Zero Trust & RBAC Trends & Vendors

Jelene Crehan
Director of Infrastructure,
University of Illinois Chicago
She/Her

Jon Young
VP, Chief Troublemaker
Vantage Technology
Consulting Group
He/His

Jacqueline Pitter
Sr Strategic Consultant
Vantage Technology
Consulting Group
She/Her

VANTAGE

Technology Consulting Group

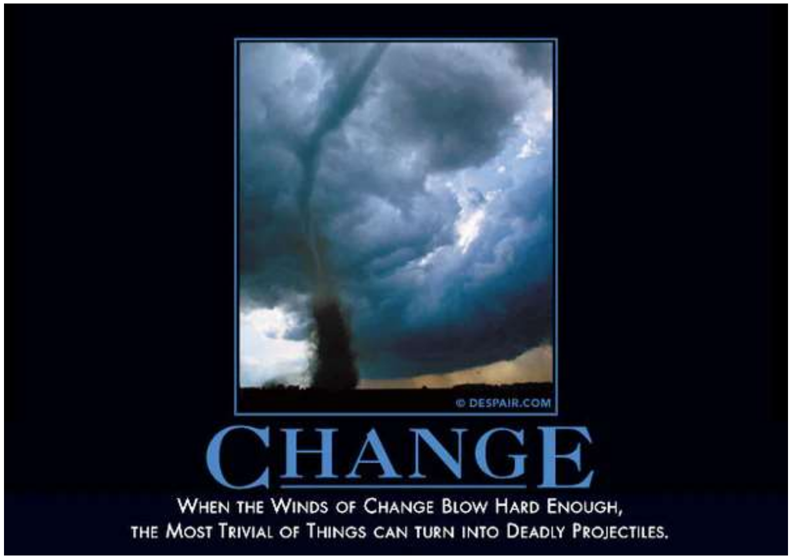
Ethereal • Boston • Los Angeles

VANTAGE
Technology Consulting Group

Download the slides:

VANTAGE
Technology Consulting Group

Y


© DESPAIR.COM
CHANGE
When the Winds of Change Blow Hard Enough,
the Most Trivial of Things can turn into Deadly Projectiles.

© DESPAIR.COM
CONSULTING
If You're Not a Part of the Solution,
There's Good Money to be Made in Prolonging the Problem.

Y

University of Illinois Chicago

Public, Research I Institution, $460M

34,000 Students, 16 Colleges, Hospital

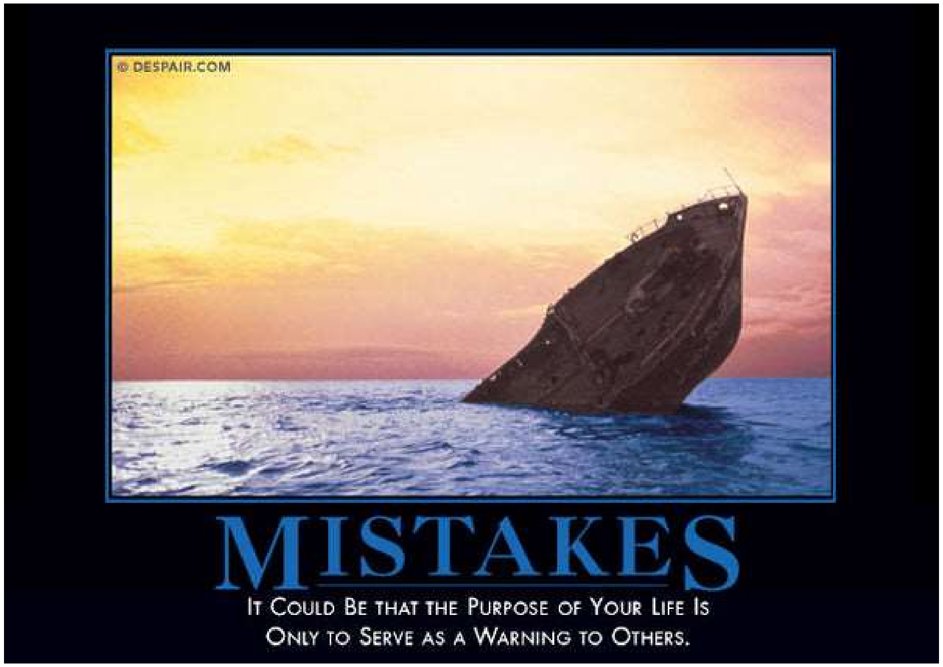
Among most culturally & ethnically diverse

Downtown Chicago, 1 mile from Willis Tower

UIC TECHNOLOGY SOLUTIONS

Today’s conversation

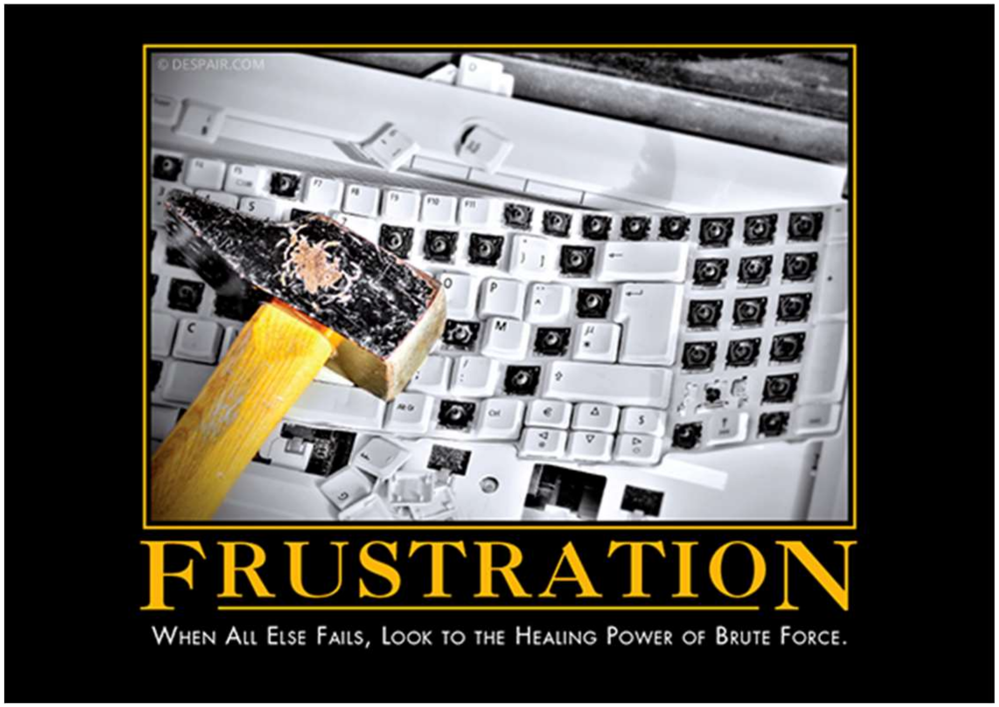
- What is ZT, RBAC, ABAC?
- Why should I care?
- NIST 800-207
- Overview of the various vendor approaches
- Next-gen ideas
- What UIC chose and why


© DESPAIR.COM
MISTAKES
It Could Be that the Purpose of Your Life Is Only to Serve as a Warning to Others.

Y

Born out of frustration and filled with unicorn farts

© DESPAIR.COM
EXPERTS
We've got a Talent for Explaining Tomorrow
Why the Predictions We Made Yesterday Didn't Come True Today.


© DESPAIR.COM
FRUSTRATION
When All Else Fails, Look to the Healing Power of Brute Force.

VANTAGE
Technology Consulting Group

Y

Overall Network Statistics

322 Elevator Call Buttons

2,000+ Network Switches

3 Data Centers

220 Silent Startel Buttons

7,700 VoIP phones

700 Remaining Centrex Lines to convert to VoIP

18,500 sq. ft. Data Center Space

~6,000 Access Points

110+ Buildings

108 Routers

~41,000 VPN Authentication in 1 year

800+ Network closets

~32,000 peak concurrent wireless devices

1,100 Telephone repairs/adds/moves/ changes this year

1900 Daily VPN Users

1700+ Emergency Startel circuits

700 Softphone Clients

2300 Active Centrex Remaining

~64,000 Network Ports

WW

What led UIC to modernize their network?

- Technical debt
- Deferred maintenance
- Leadership concerns about technology choices
- Historical outages
- Stuck in firefighting mode and challenged to step back and think strategically
- Institutional change with new goals that everyone was concerned might not be met by the existing approach

© DESPAIR.COM
INNOVATION
We Regret to Inform You that the Flying Cars We Promised Aren't Feasible, But We Do Hope You'll Enjoy the Spying Vacuums.

VANTAGE
Technology Consulting Group

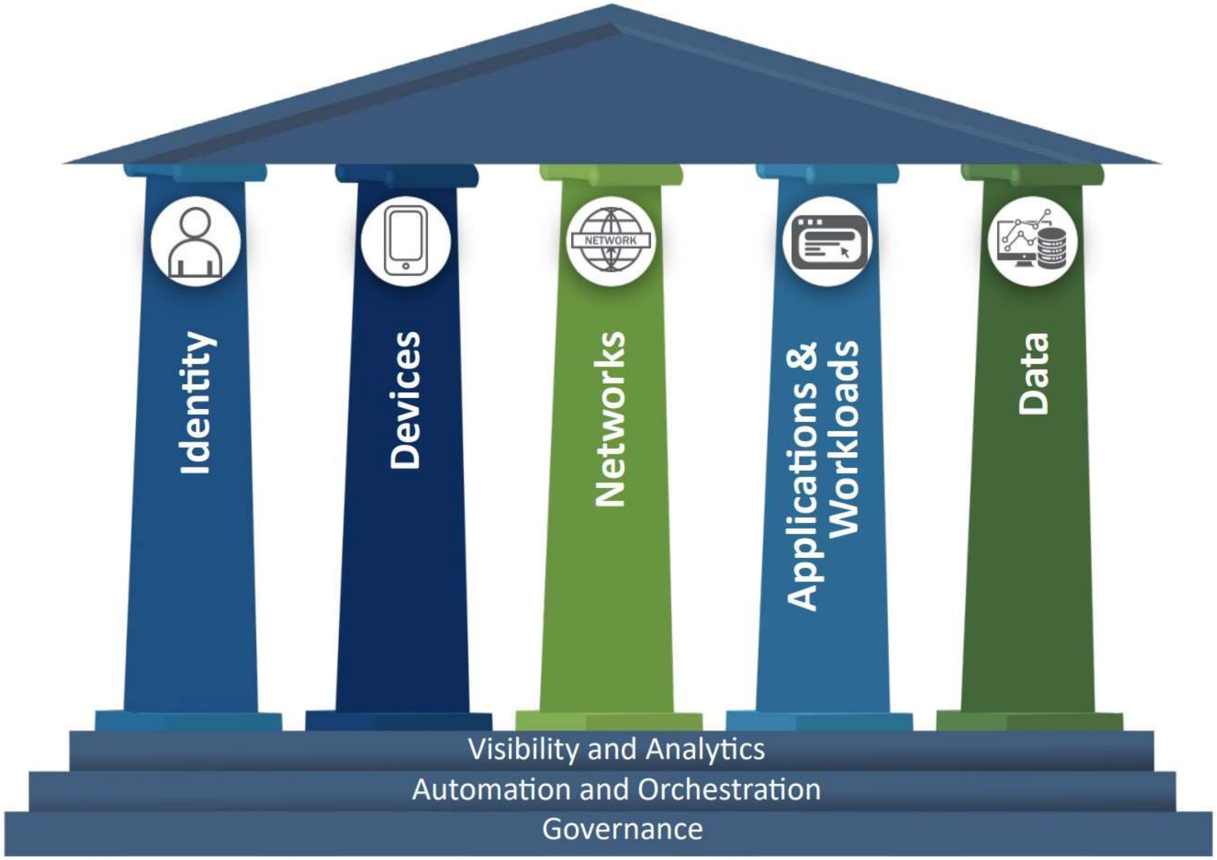
WW

ZT vs ZTA vs ZTNA

Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.

- NIST SP 800-207

CISA's ZTMM is one of the many paths to support the transition to zero trust



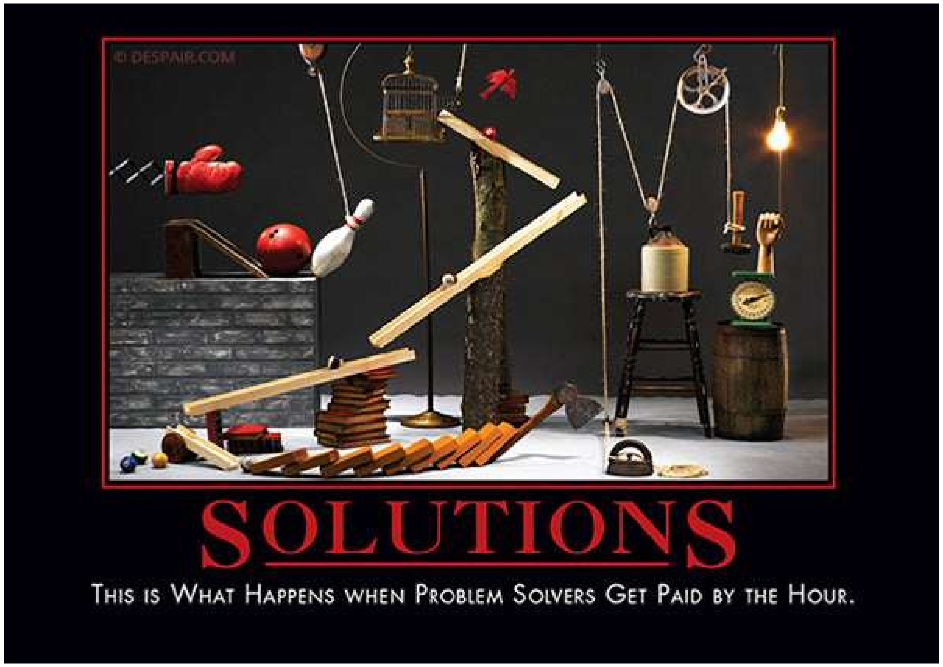
CISA Zero Trist Maturity Model v2 Figure 1: ZTMM Pillars

Y

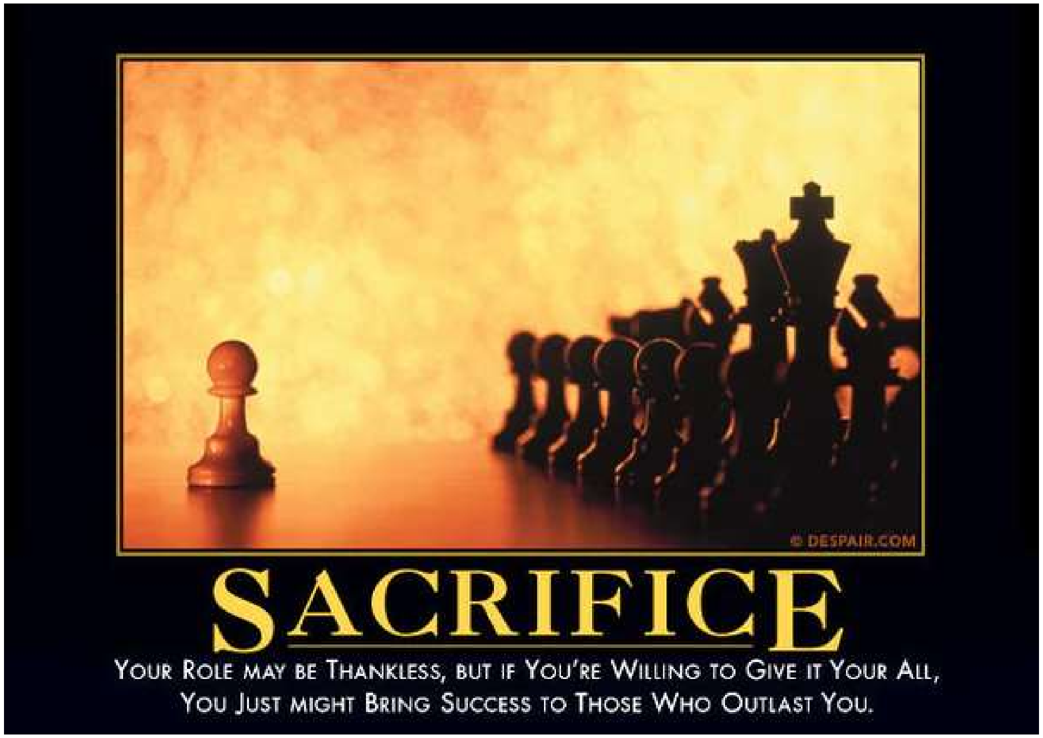
Focus on the network

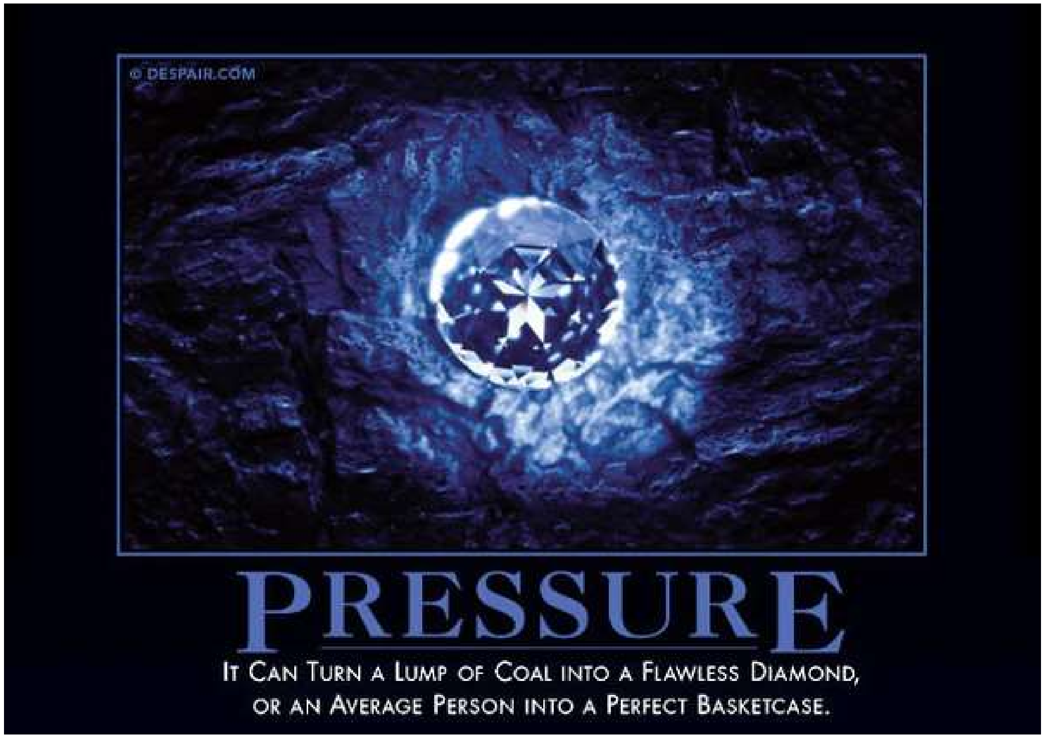
Other mechanisms to consider

- WebAuthn
- XDR
- HTTPS
- So many others


© DESPAIR.COM
SOLUTIONS
This is What Happens when Problem Solvers Get Paid by the Hour.

Why Should I Care?


© DESPAIR.COM
SACRIFICE
YOUR ROLE MAY BE THANKLESS, BUT IF YOU'RE WILLING TO GIVE IT YOUR ALL, YOU JUST MIGHT BRING SUCCESS TO THOSE WHO OUTLAST YOU.


© DESPAIR.COM
PRESSURE
IT CAN TURN A LUMP OF COAL INTO A FLAWLESS DIAMOND, OR AN AVERAGE PERSON INTO A PERFECT BASKETCASE.

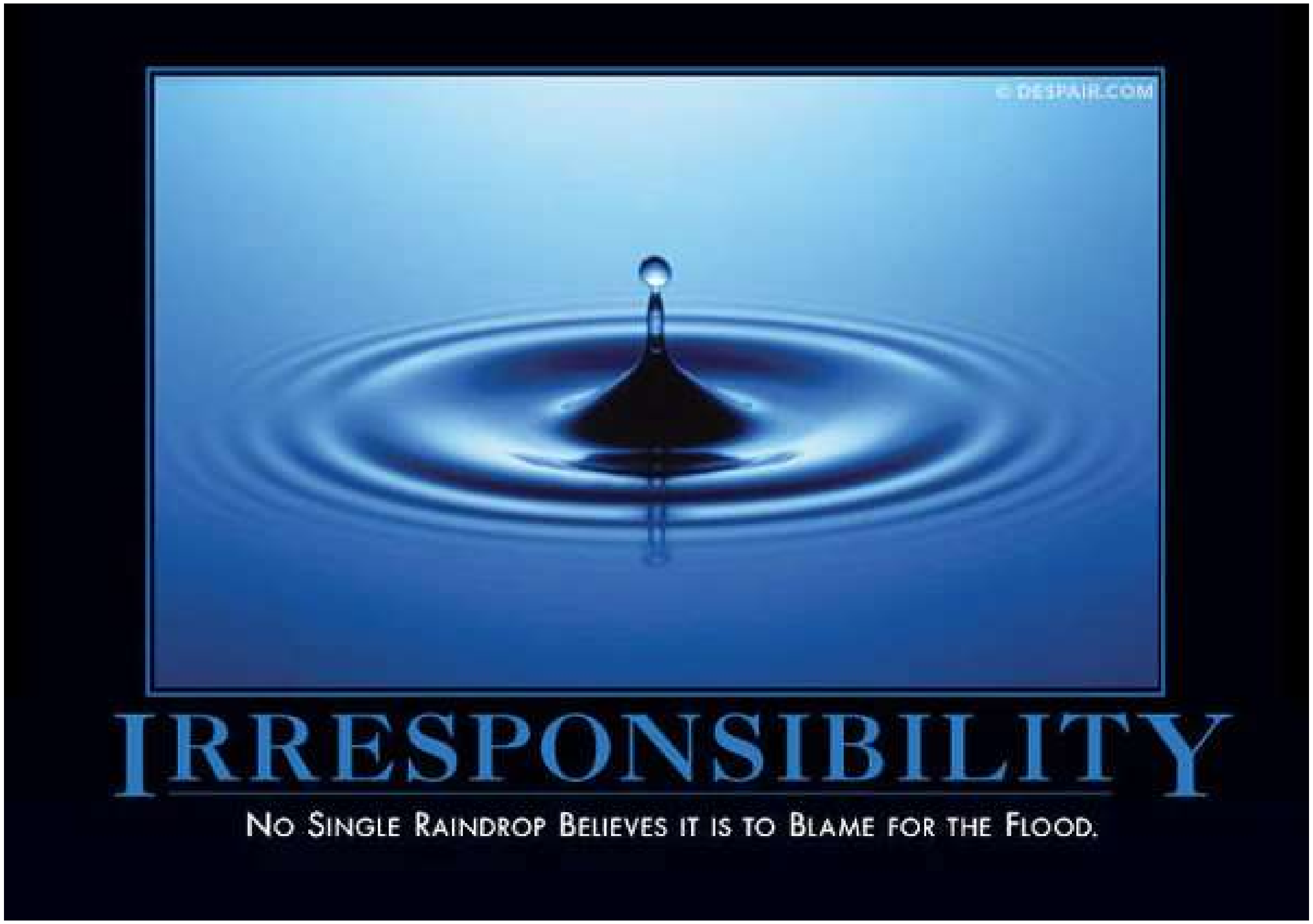
Y

VANTAGE
Technology Consulting Group

Major Element Design Goals

When You Wish Upon a Falling Star, Your Dreams Can Come True. Unless it's Really a Meteor Hurtling to the Earth Which Will Destroy All Life. Then You're Pretty Much Hosed No Matter What You Wish For. Unless it's Death By Meteorite.

- Automation & Orchestration
- Analytics (not just metrics)
- Identity-aware, dynamic segmentation (RBAC/ZT)
- Policy decision and enforcement points + device profiling
- Security fully integrated and meets compliance needs
- Easy to add performance
- Everything everywhere, all at once!
  - Wi-Fi and wired (and remote??) are a seamless experience
  - Cloud extensible

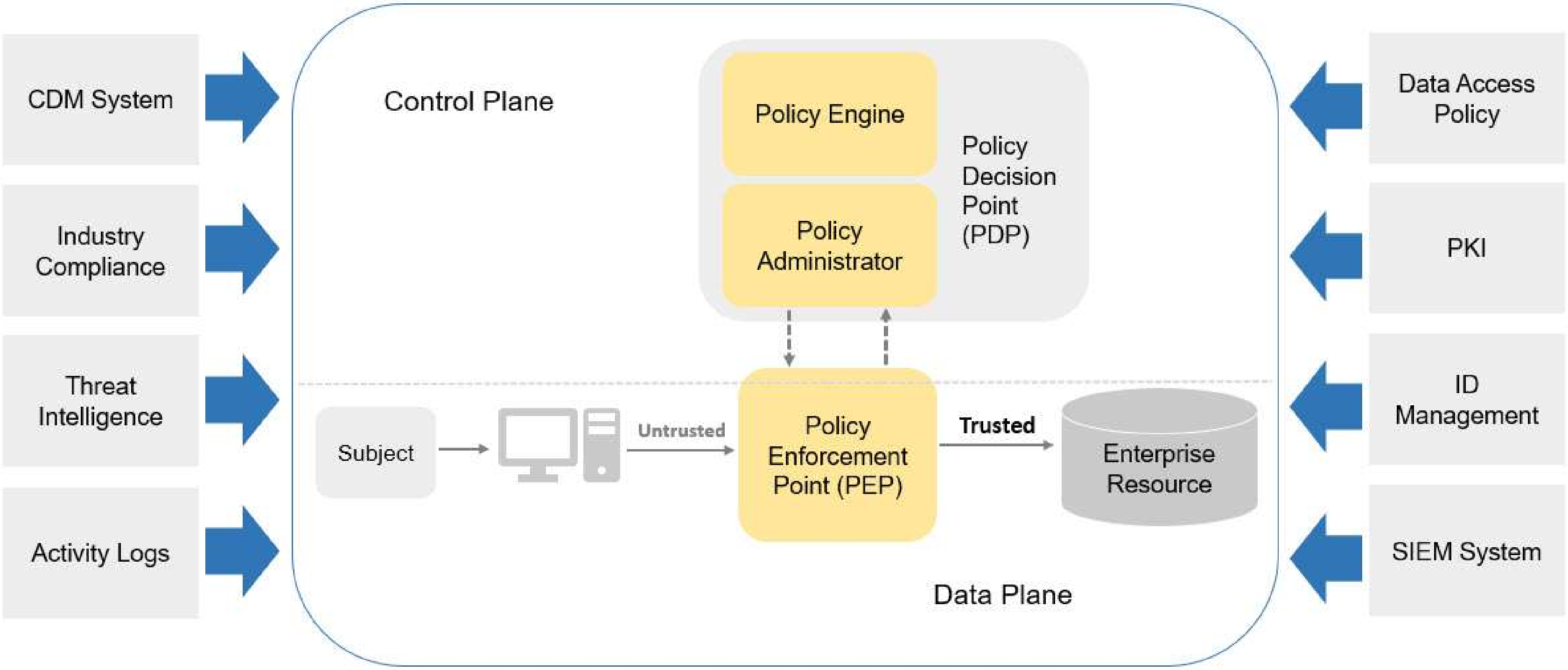


What is Zero Trust? 800-207 elements

- Authentication
- Authorization
- Shrinking implicit trust zones
- Maintaining service availability
- Minimizing temporal delays in authentication mechanisms
- Access rules are made as granular as possible to enforce least privileges required

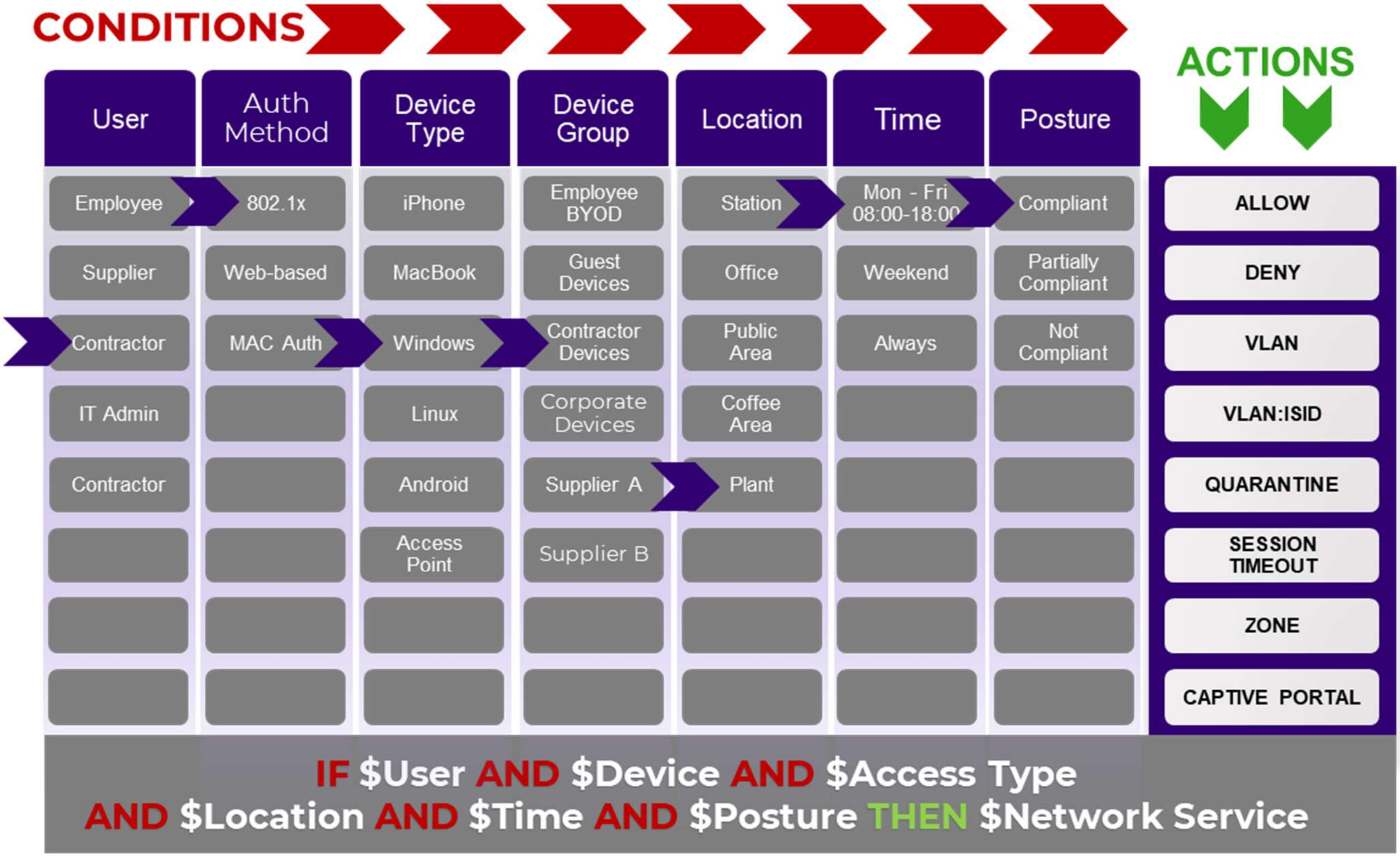
NIST SP 800-207: Zero Trust Architecture, page 4

VANTAGE
Technology Consulting Group



Core Zero Trust logical components; Source: NIST SP 800-207, Zero Trust Architecture, Figure 2.

P



CONDITIONS

User	Auth Method	Device Type	Device Group	Location	Time	Posture
Employee	802.1x	iPhone	Employee BYOD	Station	Mon - Fri 08:00-18:00	Compliant
Supplier	Web-based	MacBook	Guest Devices	Office	Weekend	Partially Compliant
Contractor	MAC Auth	Windows	Contractor Devices	Public Area	Always	Not Compliant
IT Admin		Linux	Corporate Devices	Coffee Area		
Contractor		Android	Supplier A	Plant		
		Access Point	Supplier B			

ACTIONS

- ALLOW
- DENY
- VLAN
- VLAN:ISID
- QUARANTINE
- SESSION TIMEOUT
- ZONE
- CAPTIVE PORTAL

IF $User AND $Device AND $Access Type AND $Location AND $Time AND $Posture THEN $Network Service

P

Graphics credit: Extreme Networks

Options we’ll discuss

Solution Type	Vendor Exemplars of Type
Standards-based	• Any. This is traditional RBAC
Sophisticated DACL	• Cisco (Trustsec) • Alcatel-Lucent • Extreme
Hairpins	• Aruba • Firewall vendors
Proxy	• Saife Continuum • Zscaler • Firewall vendors acting as VPN concentrators
Next-gen ideas **(shadow/overlay networks)**	• Tailscale • OpenZiti • Zero Tier

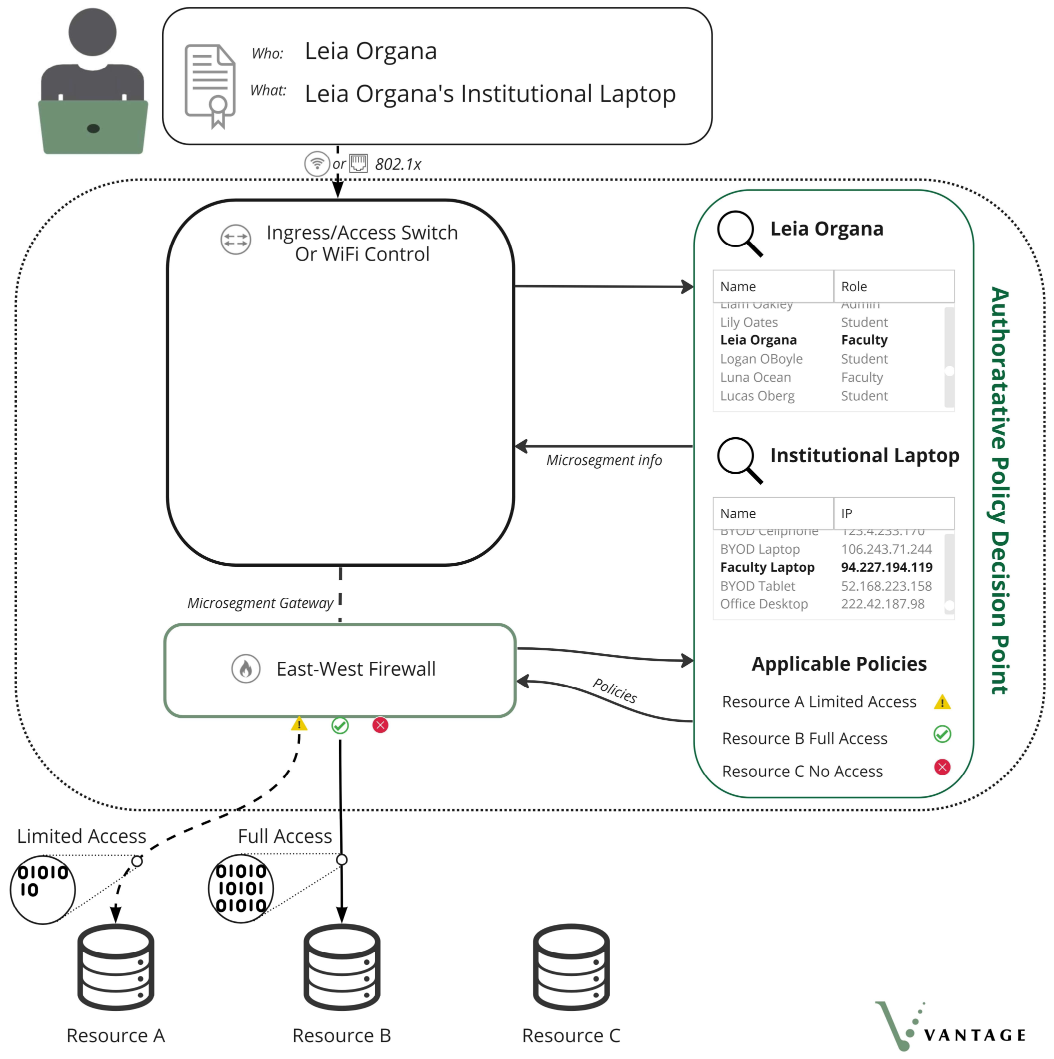
* We are over-simplifying this heavily.

Y

PRO	CON
• Provides comfort to people with a more conventional mindset. • In most topologies, can function with distributed depts on campus • Vendor agnostic • Doesn’t usually require a forklift	• May not be able to achieve true micro-segmentation. • E-W Firewall is doing a lot of work. • Difficult to fit well with geographically distributed roles.

Y

Standard East-West Firewall RBAC



Leia Organa

Name	Role
Liam Oakley	Admin
Lily Oates	Student
Leia Organa	**Faculty**
Logan OBoyle	Student
Luna Ocean	Faculty
Lucas Oberg	Student

Institutional Laptop

Name	IP
BYOD Cellphone	123.4.233.170
BYOD Laptop	106.243.71.244
Faculty Laptop	**94.227.194.119**
BYOD Tablet	52.168.223.158
Office Desktop	222.42.187.98

Applicable Policies

Resource A Limited Access ⚠

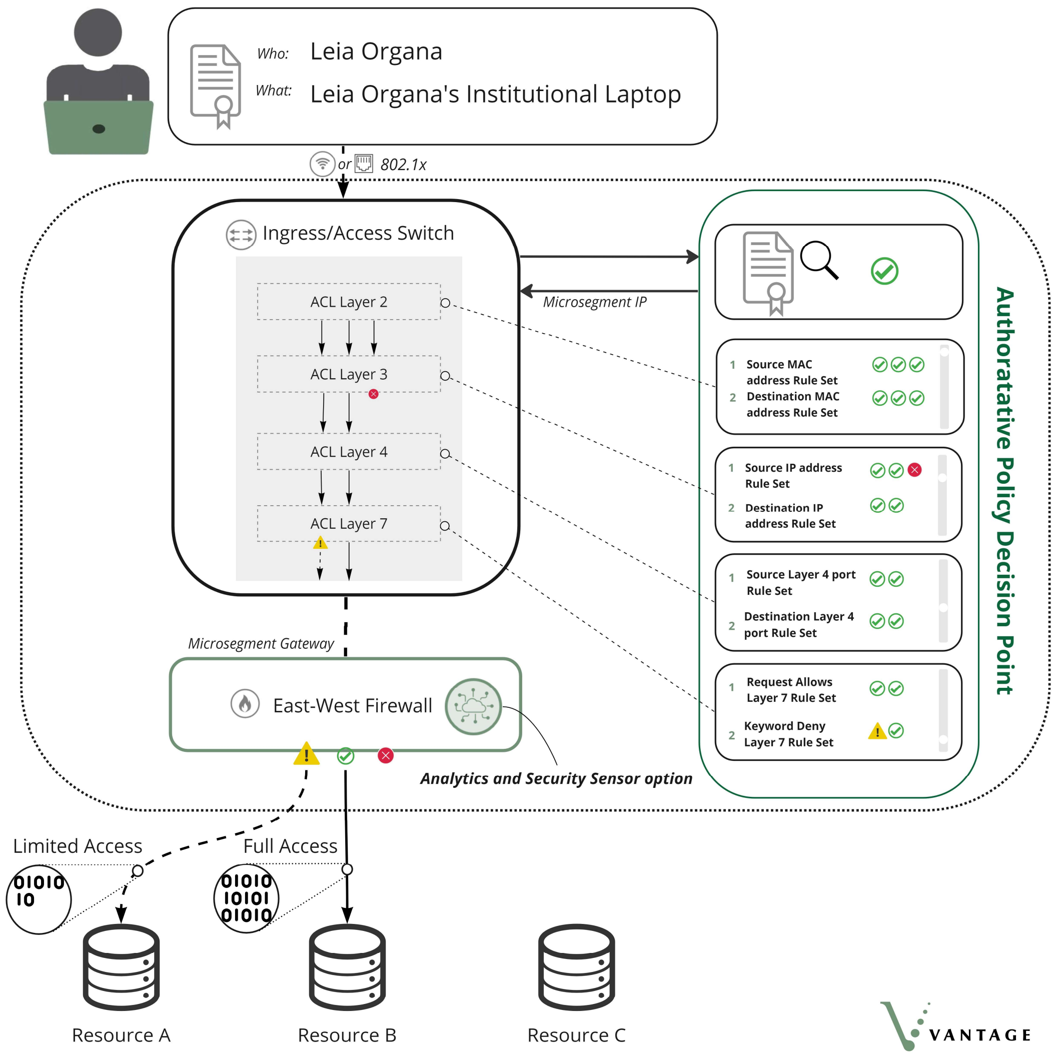
Resource B Full Access ✓

Resource C No Access ✗

PRO	CON
• Can *usually* achieve micro-segmentation. • Well-provisioned to manage IoT endpoints. • Reduces traffic filtering load off the E-W Firewall. • Enables opportunities for additional network analytics.	• If you don’t already have the right switches deployed, a lot of network equipment needs to be replaced to achieve the fabric across the distribution layer to the edge. • Learning curve for DACL creation and management may not be quick to achieve. • Usually not vendor agnostic (i.e., you need to be ok with vendor lock). • Some implementations don’t do multicast well. • No real firewalling • DACL management has major limitations

Y

Sophisticated DACL RBAC


Who: Leia Organa
What: Leia Organa's Institutional Laptop
or 802.1x
Ingress/Access Switch
ACL Layer 2
ACL Layer 3
ACL Layer 4
ACL Layer 7
Microsegment IP
Microsegment Gateway
East-West Firewall
Analytics and Security Sensor option
1 Source MAC address Rule Set
2 Destination MAC address Rule Set
1 Source IP address Rule Set
2 Destination IP address Rule Set
1 Source Layer 4 port Rule Set
2 Destination Layer 4 port Rule Set
1 Request Allows Layer 7 Rule Set
2 Keyword Deny Layer 7 Rule Set
Authoratative Policy Decision Point
Limited Access
Full Access
01010 10
01010 10101 01010
Resource A
Resource B
Resource C
VANTAGE

PRO

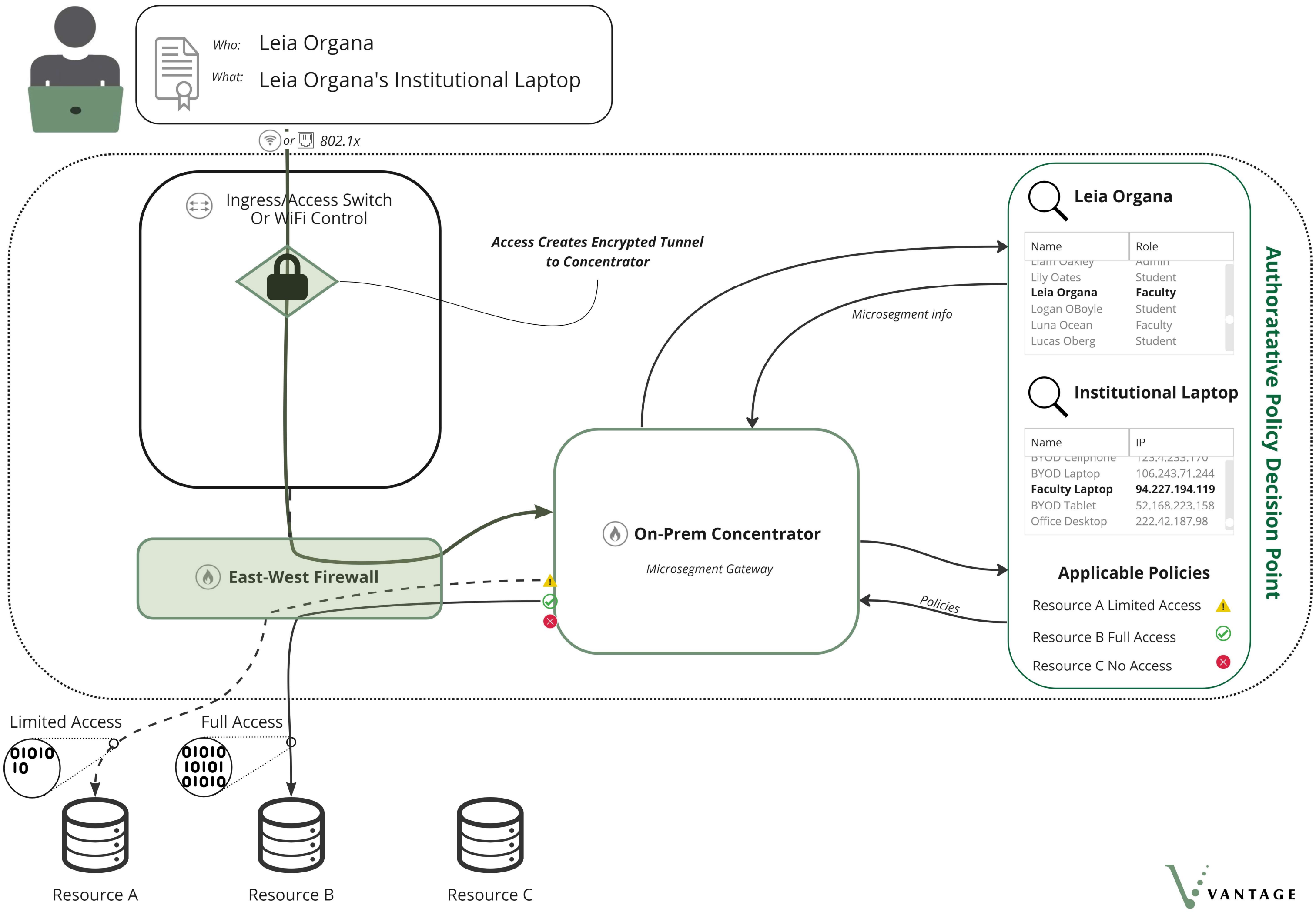
- Endpoint doesn’t require a client.
- Can achieve micro-segmentation.
- Well-provisioned to manage IoT endpoints.
- Physical network topology irrelevant to RBAC functionality.
- Network topology provides the opportunity for a small number of useful security sensors.

CON

- Concentrator is doing all the heavy traffic filtering.
- Throughput is limited, elephant flows must be routed another way.
- Traffic may need to traverse campus infrastructure multiple times for service access (path not optimized).

P

Hairpin RBAC



Name	Role
Liam Oakley	Admin
Lily Oates	Student
Leia Organa	**Faculty**
Logan OBoyle	Student
Luna Ocean	Faculty
Lucas Oberg	Student

Name	IP
BYOD Cellphone	123.4.233.170
BYOD Laptop	106.243.71.244
Faculty Laptop	**94.227.194.119**
BYOD Tablet	52.168.223.158
Office Desktop	222.42.187.98

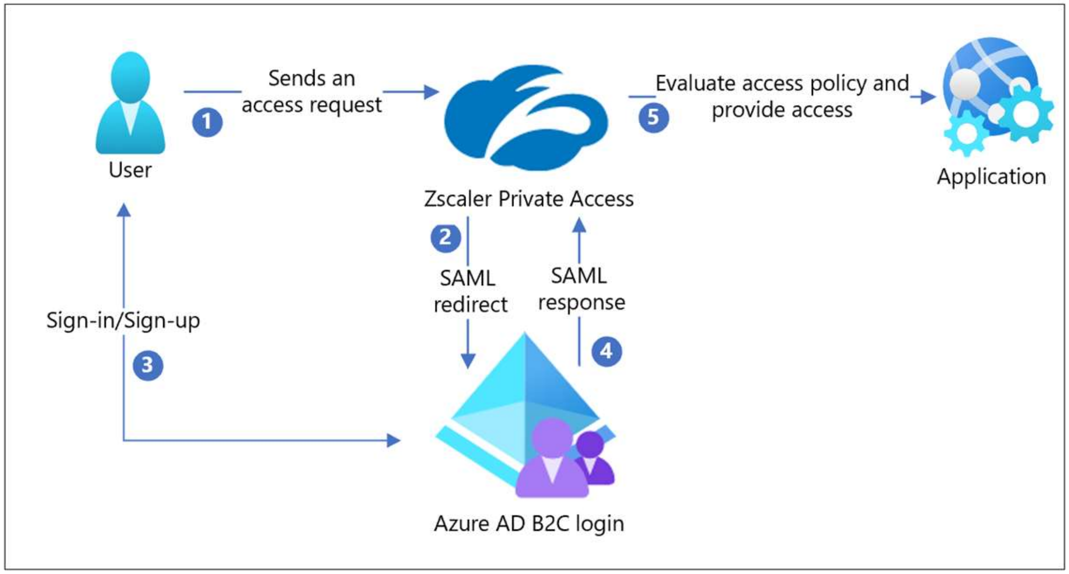
Applicable Policies	
Resource A Limited Access	⚠
Resource B Full Access	✓
Resource C No Access	✗

Proxy RBAC
Overlay with Client

PRO	CON
• Easily scalable to add services or users. • Physical network topology irrelevant to RBAC functionality. • Quick to provision new services behind. • Moving a service from on-prem to cloud can become trivial and transparent to users. • For compatible endpoints, achieves micro-segmentation. • As a MitM proxy, can perform security and analytics on traffic.	• Throughput is limited, elephant flows must be routed another way. • Traffic may need to traverse campus infrastructure multiple times for service access (path not optimized). • One more client on the endpoint. • Not all endpoints necessarily supported by client. • Licensing structure may limit supported application max.

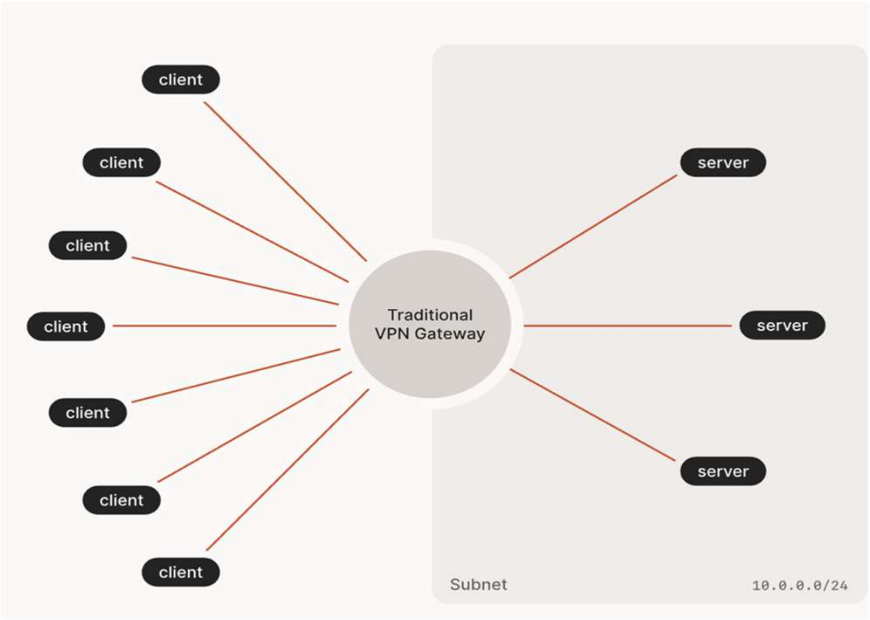
Google
CNN
Office 365
now
box
Azure
aws
IoT
ZERO TRUST EXCHANGE
OT
Factory
Data Center
Workforce
Customers

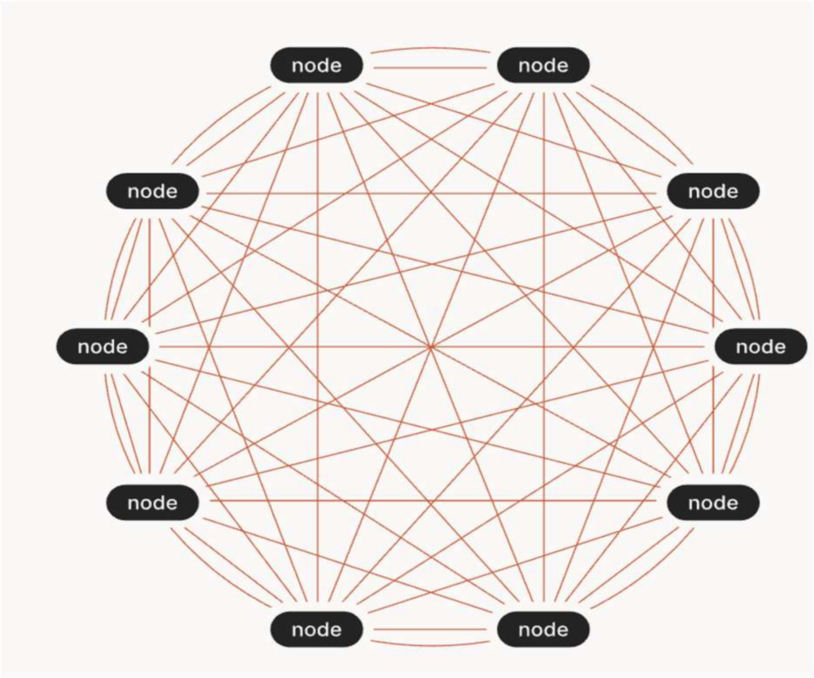
Graphics credit: Zscaler



P

What is Tailscale?



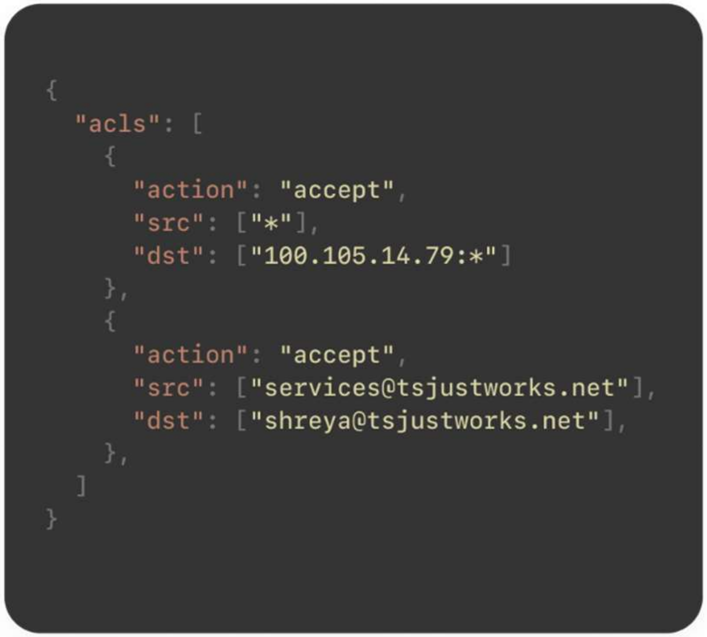


Traditional hub and spoke VPN compared with
Tailscale fully meshed, Layer 3, point-to-point solution

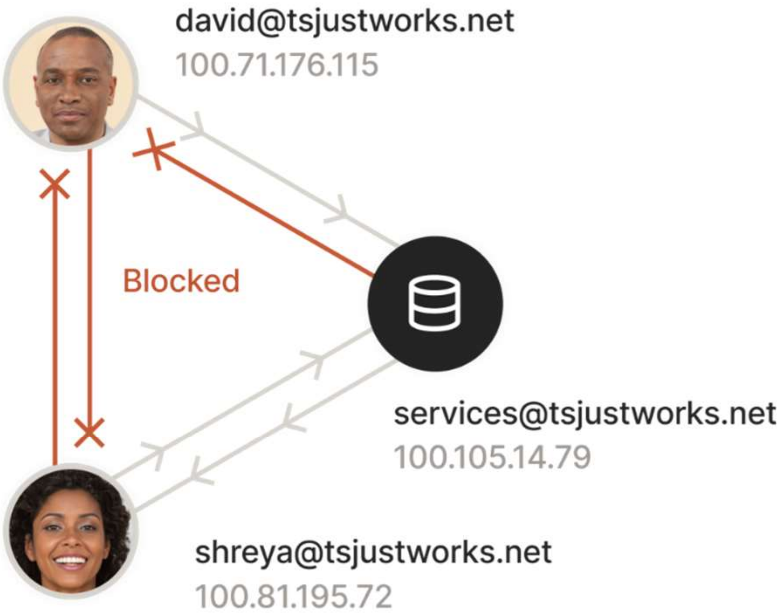
Y

Access Control Lists (ACLs)

Tailscale restricts access by SSO users, devices, and groups — not by hostname.
A central role-based access policy determines who is allowed to connect.



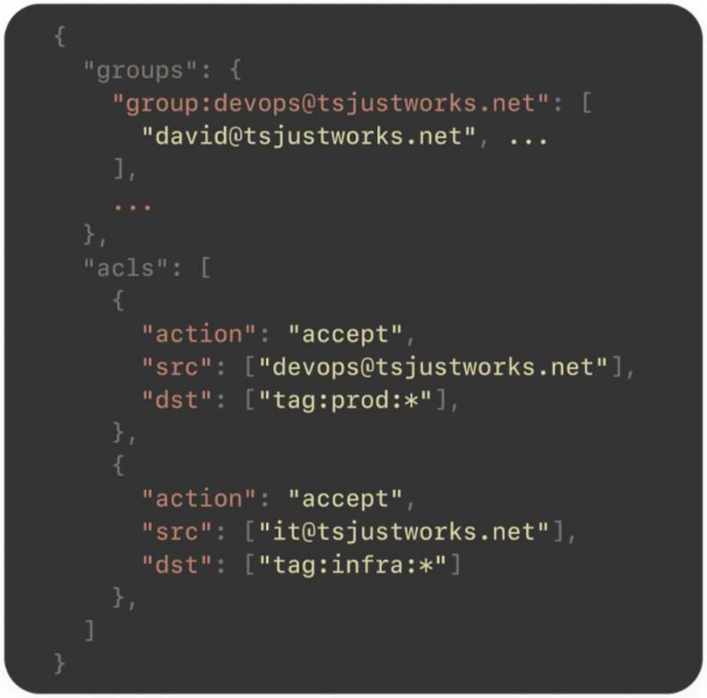
```
{
  "acls": [
    {
      "action": "accept",
      "src": ["*"],
      "dst": ["100.105.14.79:*"]
    },
    {
      "action": "accept",
      "src": ["services@tsjustworks.net"],
      "dst": ["shreya@tsjustworks.net"],
    },
  ]
}
```



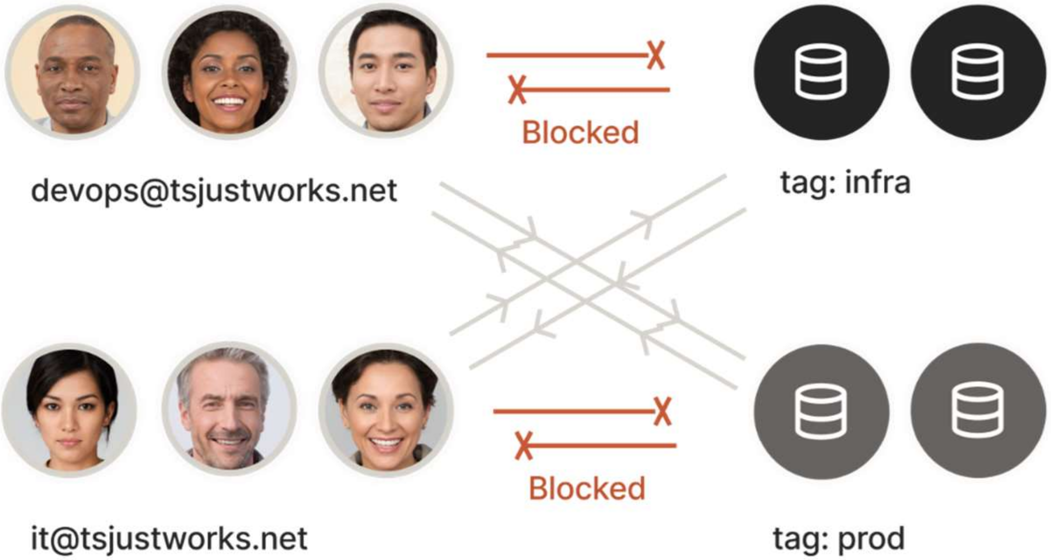
Y

Access Control Lists (ACL) Tags

Tags let you assign an identity to a device that is separate from human users.
Use that identity as part of an ACL to restrict access.



```
{
  "groups": {
    "group:devops@tsjustworks.net": [
      "david@tsjustworks.net", ...
    ],
    ...
  },
  "acls": [
    {
      "action": "accept",
      "src": ["devops@tsjustworks.net"],
      "dst": ["tag:prod:*"],
    },
    {
      "action": "accept",
      "src": ["it@tsjustworks.net"],
      "dst": ["tag:infra:*"]
    },
  ]
}
```



devops@tsjustworks.net

Blocked

tag: infra

it@tsjustworks.net

Blocked

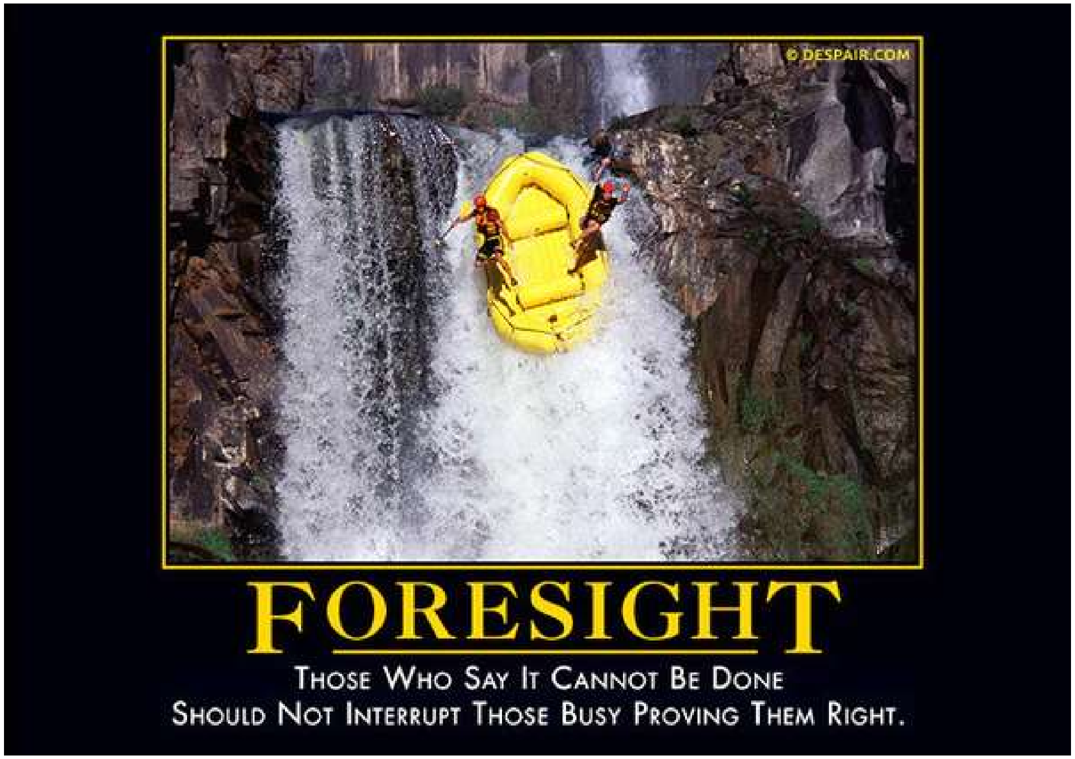
tag: prod

Y

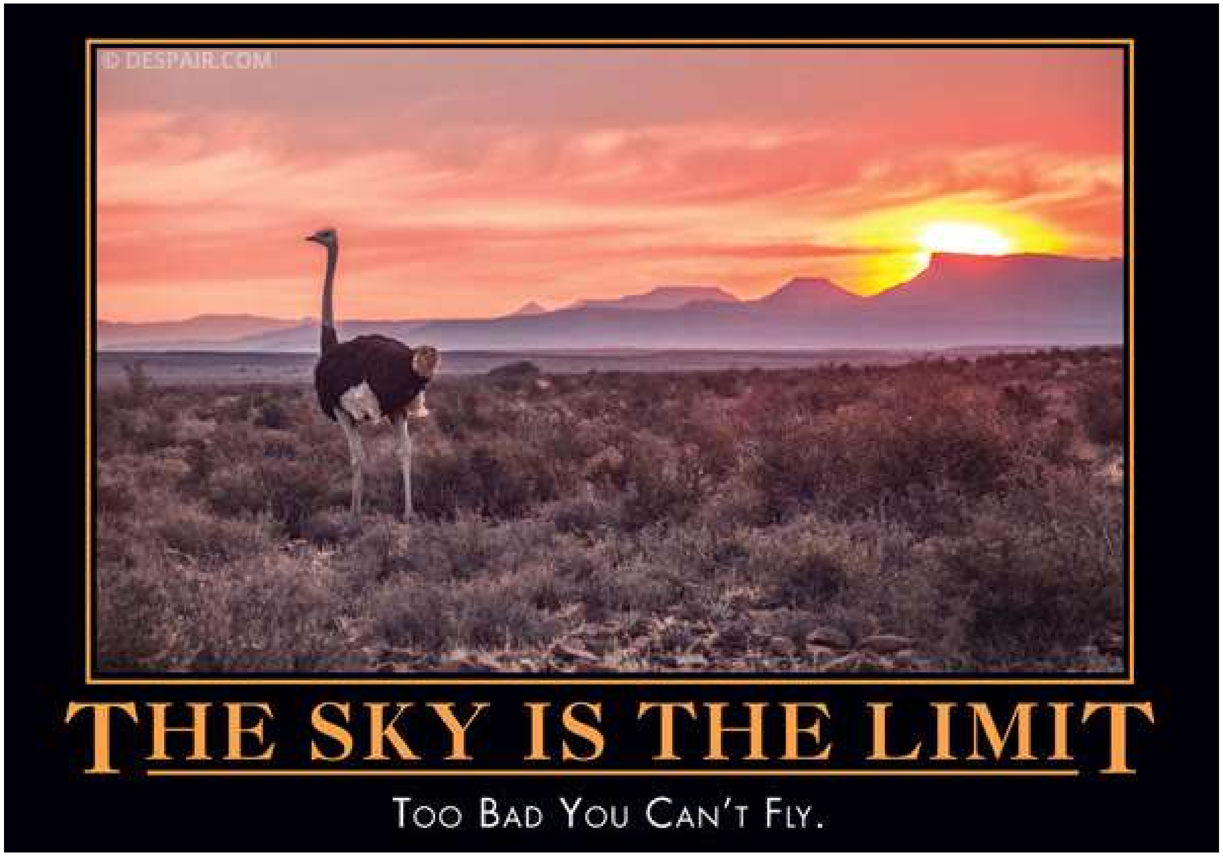
PEP Location per Vendor Solution	Secure Overlay	Proxy	Main Firewall (N/S)	ACL on fabric ingress	NG E/W Firewall	on-prem Concentrator	Distributed Firewall at Service edge	IoT friendly	Security Sensor Friendly
Cisco Firepower			X		X	X	X	X	X
Cisco TrustSec/SDA			X	X				X	X
Fortinet			X		X	X	X	X	X
Palo Alto Network			X		X	X	X	X	X
Extreme Networks			X	X				X	X
Alcatel Lucent (ALE)			X	X				X	X
Zscaler (multiple solutions)		X				X			
Netskope (proxy)		X							
Aruba - Gateway Based			X			X		X	X
Tailscale/Headscale	X							via gateway	Limited
Open ZiTi	X							via gateway	
ZeroTier	X							via gateway	

Why UIC chose the vendor agnostic approach

- Continue to get value for existing investment
- Slower migration, don't need to replace the access layer first
- Rapid time to value
- Future flexibility
- Chose to avoid vendor-lock over the long haul


© DESPAIR.COM
FORESIGHT
Those Who Say It Cannot Be Done
Should Not Interrupt Those Busy Proving Them Right.

WW



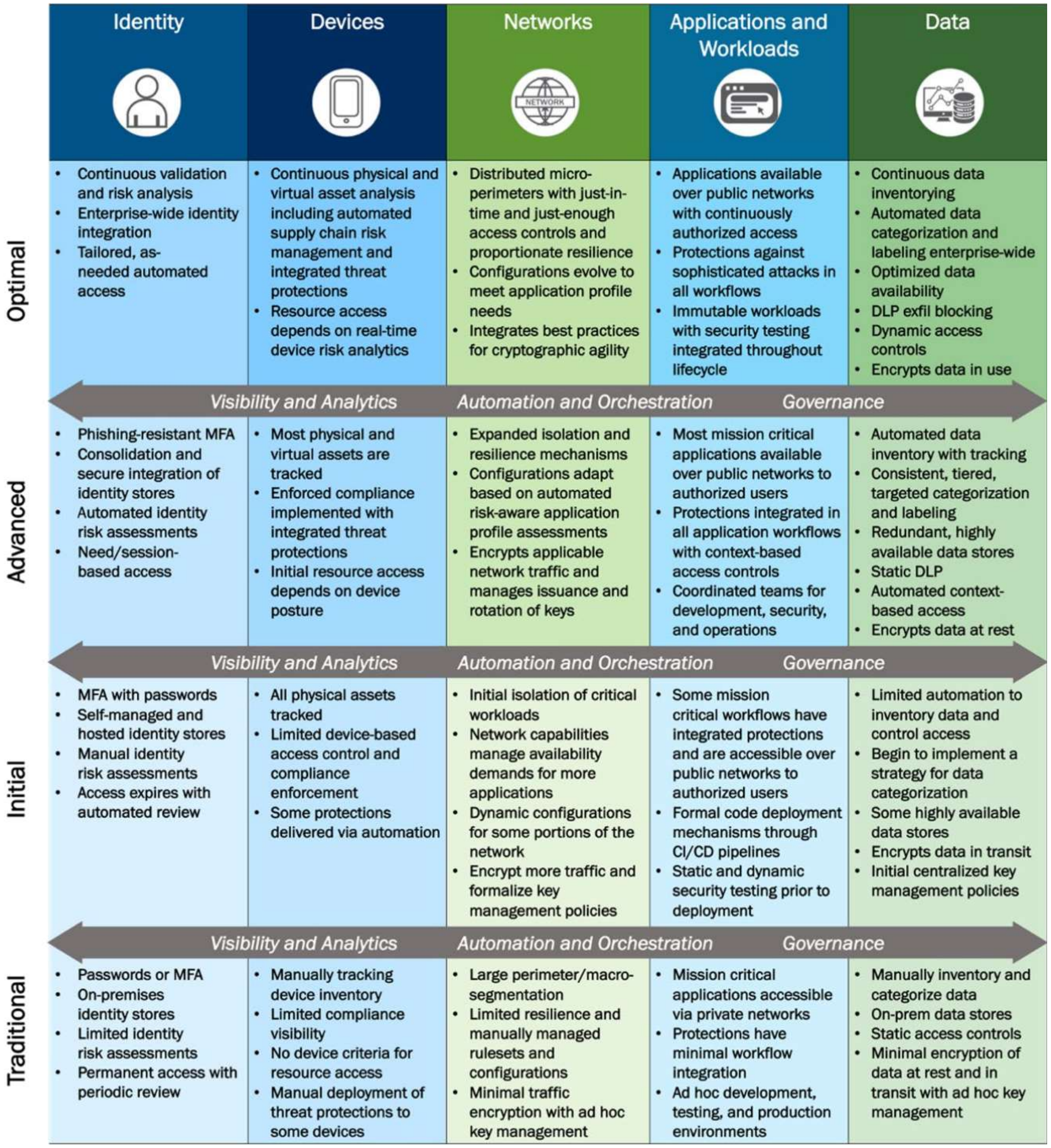
Biggest challenges

- ○ PKI (if EAP-TLS)
- ○ Transition planning
- ○ Role definitions and associated firewall rules
- ○ Business/security analyst and scaling

○ Priority: IoT

VANTAGE Technology Consulting Group

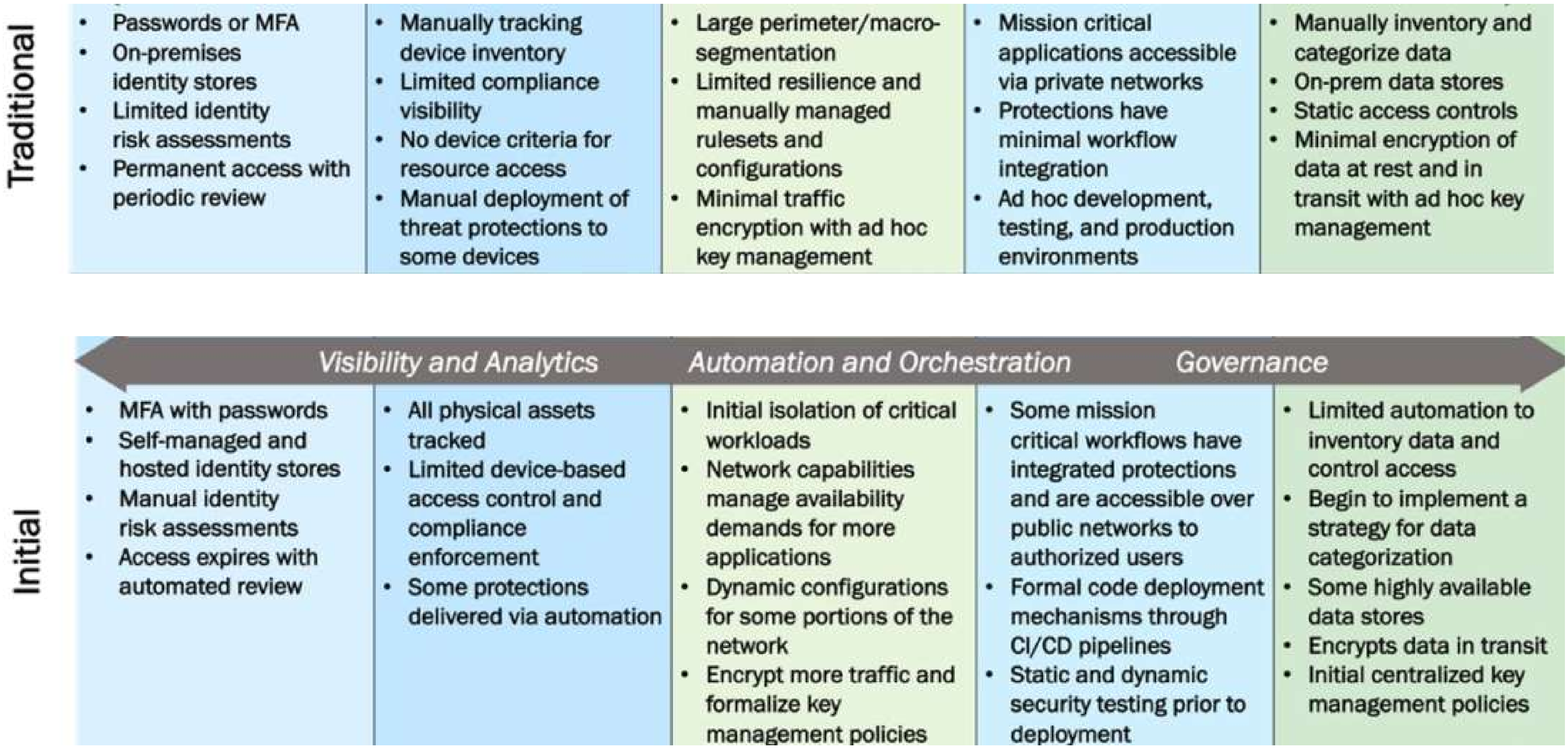
Y



	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

Y

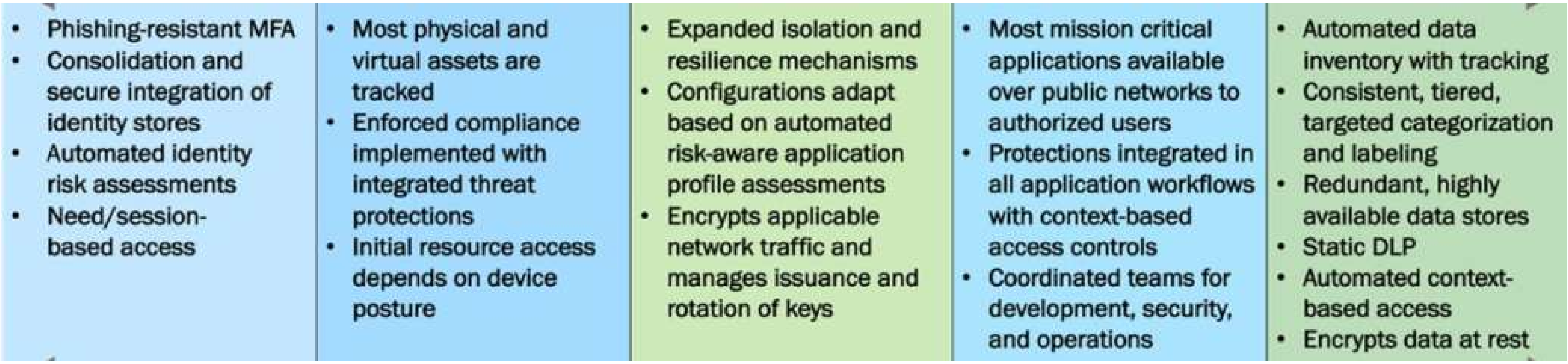
VANTAGE
Technology Consulting Group



Traditional	- Passwords or MFA - On-premises identity stores - Limited identity risk assessments - Permanent access with periodic review	- Manually tracking device inventory - Limited compliance visibility - No device criteria for resource access - Manual deployment of threat protections to some devices	- Large perimeter/macro-segmentation - Limited resilience and manually managed rulesets and configurations - Minimal traffic encryption with ad hoc key management	- Mission critical applications accessible via private networks - Protections have minimal workflow integration - Ad hoc development, testing, and production environments	- Manually inventory and categorize data - On-prem data stores - Static access controls - Minimal encryption of data at rest and in transit with ad hoc key management
		Visibility and Analytics	*Automation and Orchestration*	*Governance*	
Initial	- MFA with passwords - Self-managed and hosted identity stores - Manual identity risk assessments - Access expires with automated review	- All physical assets tracked - Limited device-based access control and compliance enforcement - Some protections delivered via automation	- Initial isolation of critical workloads - Network capabilities manage availability demands for more applications - Dynamic configurations for some portions of the network - Encrypt more traffic and formalize key management policies	- Some mission critical workflows have integrated protections and are accessible over public networks to authorized users - Formal code deployment mechanisms through CI/CD pipelines - Static and dynamic security testing prior to deployment	- Limited automation to inventory data and control access - Begin to implement a strategy for data categorization - Some highly available data stores - Encrypts data in transit - Initial centralized key management policies

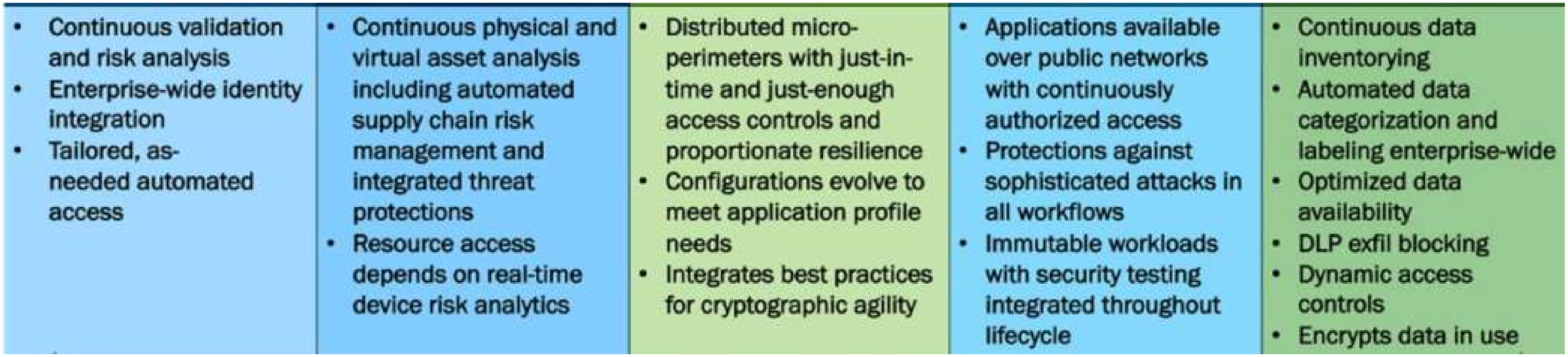
Y

Advanced



- Phishing-resistant MFA - Consolidation and secure integration of identity stores - Automated identity risk assessments - Need/session-based access	- Most physical and virtual assets are tracked - Enforced compliance implemented with integrated threat protections - Initial resource access depends on device posture	- Expanded isolation and resilience mechanisms - Configurations adapt based on automated risk-aware application profile assessments - Encrypts applicable network traffic and manages issuance and rotation of keys	- Most mission critical applications available over public networks to authorized users - Protections integrated in all application workflows with context-based access controls - Coordinated teams for development, security, and operations	- Automated data inventory with tracking - Consistent, tiered, targeted categorization and labeling - Redundant, highly available data stores - Static DLP - Automated context-based access - Encrypts data at rest

Optimal



- Continuous validation and risk analysis - Enterprise-wide identity integration - Tailored, as-needed automated access	- Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections - Resource access depends on real-time device risk analytics	- Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience - Configurations evolve to meet application profile needs - Integrates best practices for cryptographic agility	- Applications available over public networks with continuously authorized access - Protections against sophisticated attacks in all workflows - Immutable workloads with security testing integrated throughout lifecycle	- Continuous data inventorying - Automated data categorization and labeling enterprise-wide - Optimized data availability - DLP exfil blocking - Dynamic access controls - Encrypts data in use

Y

References

UIC

- UIC IT Website
- Forward Initiative

Industry

- NIST 800-207 (Zero Trust Architecture)
- CISA Zero Trust Maturity Model v2
- CISA Executive Order on Improving the Nation's Cybersecurity
- NIST 800-207A (Cloud extensible ZTA)
- Finney, George, *Project Zero Trust: A Story About a Strategy for Aligning Security and the Business*, Wiley, October 2022

Vantage

- Vantage/UIC Internet2 network modernization webinar 2023
- Vantage/UIC EDUCAUSE network modernization webinar 2021
- Paths to Zero Trust (blog, June 2023)
- The Vantage Vision for a Modernized Network (blog)
- EDUCAUSE Community Group Recording on Network Architecture (netman/commtech/wireless, facilitated by Jon) (Passcode: tV9zq!Cr)

VANTAGE Technology Consulting Group

Any questions? Presenter Contact Information

PDF of Slides:

- Jelene Crehan, jelene@uic.edu
- Jon Young, jonyoung@vantagetcg.com
- Jacqueline Pitter, jacquelinepitter@vantagetcg.com

VANTAGE
Technology Consulting Group