-Prem Gateway



ZTNA

✓

Deployment in Minutes with full automation

- Easy Orchestration, custom workflows,
- REST API based automations
- **No need for Gateway Hardware** deployment

5. Compliance to Cybersecurity Frameworks

VPN

✗

Not Compliant

- Provides basic security remote access

ZTNA

✓

Compliant to NIST 800-207 ZTA Framework

- Supports ISO 27001 and similar certification audits through deeper audit logs and optional forensics

6. Cost Effectiveness

VPN

✗

Higher cost

- Central VPN gateway capex
- Backhaul bandwidth and Opex

ZTNA

✓

Lower TCO

- No need for expensive VPN gateways
- Simple per user license subscription on-demand

ZTNA - Outcomes

Reduces the Risk of a Data Breach

Streamlined security policy creation

Improved end-user experience

Flexibility when moving apps, data and services

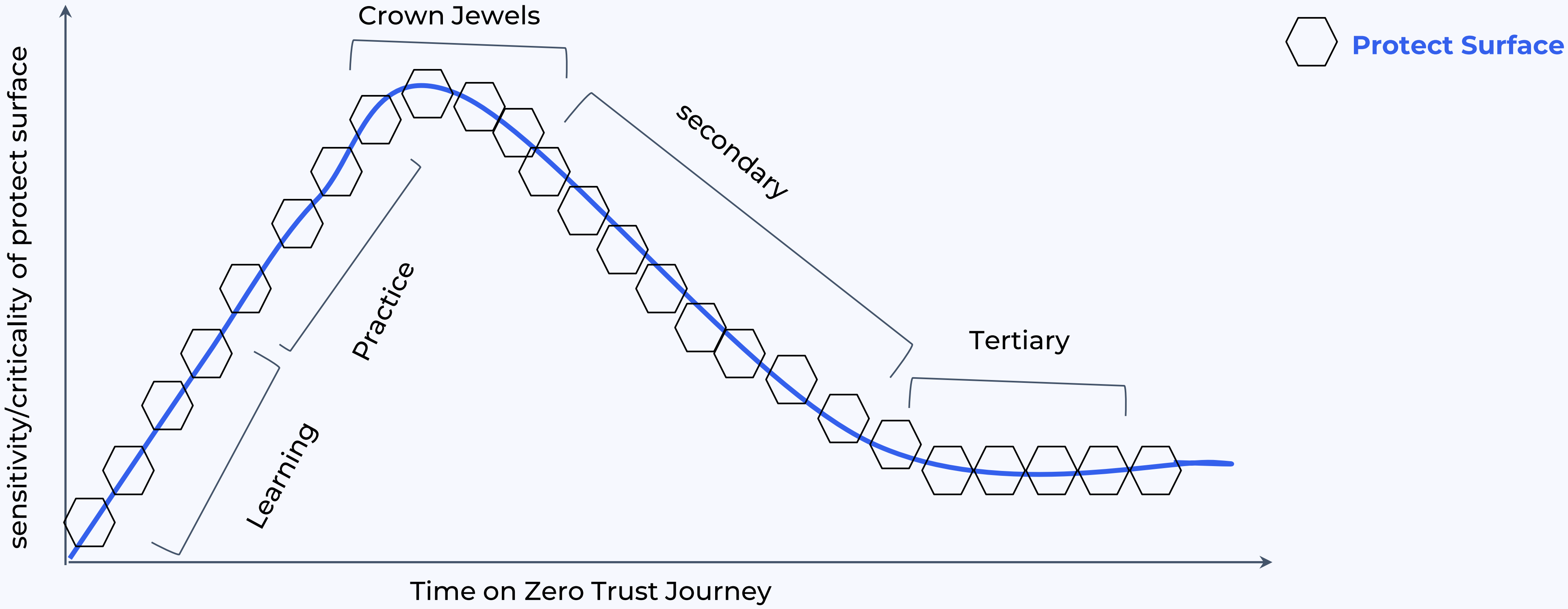
Improved Visibility & Monitoring

Improved Compliance (PCI DSS, NIST 800-207)

The End - Start Protecting your Surfaces

“ Zero Trust is incremental, protecting one (attack) surface at a time “

“ Enterprises don't need to protect all surfaces simultaneously, and should take an iterative approach.”


Crown Jewels
Protect Surface
sensitivity/criticality of protect surface
secondary
Practice
Learning
Tertiary
Time on Zero Trust Journey

Get in Touch with us !

Explore our ZTNA Product

www.cosgrid.com

Share Your Insights in Comments !