2022-10-13

Your Data Is Everywhere: Your Security Should Be Too

Steve Riley
Field CTO
sriley@netskope.com
linkedin.com/in/steverileysea

netskope

Menu

Some interesting data

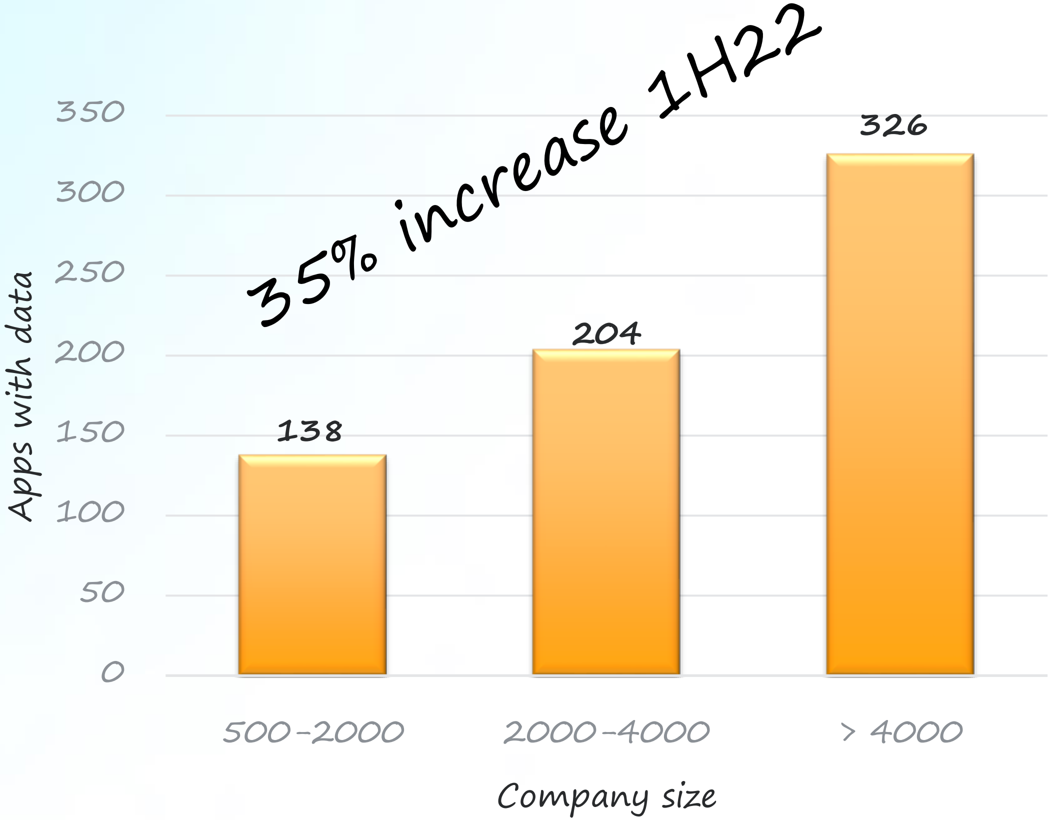
Context is the new perimeter

Dimensions of defenses

Recommendations

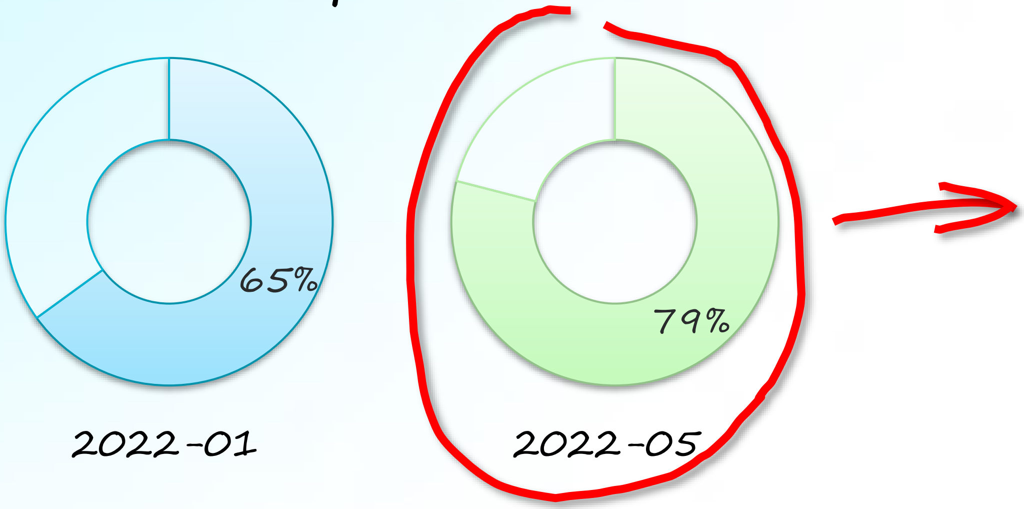
Some Interesting Data

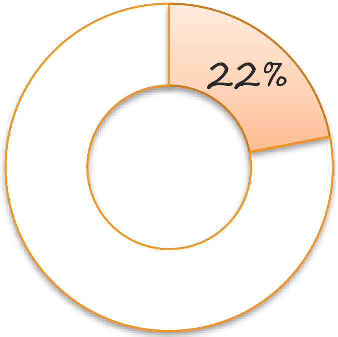
Big surprise: moar cloud everywhere



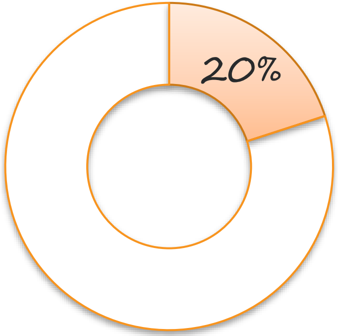
Big surprise: moar people, moar stuff

Population





Personal apps



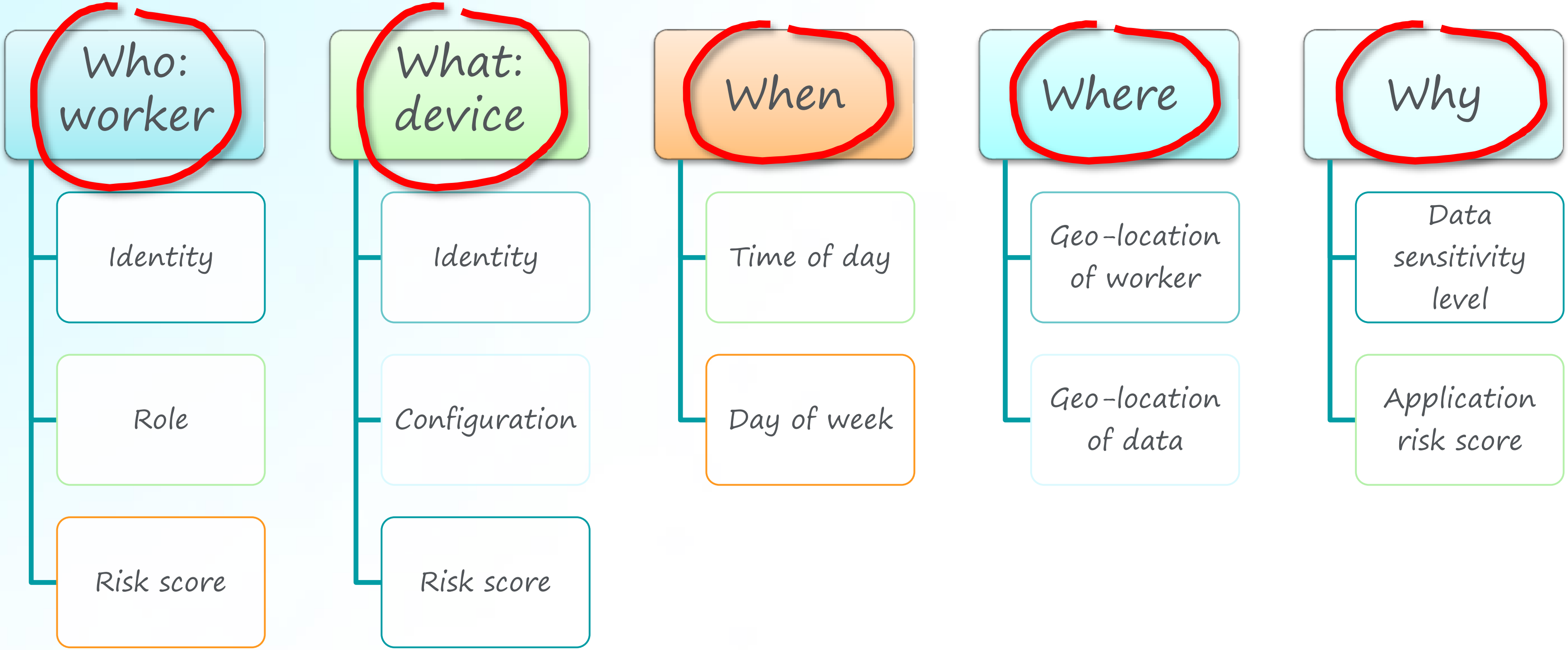
Personal apps before leaving!

netskope

Context Is The New Perimeter

netskope

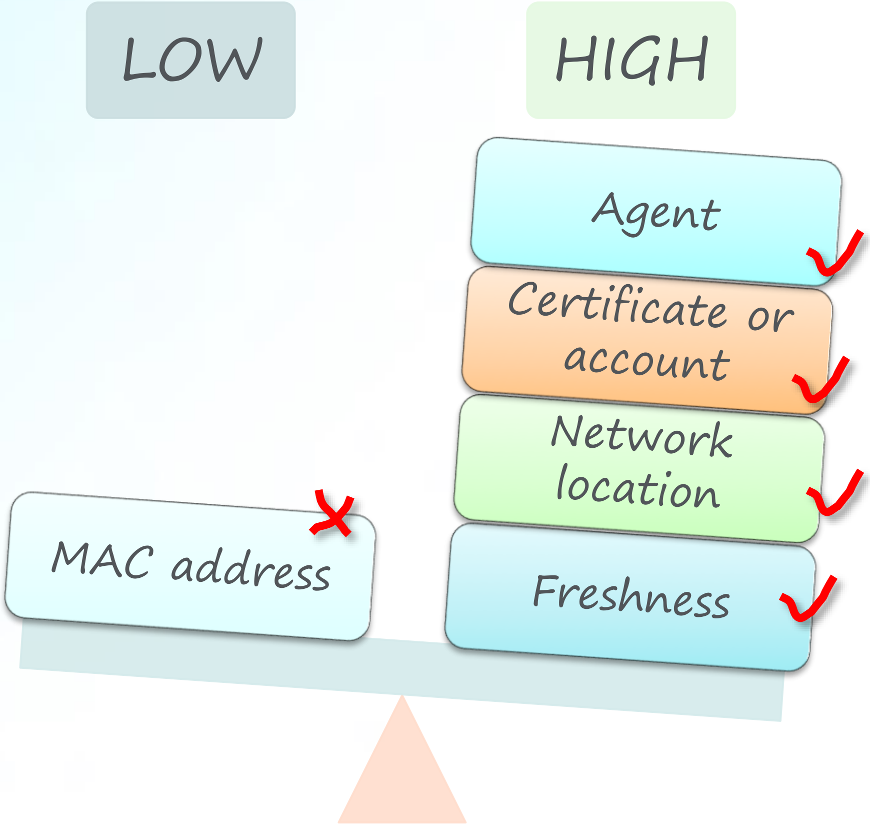
Signals indicating context



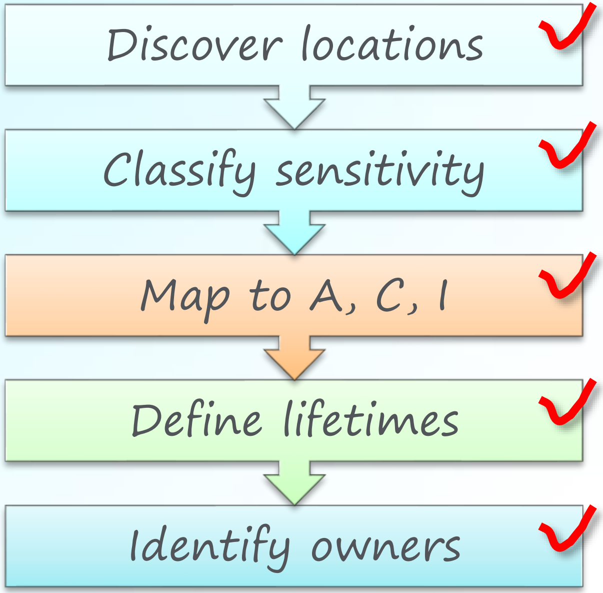
- Who: worker
  - Identity
  - Role
  - Risk score
- What: device
  - Identity
  - Configuration
  - Risk score
- When
  - Time of day
  - Day of week
- Where
  - Geo-location of worker
  - Geo-location of data
- Why
  - Data sensitivity level
  - Application risk score

netskope

Example: device context



Data context



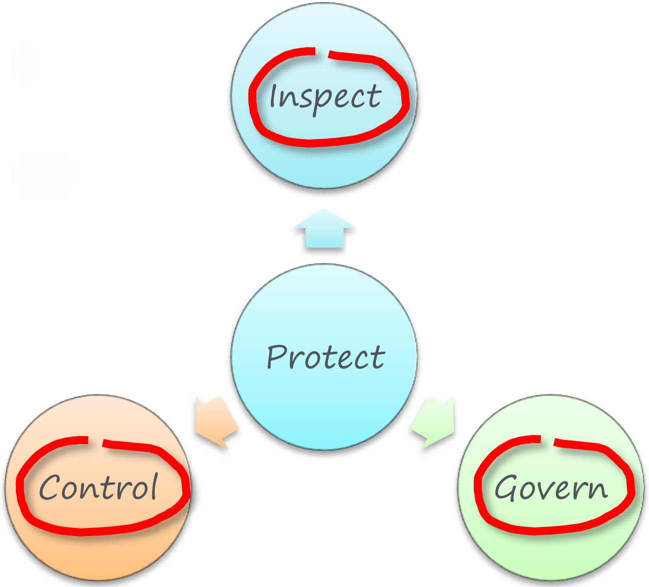
Discover locations ✓

Classify sensitivity ✓

Map to A, C, I ✓

Define lifetimes ✓

Identify owners ✓



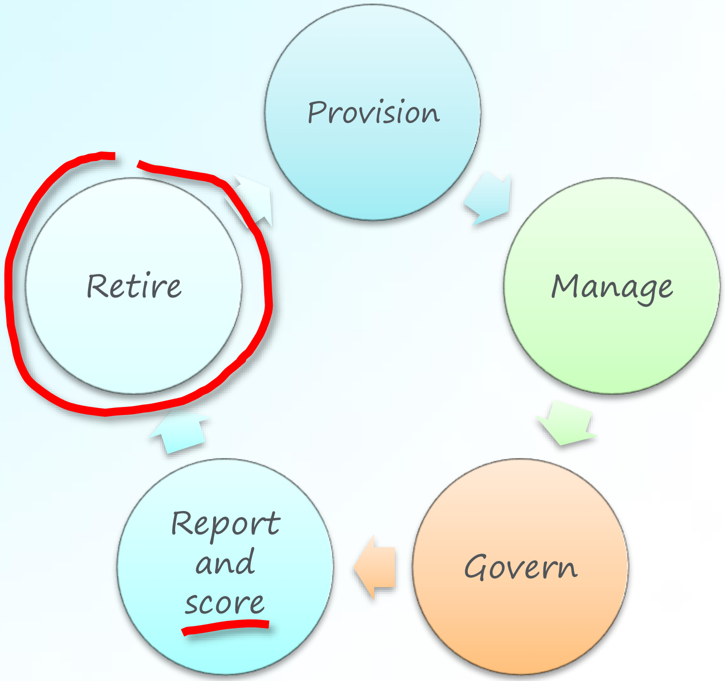
Inspect

Protect

Control

Govern

Identity context



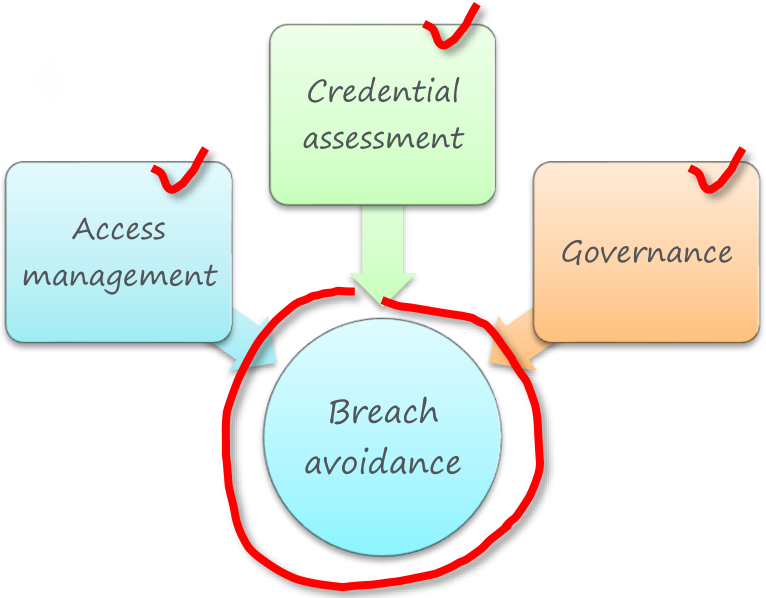
Provision

Manage

Govern

Report and score

Retire



Access management

Credential assessment

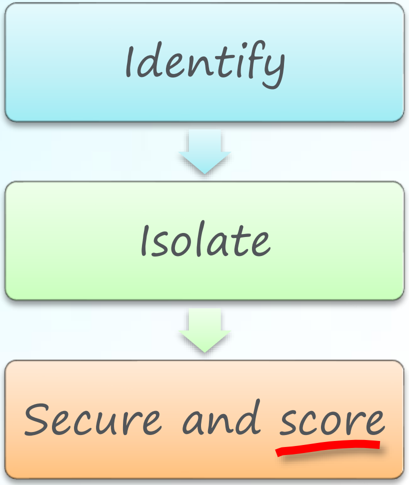
Governance

Breach avoidance

netskope

Endpoint context

MANAGED DEVICES



Identify

Isolate

Secure and score

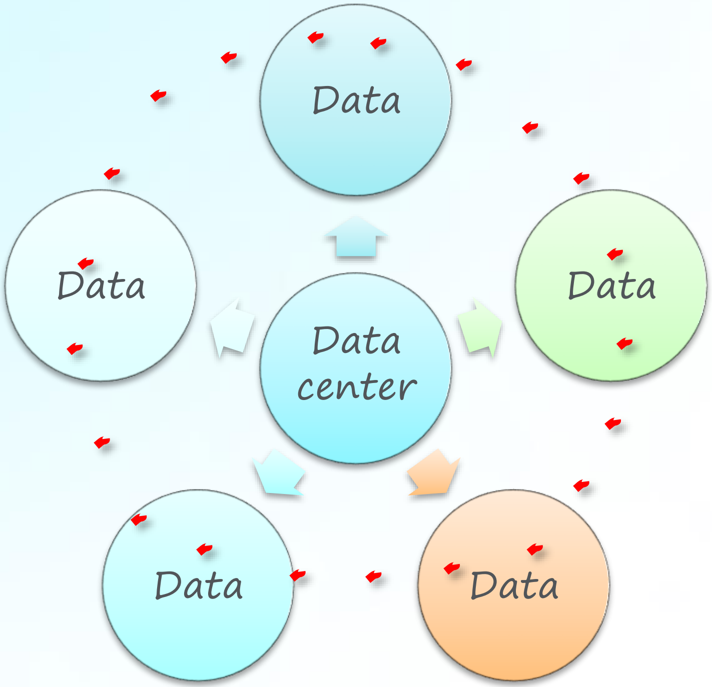
UNMANAGED DEVICES

Public	Private	Confidential
• Full ✓	• Read-only ✓	• None ✓

Application context

- Current inventory ✓
- Preferred/proposed inventory ✓
- Mapping to A, C, I ✓
- Interactions/transaction flows, all directions ✓
- External communications and access ✓
- Risk assessment and score ✓

Network context



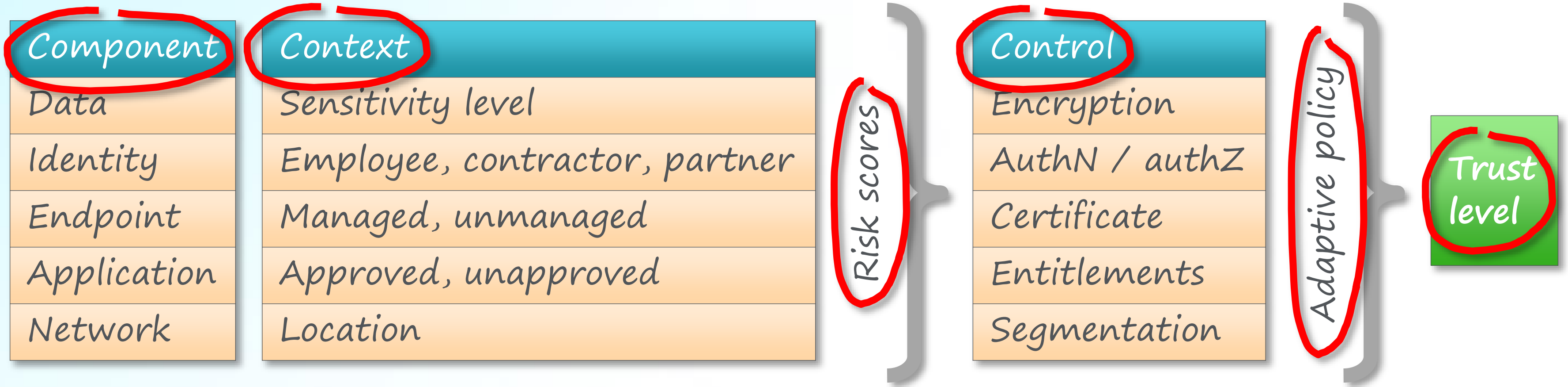
OFF-NET

- Proxies
- Agents

ON-NET

- Default deny
- No trust zones
- Micro-segmentation

context + scores = trust_level



Component	Context
Data	Sensitivity level
Identity	Employee, contractor, partner
Endpoint	Managed, unmanaged
Application	Approved, unapproved
Network	Location

Risk scores

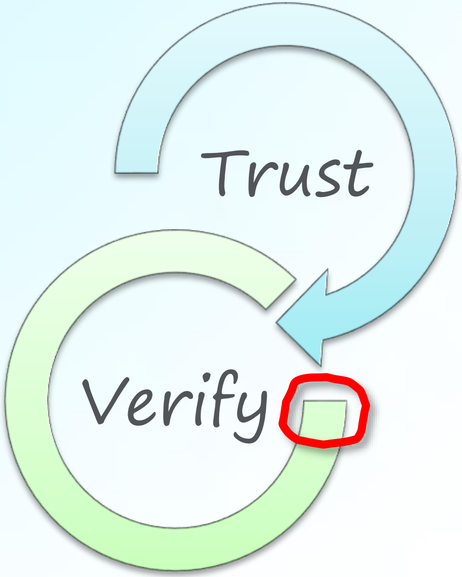
Control
Encryption
AuthN / authZ
Certificate
Entitlements
Segmentation

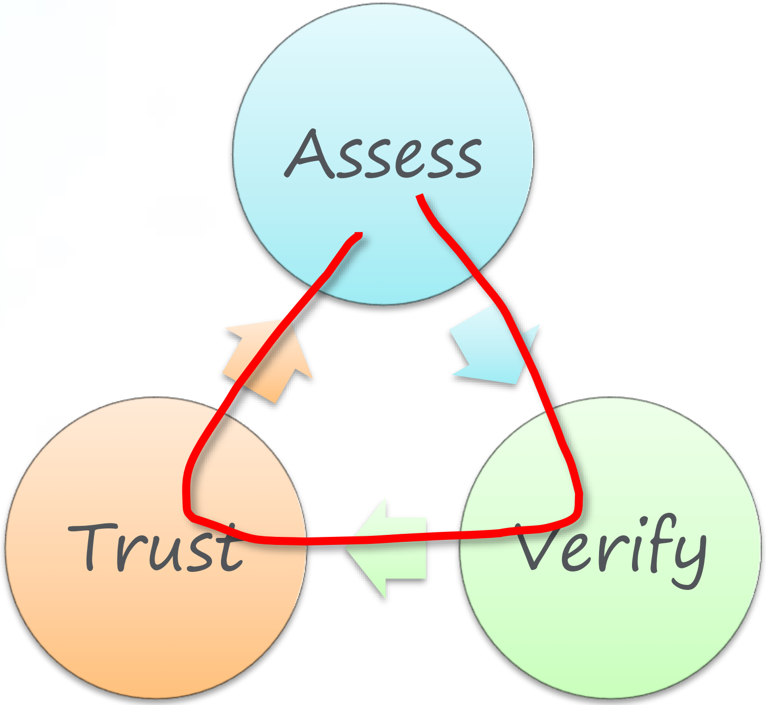
Adaptive policy

Trust level

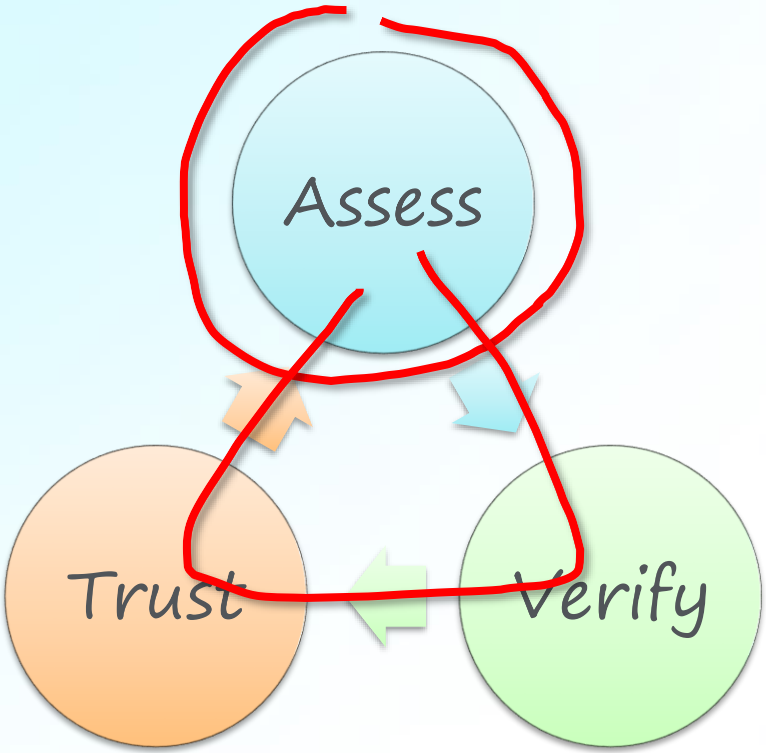
netskope

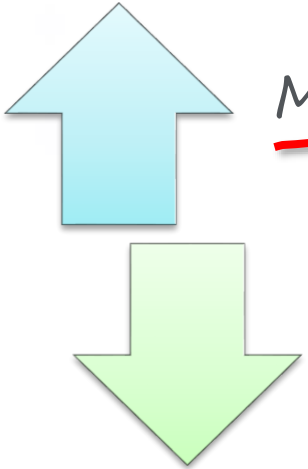
The trust problem





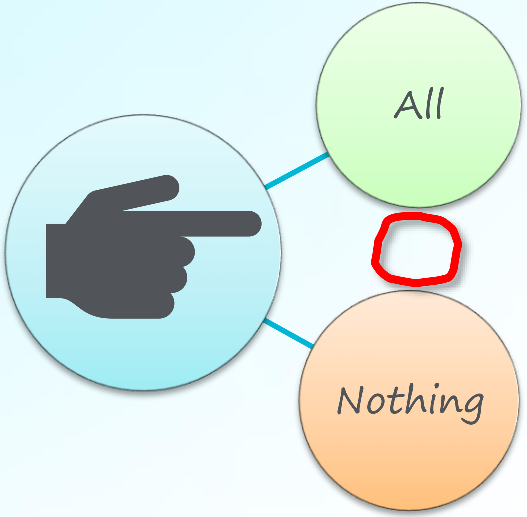
Continuous adaptive trust

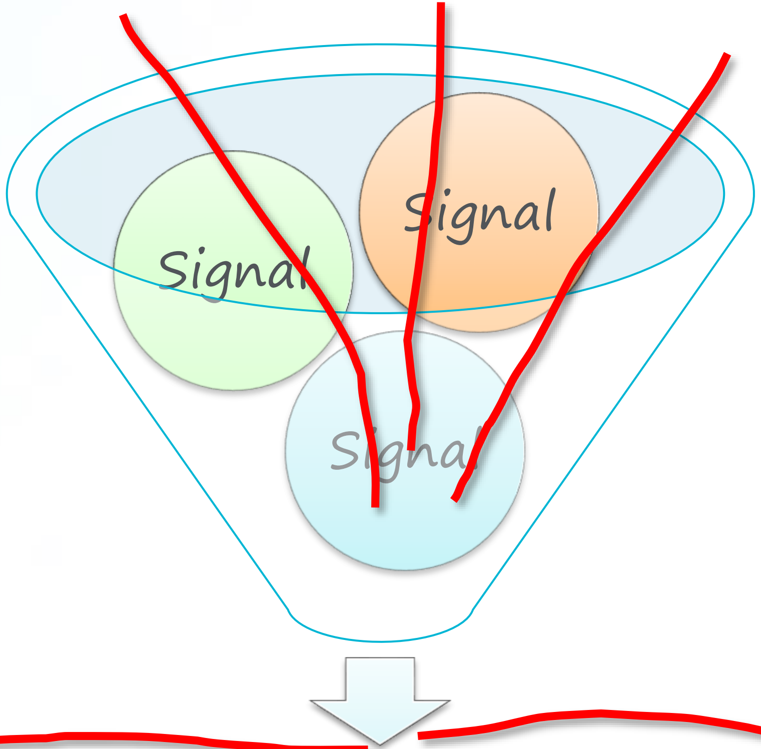




netskope

Adaptive access





Permit | Restrict | Redirect | Coach | Deny

Per application

Dimensions Of Defenses and Recommendations

Goals

Neutralize threats

- Deflect attackers from your assets

Protect data

- Control where information goes

Demonstrate good governance

- Provide evidence to boards, auditors, regulators, customers

SaaS Threats

Poor configurations

- Defaults favor ease of use
- Auditing and reporting aren't automatic

Easy to provision

- And therefore easy to overlook

Too much sharing

- Inadvertent > malicious
- Increases when a person plans to quit

Popular among attackers

- Stolen credentials grant access elsewhere

SaaS Protections

Standardize security posture

- Assess, refine, and document configuration (access, audit)
- Define policy for access by unmanaged devices

Monitor unmanaged application use

- Coach users toward approved applications
- Require business justification and business unit risk acceptance
- Limit actions in medium-risk applications; block high-risk applications

Establish sharing policy

- Disable default external sharing
- Implement self-service external sharing provision with expiration
- Detect uncharacteristically excessive downloads and uploads

Move beyond passwords

- Eliminate "attractiveness" to attackers

SaaS Further governance

Compliance

- Provider assessment != compliant usage
- Verify service can be used in ways that allow regulatory compliance, including data residency

Business continuity

- Confirm data and metadata ownership
- Enable retention capabilities
- Determine whether to investigate backup options

netskope

Web Threats

Browser attacks

- Takeovers: cookies, sessions, tokens
- MITM; leaky extensions; local proxies

Risky sites

- Ransomware and malware delivery
- Content that violates policies and laws

Email attacks

- Forged or unauthenticated origins
- Social engineering

netskope

Web Protections

Protect browsers

- Disallow unmonitored access to the non-business web
- Implement forms of isolation

Control destinations

- Verify safety and validity of every domain and URL
- Scan all downloads for presence of malware
- Scan all uploads for presence of sensitive information
- Constrain or block activities on suspicious sites

Harden email

- Quarantine unauthenticated messages
- Limit or block external delivery of sensitive information

Private Threats

Exposed applications and services

- "Open firewall for X" removes most protection for X
- Connect-then-authenticate is a bad internet pattern

Remote entry (implicit trust)

- Full network connectivity facilitates lateral movement
- Third-party access is difficult to govern

Poor configuration

- IaaS defaults are better, but mistakes still happen
- IaaS access management can be confusing

netskope

Private Protections

Hide your assets

- Attackers can't compromise what they can't find
- A better pattern: authenticate (elsewhere) then connect

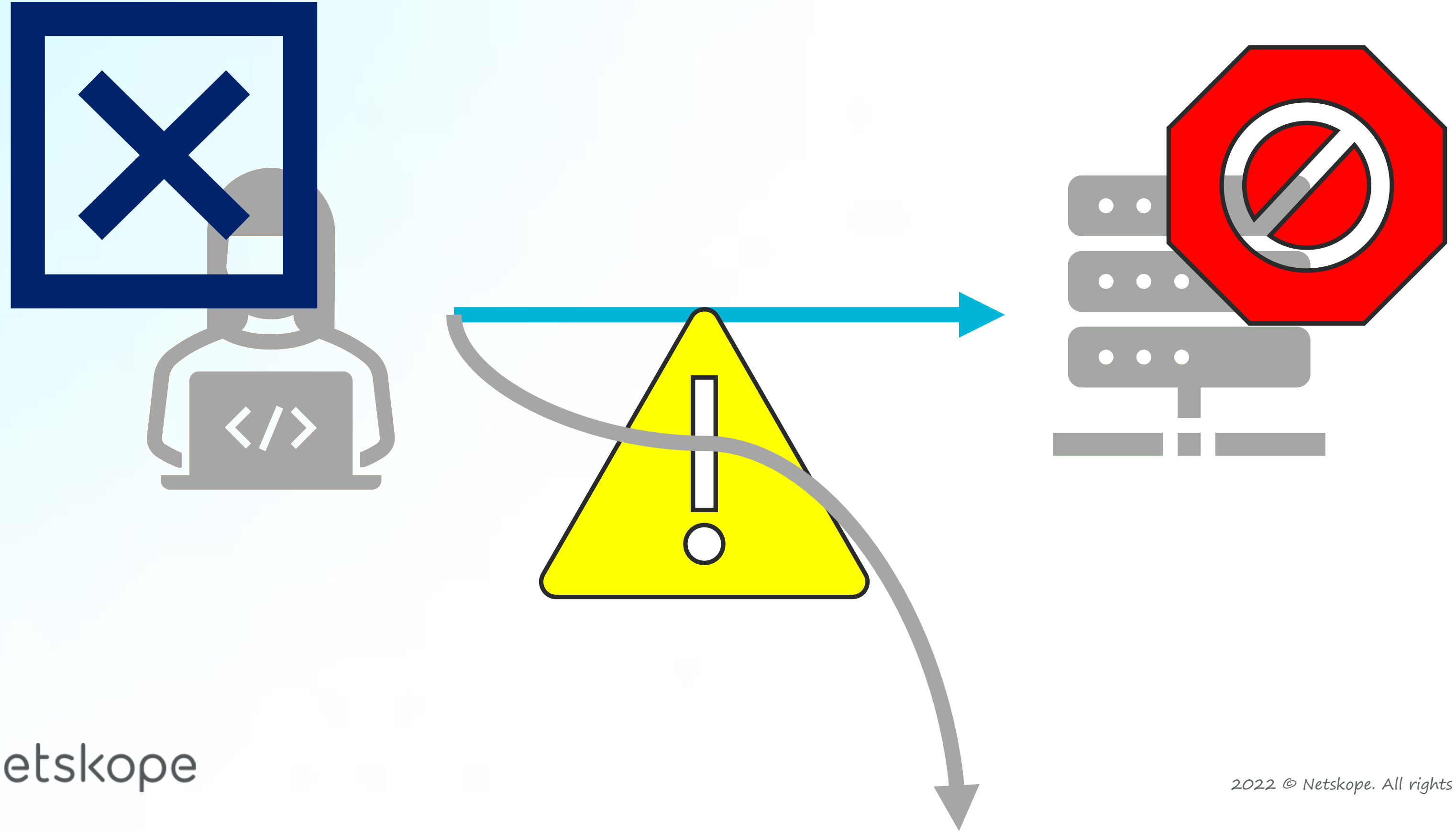
Precise access (explicit trust)

- Connect users to applications, not networks
- Adjust access according to context and content
- Monitor for suspicious activity
- Develop processes for onboarding and offboarding

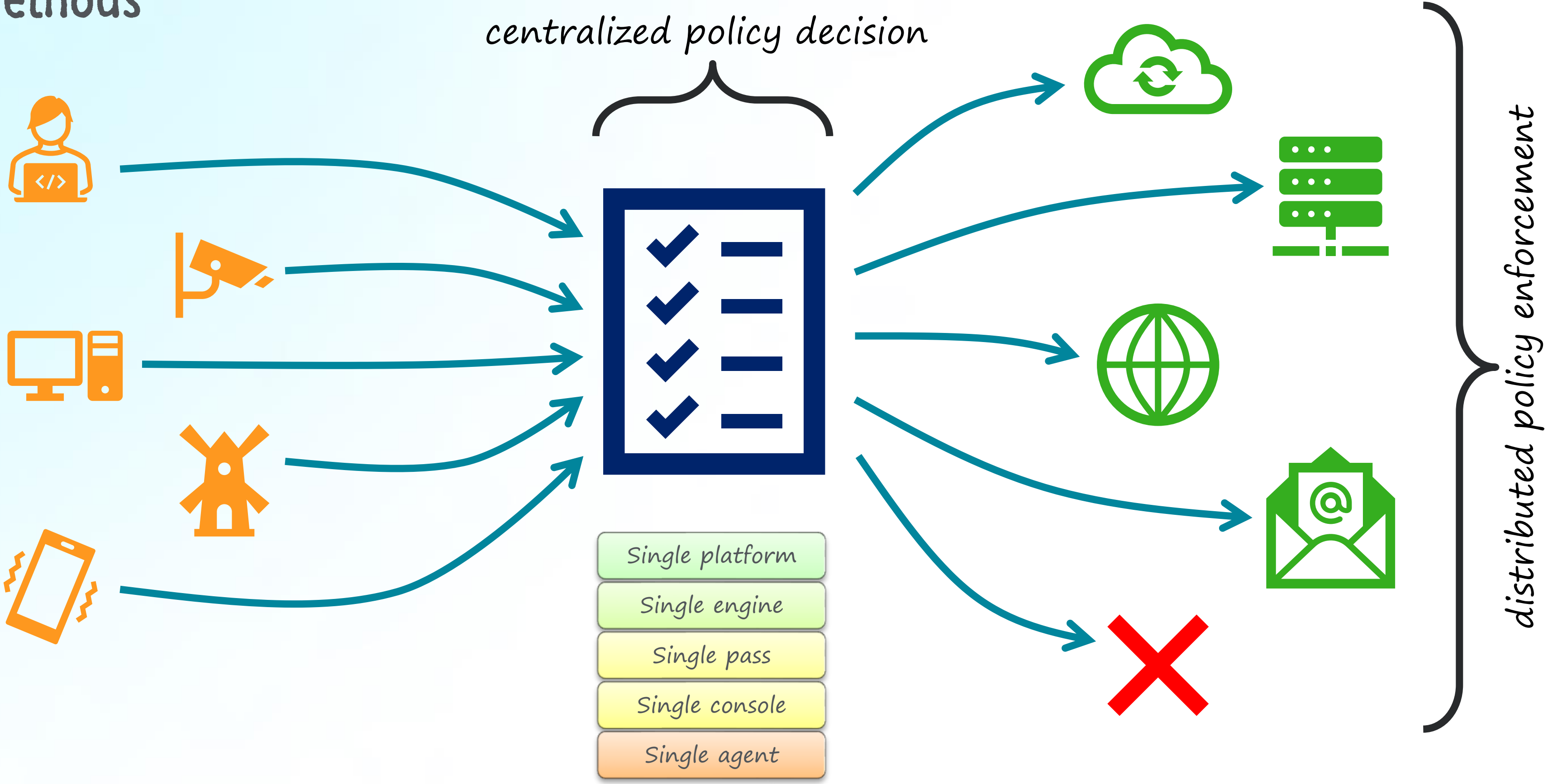
Standardize security posture

- Assess, refine, and document configuration (esp. permissions)
- Routinely scan for sensitive information and vulnerable code

Methods



Methods



Single platform

Single engine

Single pass

Single console

Single agent

2022-10-13 +

Thank You

Steve Riley
Field CTO
sriley@netskope.com
linkedin.com/in/steverileysea

netskope