Zero Trust Demystified

ThreatMatic™ Where Zero Trust network access meets seamless deployment, unparalleled ease of use, and ironclad security. Your advantage when responding to ransomware, malware threats, phishing attacks, DNS poisoning and so much more.

Get a Demo

Zero Trust Demystified

ThreatMatic™ strikes the perfect balance between security and user-friendliness. Our lightweight and powerful agent seemlessly managed from our modern admin-dashboard ensures that your most valuable assets are protected *instantaneously* - your advantage when responding to ransomware, malware threats, phishing attacks, DNS poisoning and so much more.

Simplicity Comes Standard

Enforce Zero Trust: Rooted in Identity

S/Channel secure access

On-demand micro-segmentation and app traffic control

✓ App and user ID foundation

✓ Cybersecurity Mesh Architecture (CSMA)

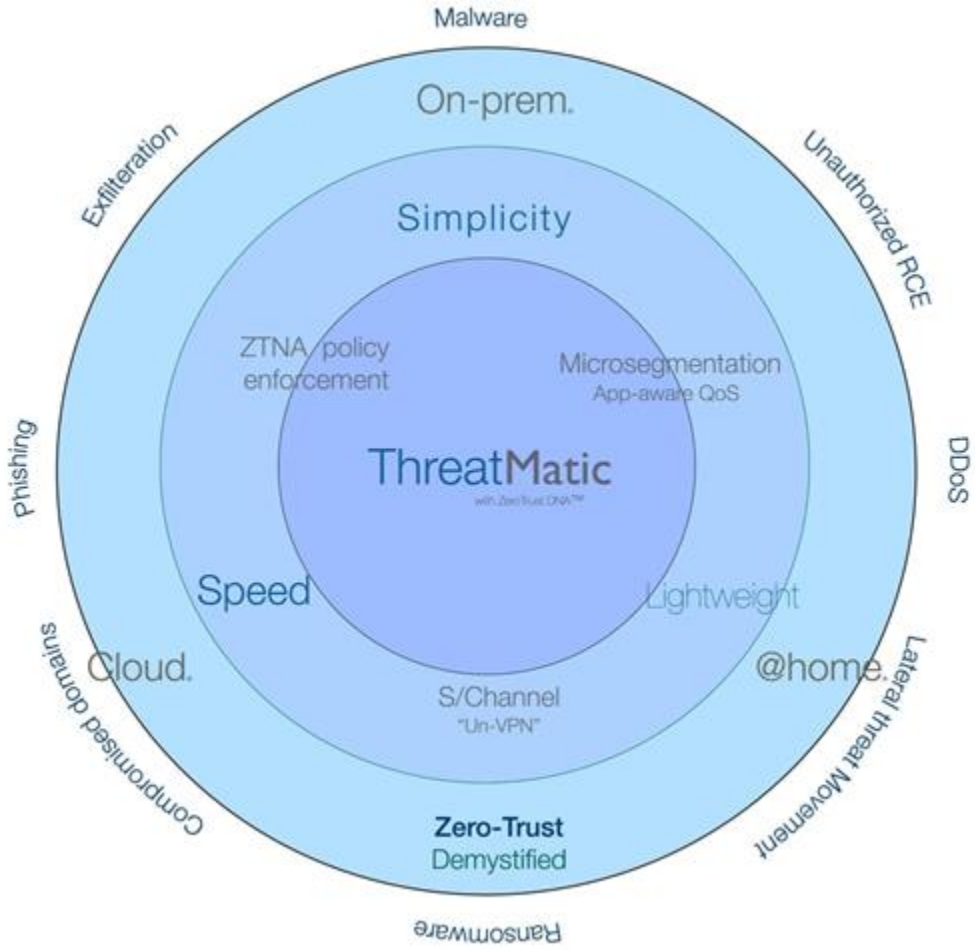
✓ Modern, elastic container-based platform

✓ Self-healing and headless operation

✓ Autoscaling on-premises or in the cloud

✓ De/identified authentication and minimal data retention

✓ Extensive, extensible ML metrics model and APIs

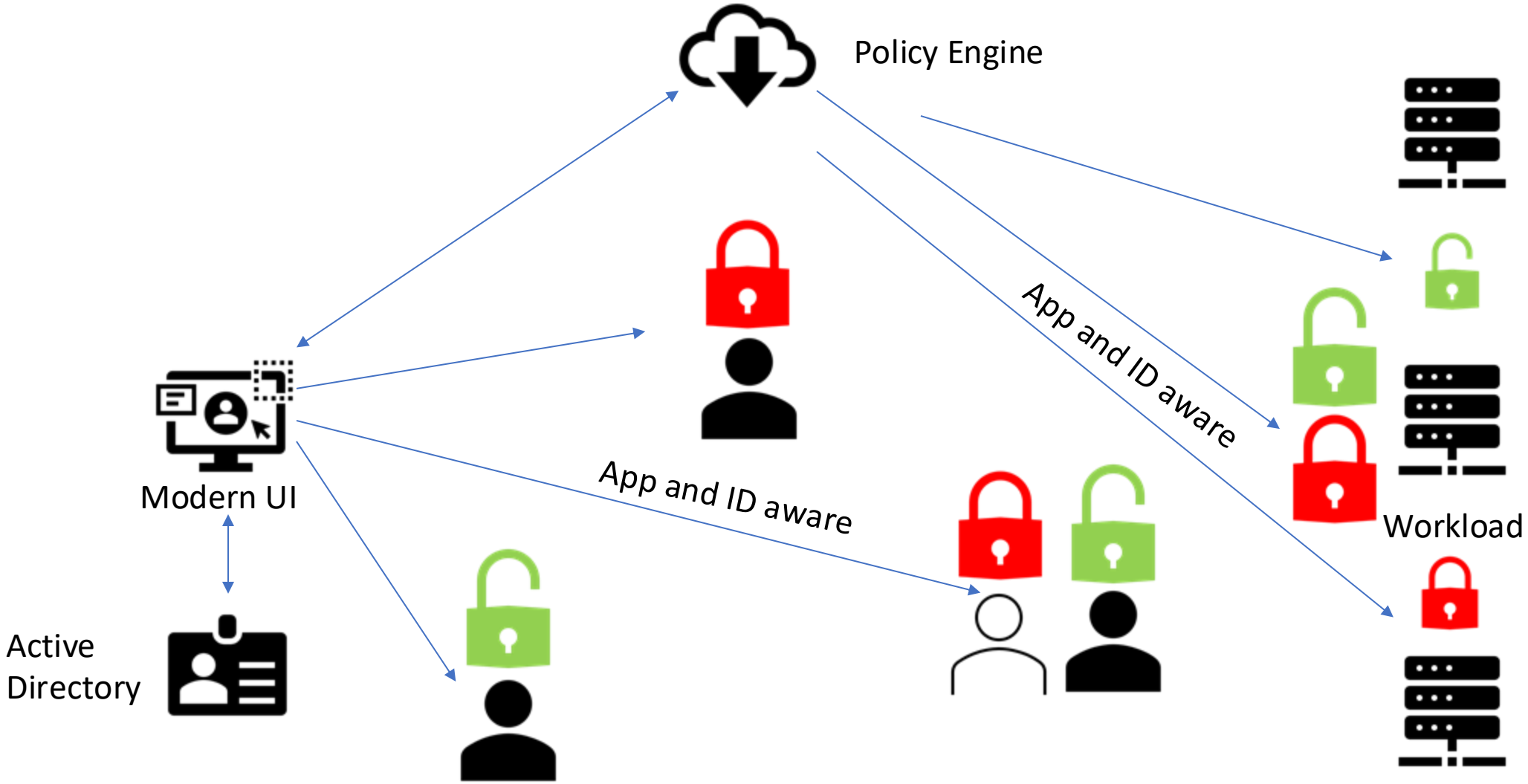


Cybersecurity:
(traditional)

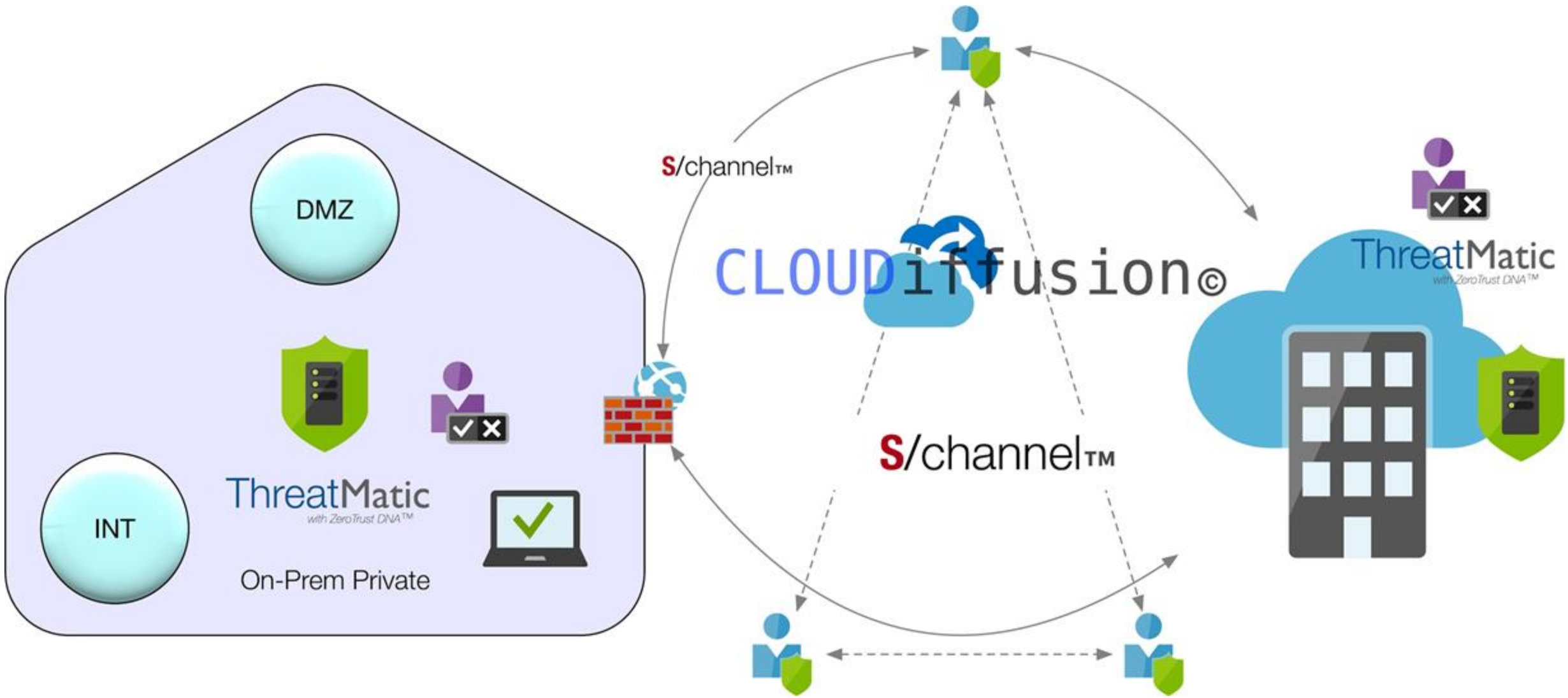
- Limited perimeter protection
- Biased for external threats
- Unilateral posture
- Vulnerable to zero-day attacks
- Malware can diffuse east-west
- Single point of enforcement
- “Trusted” to “Trusted” blindspot

- App and ID aware zero trust model
- Flexible/ALE micro-segmentation
- Cybersecurity Mesh Architecture
- Rules based on user/group/Device
- S/Channel “secure channel”
- Malware countermeasures
- Neutralize Zero-Day attacks

ThreatMatic
with ZeroTrust DNA™



ThreatMatic
with ZeroTrust DNA™



	ThreatMatic	Illumio	Microsoft	Others
User ID based rules	Yes	Yes	Yes	No
Group ID based rules	Yes	Yes	No	No
Device based rules	Yes	No	Yes	No
Windows package based rules	Yes	No	No	No
Any AD User/Group	Yes	Yes	No	No
Extra-AD device groups	Yes	No	No	No
Name resolution policy control	Yes	No	No	No
Inline bandwidth control QoS	Yes	No	No	No
Simple ergnomics UI	Yes	No	No	No
DNS over HTTP	Yes	No	No	No
DNS blacklisting	Yes	No	No	No
TrueZeroTrust default deny	Yes	No	No	No
Selective traffic steering	Yes	No	No	No
FlexWeight rule ordering	Yes	No	No	No
Granular ingress control at endpoints	Yes	No	No	No
TrustZero server and workload	Yes	No	No	No
Configurable observability	Yes	No	Yes	No
Splunk integrated	Yes	No	No	No
InfluxDB integrated	Yes	No	No	No
On-demand rules sync	Yes	No	No	No
Featherweight agent	Yes	No	No	No
Headless non-stop forwarding	Yes	No	Yes	No
mTLS gRPC channels customizable	Yes	No	No	No
Flexible policy engine placement	Yes	Yes	No	No
Cloudnative design	Yes	No	No	No

ThreatMatic
with ZeroTrust DNA™

	ThreatMatic	Illumio	Microsoft	Akamai	Zscaler	Palo Alto	FortiGate	CrowdStrike	Perimeter 81	Nordlayer
User ID based rules	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes*	Yes*
Group ID based rules	Yes	Yes	Yes	No	Yes	Yes	Yes*	Yes	Yes*	Yes*
Device based rules	Yes	No	Yes	No	No	No	No	No	No	No
Micro-segmentation	Yes	No	No	No	No	No	No	No	No	No
Windows package* based rules	Yes	No	No	No	No	No	No	No	No	No
Any AD User/Group	Yes	Yes	No	No	Yes*	Yes*	No	Yes	Yes*	No
Extra-AD device groups	Yes	No	No	No	No	No	No	No	No	No
Name resolution policy control	Yes	No	No	No	No	No	No	No	No	No
Inline bandwidth control QoS	Yes	No	No	No	No	No	No	No	No	No
Simple ergnomics UI	Yes	No	No	No	No	No	No	No	No	No
DNS over HTTP rules	Yes	No	No	No	No	No	No	No	No	No
DNS blacklisting	Yes	No	No	No	Yes	Yes	No	Yes	No	No
Default deny posture	Yes	No	No	No	No	No	No	No	No	No
Selective traffic steering	Yes	No	No	No	No	No	No	No	No	No
FlexWeight rule ordering	Yes	No	No	No	No	No	No	Yes	No	No
Granular ingress control at endpoints	Yes	Yes	No	No	No	No	No	Yes	No	No
TrustZero server and workload	Yes	No	No	No	No	No	No	No	No	No
Configurable observability	Yes	No	Yes	No	Yes	Yes	No	Yes	No	No
Splunk integrated	Yes	No	No	No	No	Yes	Yes	Yes	No	No
InfluxDB integrated	Yes	No	No	No	No	No	No	No	No	No
On-demand rules sync	Yes	No	No	No	Yes	Yes	No	Yes*	No	No
Featherweight agent	Yes	No	No	No	No	No	No	No	No	No
Headless non-stop forwarding	Yes	No	Yes	No	No	No	No	No	No	No
mTLS gRPC channels customizable	Yes	No	No	No	No	No	No	No	No	No
Flexible policy engine placement	Yes	Yes	No	No	No	No	No	No	No	No
Cloudnative design	Yes	No	No	No	No	No	No	No	No	No
sChannel Proxy	Yes	No	No	No	No	No	No	No	No	No
SideFX Threat Intelligence	Yes	No	No	No	No	No	No	No	No	No

ThreatMatic
with ZeroTrust DNA™

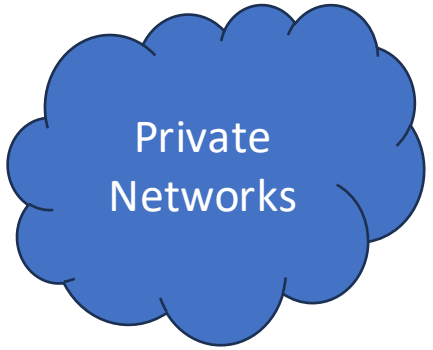
Use Cases: What can ThreatMatic with ZeroTrust DNA™ do for you?

- Defend against malicious DNS records and nameservers
- Simple policy against ID and App by user/group/device/device-group
- Identity and app/exe based microsegmentation
- S/Channel remote access (replaces VPN)
- Rapid response to malware attacks (block any app/exe everywhere)
- App security metrics with ML and AI autopiloting on roadmap
- Ingress posture control for servers and workloads
- App aware performance (QoS) on egress
- Detect anywhere and protect everywhere posture

Application blocking by user, group, device, device-pool

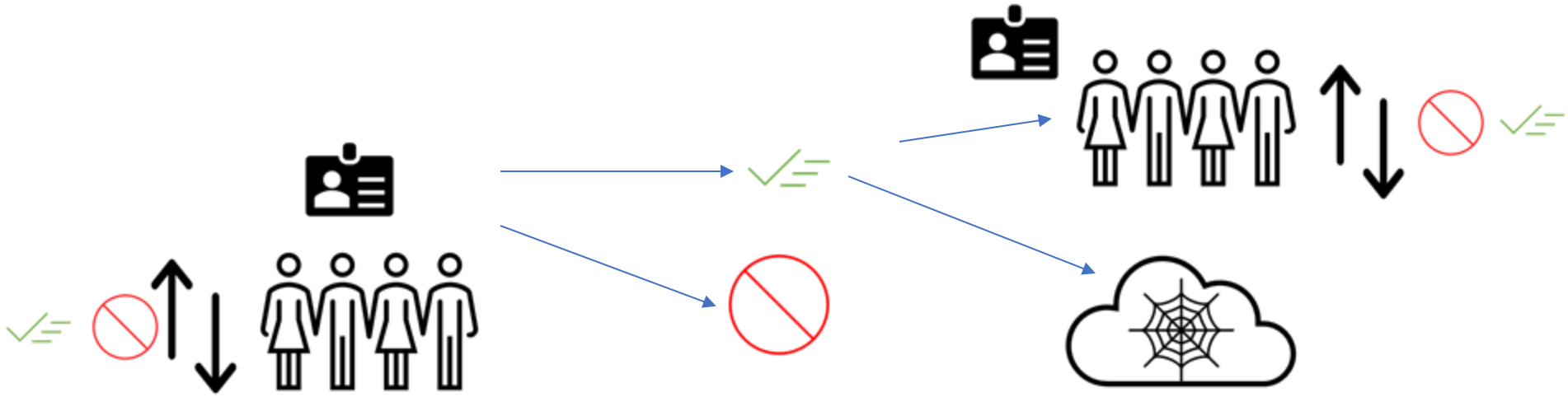
Control access precisely with app or package ID, user/group/device ID, any combination of both, at various layers of the network stack. Generate deep insights into traffic patterns and posture with drill-down analytics, ready for machine learning and auto-piloting actions.

S/channel remote access without VPN



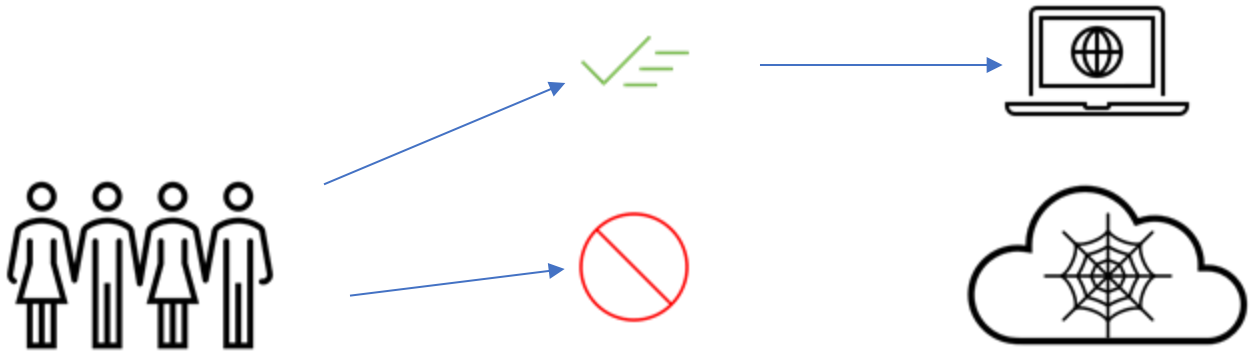
Control access precisely with app or package ID, user/group/device ID, any combination of both, at various layers of the network stack. Generate deep insights into traffic patterns and posture with drill-down analytics, ready for machine learning and auto-piloting actions.

Hostname or IP based fine grained edge egress control



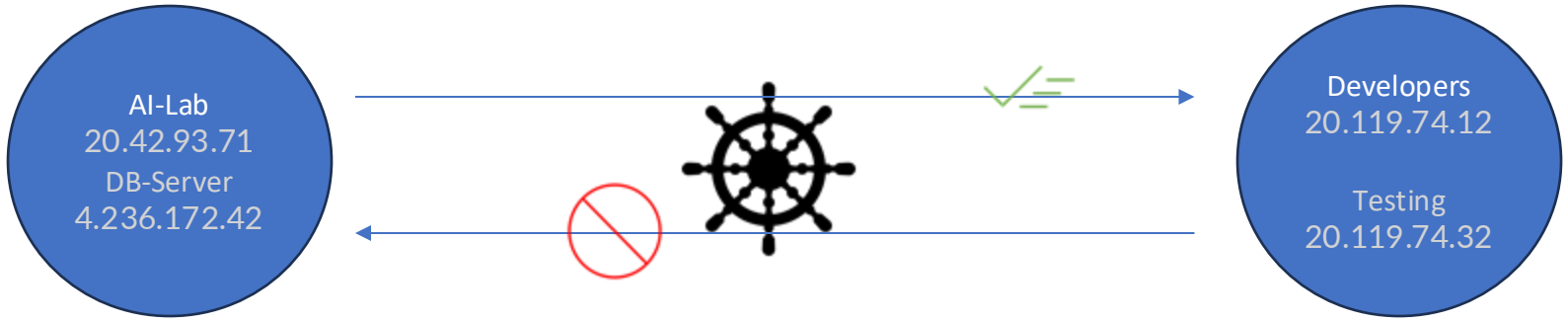
Applications, users and groups, device-groups are restricted to communicate to safe destinations only, east-west granular segmentation which is especially powerful in a multi-tenant environment.

Default-deny Posture



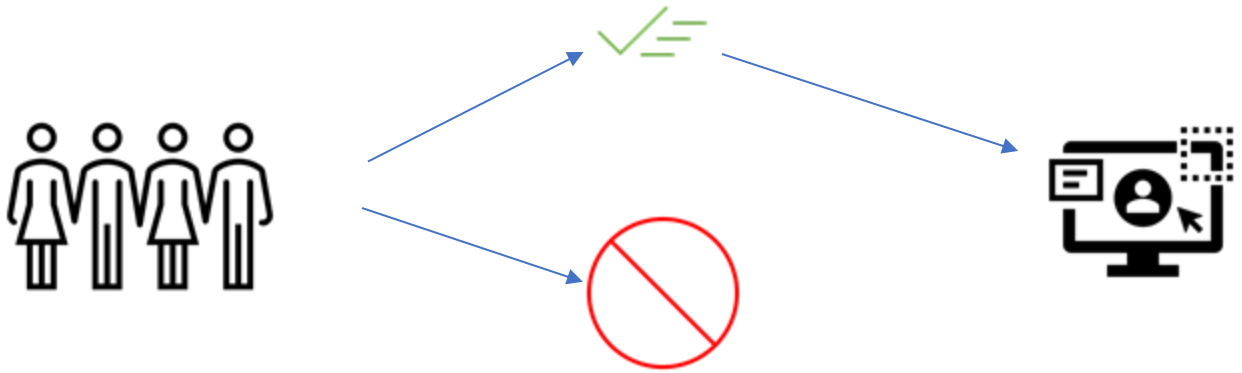
All traffic is denied by default. Only explicitly permitted applications and destinations will be permitted. Think of it a shift-left approach to iron-clad security against malware and zero-day threats.

Microsegmentation policy by user, group, device, device pool



Control host to host traffic by user/group/device/device-pool, combine with b/w management for max security and optimal performance. Cordon off any arbitrary group of endpoints and create secure islands of users and workloads.

Control software updates and access to Cloud



To counter threats posed by corrupted or compromised automatic software updates, deploy rules to block at a granular level.