Christopher Reed

Director, EUC Global Technical Strategist

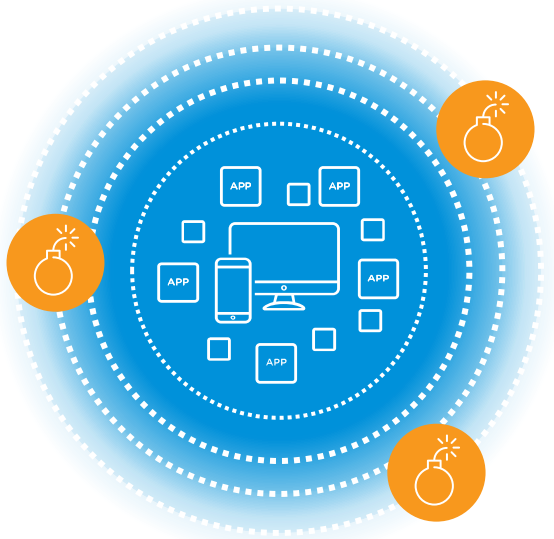
When Computing leaves the building.

How do we adapt when MOST of our employees are now FORCED to work from home?

CURRENT WORKSTYLES

THE NEW NORM Who Knows????

Congratulations !! Every network is your network.



The world has changed, and the **perimeter has collapsed**.

Majority of the workforce will likely **work from home forever**

Security breaches have significantly increased.

What is Zero Trust?

"Assumes the network is hostile and that an enterprise-owned network infrastructure is no different"

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft.pdf

NIST (National Institute for Standards and Technology)

The History of Zero Trust

In 2019
15-year Anniversary

2003/2004	..	2009	..	2014	..	2017	2018	2019

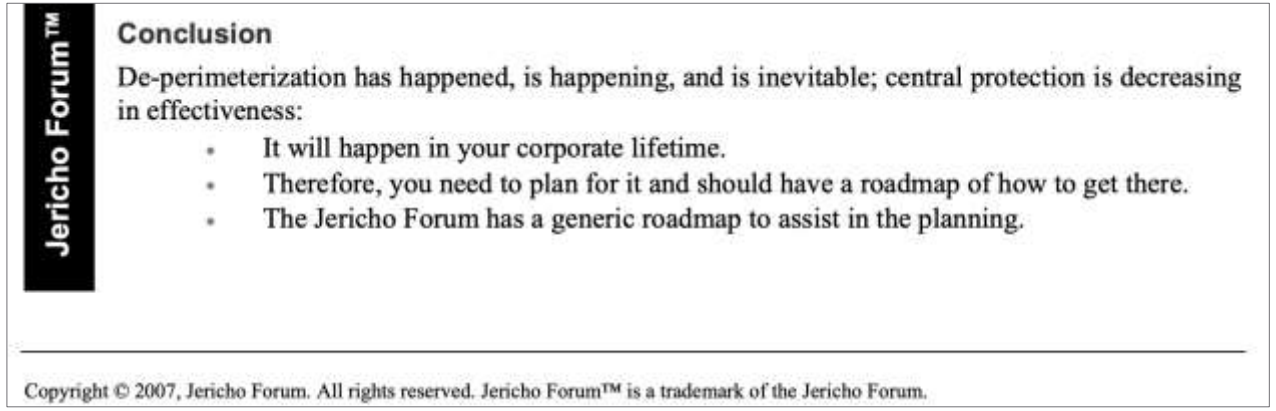
Jericho Forum - ”Outside is the new inside”

Forrester - Zero Trust Research by Jon Kindervag

The Forrester Wave™: Zero Trust eXtended (ZTX)

Google’s BeyondCorp

Gartner’s 2017 CARTA framework



Jericho Forum™

Conclusion

De-perimeterization has happened, is happening, and is inevitable; central protection is decreasing in effectiveness:

- It will happen in your corporate lifetime.
- Therefore, you need to plan for it and should have a roadmap of how to get there.
- The Jericho Forum has a generic roadmap to assist in the planning.

BeyondCorp

BeyondCorp is an implementation, by Google, of zero-trust computer security concepts creating a zero trust network. It was created in 2009 in response to an APT attack. An open source implementation inspired by Google's research paper on an access proxy is known as "transcend". Wikipedia

vmware

De-perimeterization / Zero Trust / BeyondCorp / NIST 800-207

18-year Anniversary

2003/2004	..	2009	2014	2017	2018	2019	2020	2021

Jericho Forum –"Outside is the new inside"

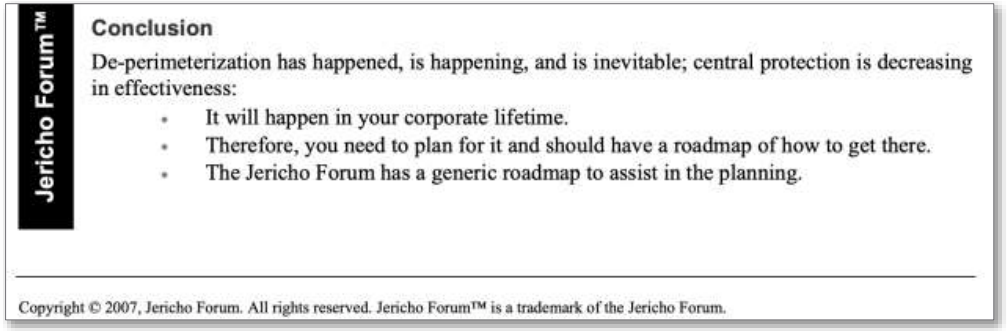
Forrester - Zero Trust Research

The Forrester Wave™: Zero Trust eXtended (ZTX)

Google's BeyondCorp

Gartner's 2017 CARTA framework

NIST 800-207
Zero Trust Architecture



Jericho Forum™

Conclusion

De-perimeterization has happened, is happening, and is inevitable; central protection is decreasing in effectiveness:

- It will happen in your corporate lifetime.
- Therefore, you need to plan for it and should have a roadmap of how to get there.
- The Jericho Forum has a generic roadmap to assist in the planning.

Executive Order 14028, "Improving the Nation's Cybersecurity",

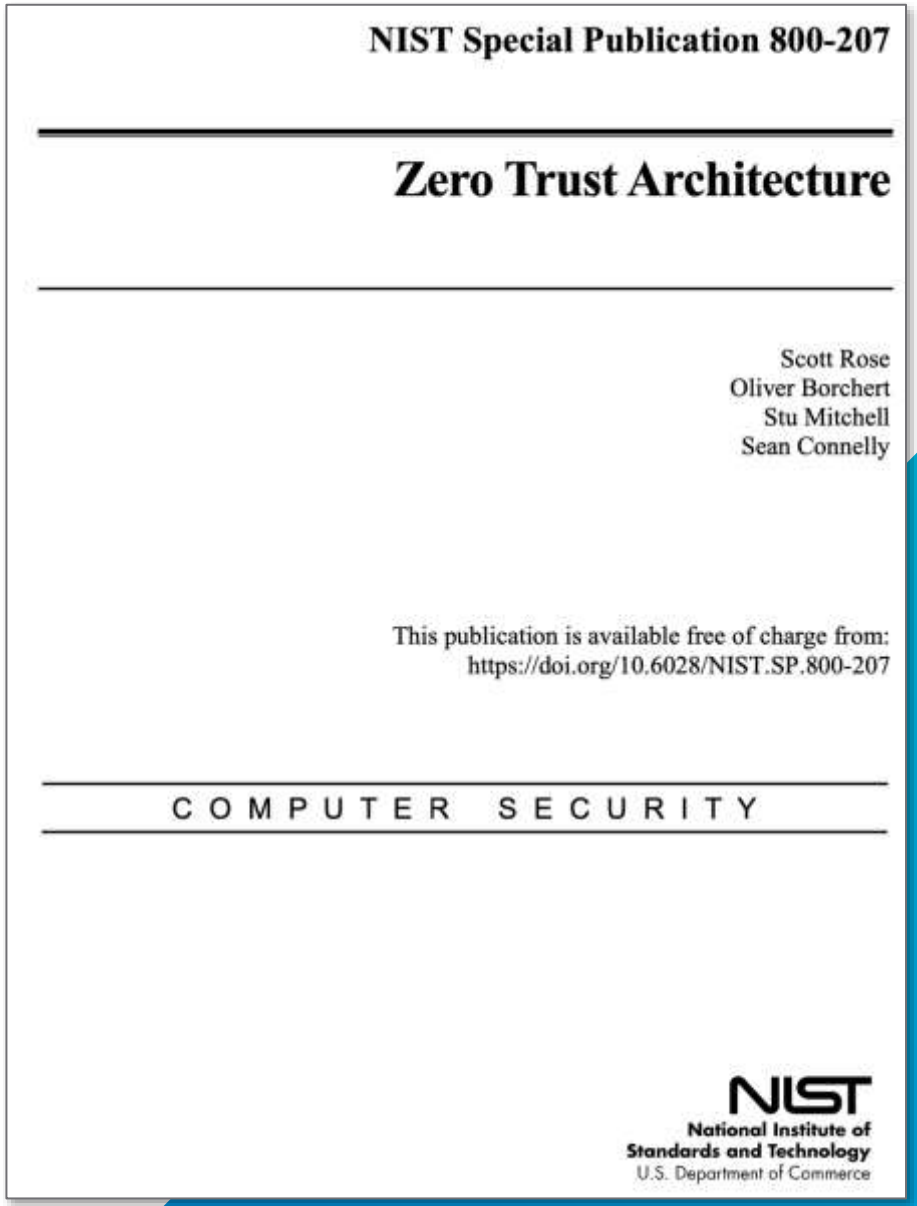
CISA Zero Trust Security Model https://www.cisa.gov/publication/zero-trust-maturity-model

DOD Zero Trust RA
https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

NIST 800-207 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

NIST

NIST.SP.800-207


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

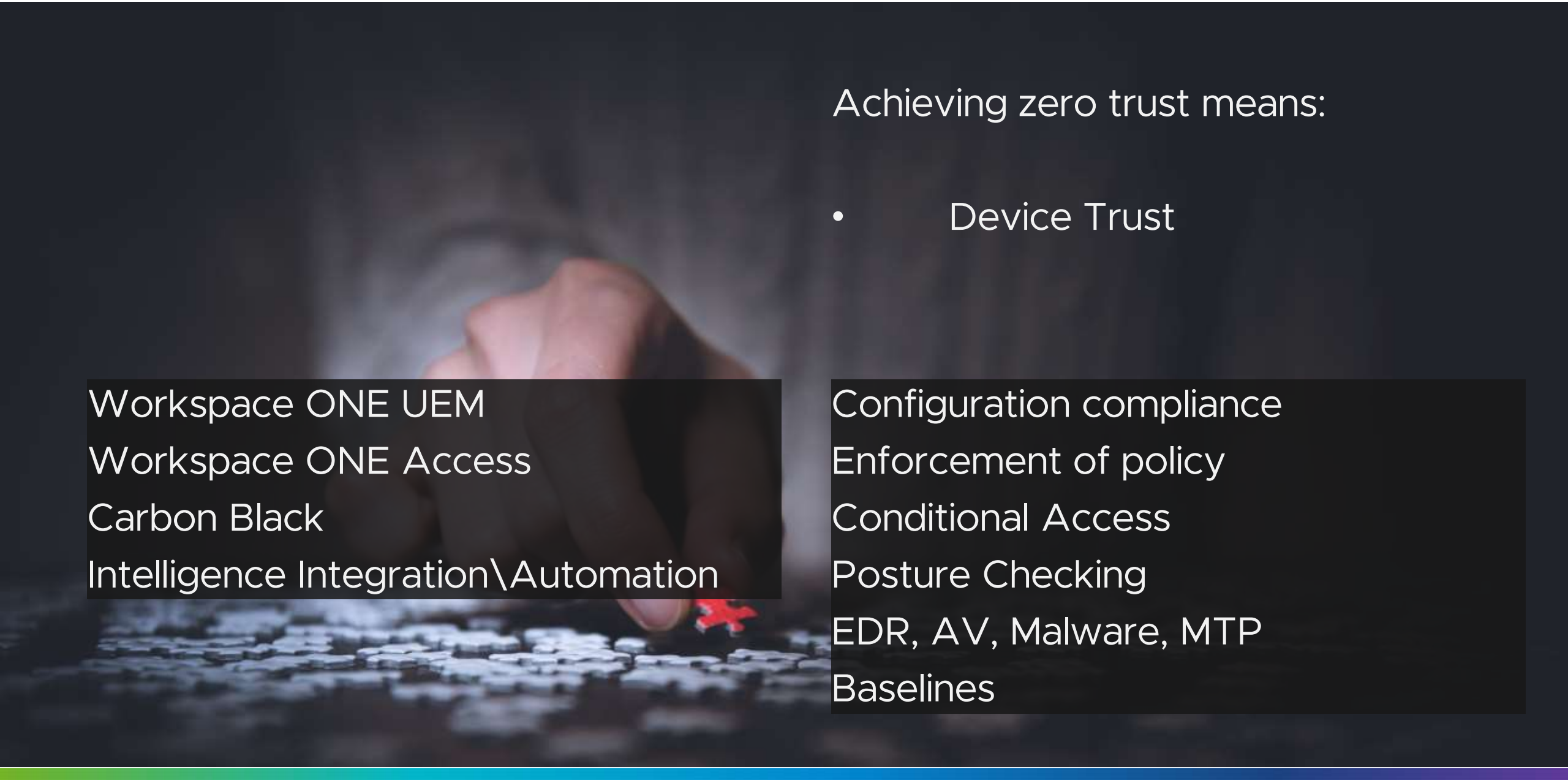
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Zero Trust Strategy

Achieving zero trust means:

- Device Trust
- Network Trust
- Application\Workload Trust
- User\Identity Trust
- Data Trust

Zero Trust Strategy



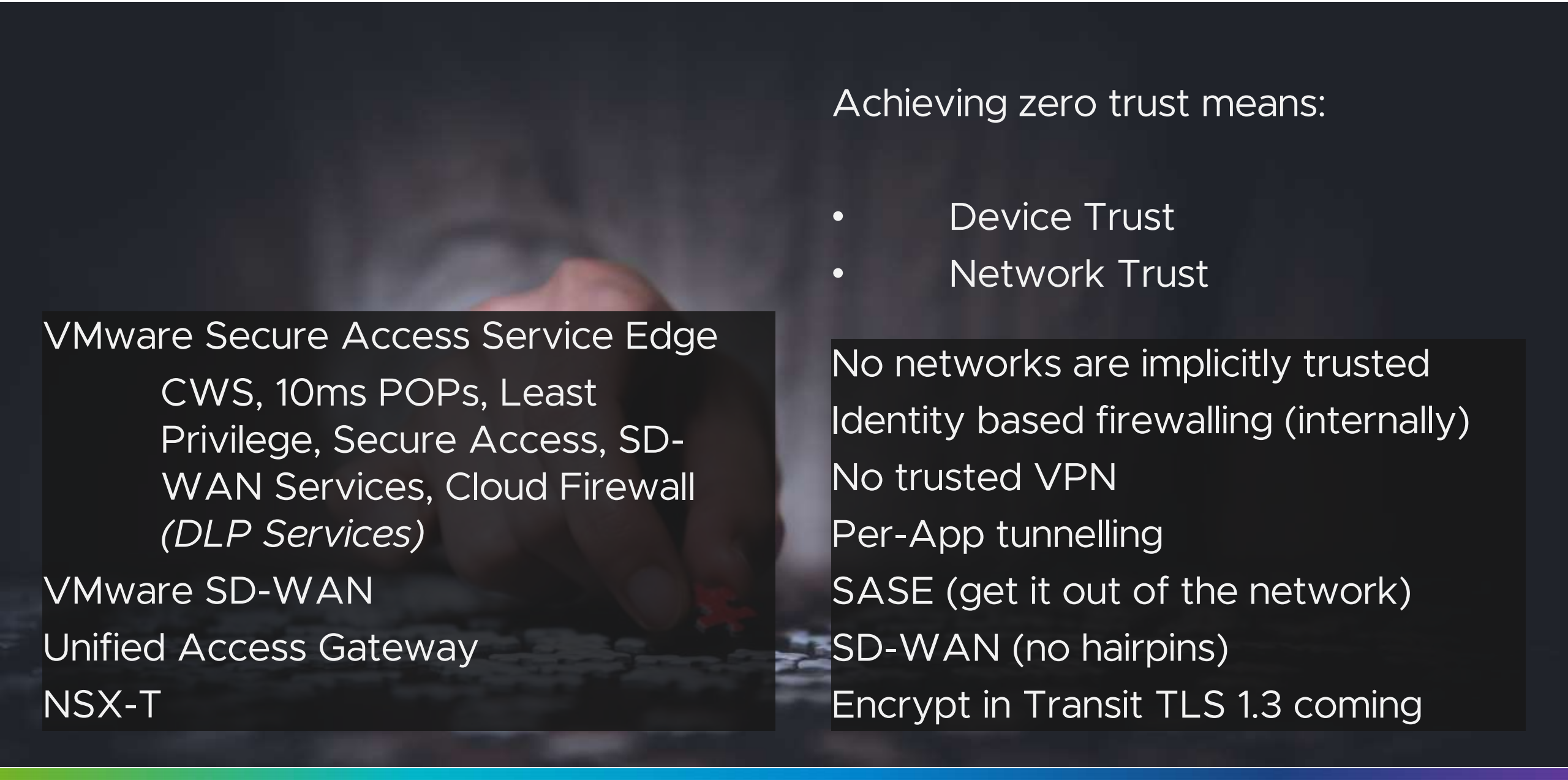
Achieving zero trust means:

- Device Trust

Workspace ONE UEM
Workspace ONE Access
Carbon Black
Intelligence Integration\Automation

Configuration compliance
Enforcement of policy
Conditional Access
Posture Checking
EDR, AV, Malware, MTP
Baselines

Zero Trust Strategy



VMware Secure Access Service Edge

CWS, 10ms POPs, Least Privilege, Secure Access, SD-WAN Services, Cloud Firewall *(DLP Services)*

VMware SD-WAN

Unified Access Gateway

NSX-T

Achieving zero trust means:

- Device Trust
- Network Trust

No networks are implicitly trusted

Identity based firewalling (internally)

No trusted VPN

Per-App tunnelling

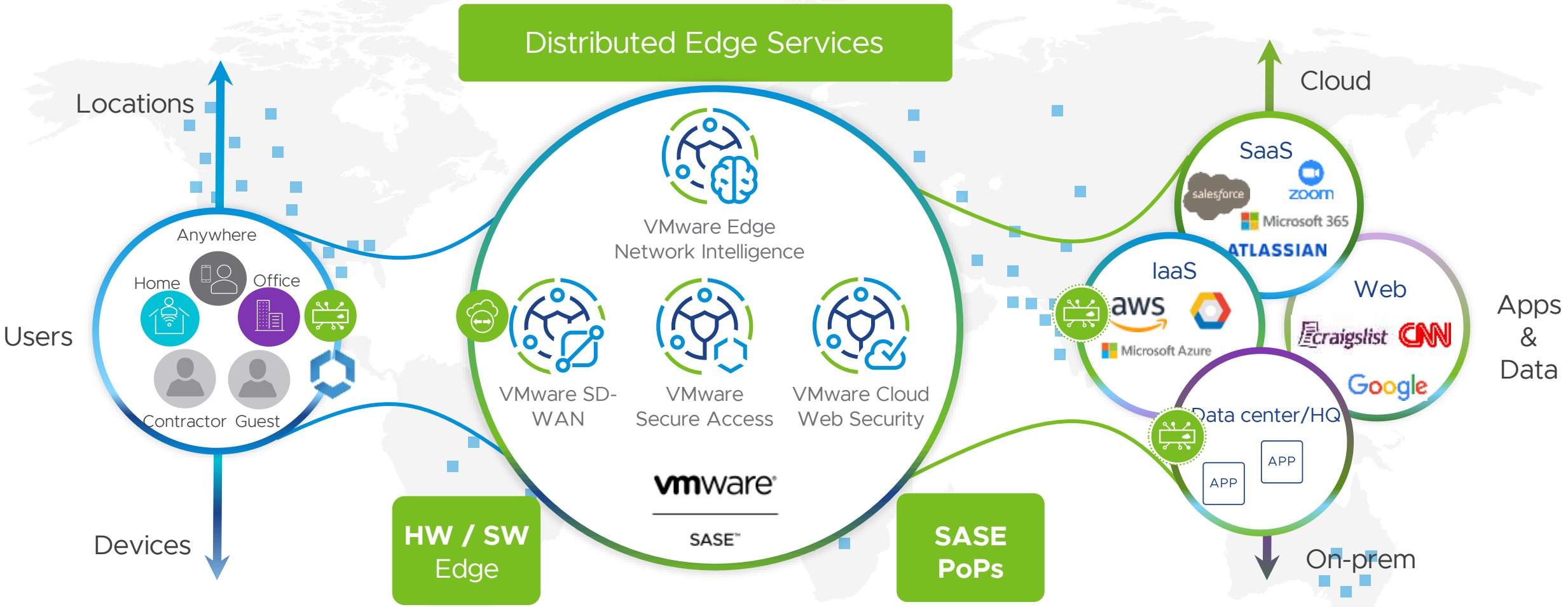
SASE (get it out of the network)

SD-WAN (no hairpins)

Encrypt in Transit TLS 1.3 coming

VMware SASE Delivers Edge Services with an Extensible Platform

Networking, Security, AND Compute



Zero Trust Strategy

Achieving zero trust means:

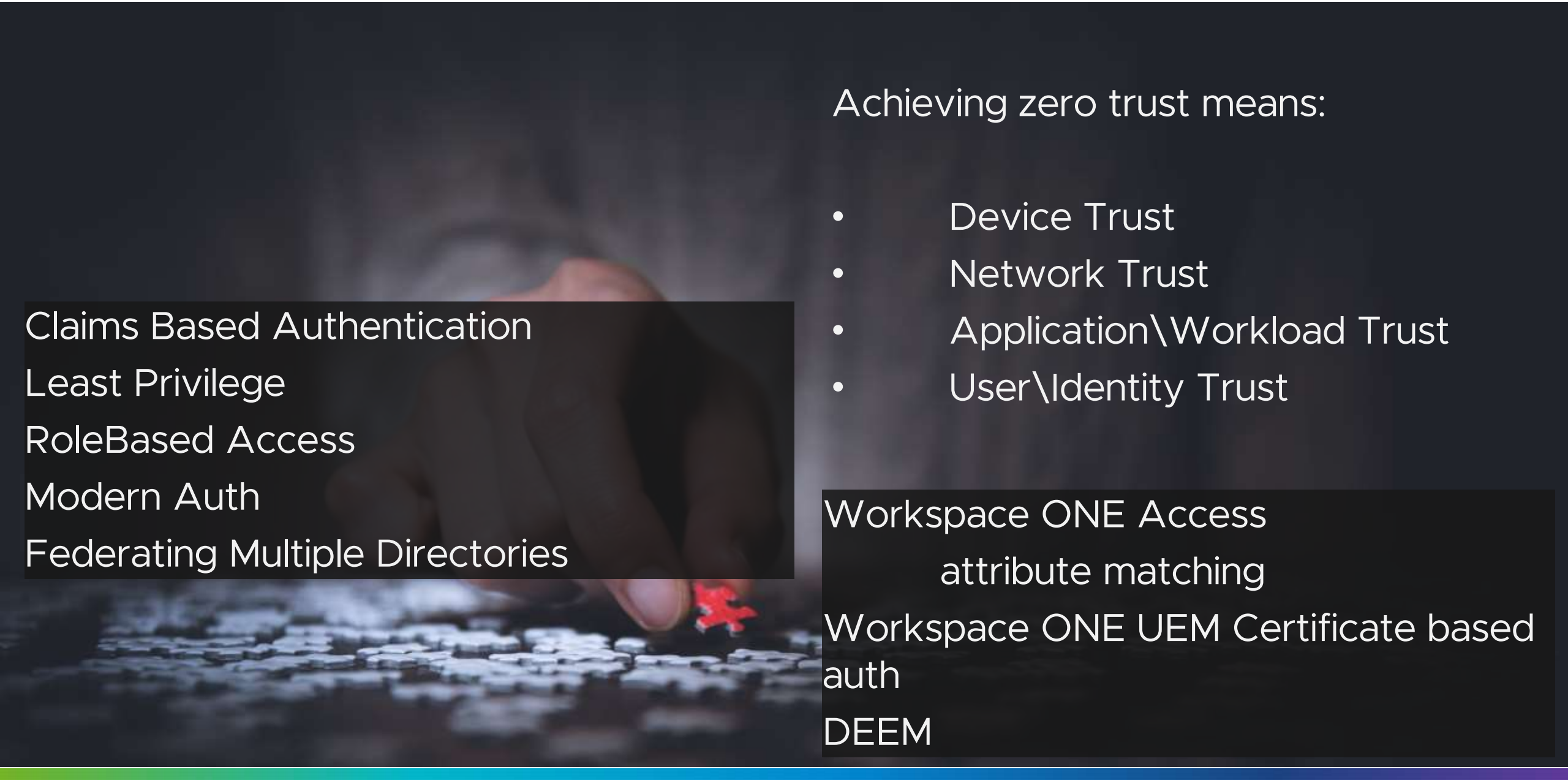
- Device Trust
- Network Trust
- Application\Workload Trust

SAAS, Mainframe, Client-Server, Mobile

PIN-Testing, UID/PWD/Role Management
Application Vulnerability reports – CISA
Isolation

VMware SaaS App Management
NSX-T

Zero Trust Strategy



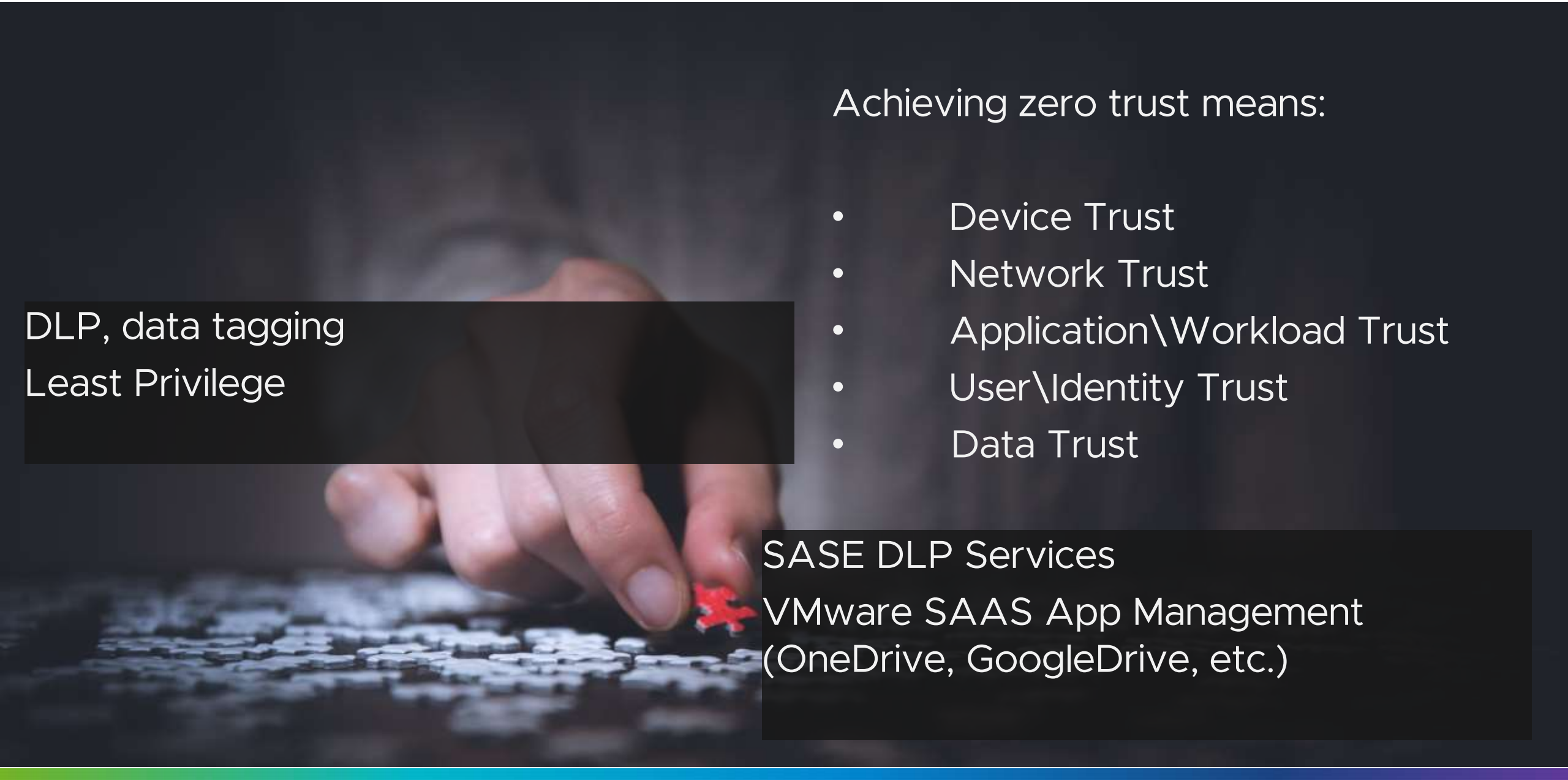
Achieving zero trust means:

- Device Trust
- Network Trust
- Application\Workload Trust
- User\Identity Trust

Claims Based Authentication
Least Privilege
RoleBased Access
Modern Auth
Federating Multiple Directories

Workspace ONE Access
attribute matching
Workspace ONE UEM Certificate based auth
DEEM

Zero Trust Strategy



DLP, data tagging

Least Privilege

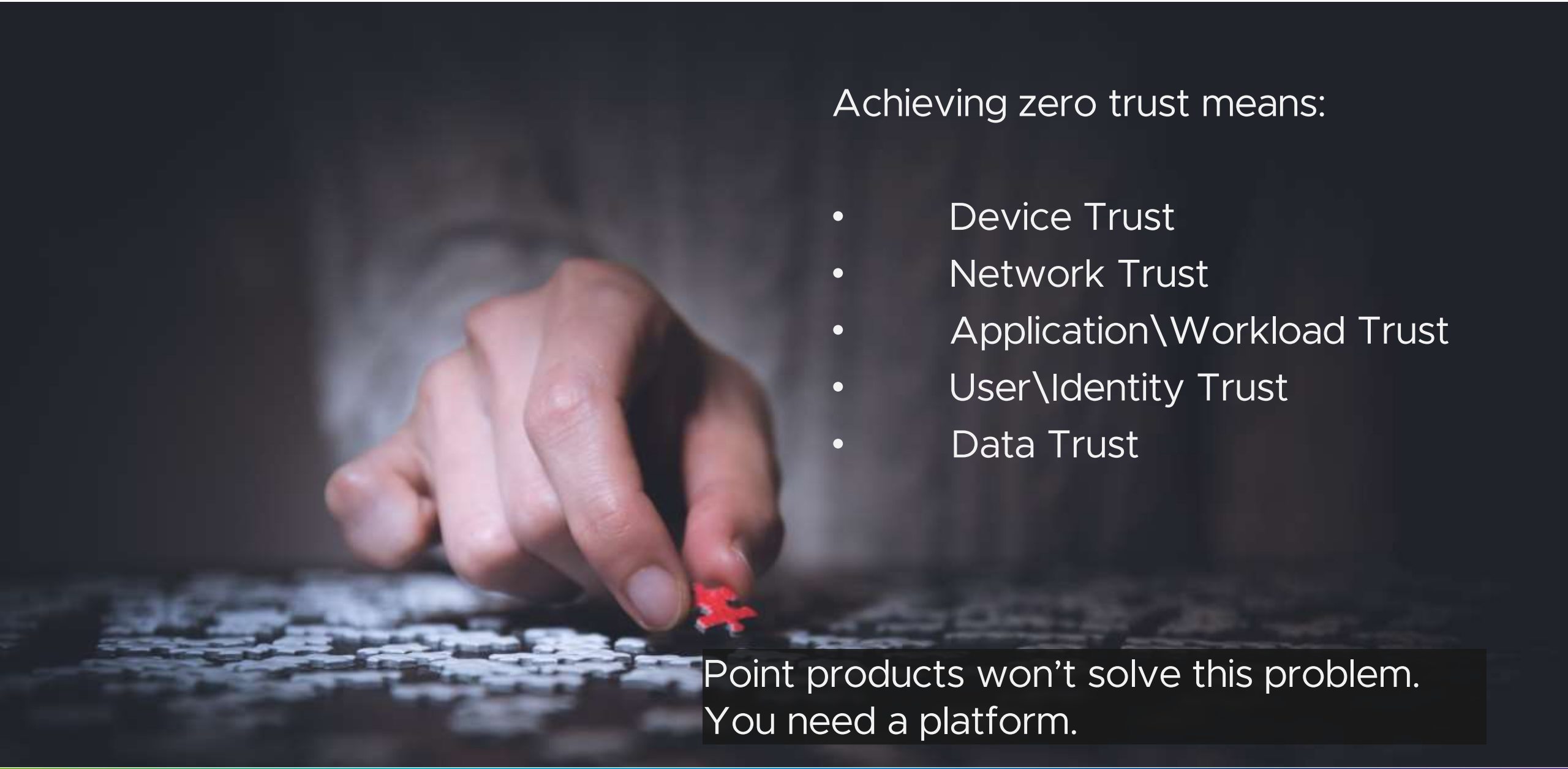
Achieving zero trust means:

- Device Trust
- Network Trust
- Application\Workload Trust
- User\Identity Trust
- Data Trust

SASE DLP Services

VMware SAAS App Management (OneDrive, GoogleDrive, etc.)

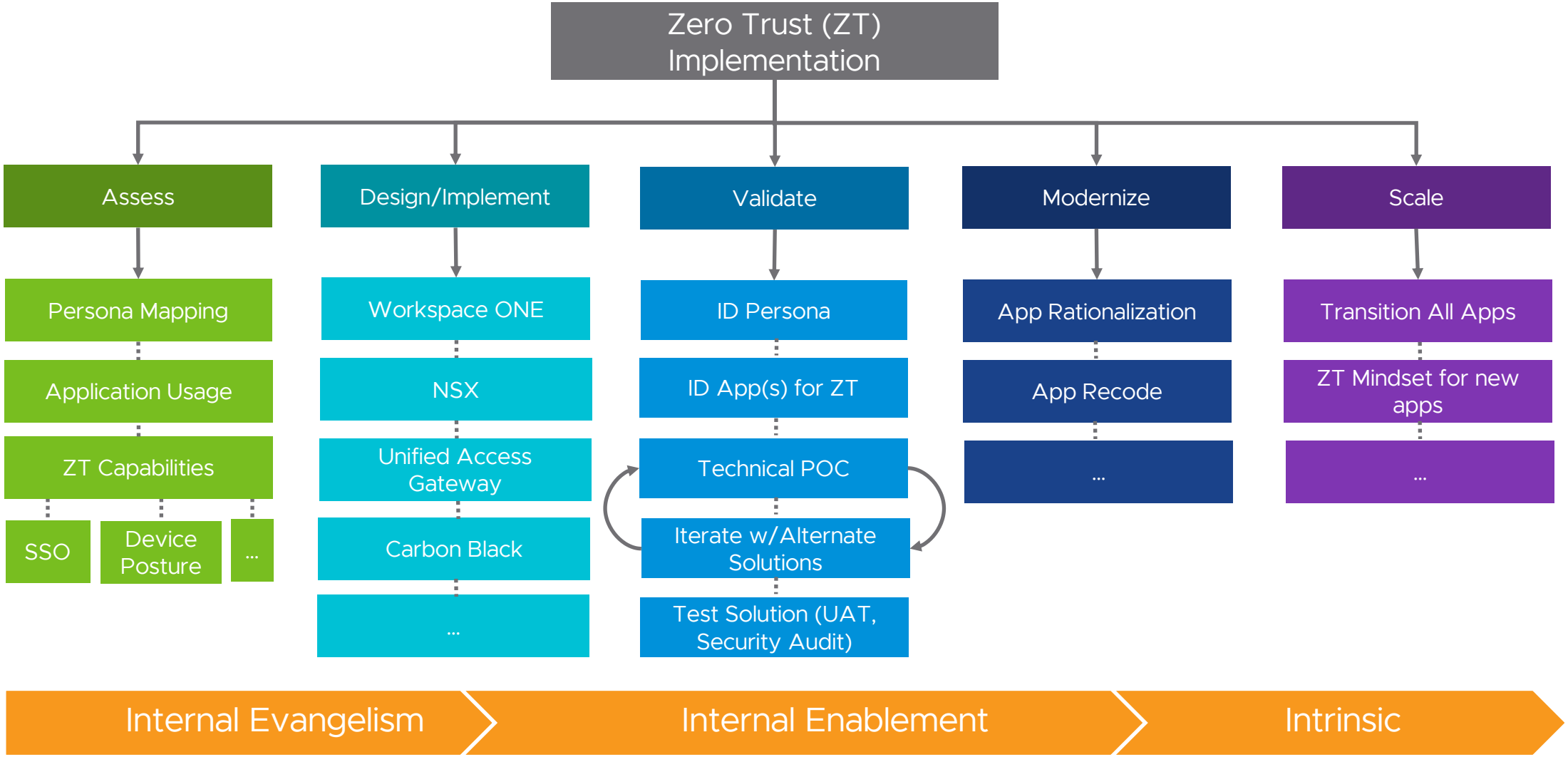
Zero Trust Strategy



Achieving zero trust means:

- Device Trust
- Network Trust
- Application\Workload Trust
- User\Identity Trust
- Data Trust

Point products won't solve this problem.
You need a platform.


Zero Trust (ZT) Implementation
Assess
Design/Implement
Validate
Modernize
Scale
Persona Mapping
Application Usage
ZT Capabilities
SSO
Device Posture
...
Workspace ONE
NSX
Unified Access Gateway
Carbon Black
...
ID Persona
ID App(s) for ZT
Technical POC
Iterate w/Alternate Solutions
Test Solution (UAT, Security Audit)
App Rationalization
App Recode
...
Transition All Apps
ZT Mindset for new apps
...
Internal Evangelism
Internal Enablement
Intrinsic

- **It's a journey**
  - Will take many years
- **All applications not suitable**
  - You will have a hybrid environment
- **You already own much of the technology needed**
  - Focus on people, processes and policies
- **Start with low hanging fruit**
  - Identify Applications with the biggest impact for most of your users
  - Allows for you and your organization to learn

Path to Zero Trust in the Digital Workspace

Not necessarily a linear journey

Device Mgmt & Compliance

- Manage device, set policy configuration
- Cloud-based compliance
- Deploy certificates for Tunnel, UAG and other services
- App mgmt. and DLP
- Attestation for unmanaged devices

Conditional Access

- Enforce conditional access policies
- Multi-factor authentication
- Broker between identity stores and providers

App Tunnel and Proxy

- Protect data center application servers
- Least privilege access to applications under defined conditions

NGAV, EDR & Risk Analytics

- Broaden view of compliance across digital workspace
- User and device risk scores
- User behavior anomaly detection

Automated Threat Remediation & Orchestration

- Remediate out of compliance conditions
- Orchestrate workflows across existing ITSM investments

vmware

Demo

vmware

Thank You