Zero Trust Data Protection Strategy

netskope

2024 © Netskope Confidential. All rights reserved.

Data Protection Clutter

2024 © Netskope Confidential. All rights reserved.

Give me a lever large enough and I will move the earth'

Principles of Zero Trust Strategy-

Continuous verification Always verify access, all the time, for all resources.

Limit the “blast radius Minimize impact if an external or insider breach does occur.

Explicit to Implicit trust-Drive to conditional access.

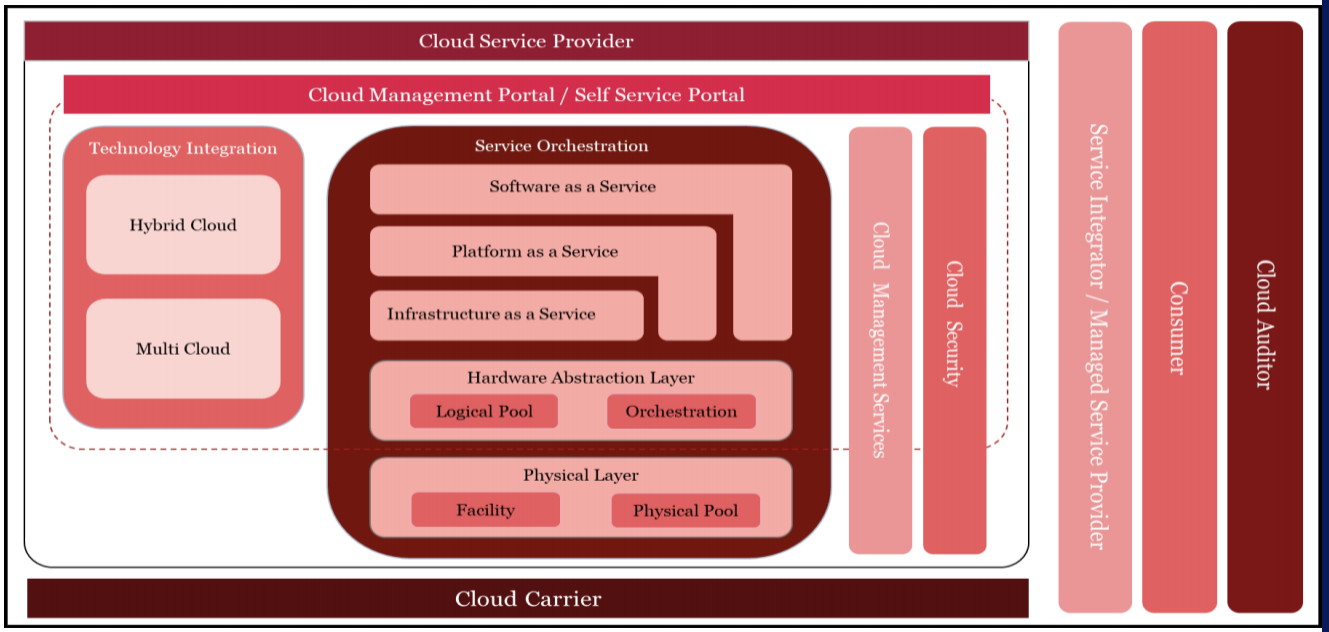
Automate context collection and response. Incorporate behavioral data and get context from the entire IT stack (identity, endpoint, workload, etc..) for the most accurate response.

netskope

2024 © Netskope Confidential. All rights reserved.

Government Zero Trust Initiative– View

‘Its so easy even government can do it’



Zero Trust Architecture

Zero Trust Architecture defines a framework for structural cyber security of modern enterprises. It combines some of the already well known and established security guidelines and highlights them as the basic of tenets of the framework.

R S MANI
Deputy Director General, NIC

2024 © Netskope Confidential. All rights reserved.

Identity and Access-one part of it…

”Trust in Zero Things-solar winds'

”Multiple fall backs'

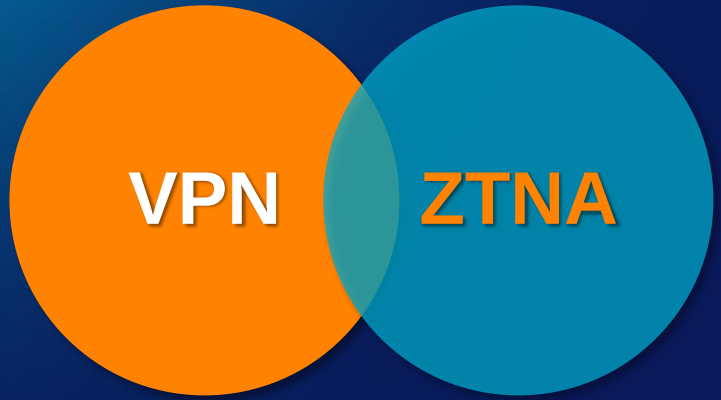
”No SMS based two factor auth'

netskope

2024 © Netskope Confidential. All rights reserved.

Private **Application Access**-Traditional VPN to ZTNA

- Connect first, authenticate later
- Coarse access – all or nothing
- Open ports are visible to attackers
- Connect devices to networks (IP-based)



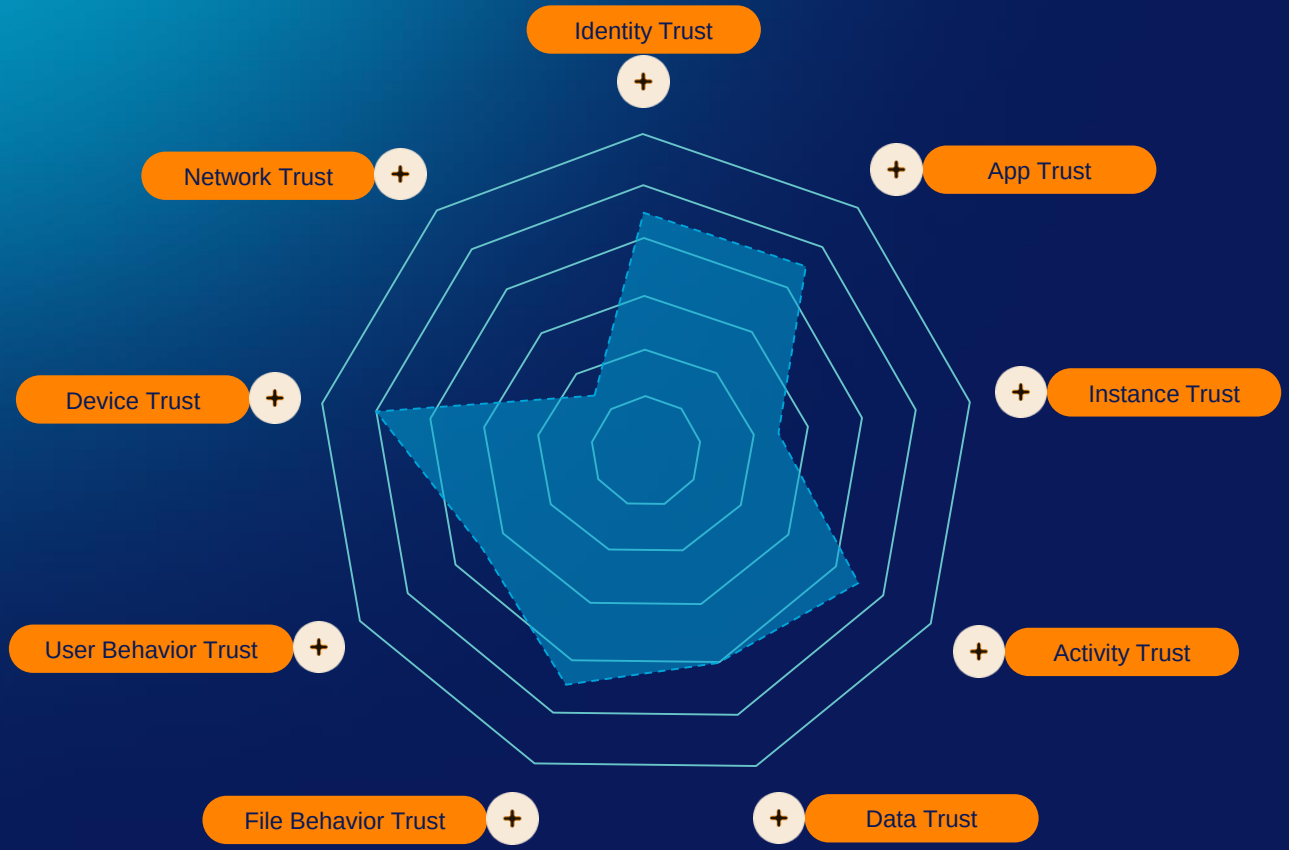
- Provide remote access
- Per application access
- Encryption connection
- Authorized users only
- **Data Loss Controls**

- Authenticate first, connect later
- Granular access – constrain lateral movement
- Inside-out connectivity hides assets
- Connect users to specific resources

”Log into app not into network'

netskope

2024 © Netskope Confidential. All rights reserved.



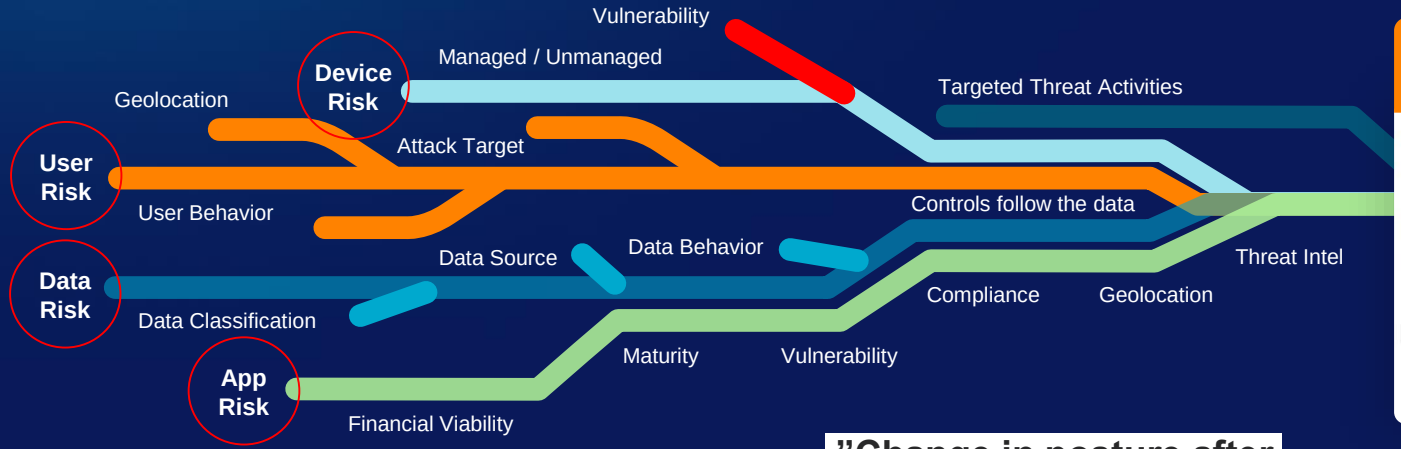
What *action* should take place for this transaction based on the *current risk landscape*?

netskope

nfidential. All rights reserved.

Dynamic & Adaptive Policies

Identity	Device Risk	SaaS App	App Instance	App Risk	URL Category	Activity Controls	User Risk	Threat	Data Risk (DLP)	Policy Action
Pat Smith Accounting Logged in as psmith@gmail.com	Managed Personal/ BYOD	Google Drive Sanctioned Unsanctioned	Company Personal	93 Excellent rating (low risk) Breadth of 50K+ Apps	Cloud Storage 130+ categories	Upload Share Create Delete Move Download (120+)	↓863 Behavior Tracking (moderate risk) (UEBA)	Threat Intel AV Sandbox IPS ML CTE	GDPR AU Privacy Act Over 3000+ classifiers	Contextual: Allow Coach Block Encrypt Legal Hold Quarantine



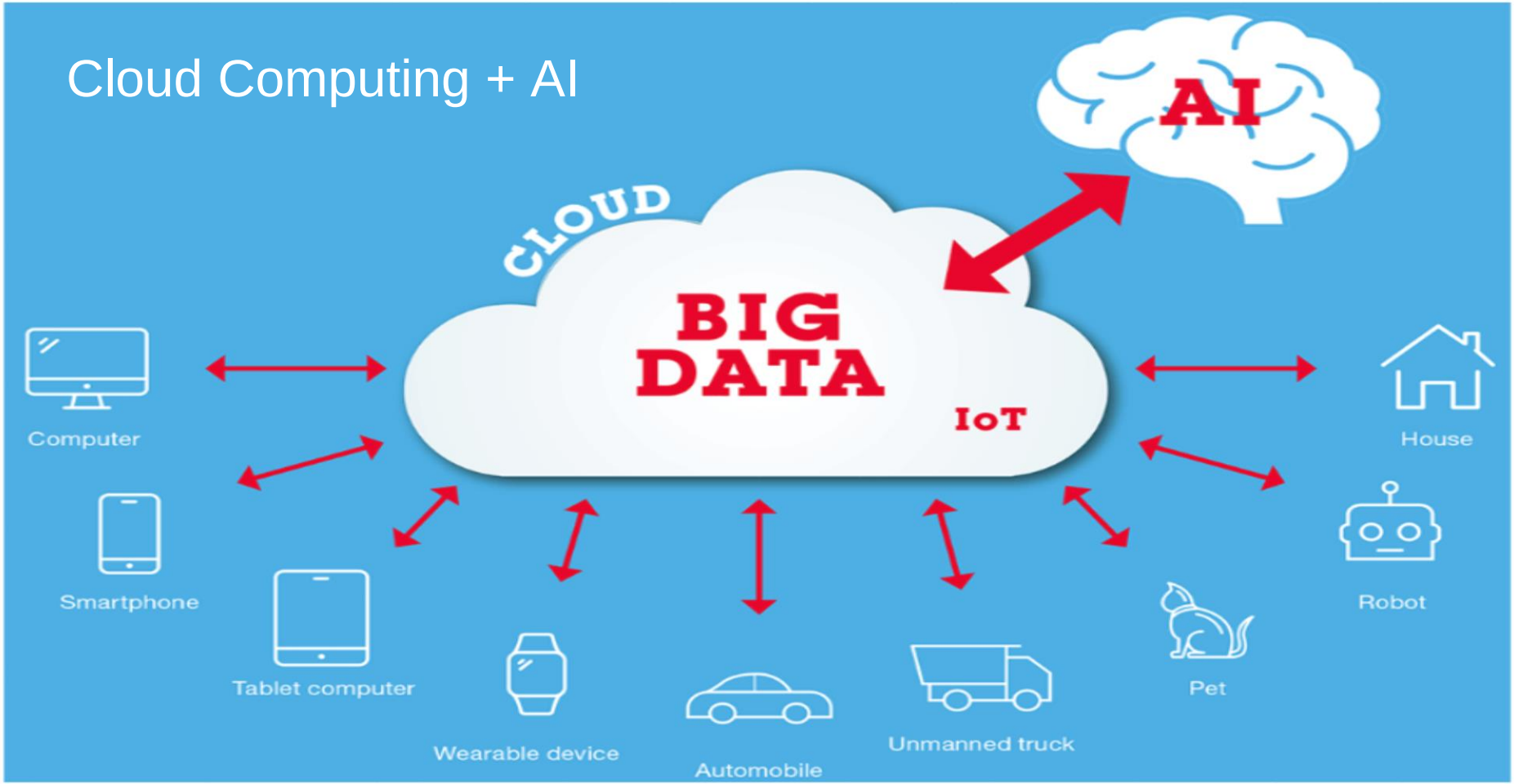
Real-time, Customizable User Coaching

"Change in posture after Auth'

netskope

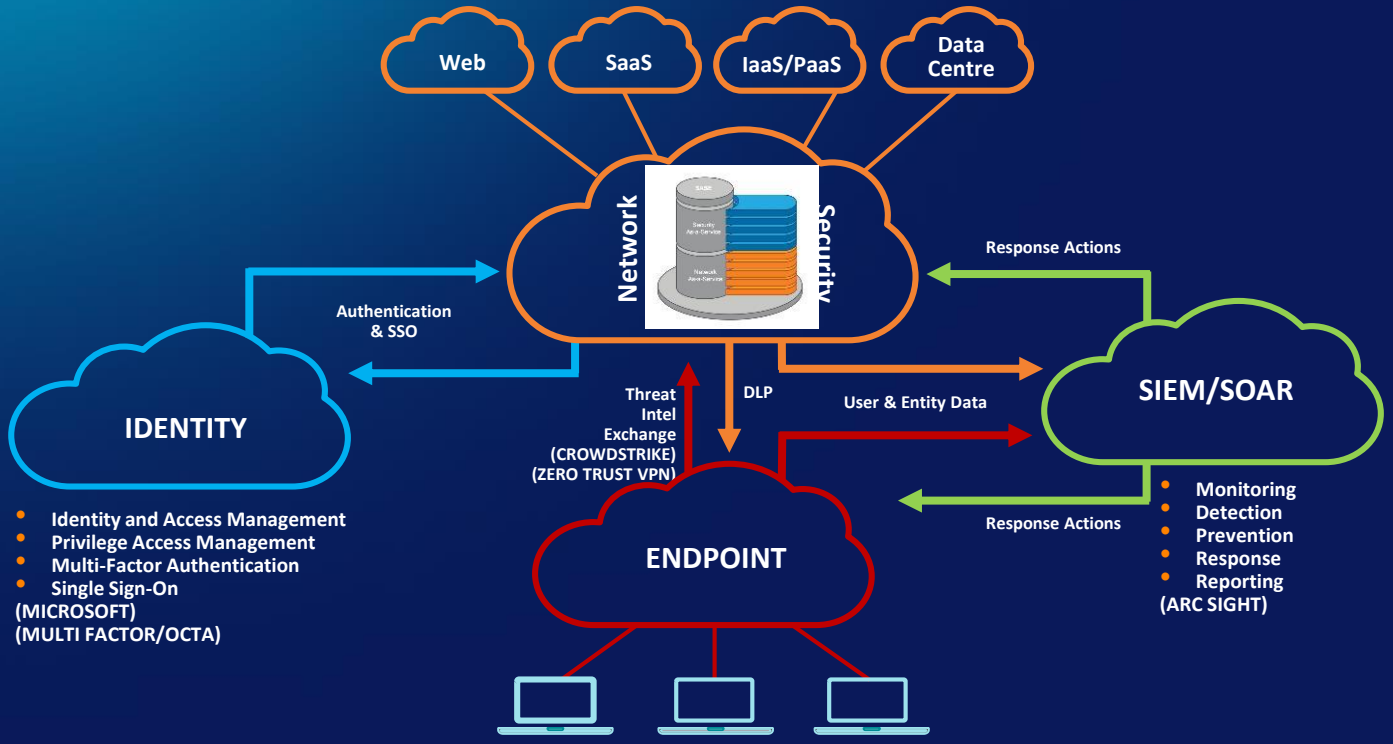
2024 © Netskope Confidential. All rights reserved.

Cloud Computing + AI



2024 © Netskope Confidential. All rights reserved.

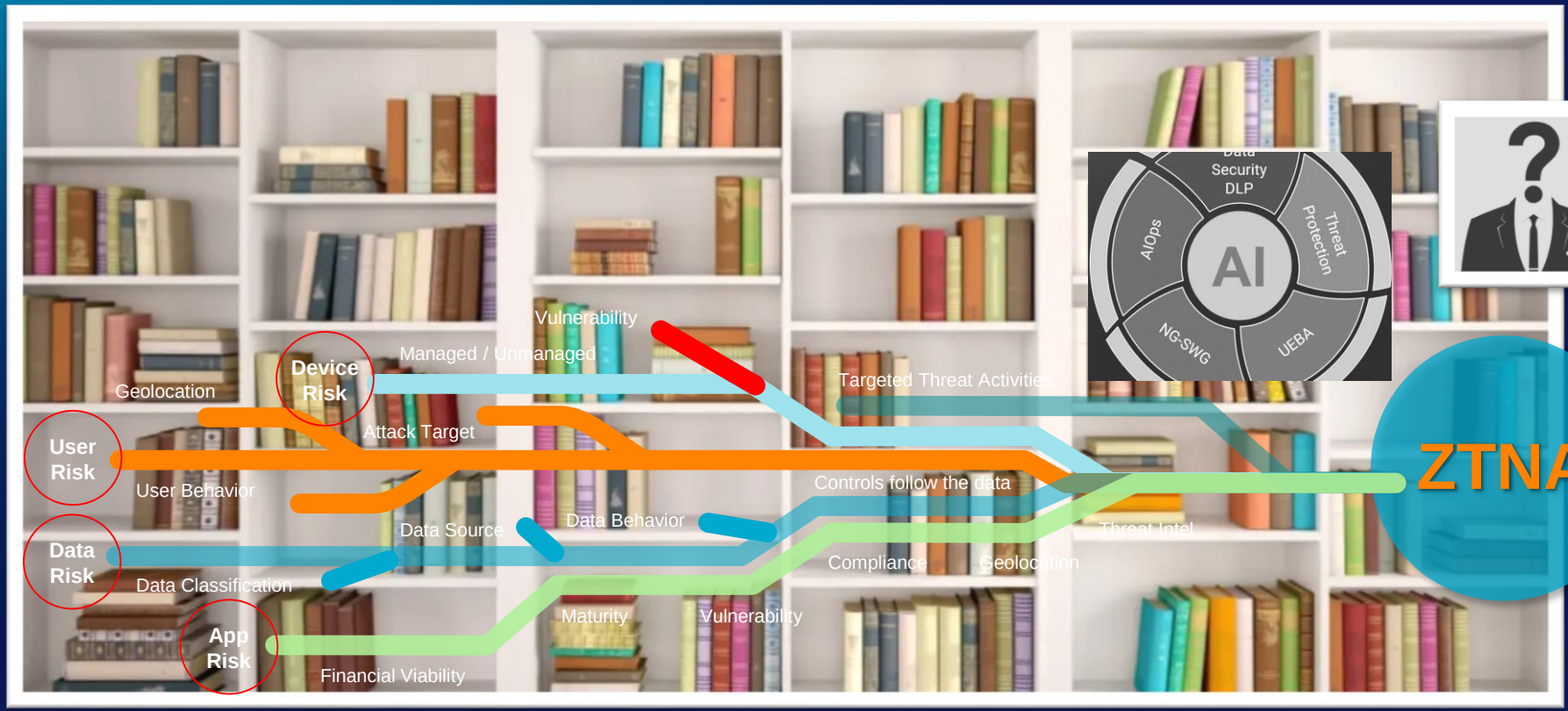
Building Zero Trust Ecosystem-



2020 © Netskope Inc. All rights reserved.

2024 © Netskope Confidential. All rights reserved.

Zero Trust Data Protection



2024 © Netskope Confidential. All rights reserved.


Reduce attacks
Intelligent Data Classification & Access
Better and Fast Incident Response
Faster Attack identification/ Response
Secured Acess
Improved Accuracy/ Reduce falsepositives

Smart City Key Network Components

1. **Edge Devices**: Smart traffic lights, environmental sensors, surveillance cameras.

2. **Communication Networks**: 5G networks connecting devices across the city.

3. **Data Centers and Cloud**: Processing and storage of the vast amounts of data generated by city systems.

4. **AI Systems**: Predictive algorithms for traffic and public safety.

5. **Governance Platforms**: Dashboards for city administrators to monitor and manage city services.

netskope

2024 © Netskope Confidential. All rights reserved.

User Behaviour & Risk Tracking

Automatically isolate, monitor, and reduce access for risky users

Shadow IT Discovery with Context

Eg: Himanshu exported 6 sensitive files from Sharepoint and uploaded them to his personal GDrive

Netskope POPs in

Delhi
Chennai
Mumbai

All our own hardware/compute.
No on-prem appliance footprint.

VPN Consolidation

Close off inbound attack surface required for VPNs and apps

Ecosystem Integration

Integrate with existing investments to reduce operational overhead

ARCTIC WOLF · Microsoft · aws · Jira · vmware · Azure Active Directory

Advanced Threat Protection

CASB

Cloud Firewall

SWG & Cloud Proxy

Zero Trust Network Access

DLP

Security for every user, device, and location
All cloud delivered & managed via a single UI

Why Netskope for your business?

Industry leading threat protection

Cloud Threat Feeds
IPS
Sandboxing
Machine Learning
Phishing Prevention
IOC/Intel Sharing

Comprehensive DLP and CASB

Covering:
Managed users, BYOD & 3rd parties, and data stored at rest

Across all of:
Web, SaaS, IaaS, Email, Private Apps , & Endpoint

Leader

in the 2024 Gartner Magic Quadrant for SSE

Clientless security for 3rd parties and BYOD

90%

Average reduction in users connecting to risky apps with User Coaching enabled

IP Address Preservation

Ability to preserve egress IP for IP whitelisting, conditional access, and MFA rules

Native browser isolation

Owned & Operated by Netskope (not OEM'ed)

IaaS & SaaS Posture Management

Continuously scan IaaS and SaaS tenancies to ensure compliance with security best practice and standards like ISO 27001, PCI-DSS, etc.

Q&A

gurinder@netskope.com

2024 © Netskope Confidential. All rights reserved.