CISCO
SECURE

The bridge to possible

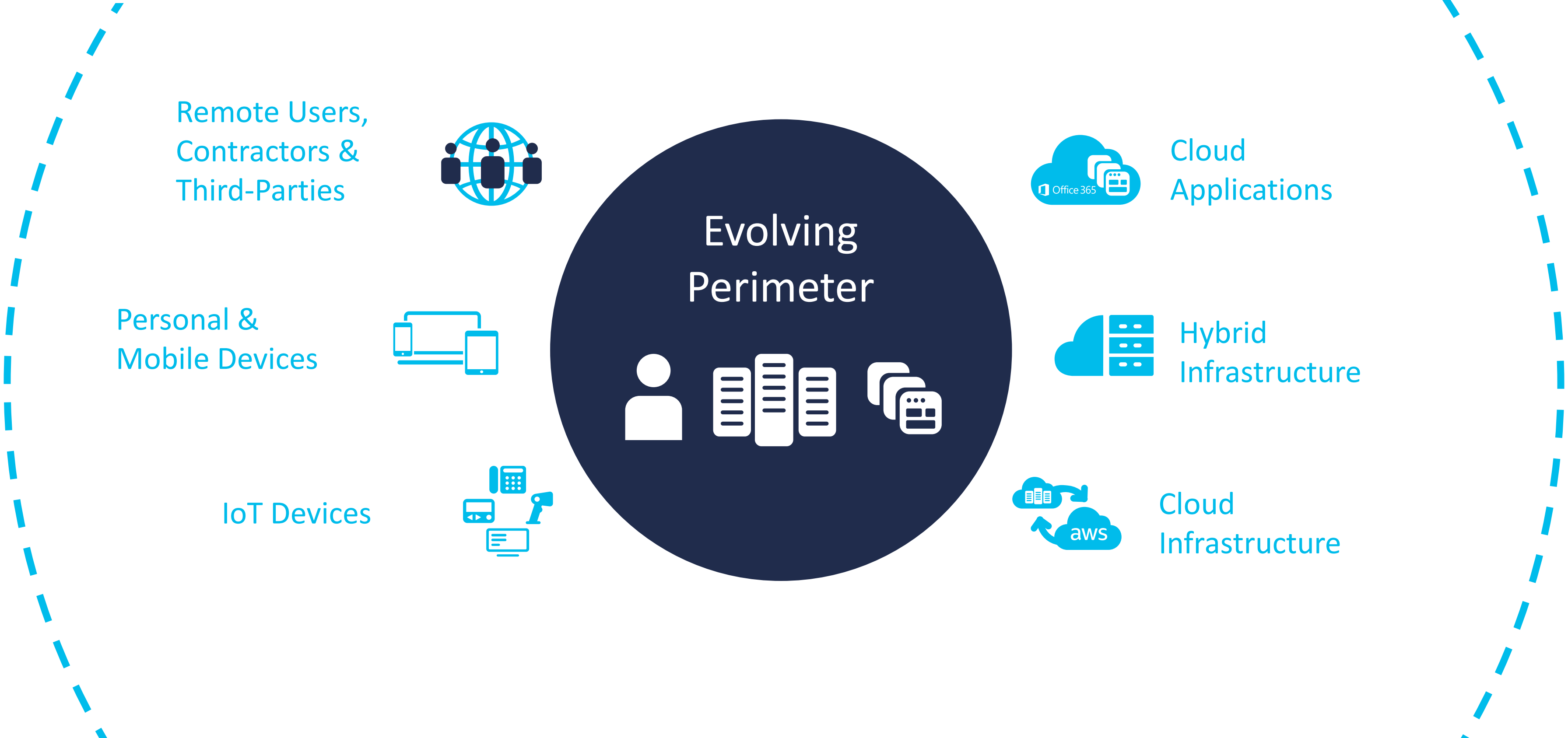
Cisco Zero Trust Solutions

A Model For More Efficient Security

Dragan Novaković
Security Solutions Engineer

Shift in IT Landscape

Users, devices and apps are everywhere



Remote Users, Contractors & Third-Parties

Personal & Mobile Devices

IoT Devices

Evolving Perimeter

Cloud Applications

Hybrid Infrastructure

Cloud Infrastructure

Threats Today, As a Result

A new approach to security is needed – zero trust – to address identity, app & network threats.

Targeting Identity

81% of breaches involved compromised credentials

Targeting Apps

54% of web app vulnerabilities have a public exploit available

Targeting Devices

300% increase in IoT malware variants

It’s segmentation

It’s ZTNA

It’s endpoint security

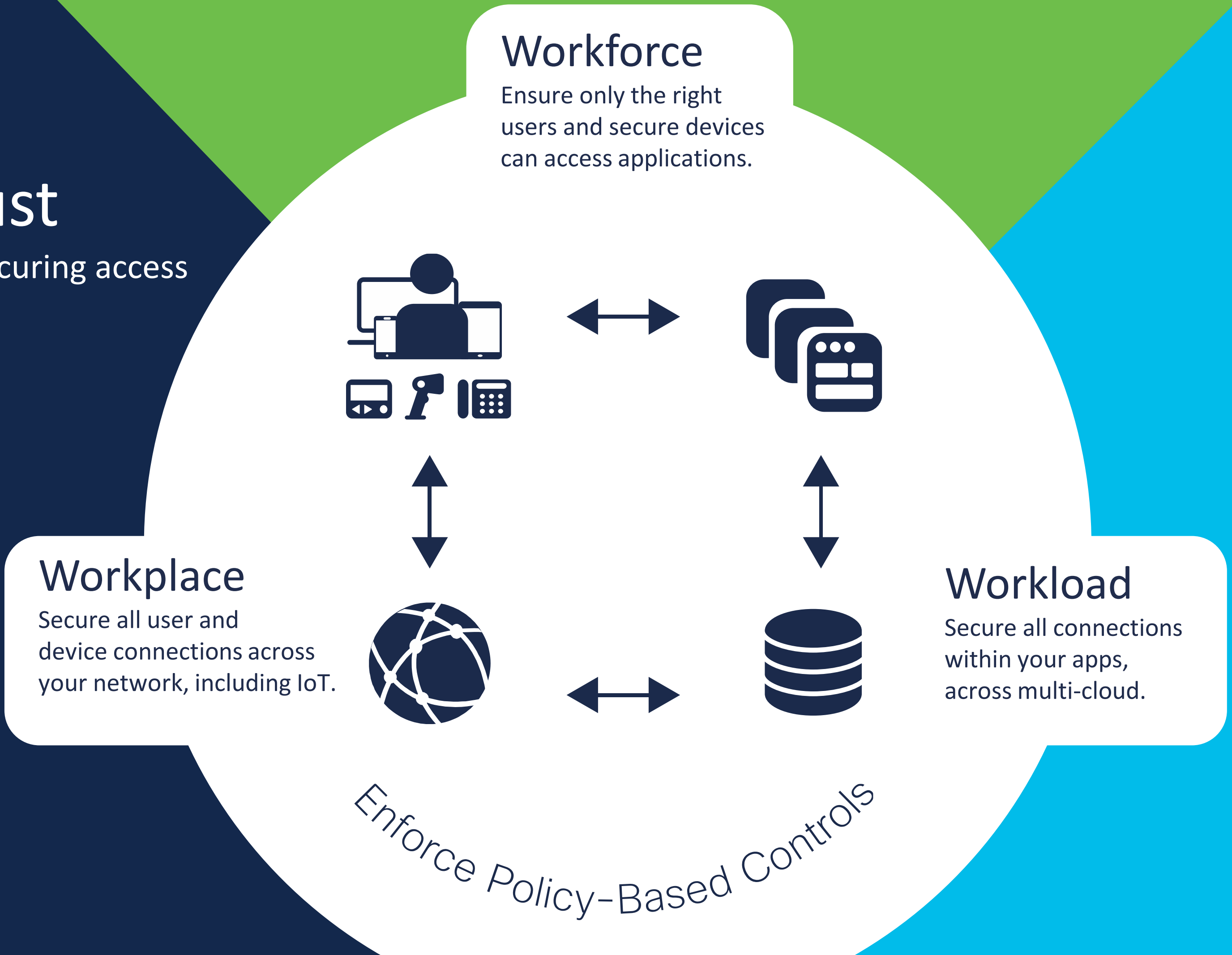
It’s firewall

It’s identity

Zero Trust means different things to different people

Cisco Zero Trust

A zero-trust approach to securing access across your applications and environment, from any user, device and location.



Workforce

Ensure only the right users and secure devices can access applications.

Workplace

Secure all user and device connections across your network, including IoT.

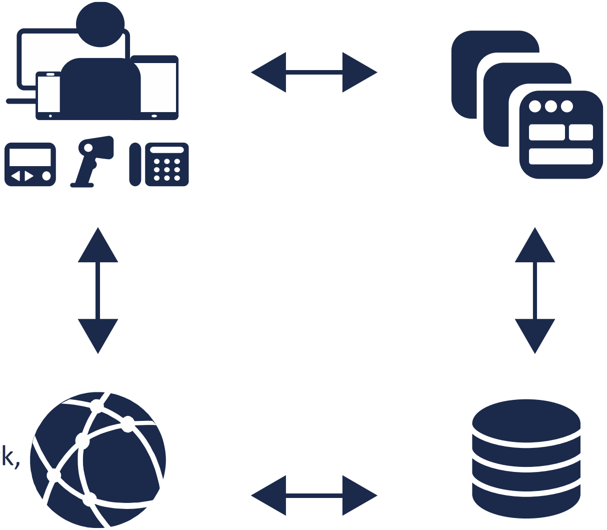
Workload

Secure all connections within your apps, across multi-cloud.

Enforce Policy-Based Controls

Cisco Zero Trust

Secure access for your workforce, workloads and workplace.



Duo for Workforce

Ensure only the right users and secure devices can access applications.

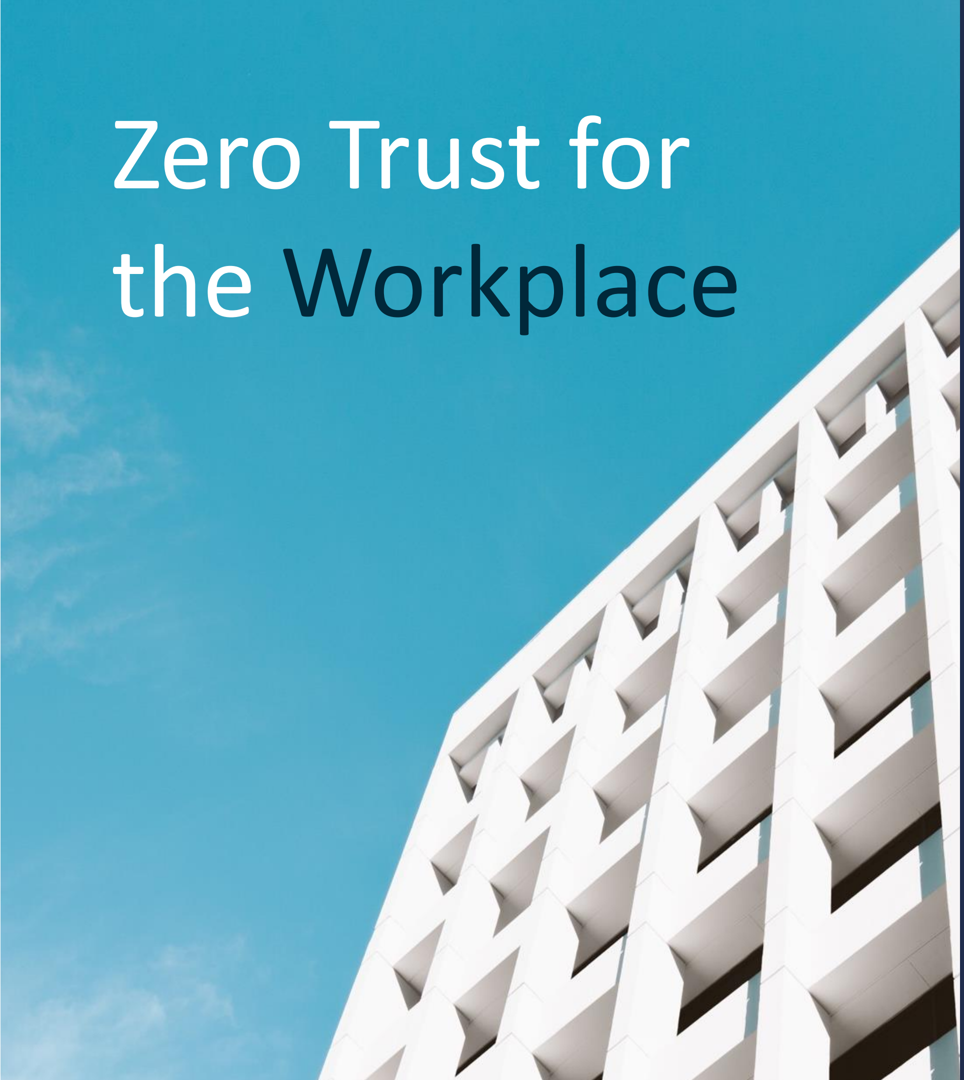
ISE for Workplace

Secure all user and device connections across your network, including IoT.

Secure Workload

Secure all connections within your apps, across multi-cloud.

Enforce Policy-Based Controls



Zero Trust for the Workplace

Problems Solved:

- Complete network visibility
- Prevent lateral movement
- Prevent unauthorized access

Solution: Cisco ISE

With ISE, secure
all user and device connections across
your network, including IoT.

Workplace

Zero-Trust Security

Establish Trust

Discover & classify devices with IoT device profiling, BYOD & user device posture.

Enforce Trust-Based Access

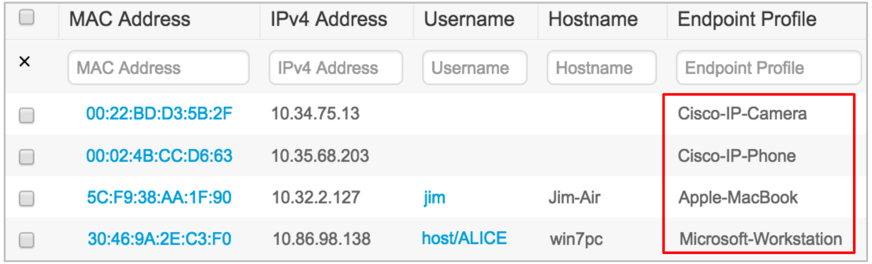
Network access control policies for users & devices with network segmentation.

Continuously Verify Trust

Continuous monitoring with vulnerability assessments & identifying indicators of compromise.

Workplace: Establish Trust

Network Visibility



□	MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
×	MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
□	00:22:BD:D3:5B:2F	10.34.75.13			Cisco-IP-Camera
□	00:02:4B:CC:D6:63	10.35.68.203			Cisco-IP-Phone
□	5C:F9:38:AA:1F:90	10.32.2.127	jim	Jim-Air	Apple-MacBook
□	30:46:9A:2E:C3:F0	10.86.98.138	host/ALICE	win7pc	Microsoft-Workstation

Gain Insight Into:

- User groups
- Device types
- Location/time
- Posture
- Threats
- Behavior
- Vulnerability

And devices:

- Uses probes in Identity Services Engine (ISE) & network infrastructure
- Profiles and determines device type
- Determines access for IoT devices

Workplace: Establish Trust

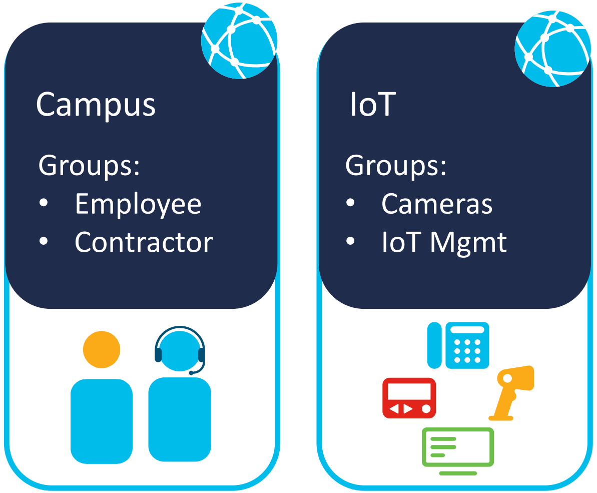
Classification

Classify devices by groups based on their specific access needs and function

After assets are identified, they’re tagged & classified by groups using either dynamic or static classification methods, or by assigning a tag to an IP address.

Clearly identify what needs to be protected. Example: Production servers; employees, guests or contractors; printers, etc.

Examples of Virtual Networks & Groups



Campus

Groups:
- Employee
- Contractor

IoT

Groups:
- Cameras
- IoT Mgmt

Workplace: Enforce Trust-based Access

Network Segmentation

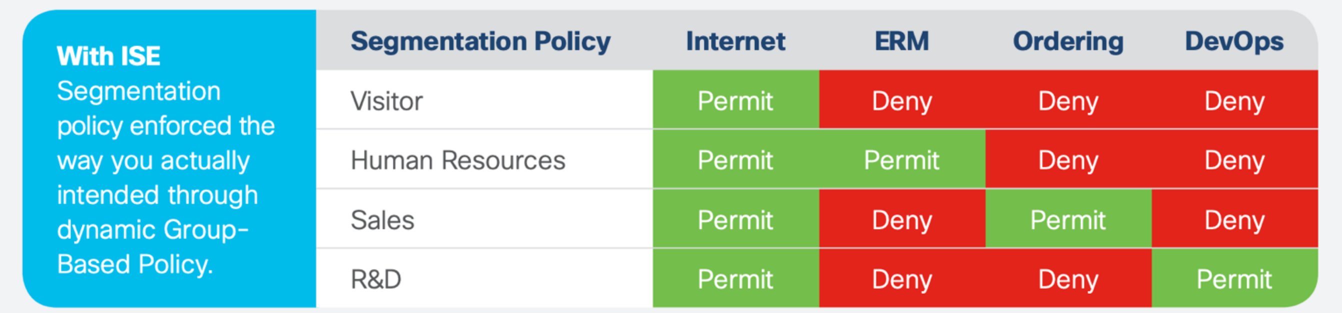
With Cisco ISE, you can:

- Segment network access based on only what the device needs to access, and nothing more

- Partition your network to contain a breach
- Enable dynamic segmentation for growing networks, changing conditions & threats

Workplace: Enforce Trust-based Access

Network Segmentation: Policy

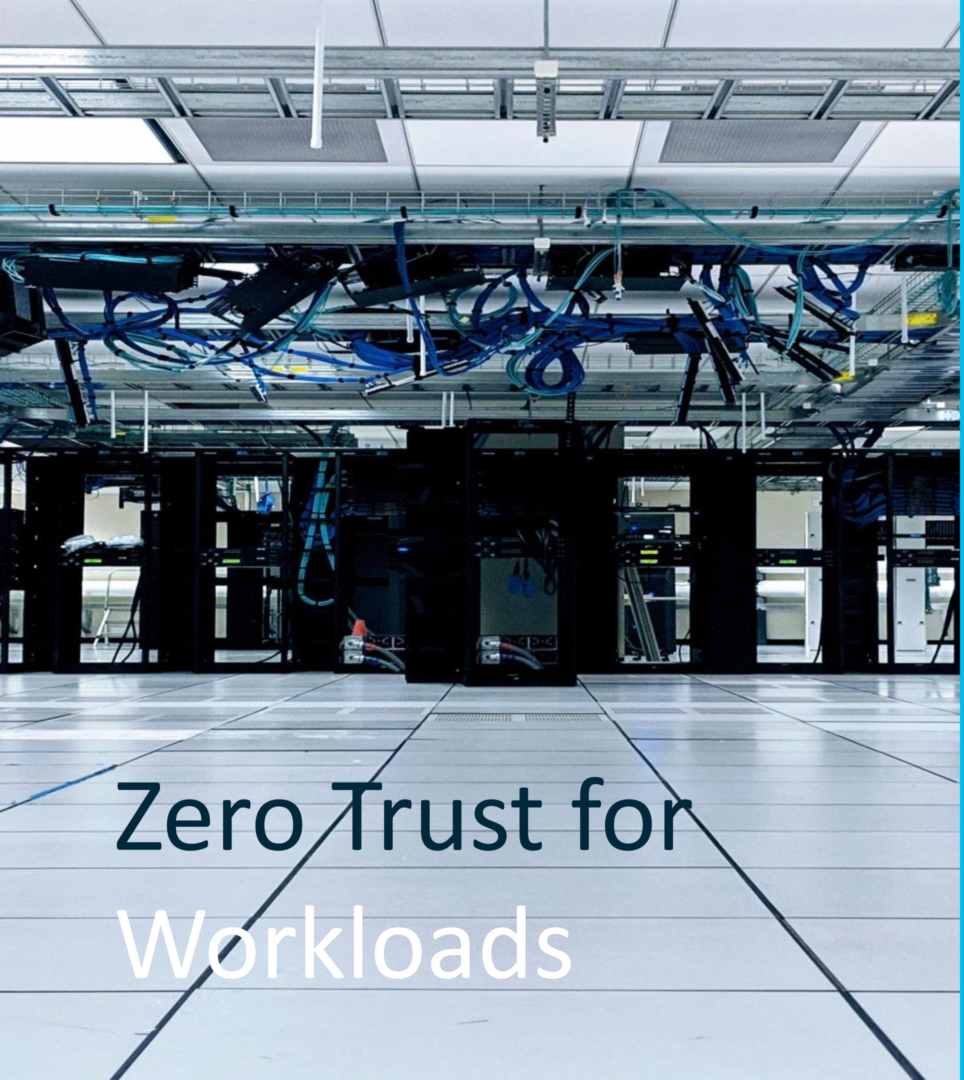


With ISE
Segmentation policy enforced the way you actually intended through dynamic Group-Based Policy.

Segmentation Policy	Internet	ERM	Ordering	DevOps
Visitor	Permit	Deny	Deny	Deny
Human Resources	Permit	Permit	Deny	Deny
Sales	Permit	Deny	Permit	Deny
R&D	Permit	Deny	Deny	Permit

With Trust-Based Access, you can:

- Enforce network authorization policies based on device classification & access needs
- Enforce segmentation policy across wireless, wired and VPN connections
- Manage segmentation via ISE thru policy manager
- Distribute policy dynamically to network devices
- Simplify segmentation with group-based policy



Zero Trust for Workloads

Problems Solved:

- Complete Application Visibility
- Contain Breaches
- Prevent Lateral Movement

Solution: Secure Workload

With Tetration, secure all connections within your apps, across multi-cloud.

Workloads

Zero-Trust Security

Establish Trust

Gain visibility into what's running & critical by identifying workloads & enforcing policies

Enforce Trust-Based Access

Contain breaches & minimize lateral movement with application micro-segmentation

Continuously Verify Trust

Alert or block communications by continuously monitoring & responding to indicators of compromise

Workload: Establish Trust

Workload Visibility

Visibility:

- Every packet & data center flow
- East-west communication
- Process info & installed software
- Long-term data retention for telemetry & forensics

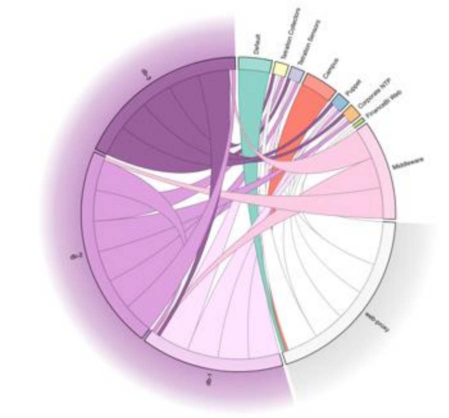
How Data is Collected:

- Software sensors for bare-metal, virtual machines & containers
- Endpoint & flow visibility through Cisco AnyConnect & Identity Services Engine (ISE)

Workload: Establish Trust

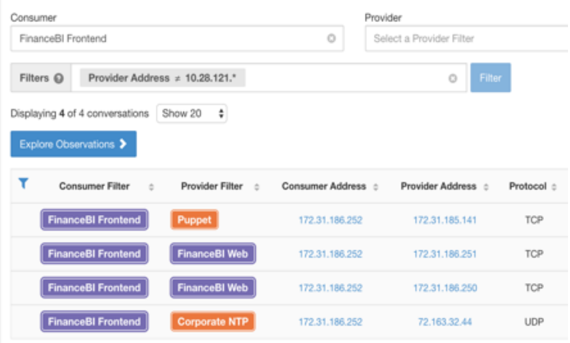
Application Insight

Tetration maps your application dependencies, giving you insight into app communications.



Cluster View

Snapshot of communication between app components, grouped into clusters (VM, bare-metal)



Consumer: FinanceBI Frontend

Provider: Select a Provider Filter

Filters: Provider Address ≠ 10.28.121.*

Displaying 4 of 4 conversations Show 20

Consumer Filter	Provider Filter	Consumer Address	Provider Address	Protocol
FinanceBI Frontend	Puppet	172.31.186.252	172.31.185.141	TCP
FinanceBI Frontend	FinanceBI Web	172.31.186.252	172.31.186.251	TCP
FinanceBI Frontend	FinanceBI Web	172.31.186.252	172.31.186.250	TCP
FinanceBI Frontend	Corporate NTP	172.31.186.252	72.163.32.44	UDP

Conversation View

All communication details between different app components

Shared Services

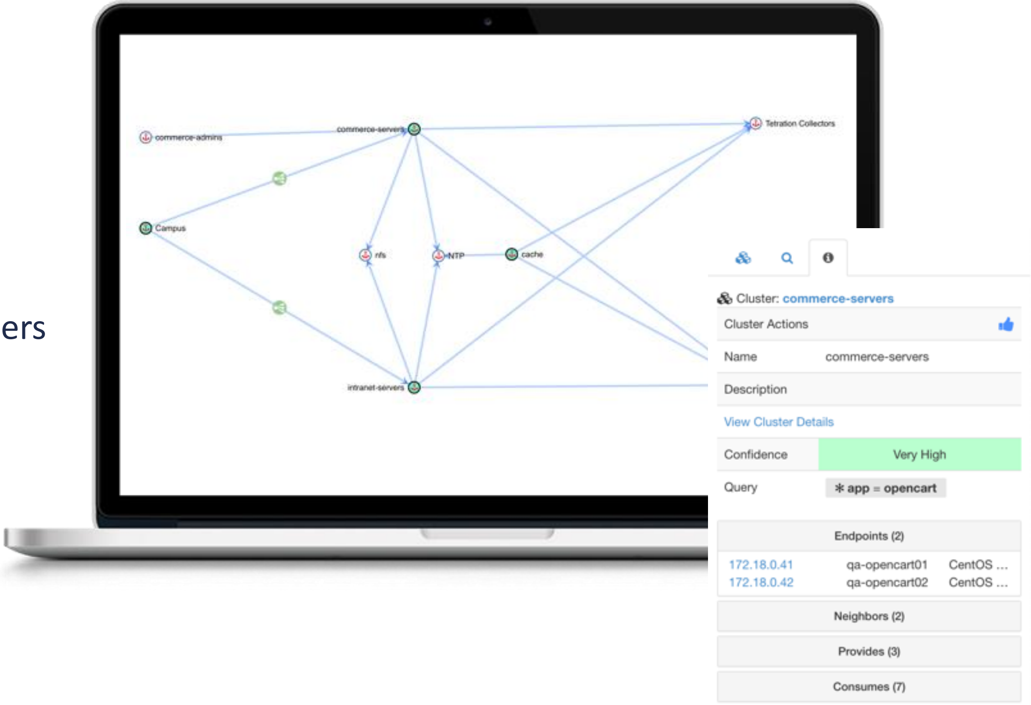
Services commonly shared among multiple apps (orchestration, DNS, AAA servers, etc.)

Workload: Establish Trust

Application Insight Dependency Map

Get visibility into:

- How different application tiers are communicating
- About direct connections to database servers
- Communications through load balancers
- If there are outgoing connections that shouldn't be allowed



Cluster: commerce-servers

Cluster Actions

Name	commerce-servers
Description	

View Cluster Details

Confidence	Very High
Query	* app = opencart

Endpoints (2)

172.18.0.41	qa-opencart01	CentOS ...
172.18.0.42	qa-opencart02	CentOS ...

Neighbors (2)

Provides (3)

Consumes (7)

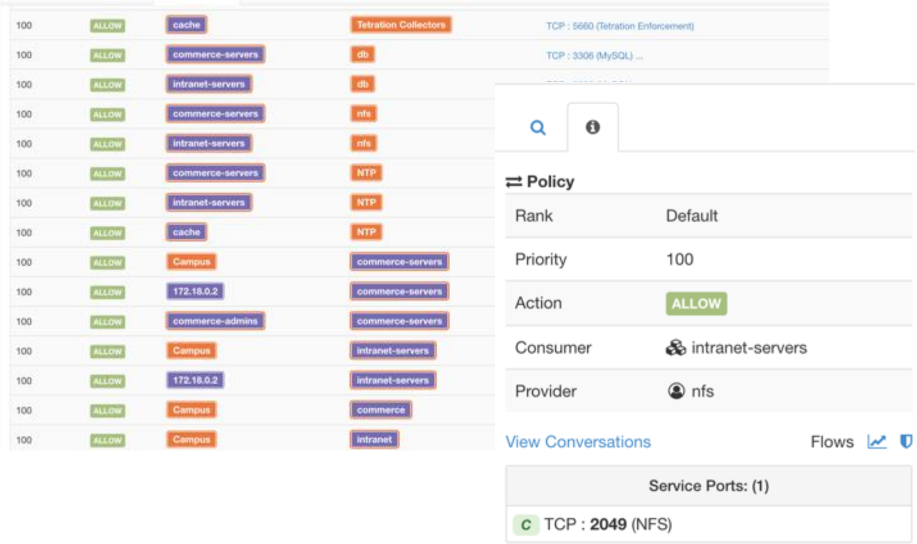
Workload: Enforce Trust-Based Access

Zero Trust Policy: Application Segmentation

Tetration generates policies based on application behavior.

For example:

- Production may not talk to non-production
- Certain applications are not accessible via the internet
- Allow or deny traffic between app components & infrastructure elements



100	ALLOW	cache	Tetration Collectors	TCP : 5660 (Tetration Enforcement)
100	ALLOW	commerce-servers	db	TCP : 3306 (MySQL) ...
100	ALLOW	intranet-servers	db	
100	ALLOW	commerce-servers	nfs	
100	ALLOW	intranet-servers	nfs	
100	ALLOW	commerce-servers	NTP	
100	ALLOW	intranet-servers	NTP	
100	ALLOW	cache	NTP	
100	ALLOW	Campus	commerce-servers	
100	ALLOW	172.18.0.2	commerce-servers	
100	ALLOW	commerce-admins	commerce-servers	
100	ALLOW	Campus	intranet-servers	
100	ALLOW	172.18.0.2	intranet-servers	
100	ALLOW	Campus	commerce	
100	ALLOW	Campus	intranet	

⇄ Policy

Rank	Default
Priority	100
Action	ALLOW
Consumer	intranet-servers
Provider	nfs

View Conversations   Flows

Service Ports: (1)
C TCP : **2049** (NFS)

Workload: Enforce Trust-Based Access

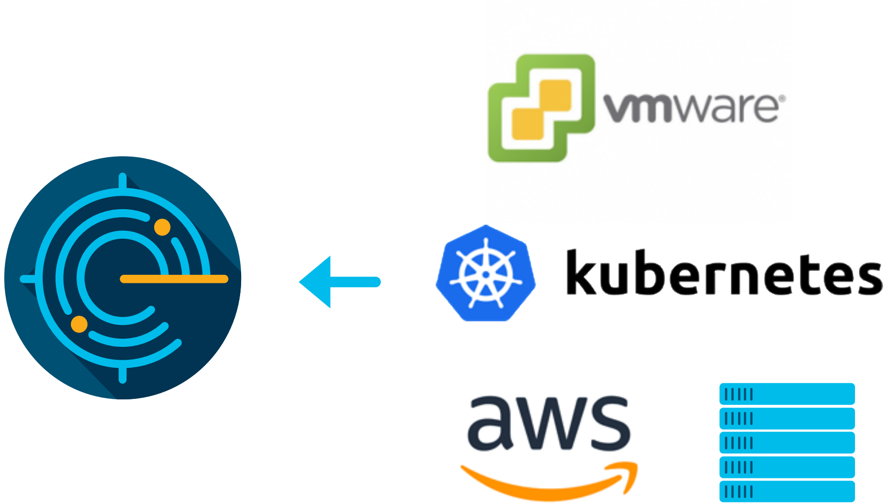
Zero Trust Policy: Workload Context

Get more context from:

- vCenter, for VM info
- Kubernetes or OpenShift, for container tags
- AWS, for security tags
- IP address management system, for IP/subnet info
- DNS servers, for domain name info

Using:

- Standard APIs to query info
- Periodic data collection
- Read-access only



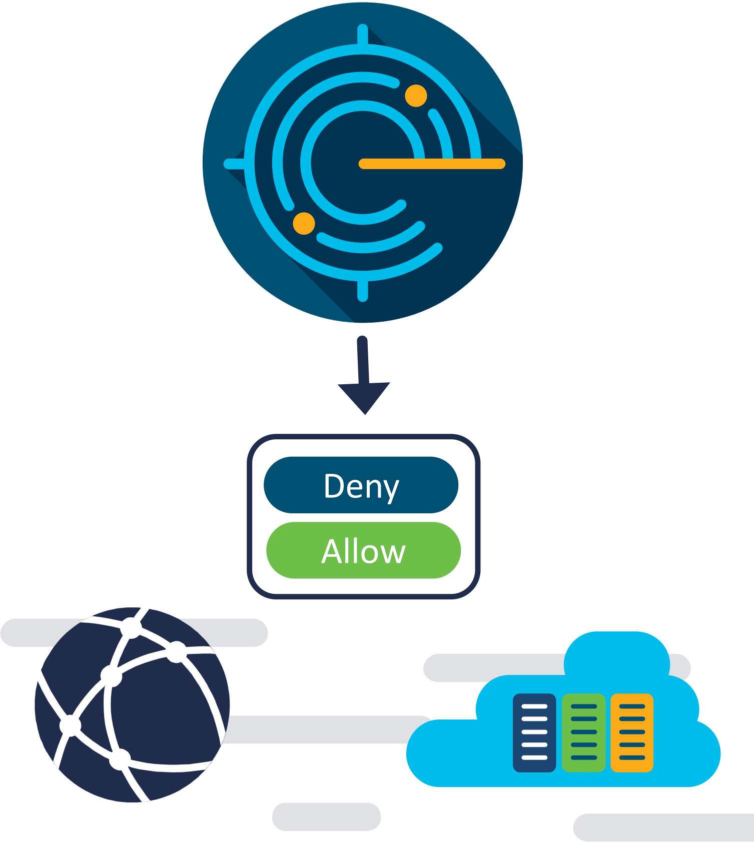
Workload: Enforce Trust-Based Access

Zero Trust Policy: Enforcing Micro-Segmentation Policies

Intent informs trust-based policies.

Intent is rendered as security rules
in native OS firewalls.

Converted into blacklist/whitelist rules
Example: Block non-production apps from talking to production apps.



Workload: Continuously Verify Trust

Continuous Monitoring & Response

Tetration’s proactive response

Baseline process behaviors for:

- Faster detection of indicators of compromise

Identify software vulnerabilities & exposures:

- Quarantine servers
- Block communication when policy violations are detected
- Reduce attack surface

Zero Trust for the Workforce

Pain Points

- Phishing
- Malware
- Credential Theft

Solution: Duo

With Duo Security, ensure only the right users and secure devices can access applications.

Workforce: Establish Trust

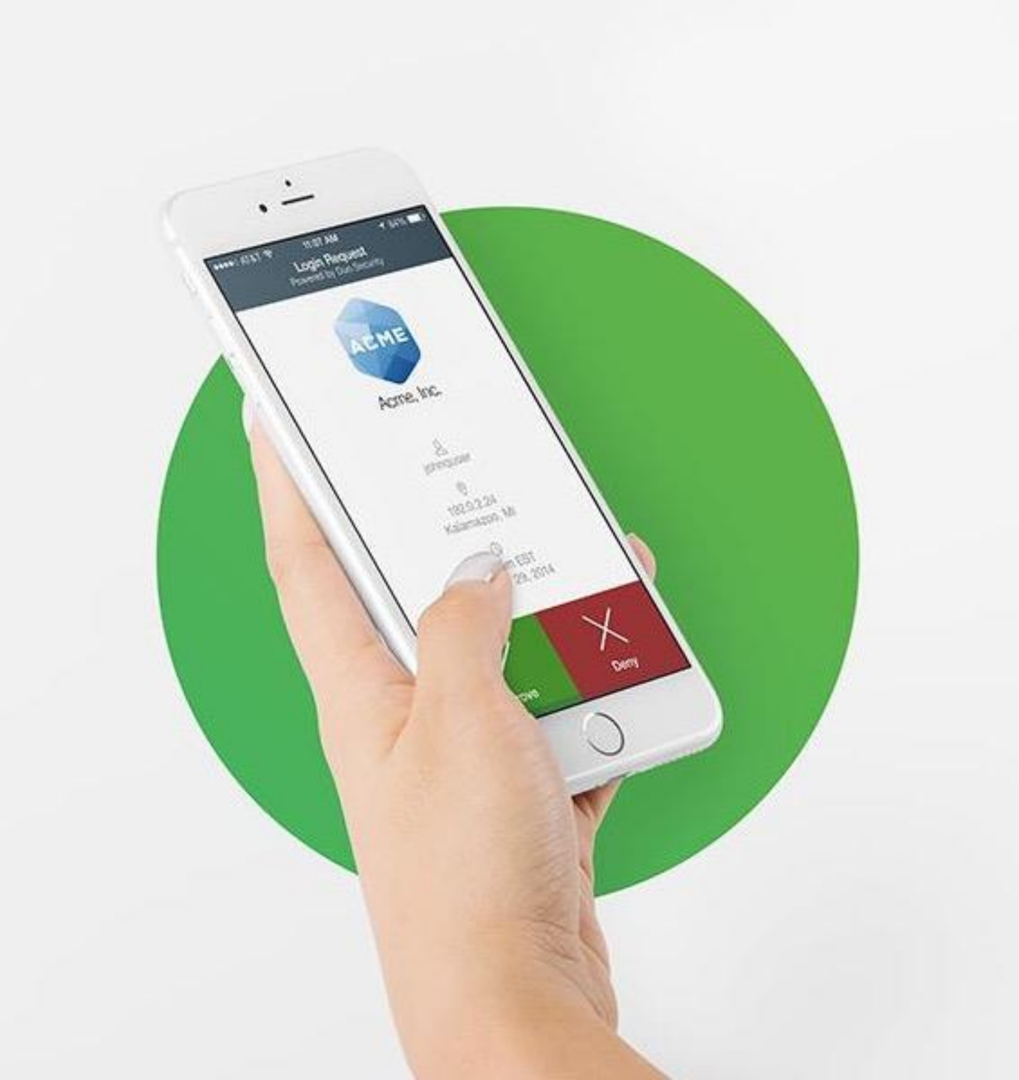
Verify User & Device Trust

Duo's Multi-Factor Authentication (MFA)

- Users authenticate in seconds – one-tap approval
- Scalable service that can be deployed in hours
- Natively integrates with all apps

Device Trust

- Check devices for vulnerable software & security features
- Identify managed vs. unmanaged
- Notify users of out-of-date devices



Workforce: Establish Trust

Broad MFA Options for Every Use

You can configure authentication:

- Per-application or user group
- Based on sensitivity of application data
- Or based on user scenario

Additionally, allow multiple options for ease of usability and flexibility:

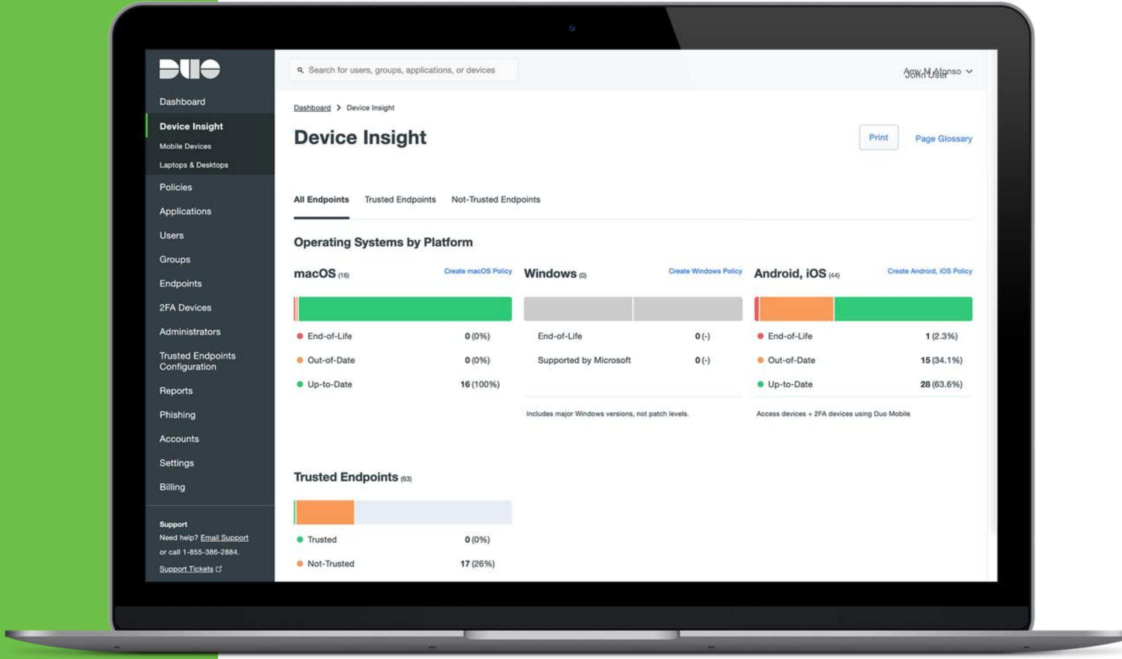
- Push notification
- Mobile passcode
- Phone
- SMS
- HOTP token
- U2F/WebAuthn

Workforce: Continuously Verify Trust

Monitor Risky Devices

Duo's Device Trust:

- At every login, Duo checks users' devices for security health & status
- Duo detects managed and unmanaged mobile & desktop devices
- Enforce device-based access policies to protect against vulnerable devices



Support
Need help? Email Support
or call 1-855-386-2884.
Support Tickets

Device Insight

Operating Systems by Platform

macOS (16)

● End-of-Life	0 (0%)
● Out-of-Date	0 (0%)
● Up-to-Date	16 (100%)

Windows (0)

End-of-Life	0 (-)
Supported by Microsoft	0 (-)

Includes major Windows versions, not patch levels.

Android, iOS (44)

● End-of-Life	1 (2.3%)
● Out-of-Date	15 (34.1%)
● Up-to-Date	28 (63.6%)

Access devices + 2FA devices using Duo Mobile

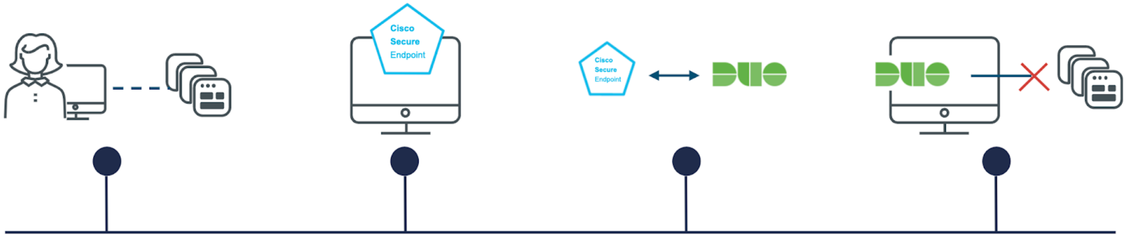
Trusted Endpoints (63)

● Trusted	0 (0%)
● Not-Trusted	17 (26%)

Never Trust, Always Verify

Device Hygiene

- Browser type and version
- Firewall state
- Endpoint security agent
- Compromised state
- OS version (major + minor)
- Disk encryption status
- System password set
- Others



Users use their devices to access application.

Cisco Secure Endpoint Running on the device detected malware.

Cisco Secure Endpoint tells Duo about the device infection.

Duo blocks that device from accessing apps.

Workforce: Establish Trust

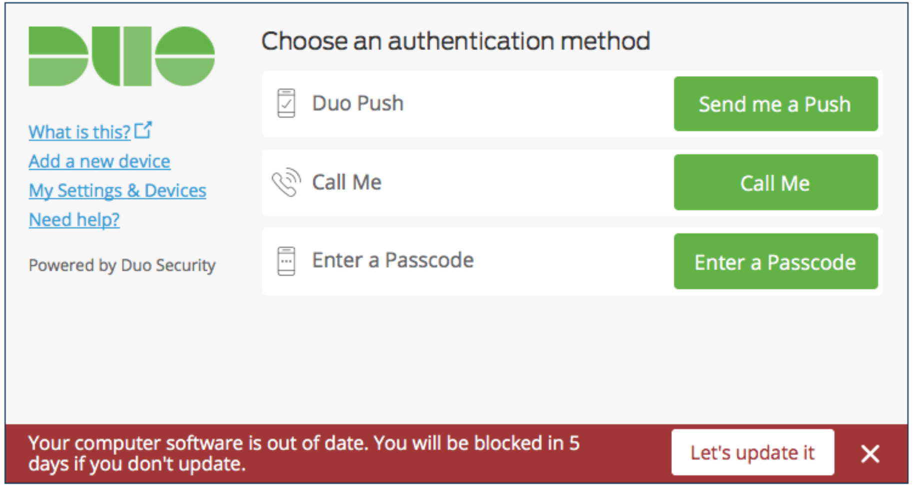
Inform Users

Improve your security posture & notify users of out-of-date devices

If users do not update by a certain day, the endpoints are blocked.

End users get notified about out-of-date OS, browsers, Flash and Java.

Quickly improve security without support desk help



Your computer software is out of date. You will be blocked in 5 days if you don't update.

Duo’s Adaptive Policies

Reduce friction and risk to applications with customizable, granular access policies

Role-Based Policy

Based on individual users or groups, enforce policies to determine who can access what applications.

Device-Based Policy

Allow access by only secure, up-to-date or managed devices, and prevent access by risky devices.

Location-Based Policy

Prevent authorized access to your applications from any geographic location.

Network-Based Policy

Grant or deny access based on a set of IP address ranges or from anonymous networks like Tor.

Protect Every Application

VPN RA	Multicloud	Email/MSFT	On-Prem	SSO	Custom
cisco	Google Apps	Office 365	Epic	Microsoft Azure	REST APIS
JUNIPer NETWORKS	salesforce	Outlook	ORACLE PEOPLESOFT	AD FS	WEB SDK
citrix	aws	Microsoft Remote Desktop Services	vmware Horizon View	okta	RADIUS
paloalto NETWORKS	box	Windows Server	>_SSH	Centrify	SAML
Pulse Secure	Dropbox	RRAS	Shibboleth	onelogin	OIDC

Learn more about application integrations

Thank You