PRISMA
BY PALO ALTO NETWORKS

# ZTNA 2.0- Zero trust with Zero Exceptions, changing the game in SASE

Angeliki Filippopoulou
Greece Regional Sales Manager

March 2022

paloalto NETWORKS

## 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)

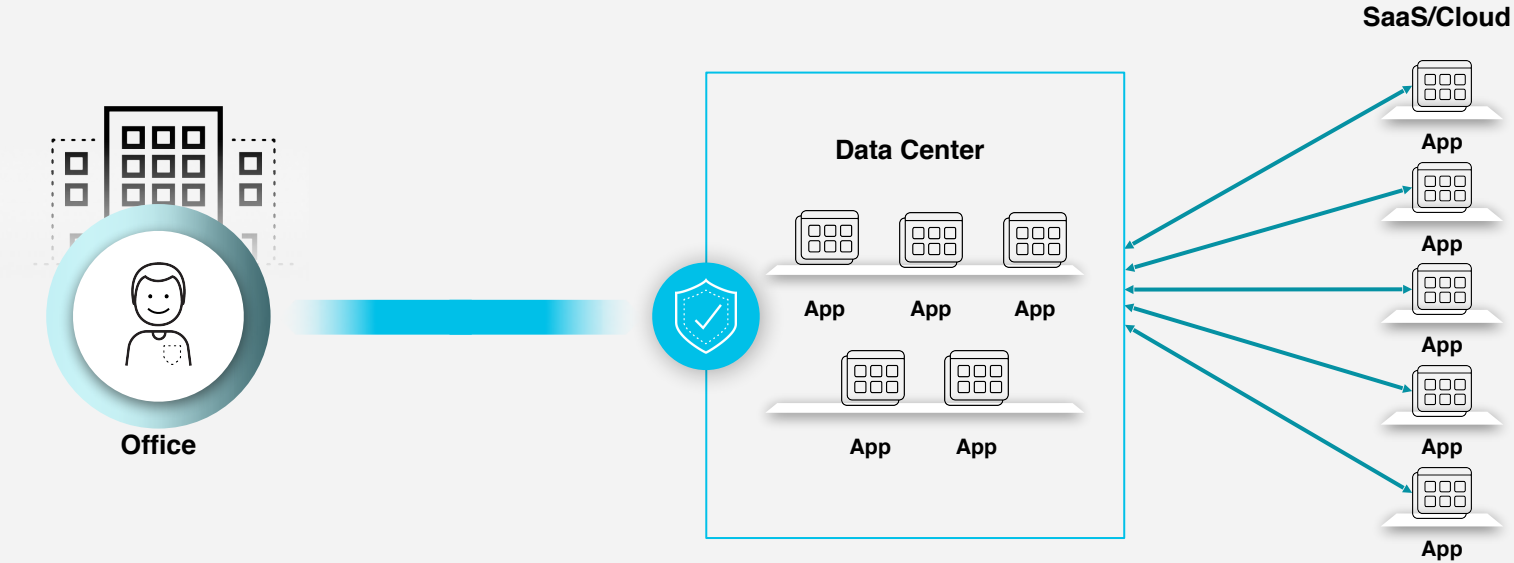
### USERS ARE EVERYWHERE

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

(The State of Hybrid Workforce Security, 2021)

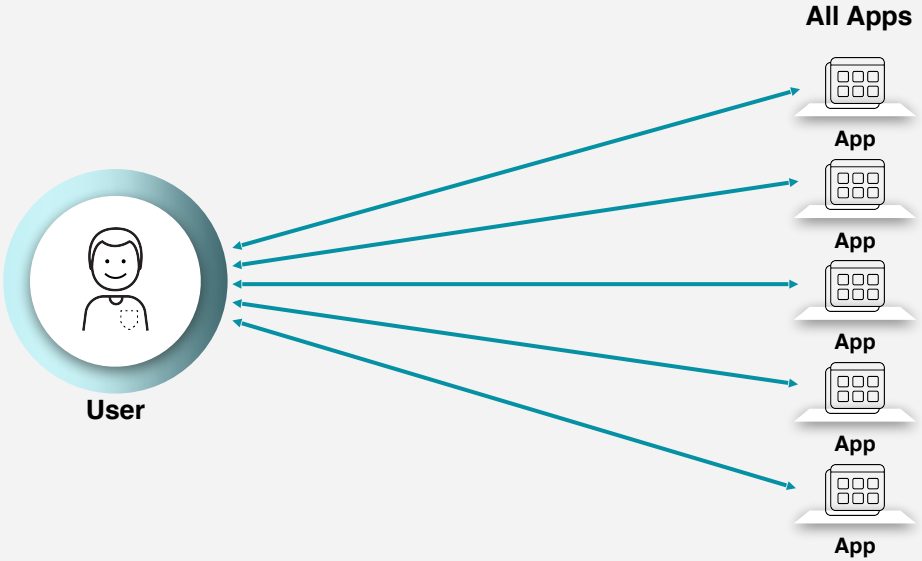
SECURITY WAS SIMPLE WHEN

# WORK WAS A PLACE YOU WENT TO



THE SECURITY IMPLICATIONS OF HYBRID WORK:

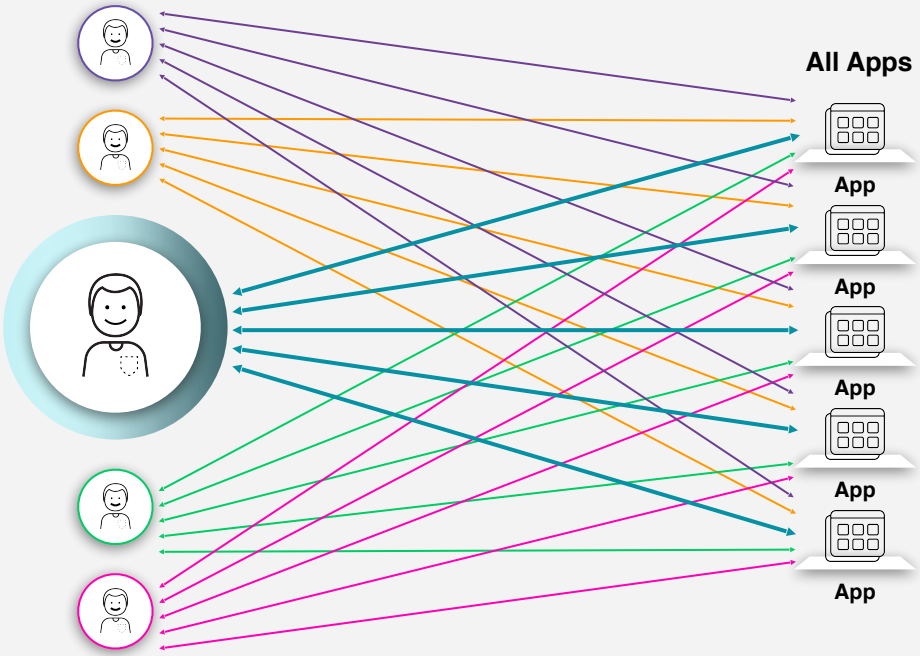
# USERS ARE NOW GOING DIRECTLY TO APPS




- 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%**

of technology executives said that their companies experienced a cyber attack over the past 12 months.

(FORRESTER, 2021)

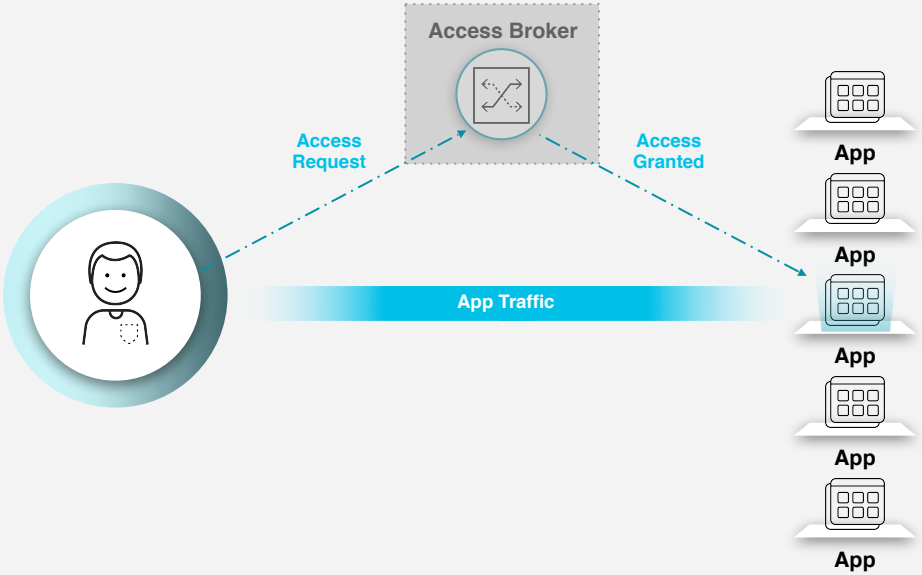
A NEW THREAT, A NEW SECURITY TOOL

**76**

The average number of security tools in an organization. (+19% over the past two years, from 64 to 76)

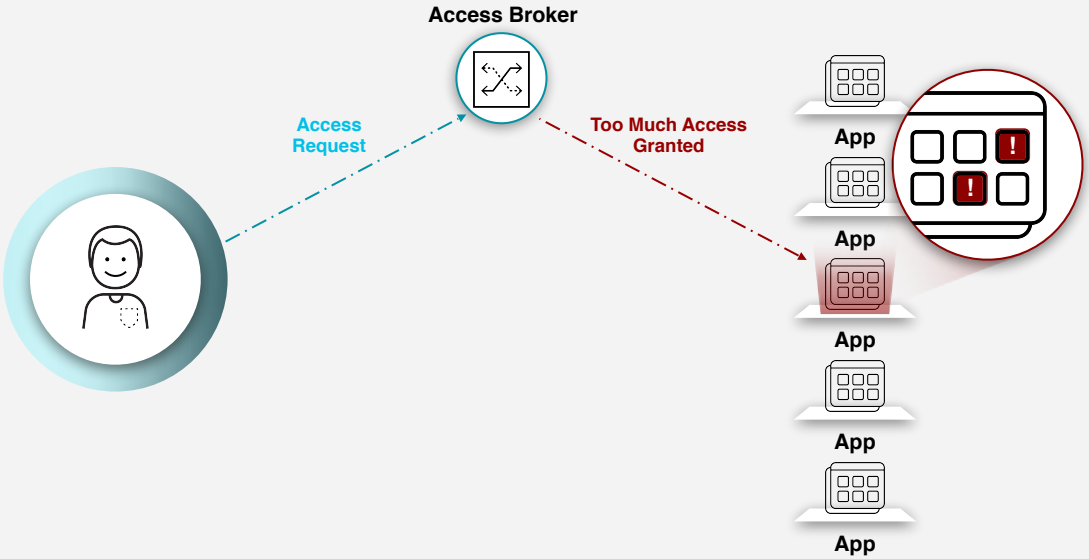
(PANASEER, 2022)

# THE INDUSTRY TRIED TO SOLVE SECURE ACCESS WITH ZTNA 1.0



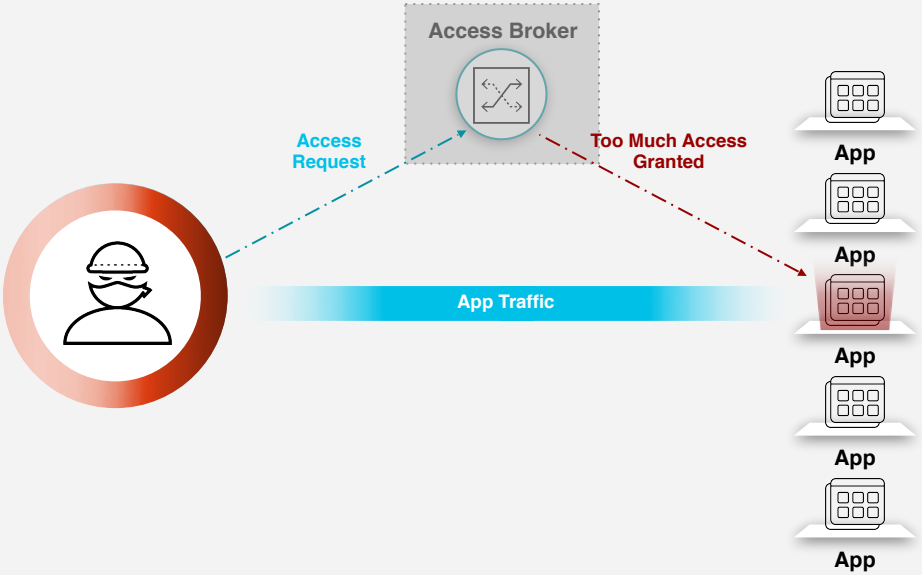

- User connects to the access broker
- Access is granted
- User communicates directly with the app

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



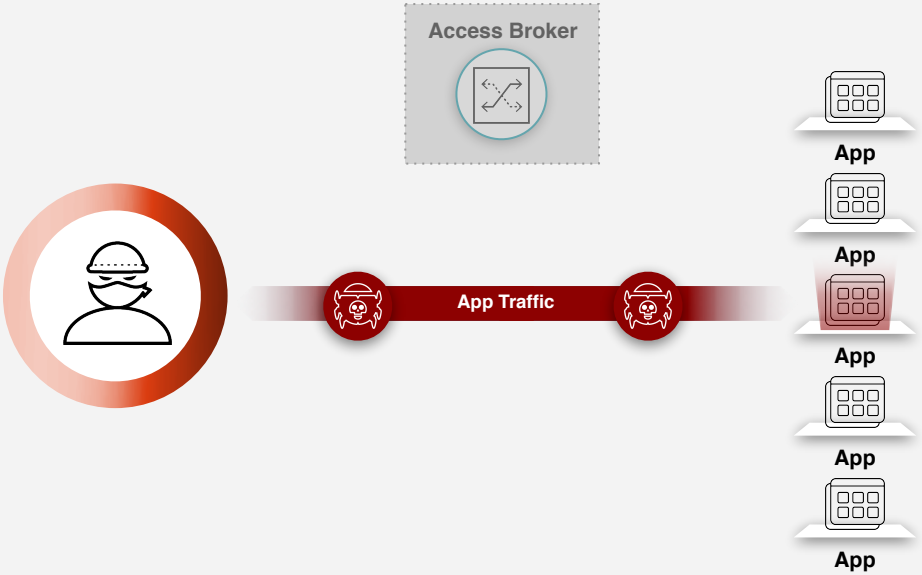

- App is defined only based on IP and port
- Grants too much access
- Apps can have dynamic ports or port ranges

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



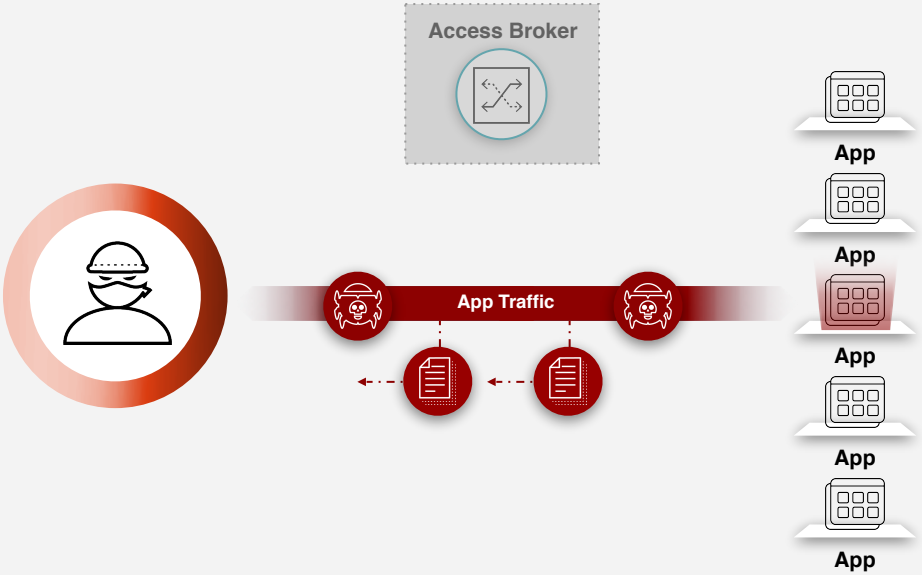

- Once access is granted, everything is trusted
- Assumes user and the app behavior won't change
- 100% of breaches happen on allowed activity

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



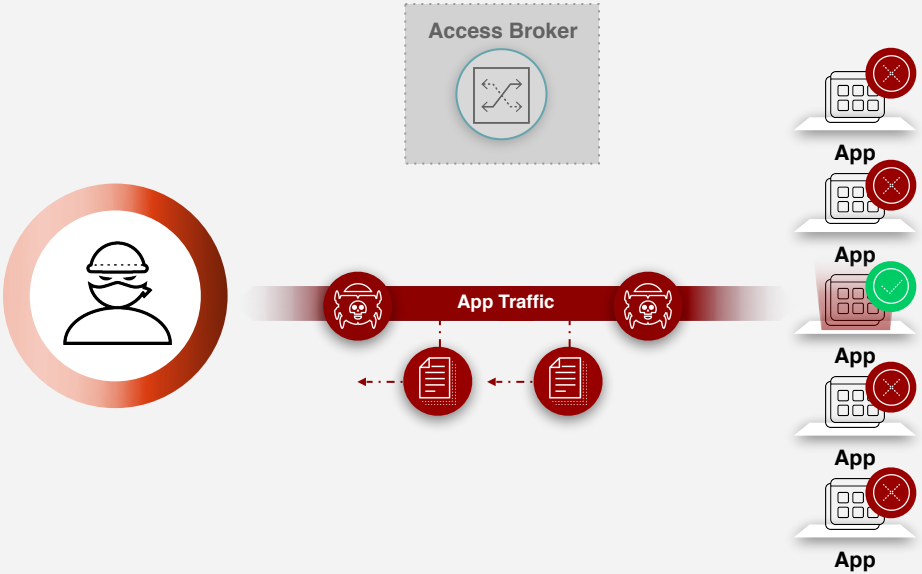

- App traffic is never inspected
- Cannot prevent malware or lateral movement
- Security through obscurity only

# 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

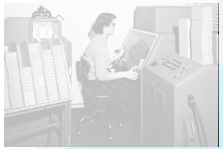
# THE WORLD NEEDS A PARADIGM SHIFT.

2022 -

## ZTNA 2.0

2010s

## ZTNA 1.0



PRE-2010

## VPN

# A Ten-Time Leader in Gartner Network Firewall Magic Quadrant

- **Positioned as a LEADER** in the 2021 Gartner® Magic Quadrant™ Network Firewalls **for the tenth consecutive year**.
- Achieved the **highest position** for ability to execute and **furthest position** for completeness of vision.
- Powered by over a decade of industry-first innovations, our **ML-Powered NGFWs** provide critical protection from the threats of today and tomorrow, while extending security to all users and all applications throughout the enterprise.

**Figure 1: Magic Quadrant for Network Firewalls**


As of August 2021 © Gartner, Inc

Gartner and Magic Quadrant are registered trademarks of Gartner, Inc and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Gartner, Magic Quadrant for Network Firewalls, Rajpreet Kaur I Adam Hils I Jeremy D'Hoinne I Nat Smith I Aaron McQuaid, 1 November 2021. Source: Gartner (November 2021)

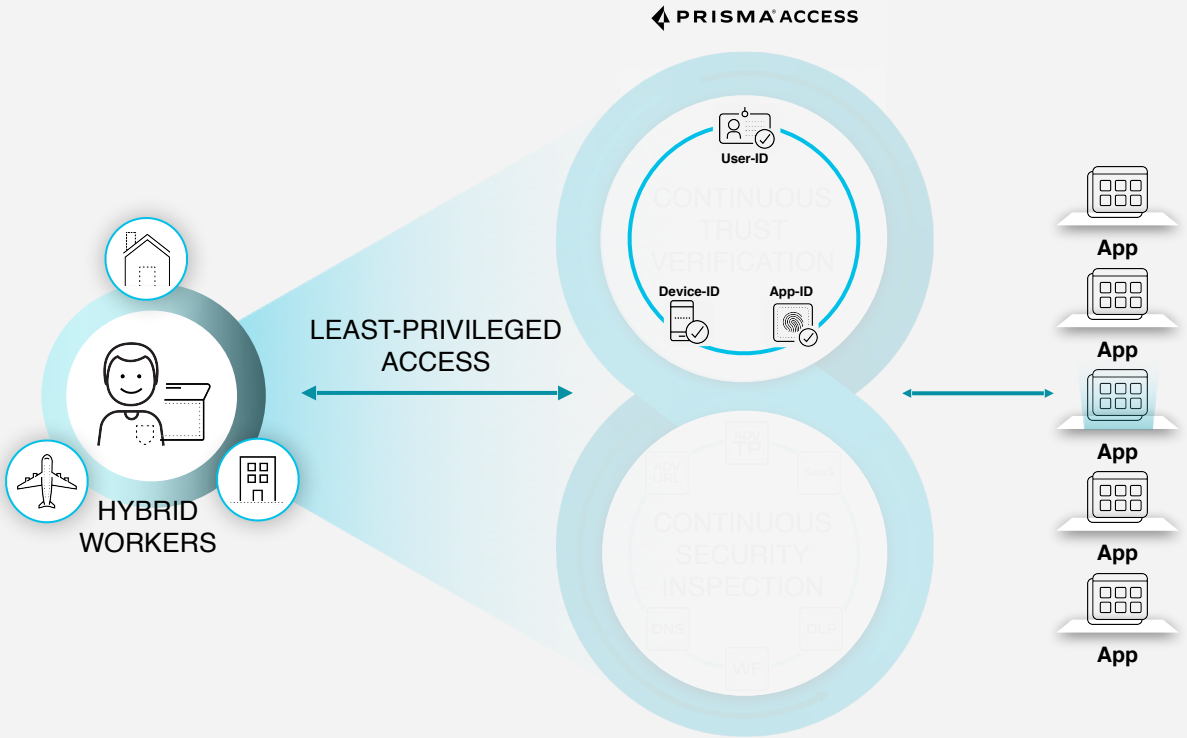
This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Palo Alto Networks.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

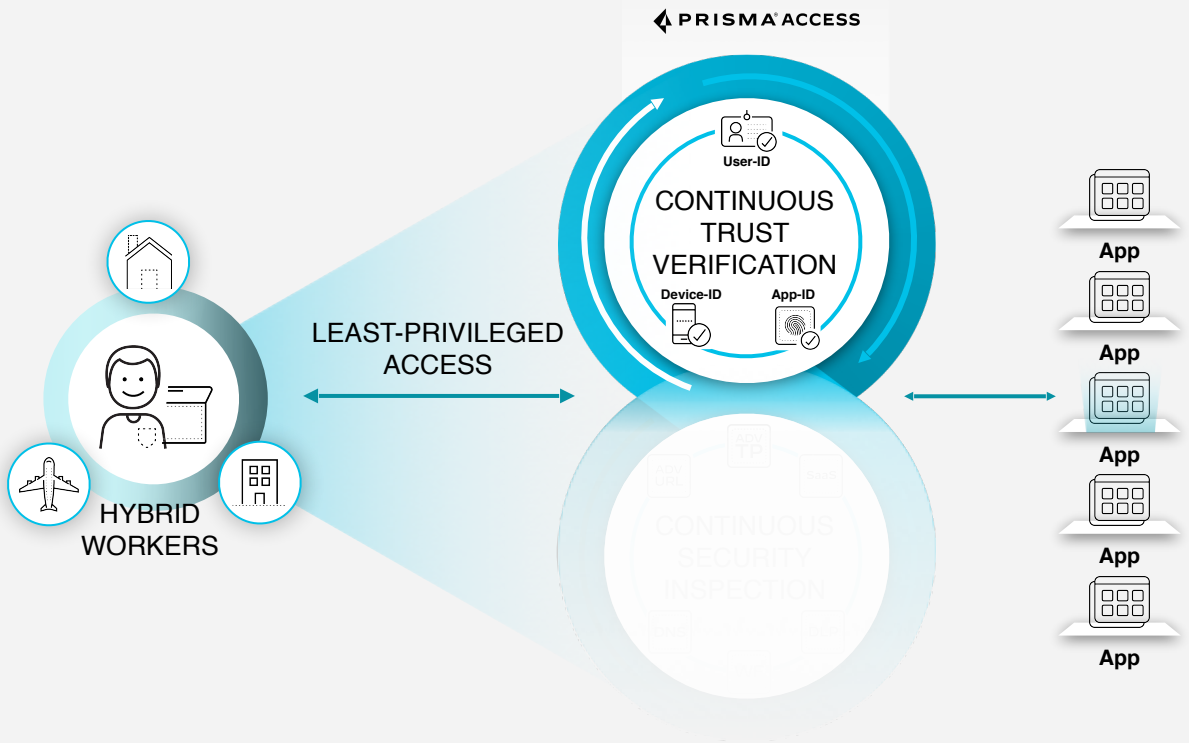
INTRODUCING

# ZTNA 2.0

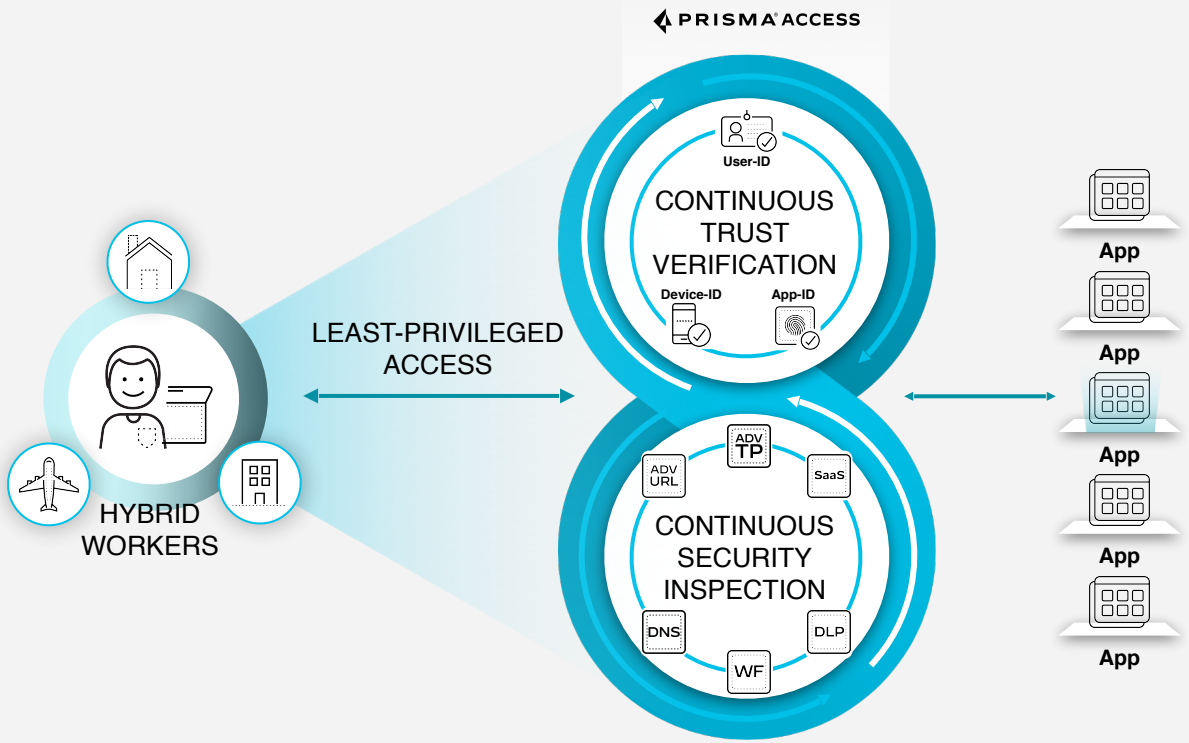
| ZTNA 1.0 | ZTNA 2.0 |
| --- | --- |
| Violates the principle of least privilege | Least-privileged access |
| Allows and ignores | Continuous trust verification |
| No security inspection | Continuous security inspection |
| Doesn't protect data | Protects all data |
| Can't secure all apps | Secures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



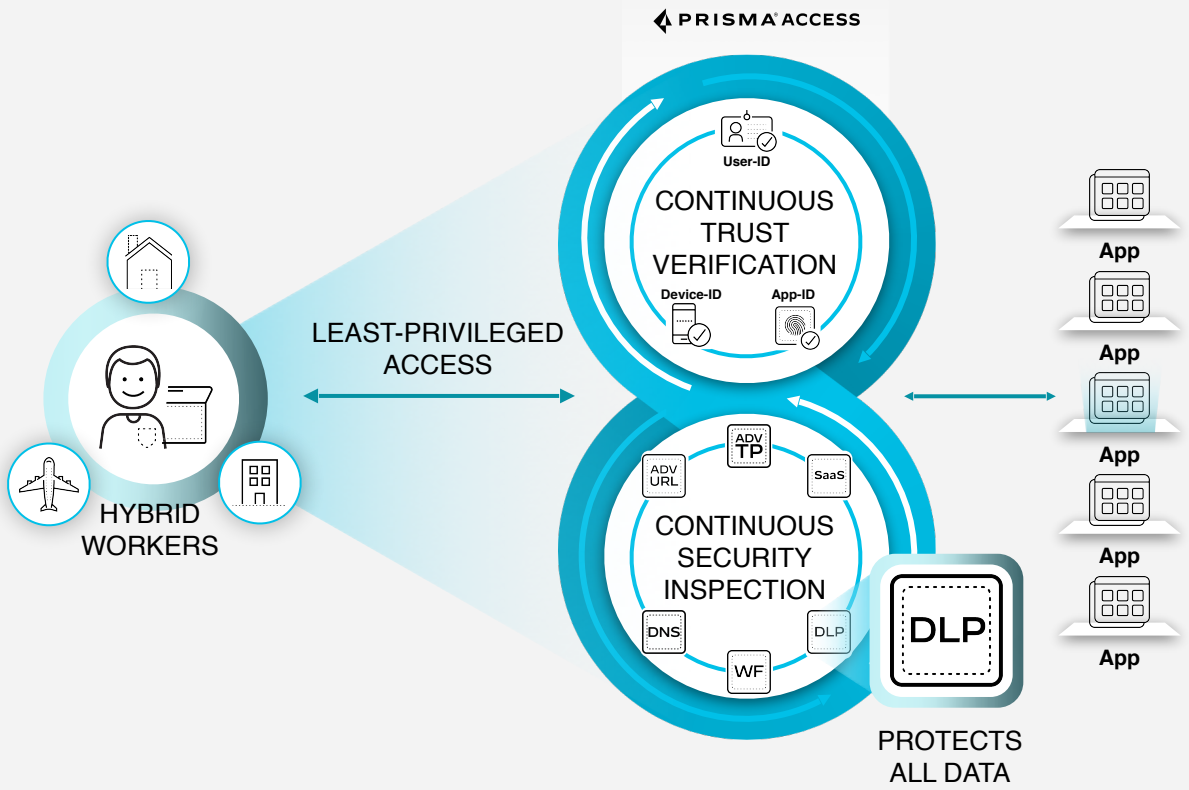

Enables you to fully realize the principle of least privilege by identifying applications based on App-IDs at Layer 7.



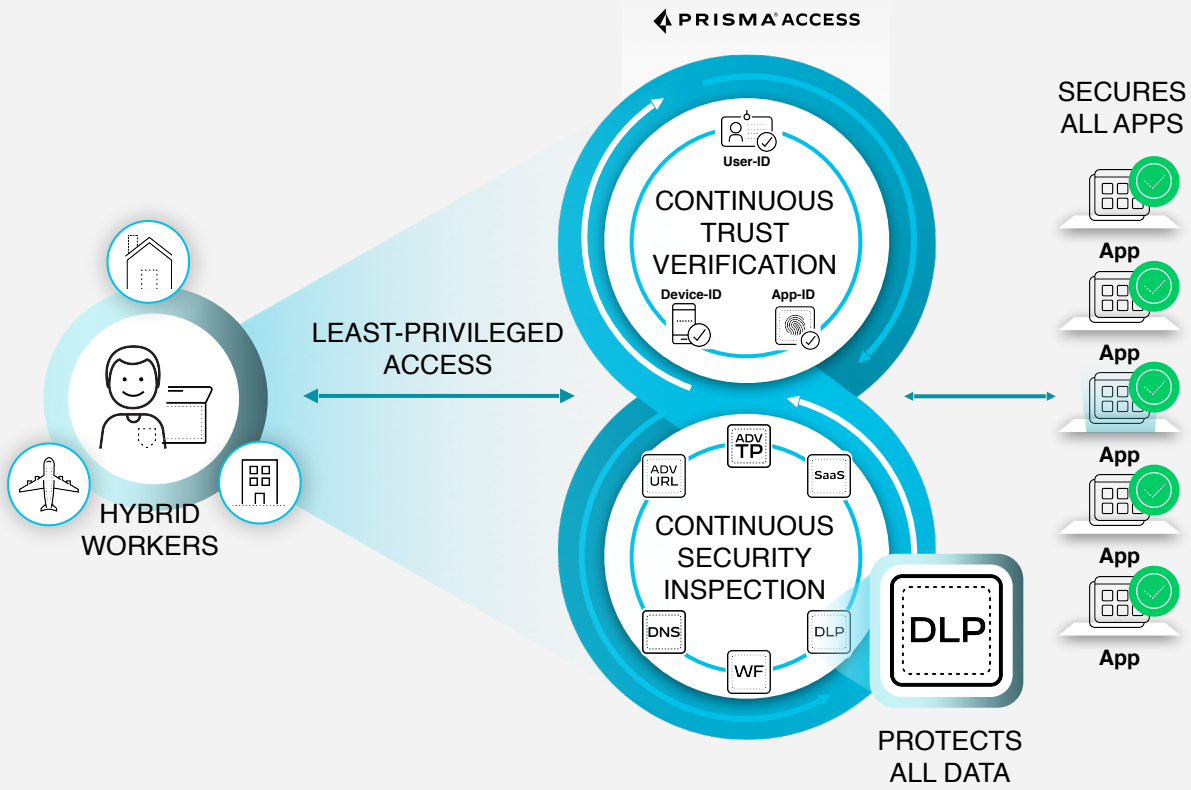

Once access to an app is granted, trust is continually assessed based on changes in device posture, user behavior, and app behavior.



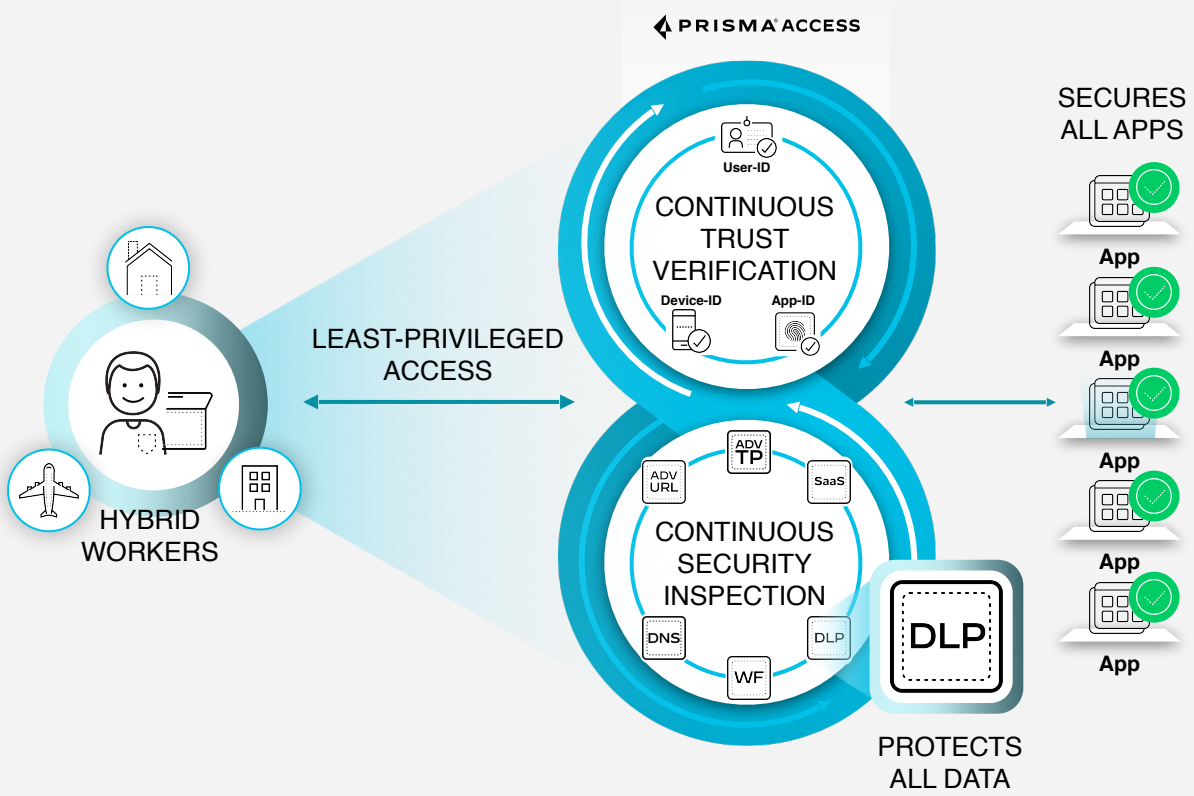

Provides deep and ongoing inspection of all traffic, even for allowed connections to prevent all threats, including zero-day threats.




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.




## Prisma Access: Delivering on the Vision of ZTNA 2.0

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

# PRISMA ACCESS DELIVERS THE BEST USER EXPERIENCE IN THE INDUSTRY

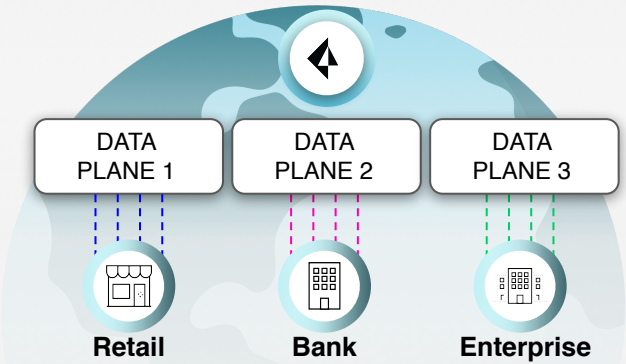
**Highest availability**
**99.999%**
**uptime.**

**Lowest latency**
**10ms**
**security processing.**

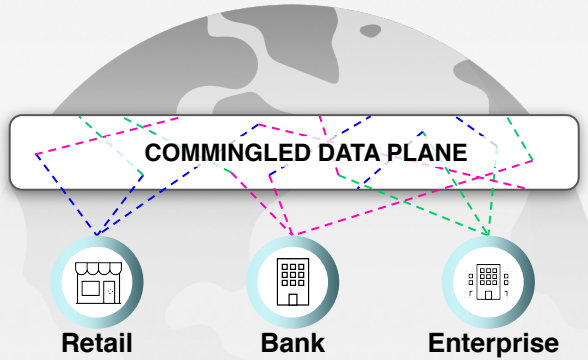
**Industry's only**
**SaaS**
**performance SLA.**

# DATA PLANE ISOLATION

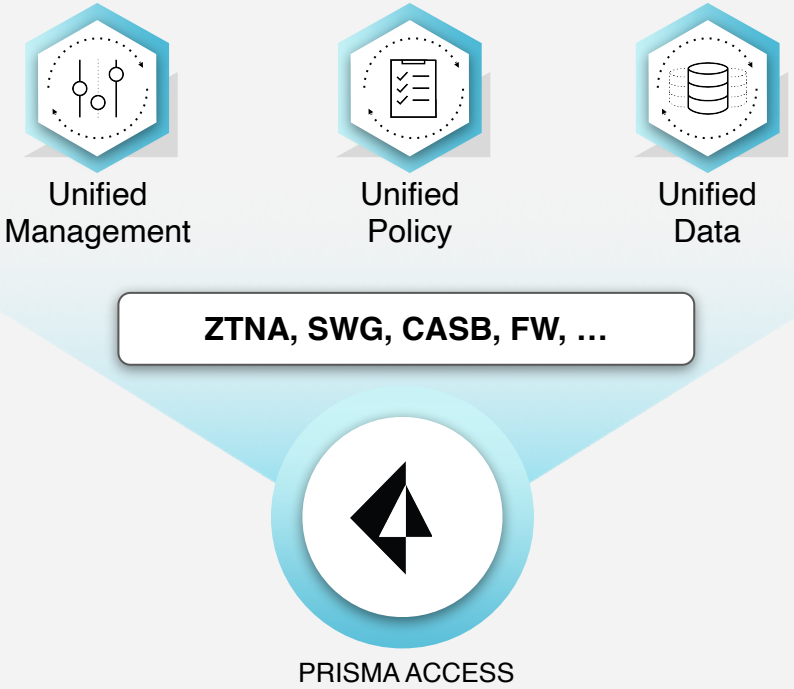
PRISMA ACCESS




Other Solutions



# A UNIFIED PRODUCT WITH PRISMA ACCESS




**Unified product delivers superior security and operational outcomes**

# CUSTOMER PROJECTS DRIVING ZTNA TRANSFORMATION

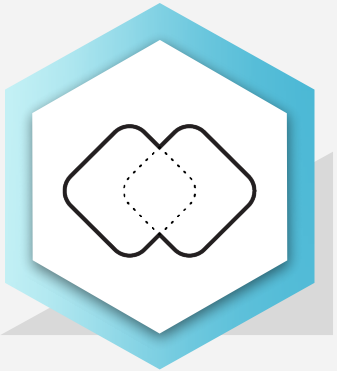

## VPN Replacement / ZTNA Project

- Zero Trust Model for access to private apps
- Support for managed or unmanaged client access
- Consistent protection across the enterprise

# KEY BENEFITS FOR VPN REPLACEMENT PROJECTS

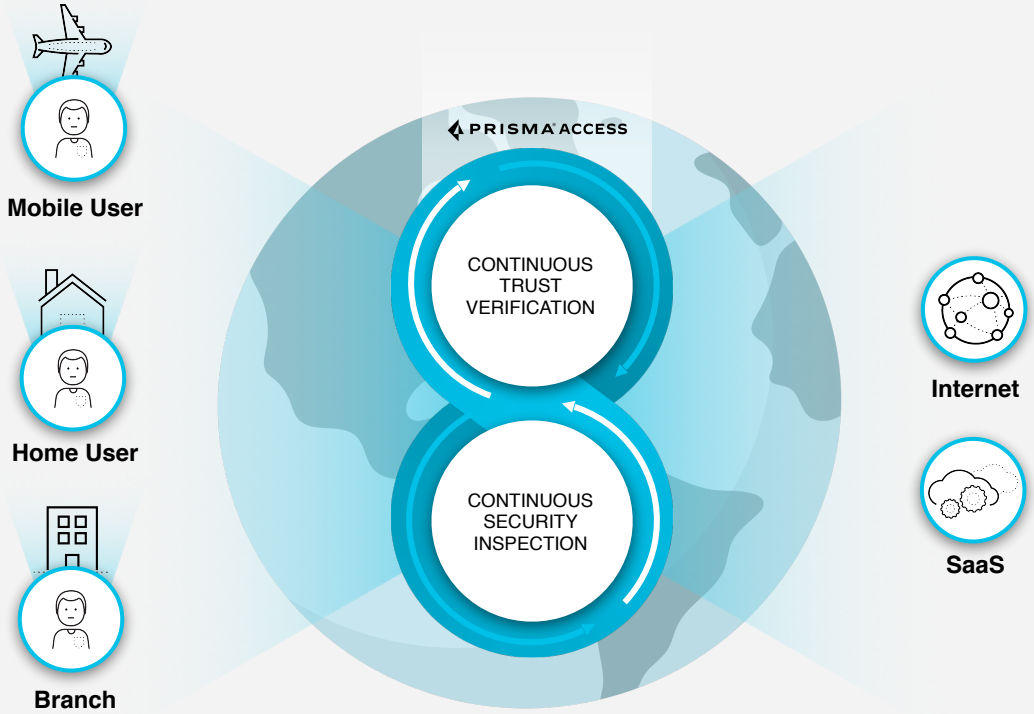
ZTNA
2.0

BEST USER
EXPERIENCE



UNIFIED
PRODUCT

INTEGRATED SD-WAN




## SWG Replacement / Cloud SWG Project

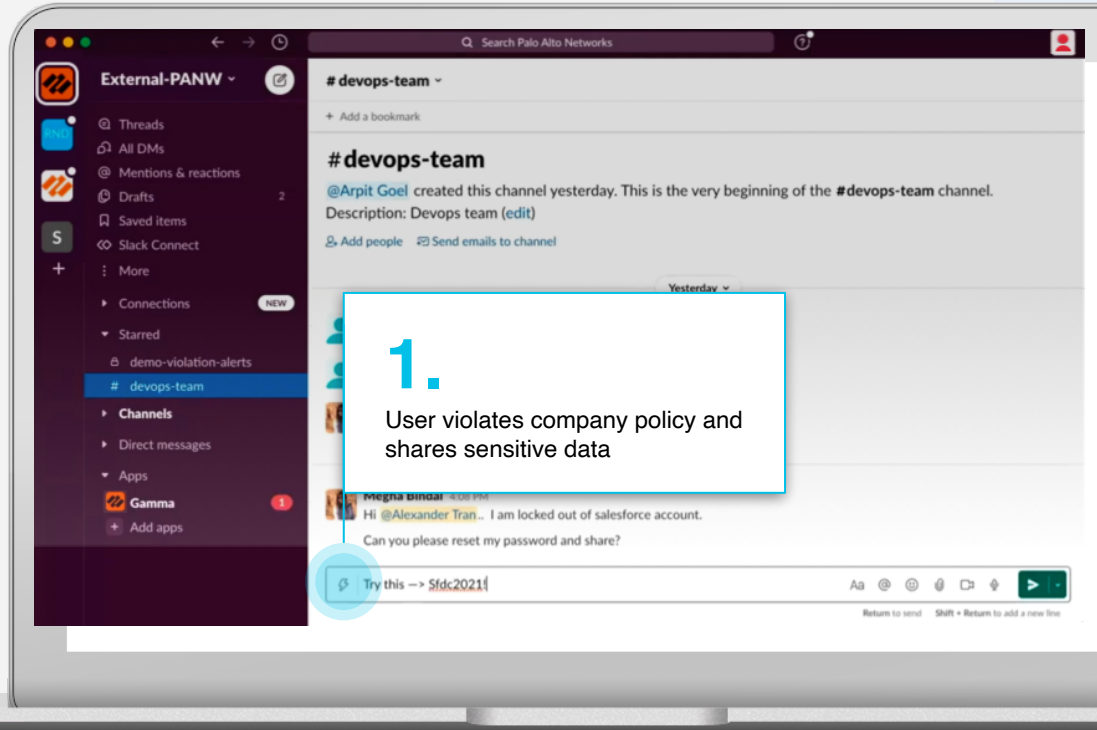
- Support for explicit proxy; no network changes required
- Optional agent for security of all ports and protocols
- Consistent policy across mobile, home, and branch users


## Advanced SaaS App Security / Next-Gen CASB Project

- SaaS app visibility and control, shadow IT
- Protection of sanctioned SaaS apps
- Advanced DLP

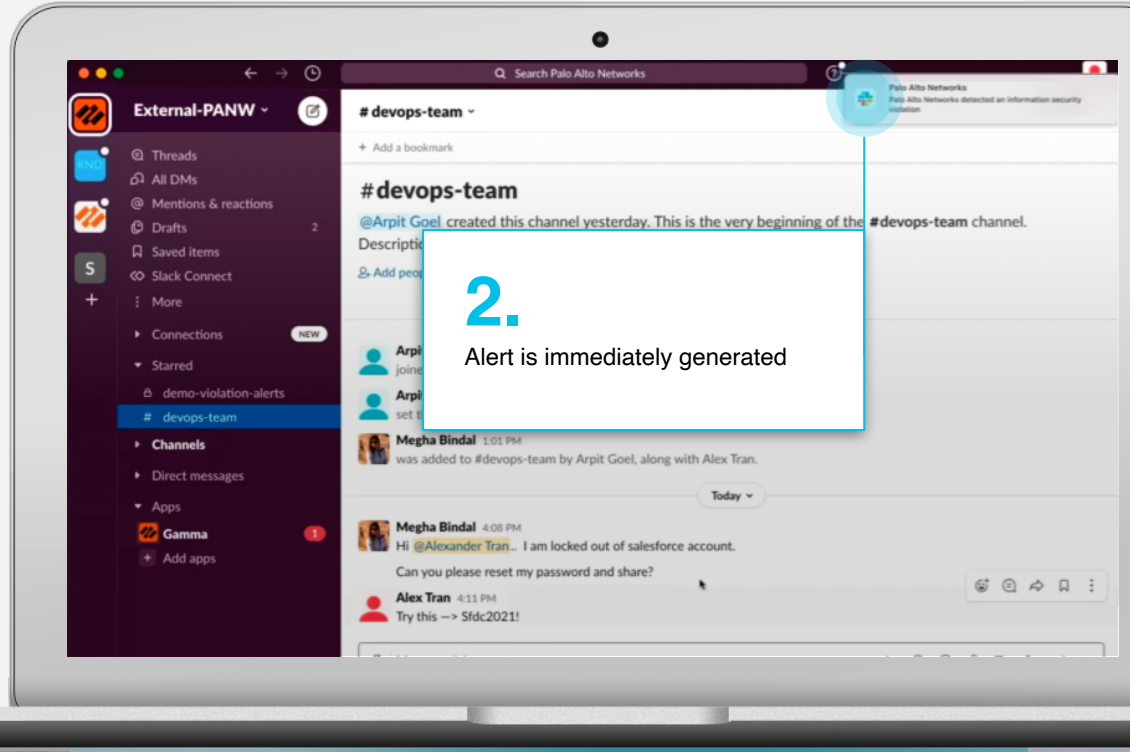
## ADVANCED DLP

- Accurately protect sensitive data in real time
- 1K+ data identifiers, EDM, OCR, ML classification, and natural language processing to detect and protect sensitive data across conversations
- Delivered consistently across SaaS, IaaS, network, branch, and remote workforces



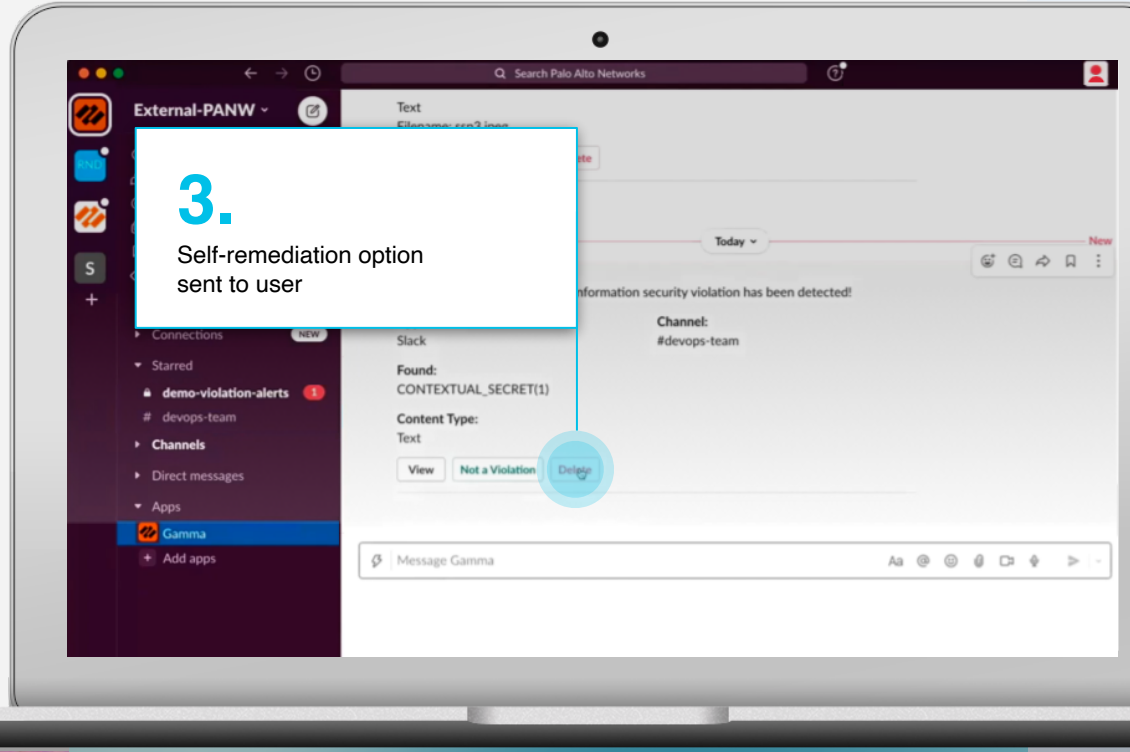
## ADVANCED DLP

- Accurately protect sensitive data in real time
- 1K+ data identifiers, EDM, OCR, ML classification, and natural language processing to detect and protect sensitive data across conversations
- Delivered consistently across SaaS, IaaS, network, branch, and remote workforces



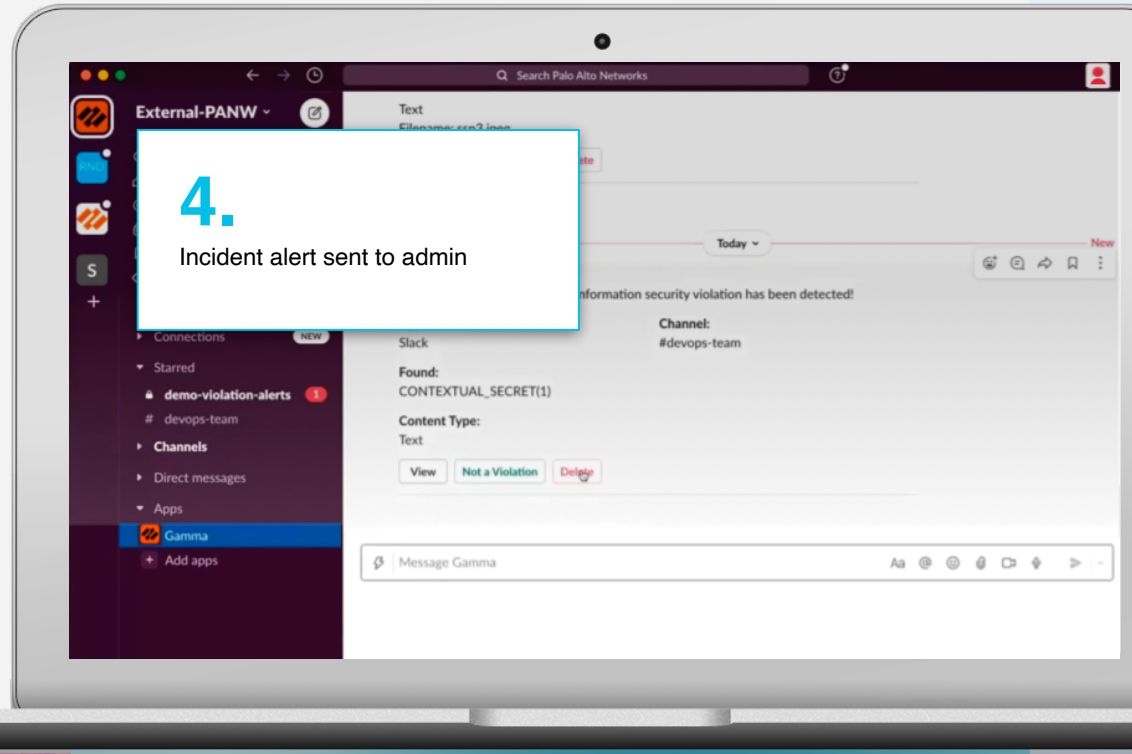
## ADVANCED DLP

- Accurately protect sensitive data in real time
- 1K+ data identifiers, EDM, OCR, ML classification, and natural language processing to detect and protect sensitive data across conversations
- Delivered consistently across SaaS, IaaS, network, branch, and remote workforces



## ADVANCED DLP

- Accurately protect sensitive data in real time
- 1K+ data identifiers, EDM, OCR, ML classification, and natural language processing to detect and protect sensitive data across conversations
- Delivered consistently across SaaS, IaaS, network, branch, and remote workforces



# PRISMA ACCESS: INDUSTRY AND ANALYST RECOGNITION

LEADER

FORRESTER®

ZTNA Wave

LEADER

FROST & SULLIVAN

Secure Web Gateway

LEADER

Gartner®

Firewall Magic Quadrant

CHALLENGER

Gartner®

Security Service Edge Magic Quadrant

LEADER

Gartner®

WAN Edge Magic Quadrant

# THE LARGEST ORGANIZATIONS AND GOVERNMENTS IN THIS WORLD

## USE PRISMA ACCESS FOR ZTNA 2.0

| | | | | | | |
|---|---|---|---|---|---|---|
| Automotive | AISIN | TOYOTA | IVECO | HONDA | VOLKSWAGEN | MICHELIN |
| BFSI | AON | ZURICH | MASTERCARD | ALLY | MOODY'S | FIS GLOBAL |
| Services | ACCENTURE | MCKINSEY & COMPANY | DELOITTE | PWC | KPMG | AMEX GLOBAL BUSINESS TRAVEL |
| Retail and Manufacturing | STARBUCKS | THE HOME DEPOT | RALPH LAUREN | BOEING | DANONE | NESTLE |
| Energy and Utilities | SCHLUMBERGER | BASF | ENEL | EDF ENERGY | EXELON | BAKER HUGHES |
| Technology | FUJITSU | SAP | IBM | HP | SPLUNK | DELL |
| Media and Entertainment | VIACOM CBS | NBC UNIVERSAL | GANNETT | WALT DISNEY TELEVISION | MGM RESORTS | WARNER MUSIC |
| Healthcare | PFIZER | PROVIDENCE ST. JOSEPH HEALTH | CAREFIRST | MOLINA HEALTHCARE | MCKESSON | SUTTER HEALTH |
| Government | U.S. DEPT OF HOMELAND SECURITY | U.S. DEPT OF VETERAN AFFAIRS | DEFENSE INNOVATION UNIT | U.S. DEPT OF ENERGY | U.S. DEPT OF THE INTERIOR | U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES |

**224B**
Threats blocked per day

**4.3M**
Unique security updates delivered per day

BONNEVILLE POWER ADMINISTRATION



paloalto NETWORKS

PRISMA
BY PALO ALTO NETWORKS

# Thank you

paloaltonetworks.com

paloalto NETWORKS