RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PART1-T08**

Why Zero Trust Network Access is Broken, and How to Fix It

Kumar Ramachandran

SVP Products
Palo Alto Networks

Josh Dye

SVP, Information Security
Jefferies

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

WORK IS
AN ACTIVITY, NOT A PLACE

APPS ARE EVERYWHERE

80% of organizations have a hybrid cloud strategy, and the average organization uses **110 SaaS apps.**

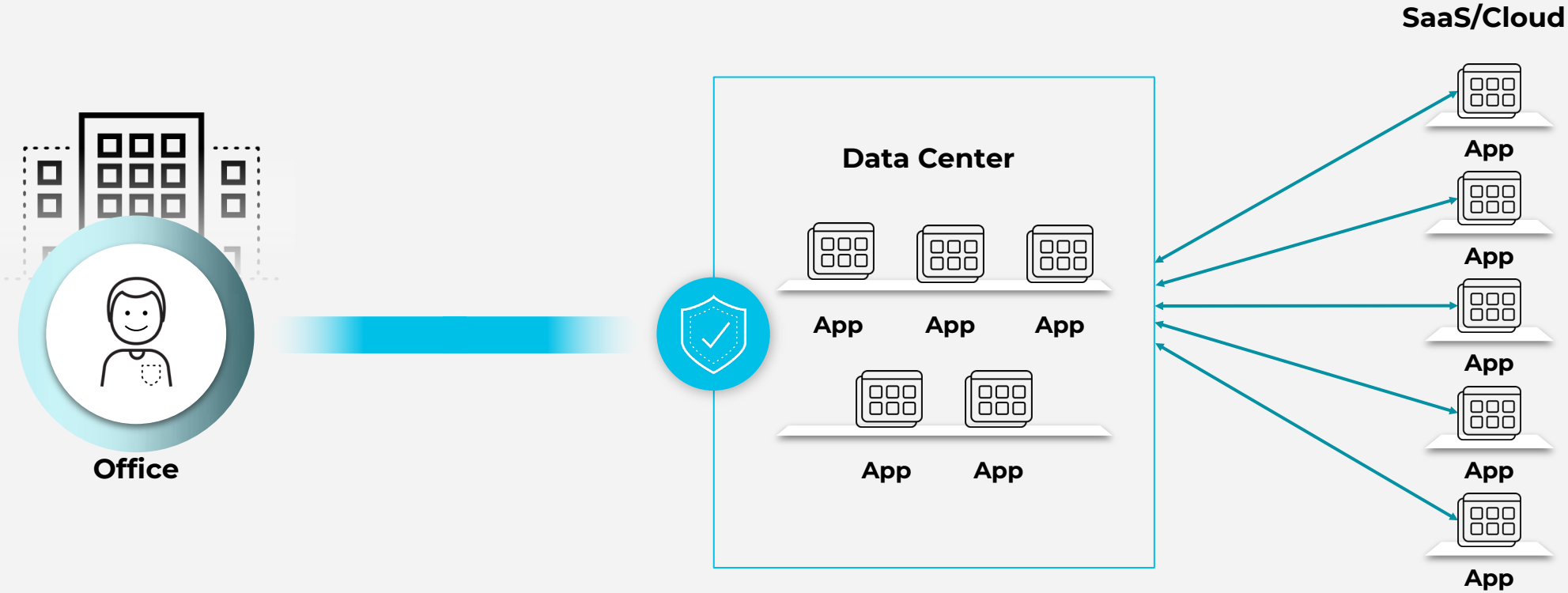
(FLEXERA, 2021; STATISTA, 2021)

USERS ARE EVERYWHERE

76% of employees want to be hybrid, even after the pandemic.

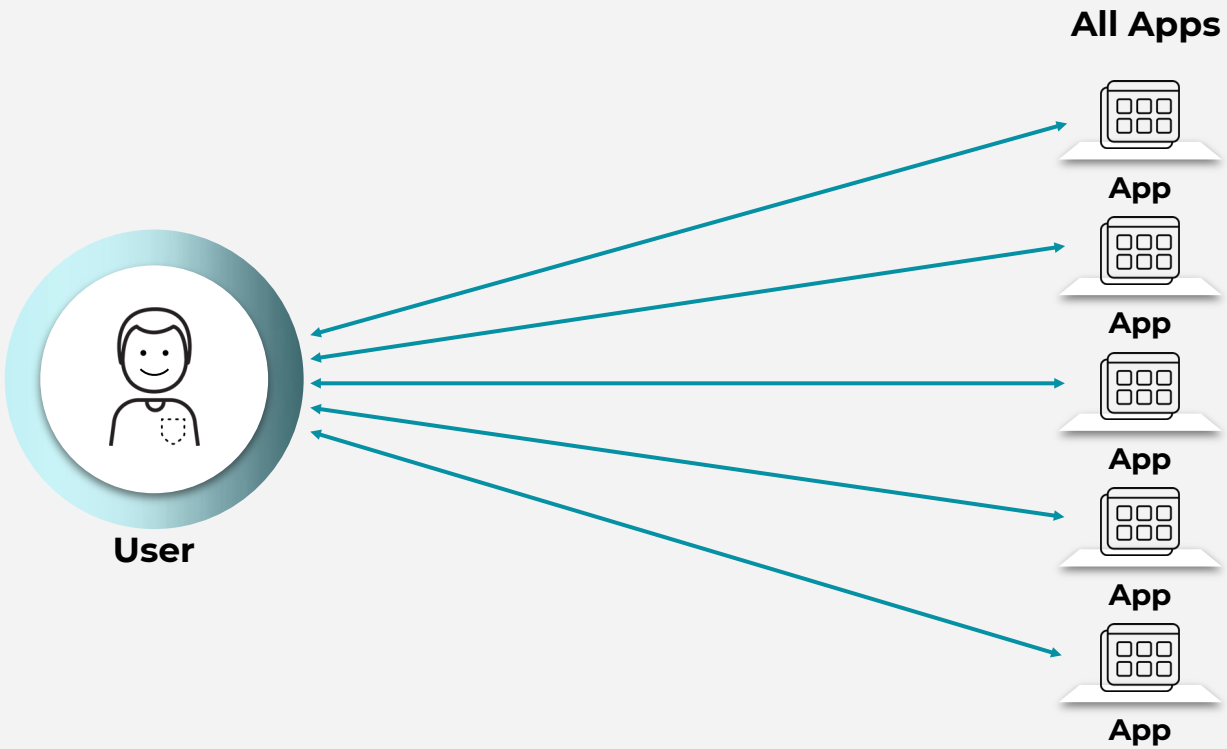
(The State of Hybrid Workforce Security, 2021)

SECURITY WAS SIMPLE WHEN
WORK WAS A PLACE YOU WENT TO



THE SECURITY IMPLICATIONS OF HYBRID WORK:

USERS ARE NOW GOING DIRECTLY TO APPS



- Most apps now live outside the data center
- Users are working from home and the office
- Direct to app architecture needed

THE SECURITY IMPLICATIONS OF HYBRID WORK:

THE ATTACK SURFACE HAS EXPLODED

BIGGER ATTACK SURFACE = MORE ATTACKS

92%

experienced a cyber attack over the past 12 months.

(FORRESTER, 2021)

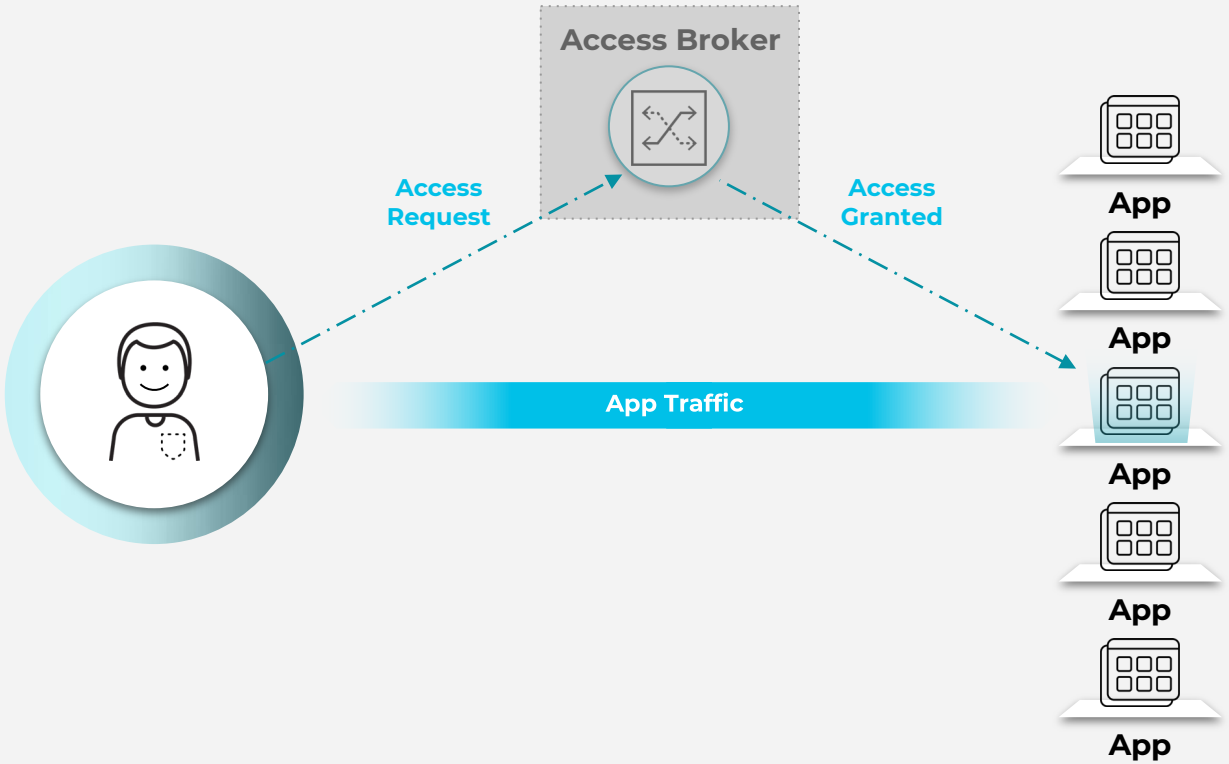
A NEW THREAT, A NEW SECURITY TOOL

76

Average number of security tools in an organization.

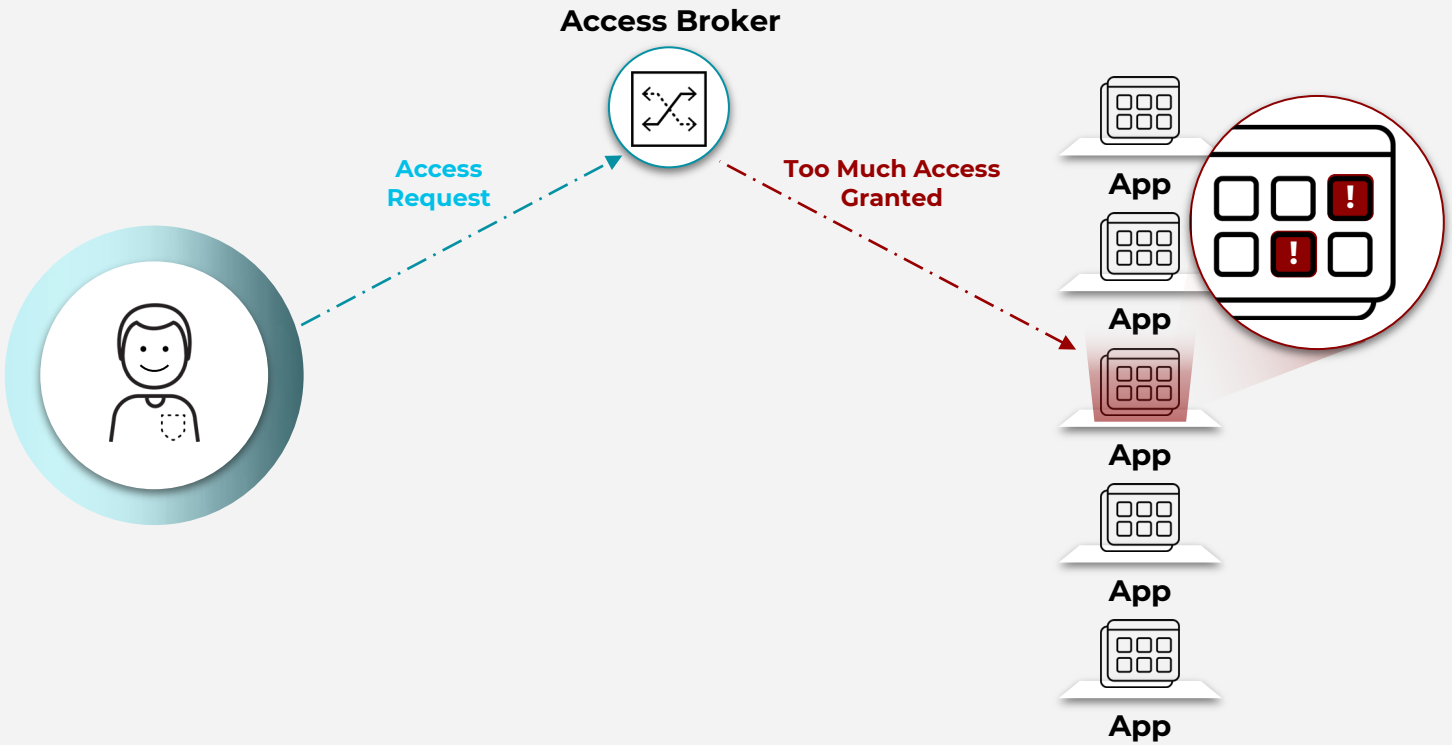
(PANASEER, 2022)

THE INDUSTRY TRIED TO SOLVE SECURE ACCESS WITH ZTNA 1.0



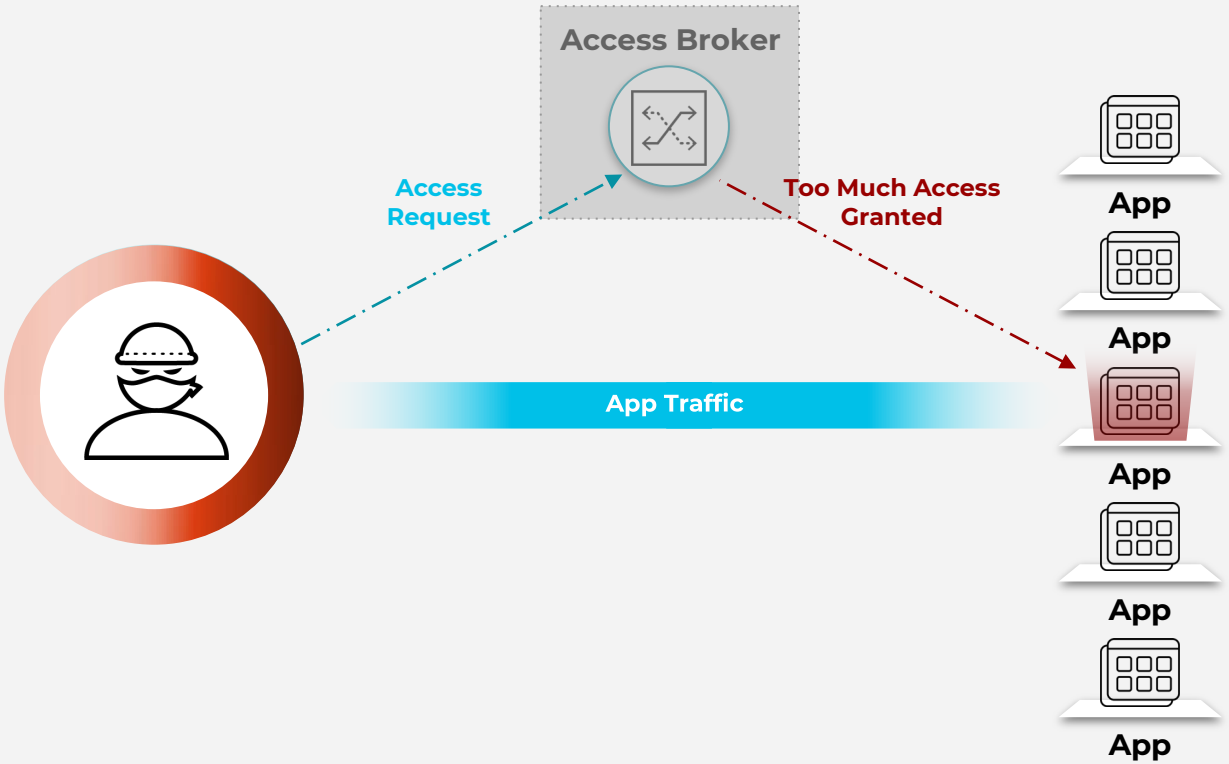
- User connects to the access broker
- Access is granted
- User communicates directly with the app

BUT ZTNA 1.0 FALLS SHORT IN MANY WAYS:
VIOLATES THE PRINCIPLE OF LEAST PRIVILEGE



- App is defined only based on IP and port
- Grants too much access
- Apps can have dynamic ports or port ranges

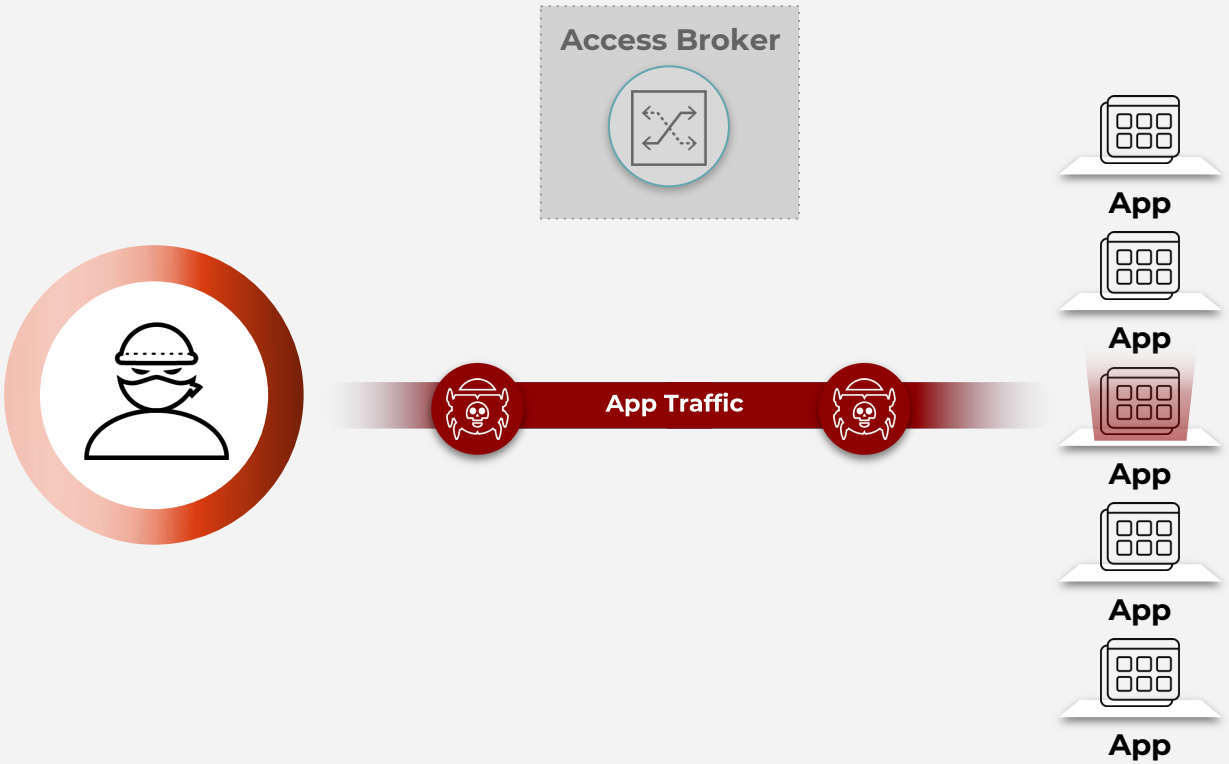
BUT ZTNA 1.0 FALLS SHORT IN MANY WAYS: ALLOW AND IGNORE



- Once access is granted, everything is trusted
- Assumes user and the app behavior won't change
- 100% of breaches happen on allowed activity

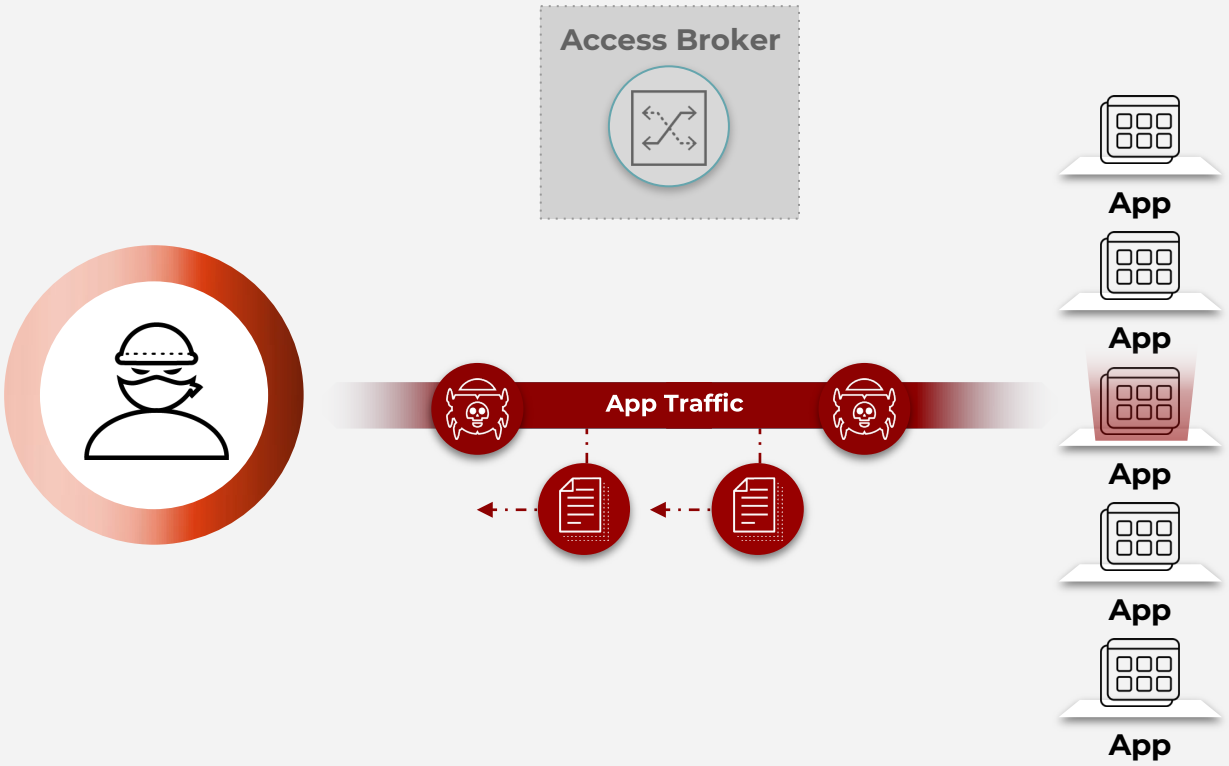

[IP SW 10] Camera 1
Live
[IP SW 13] Camera 1
Live
[IP SW 15 Static] Camera 1
[IP SW 17] Camera 1
[MBAC Internal 2] Camera 1
[IP SW 17] Camera 1

BUT ZTNA 1.0 FALLS SHORT IN MANY WAYS:
NO SECURITY INSPECTION



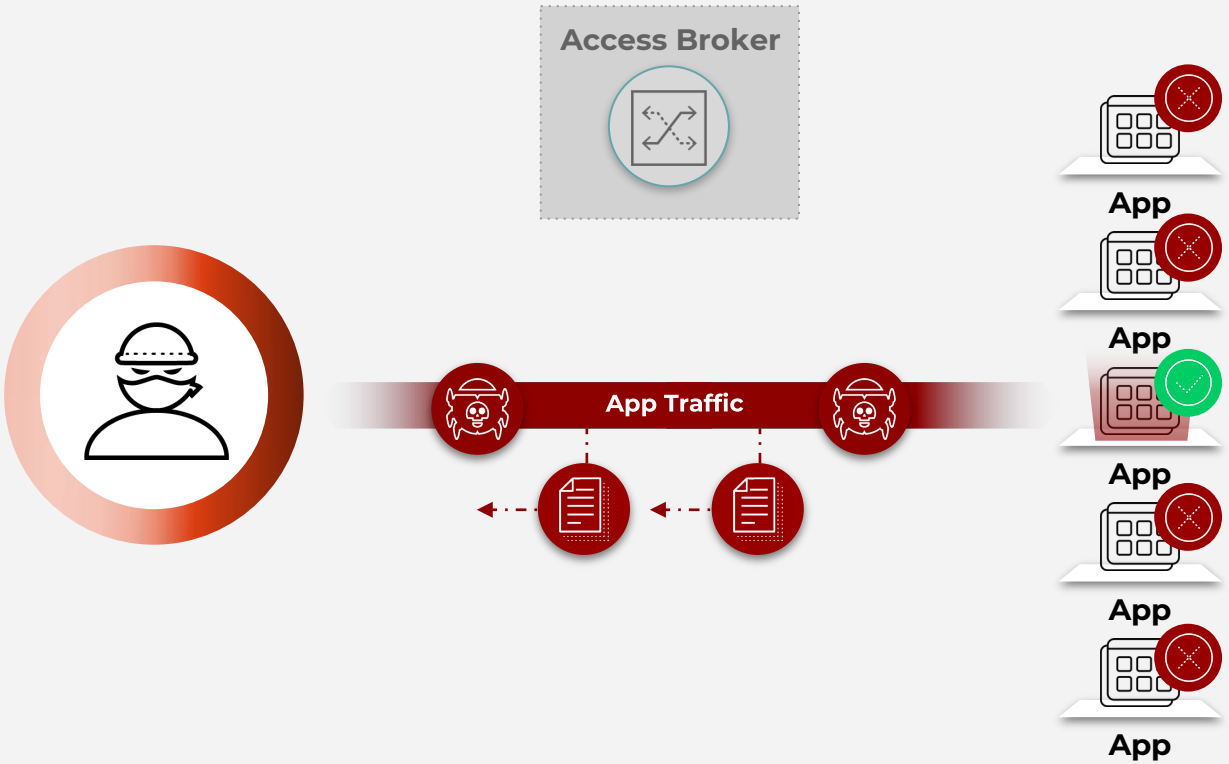
- App traffic is never inspected
- Cannot prevent malware or lateral movement
- Security through obscurity only

BUT ZTNA 1.0 FALLS SHORT IN MANY WAYS: NO DATA PROTECTION



- No visibility or control of data
- Can't stop data exfiltration from malicious insiders or external attackers

BUT ZTNA 1.0 FALLS SHORT IN MANY WAYS: CAN'T SECURE ALL APPS



- Only supports a subset of private apps
- Cannot address cloud native apps, apps with dynamic ports, or server-initiated apps
- Completely ignores SaaS apps

YOU CAN'T TEACH OLD SECURITY NEW TRICKS

THE WORLD NEEDS A PARADIGM SHIFT.

PRE-2010

VPN

2010s

ZTNA 1.0

YOU CAN'T TEACH OLD SECURITY NEW TRICKS

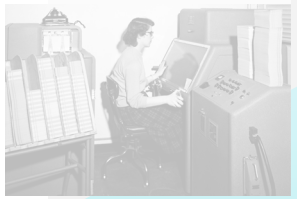
THE WORLD NEEDS A PARADIGM SHIFT.

2022 -

ZTNA 2.0

2010s

ZTNA 1.0



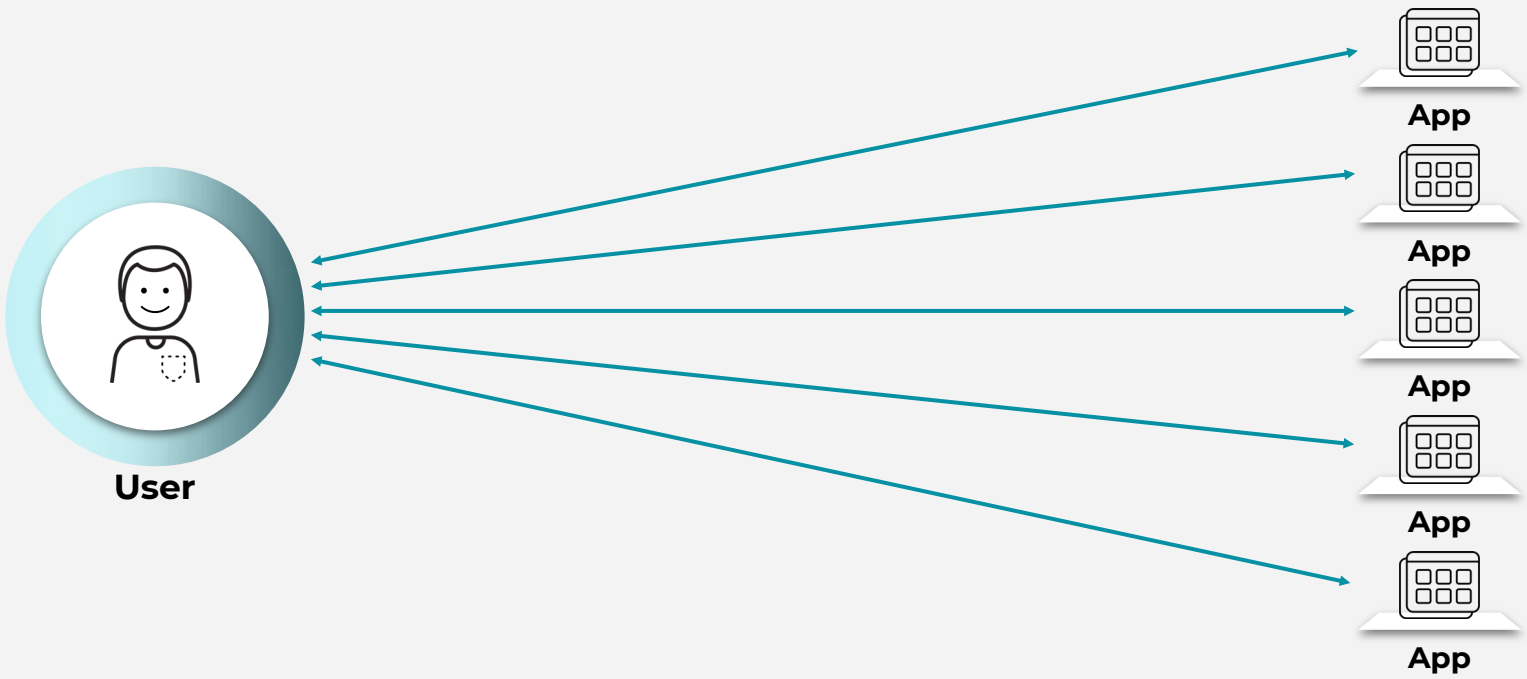
PRE-2010

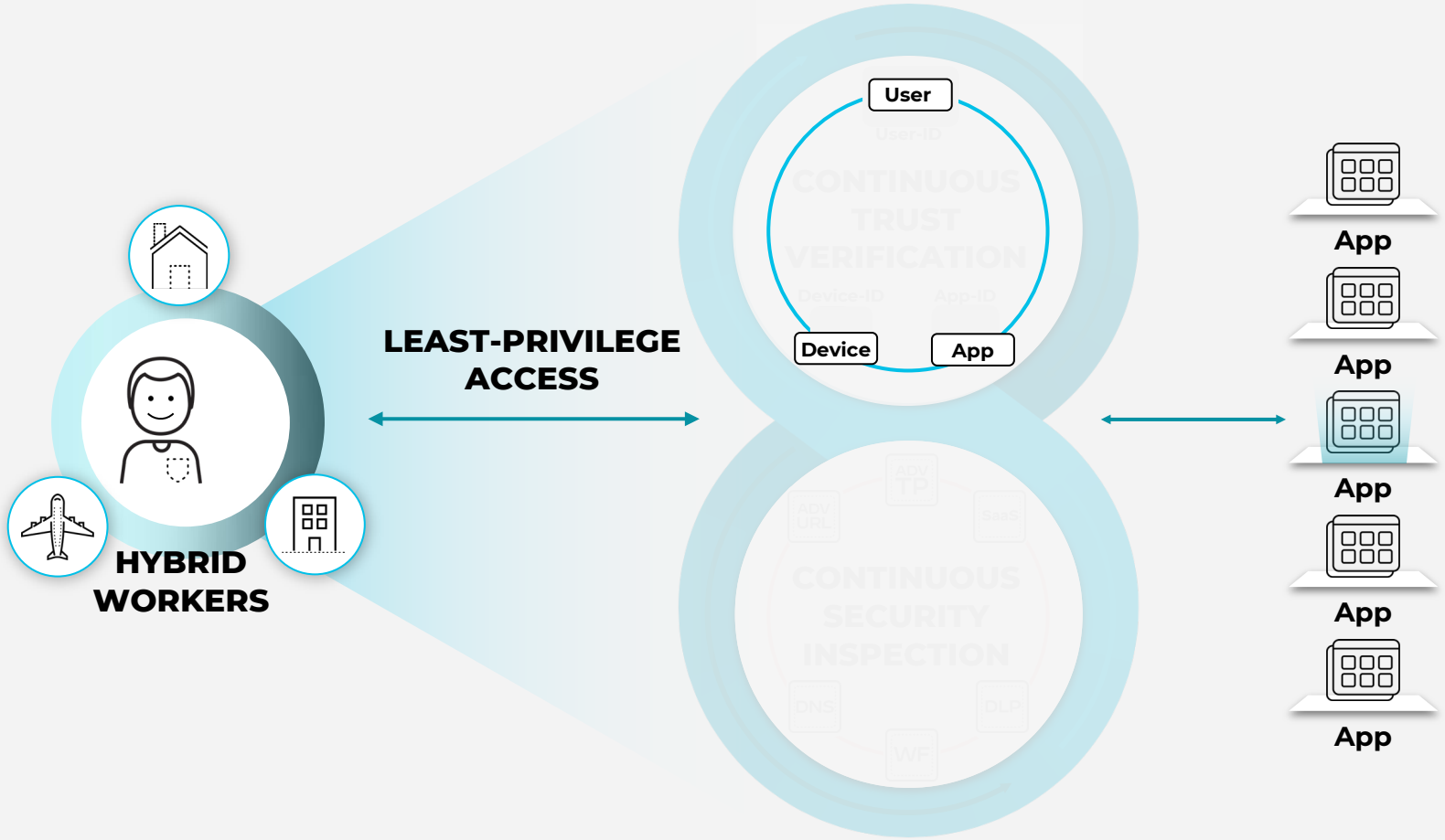
VPN

INTRODUCING

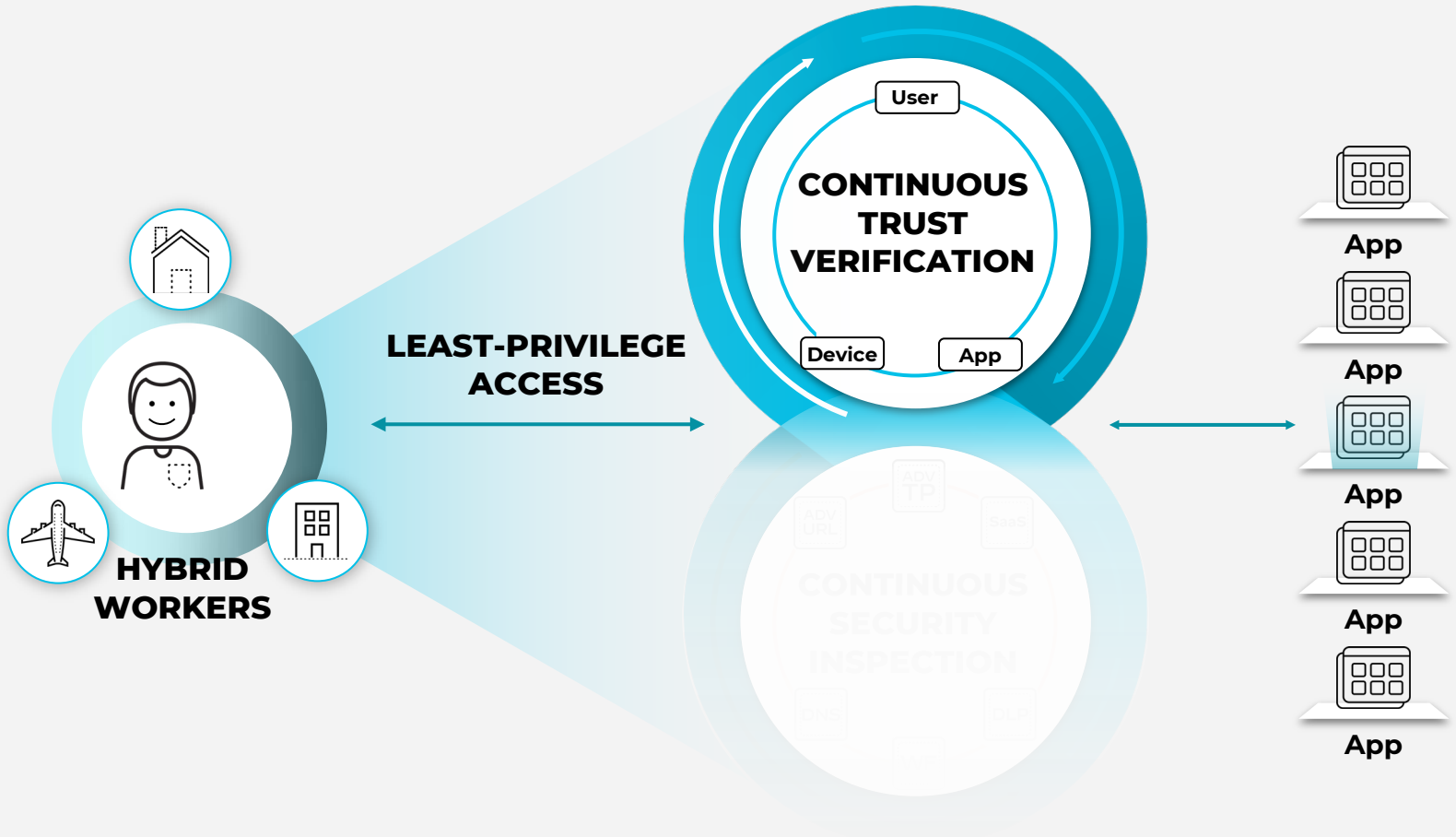
ZTNA 2.0

ZTNA 1.0	ZTNA 2.0
Violates the principle of least privilege	**Least-privileged access**
Allows and ignores	**Continuous trust verification**
No security inspection	**Continuous security inspection**
Doesn't protect data	**Protects all data**
Can't secure all apps	**Secures all apps**

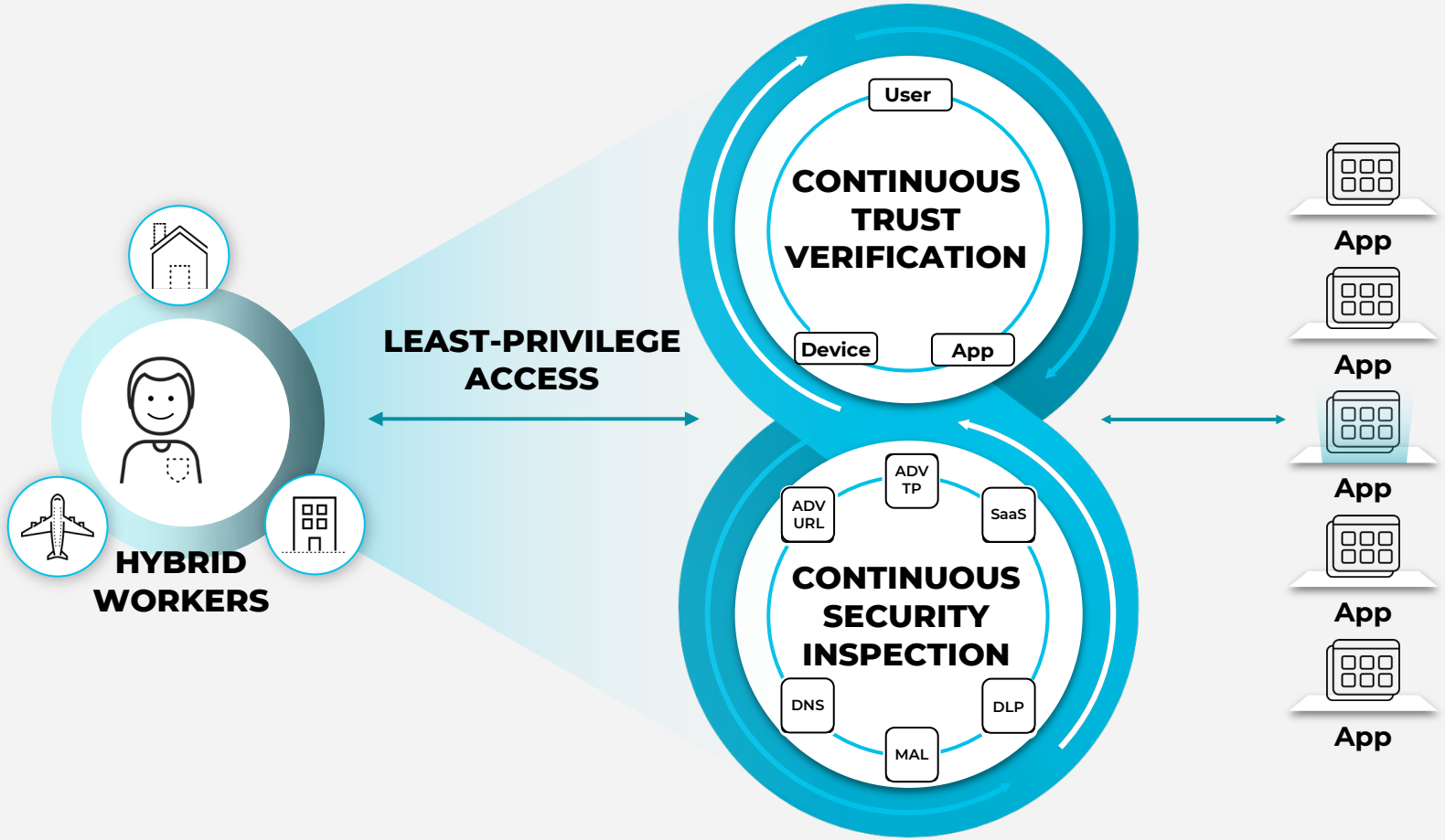

App
App
App
App
App
User



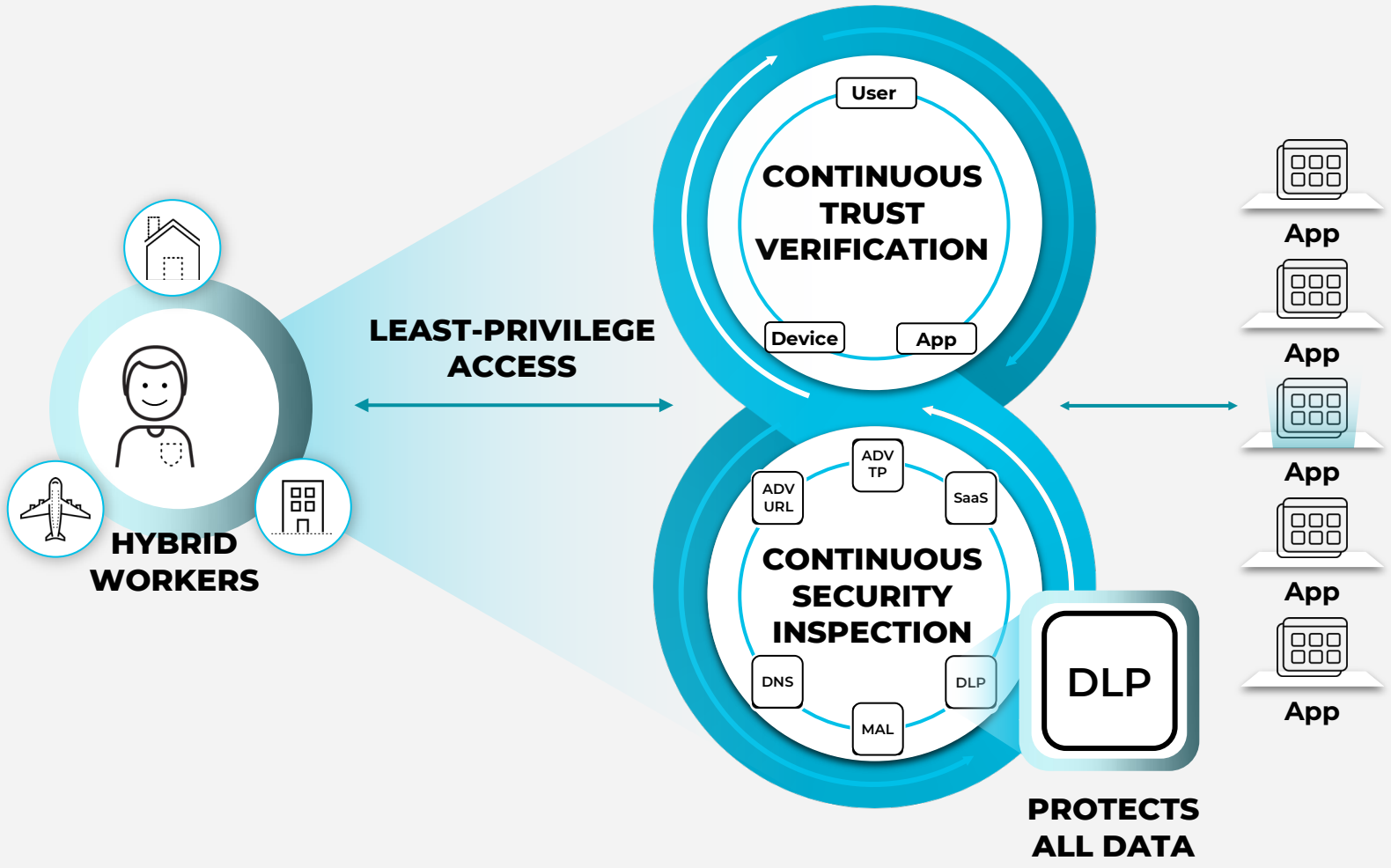
Enables you to fully realize the principle of least privilege by identifying applications based on App-IDs at Layer 7.



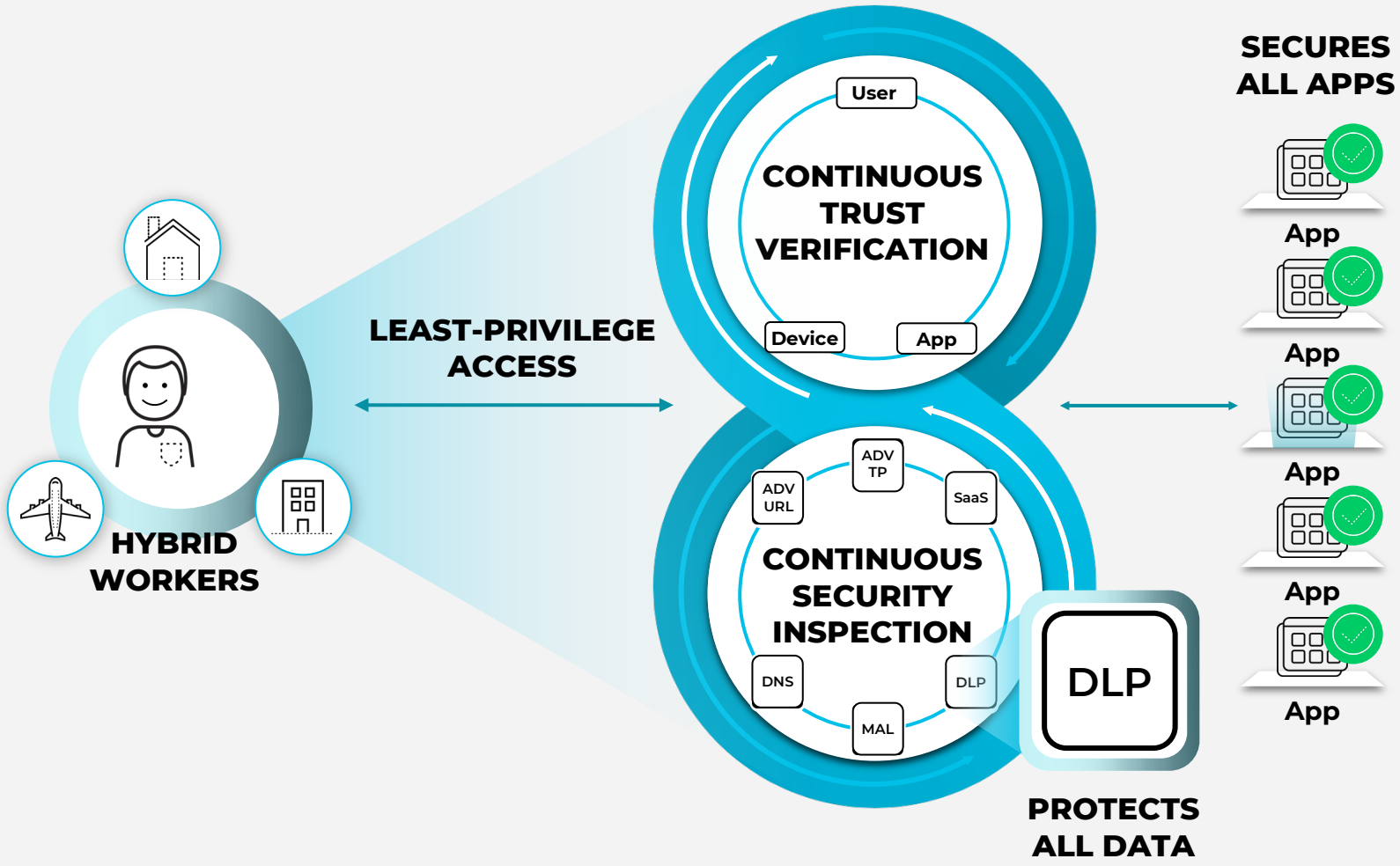
Once access to an app is granted, trust is continually assessed based on changes in device posture, user behavior, and app behavior.



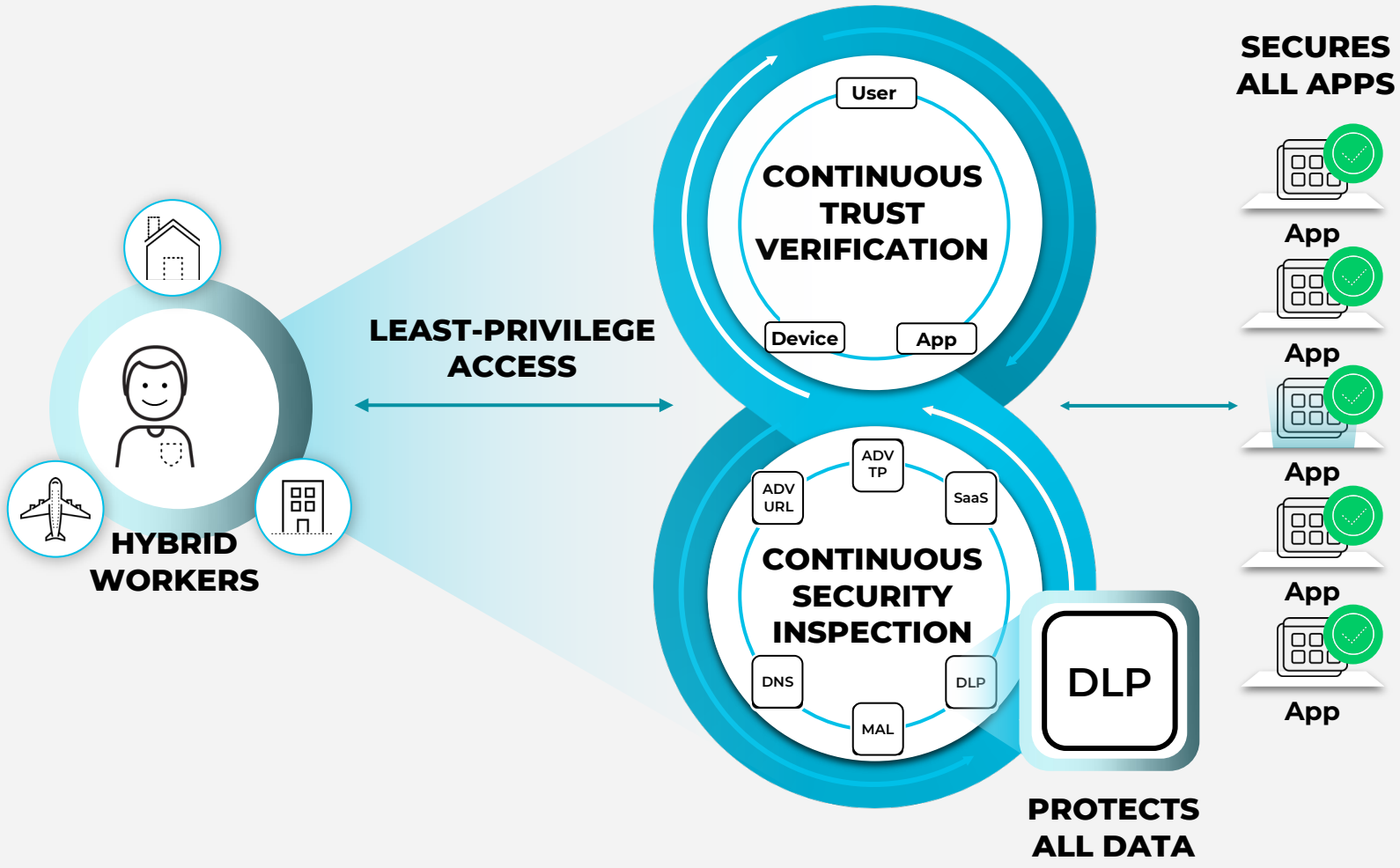
Provides deep and ongoing inspection of all traffic, even for allowed connections to prevent all threats, including zero-day threats.



Consistent data protection across all apps used in the enterprise, including private apps and SaaS, with a single DLP policy.



Consistently secures all applications used across the enterprise, including modern cloud native apps, legacy private apps, and SaaS apps.



Delivering on the Vision of ZTNA 2.0

- Least-Privileged Access
- Continuous Trust Verification
- Continuous Security Inspection
- Protect All Data
- Secures All Apps

ONLY A UNIFIED SASE PRODUCT CAN TRULY DELIVER:

ZTNA 2.0

BEST USER EXPERIENCE

UNIFIED PRODUCT

Josh Dye

Senior Vice President of Global Information Security
Jefferies

ZTNA 2.0 Takeaways

- Get rid of VPN
- Select a ZTNA solution that can:
  - Enforce Least Privilege Access with fine-grained access controls
  - Enable behavior-based continuous trust verification
  - Secure all apps, all the time
  - Enable deep and ongoing security inspection
  - Ensure consistent visibility with a single DLP policy to secure both access and data

THANK YOU