SASE

February 2025

PwC and Palo Alto Networks

Palo Alto Networks:

Palo Alto Networks is the leading cybersecurity company that focuses on protecting digital environments.

PwC:

PwC is a Global System Integrator for Palo Alto Networks and has a global network of skilled professionals.

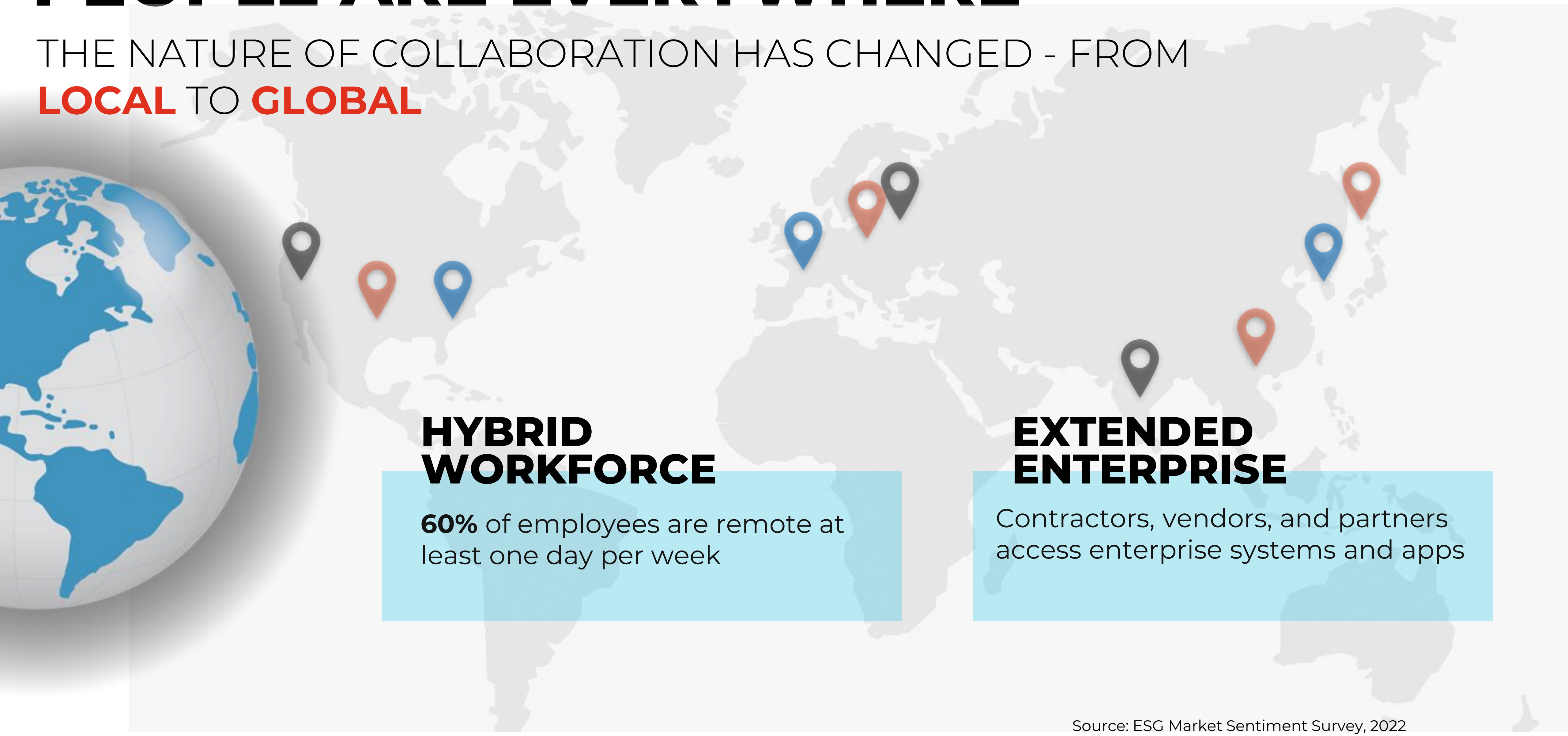
PwC Denmark has been rewarded Advisory Partner of the year in 2022, 2023 and 2024 by Palo Alto Networks.

What is SASE?

Secure Access Service Edge (SASE) is a network architecture that combines wide-area networking (WAN) and network security services, such as secure web gateways (SWG), cloud access security brokers (CASB), firewall-as-a-service (FWaaS), and zero-trust network access (ZTNA), into a single, cloud-delivered service model.

PEOPLE ARE EVERYWHERE

THE NATURE OF COLLABORATION HAS CHANGED - FROM **LOCAL** TO **GLOBAL**



HYBRID WORKFORCE

60% of employees are remote at least one day per week

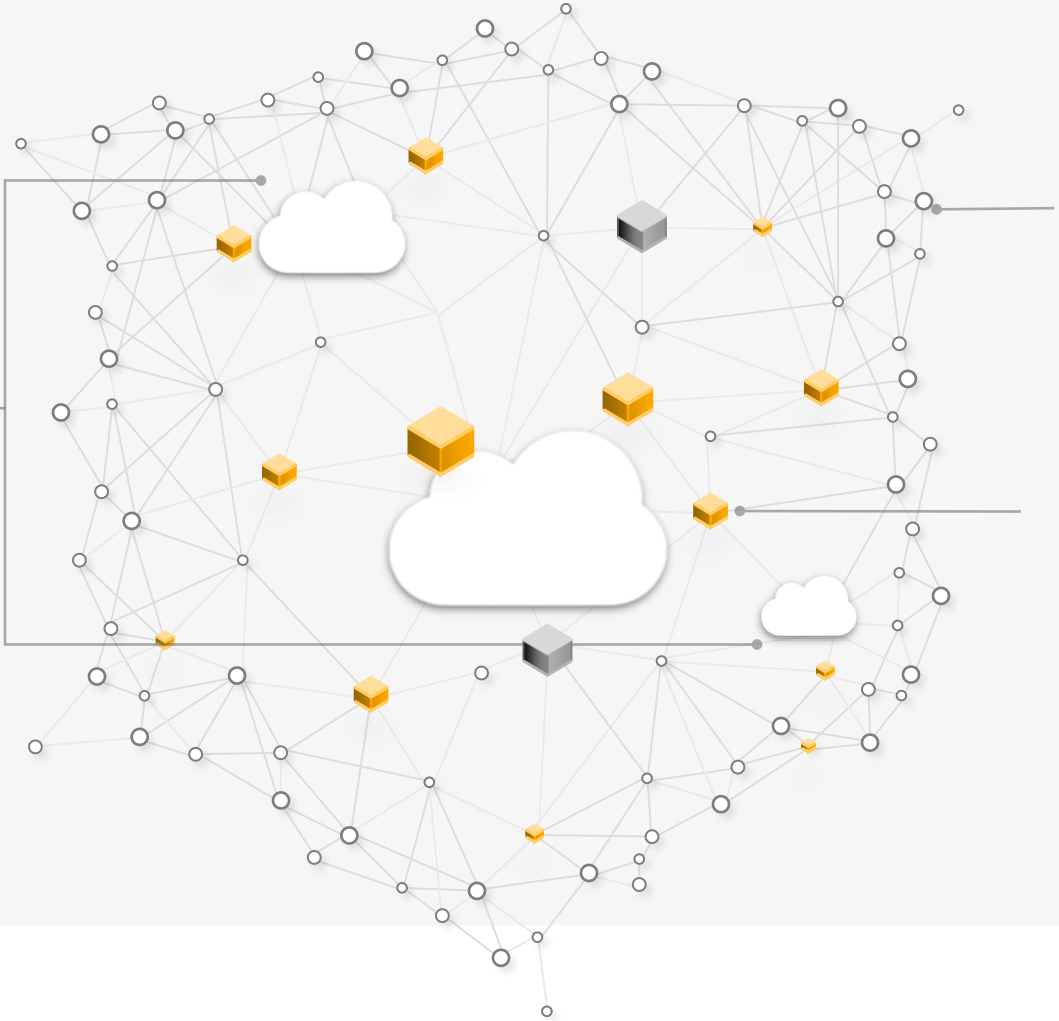
EXTENDED ENTERPRISE

Contractors, vendors, and partners access enterprise systems and apps

Source: ESG Market Sentiment Survey, 2022

DATA ARE EVERYWHERE

THE PERIMETER HAS **CHANGED**.



CLOUD SERVICES

Enterprise data is dispersed across various SaaS applications

PERSONAL DEVICES

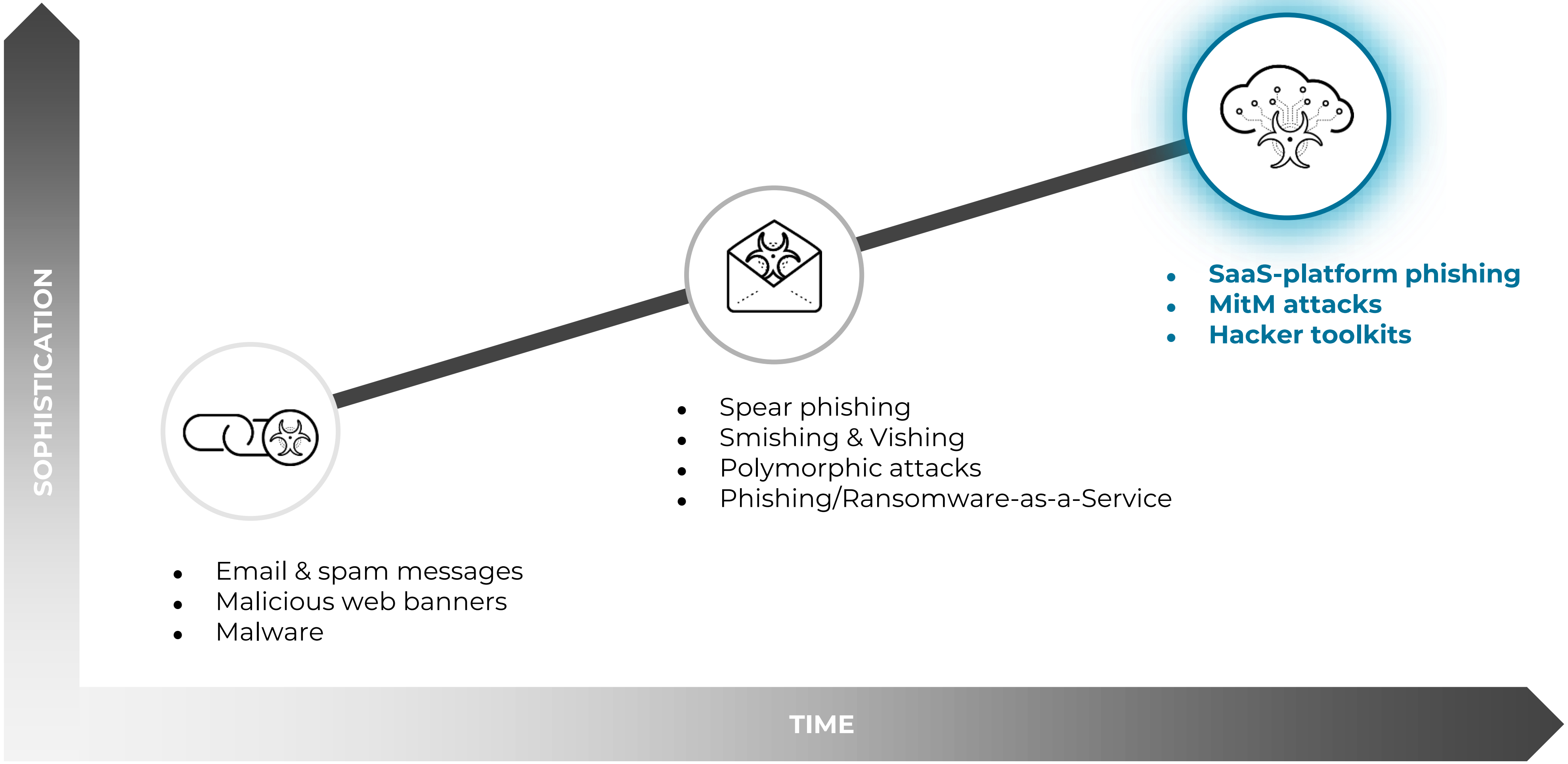
Interchanging of corporate devices for personal use or work on personal devices

SERVERS & IoT

Branch servers and IoT devices connect and exchange data over the Internet

WEB THREATS ARE EVERYWHERE

AND MORE **EVASIVE**, **SOPHISTICATED**, AND **WIDESPREAD**



- Email & spam messages
- Malicious web banners
- Malware

- Spear phishing
- Smishing & Vishing
- Polymorphic attacks
- Phishing/Ransomware-as-a-Service

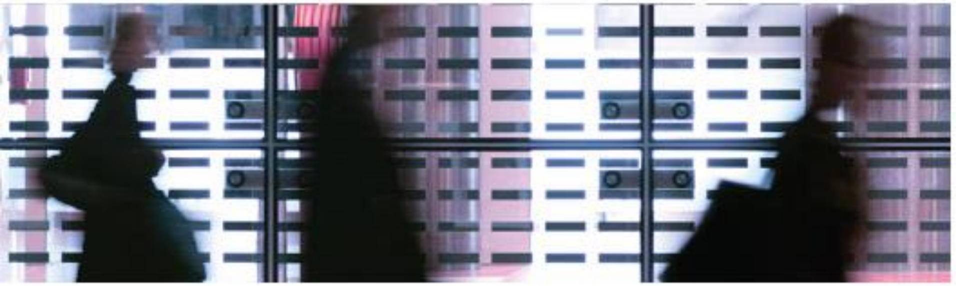
- **SaaS-platform phishing**
- **MitM attacks**
- **Hacker toolkits**

61 %

anvender eller planlægger at anvende AI i arbejdet med cybersikkerhed

60 %

er mere bekymrede for cybertrusler i dag end for 12 måneder siden



Cybercrime Survey 2024

41 %

af virksomhederne har beredskab som højest prioriterede investering

pwc

PwC

WHAT'S AT RISK?

THE THREE P'S

PROTECTION

Poor security defenses will increase the risk of a data breach

84% CCS

of organizations faced at least one successful phishing attack

PRODUCTIVITY

Poor user experience will impact remote workforce collaboration

83%

have increased connectivity issues from remote users

PERFORMANCE

Poor network connectivity and availability will impact IT operations

$5,600

lost for every minute of downtime according to Gartner

Sources: State of the Phish, Proofpoint, 2023
Market Sentiment Survey, ESG, 2022

SASE Business values

- **Enhanced Security**: SASE provides a comprehensive security framework that helps protect against a wide range of threats by integrating multiple security functions into a unified solution.
- **Simplified Management**: By consolidating networking and security services into a single platform, SASE simplifies management and reduces the complexity associated with managing multiple disparate solutions.
- **Scalability:** As a cloud-delivered service, SASE can easily scale up or down based on organizational needs, making it ideal for businesses of all sizes, including those with a distributed workforce.
- **Improved Performance**: SASE leverages a global network of points of presence (PoPs) to reduce latency and improve application performance, ensuring a better user experience.
- **Cost Efficiency:** By reducing the need for multiple on-premises hardware appliances and streamlining operations, SASE can lower overall IT and security costs.
- **Support for Remote Work**: With more employees working remotely, SASE provides secure and seamless access to applications and data from anywhere, supporting a distributed workforce.
- **Zero Trust Network Access (ZTNA):** SASE incorporates ZTNA principles, ensuring that access to resources is granted based on strict identity verification and continuous trust assessment, reducing the risk of unauthorized access.
- **Cloud Readiness**: SASE is designed to support cloud-native environments, making it easier for organizations to adopt and secure cloud services and applications.
- **Overall,** SASE offers a modern approach to networking and security that aligns with the needs of today's dynamic and distributed IT environments.

Prisma SASE 3.0

Introducing the
Next Chapter of SASE

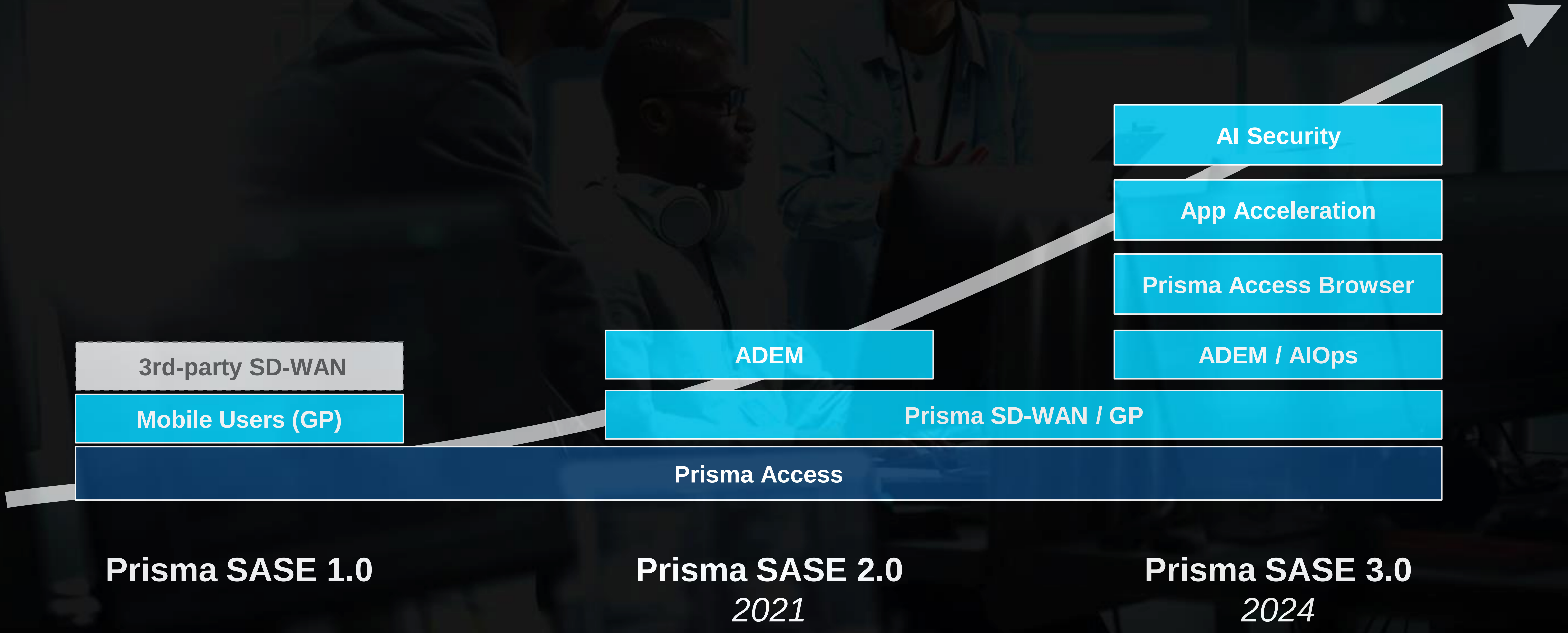
Kim Elgaard

PRISMA SASE

The industry’s only SASE solution that secures both managed and unmanaged devices with a natively integrated enterprise browser.

Any user. Any device. Any application.

Prisma SASE 3.0: The next chapter of SASE at Palo Alto Networks



AI Security

App Acceleration

Prisma Access Browser

3rd-party SD-WAN

ADEM

ADEM / AIOps

Mobile Users (GP)

Prisma SD-WAN / GP

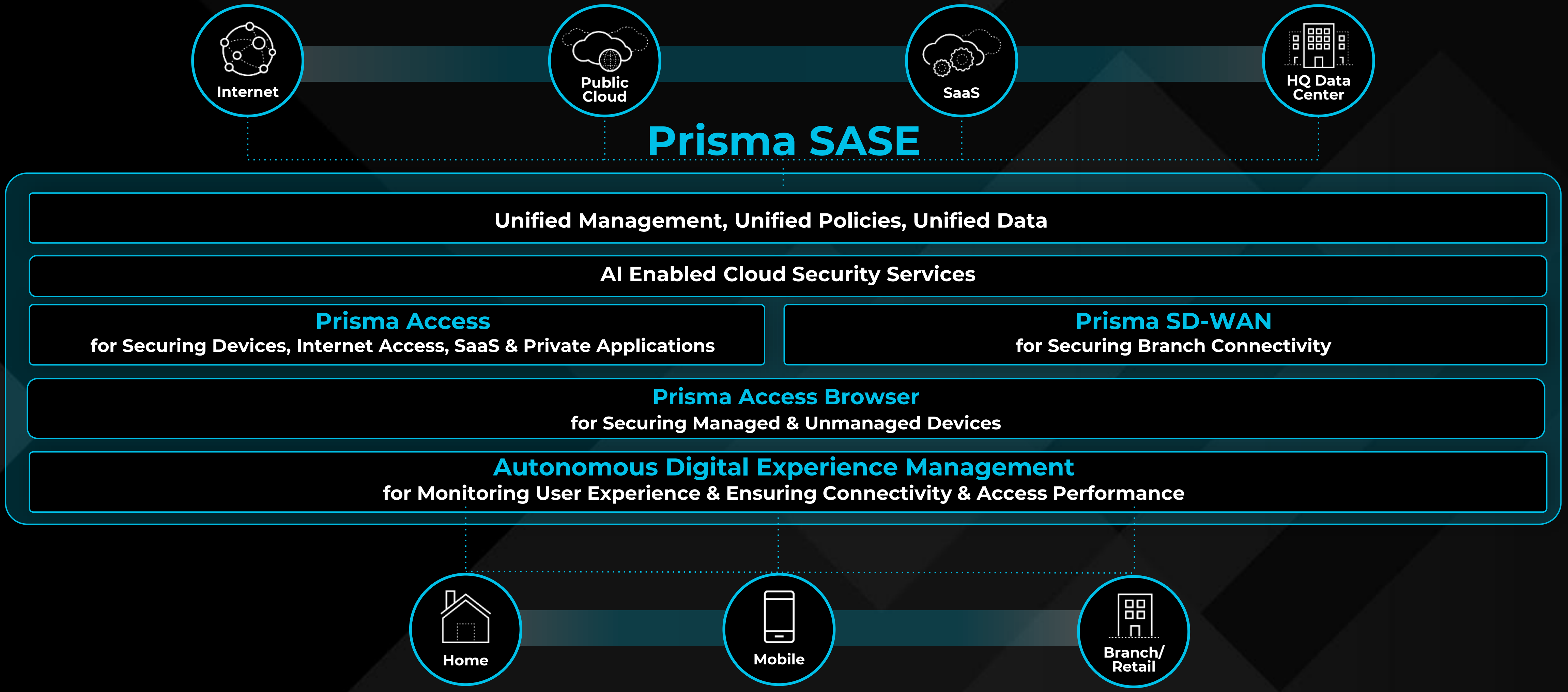
Prisma Access

Prisma SASE 1.0

Prisma SASE 2.0
2021

Prisma SASE 3.0
2024

Removing point products, consolidating vendors, reducing complexity, evolving security



Prisma SASE

Unified Management, Unified Policies, Unified Data

AI Enabled Cloud Security Services

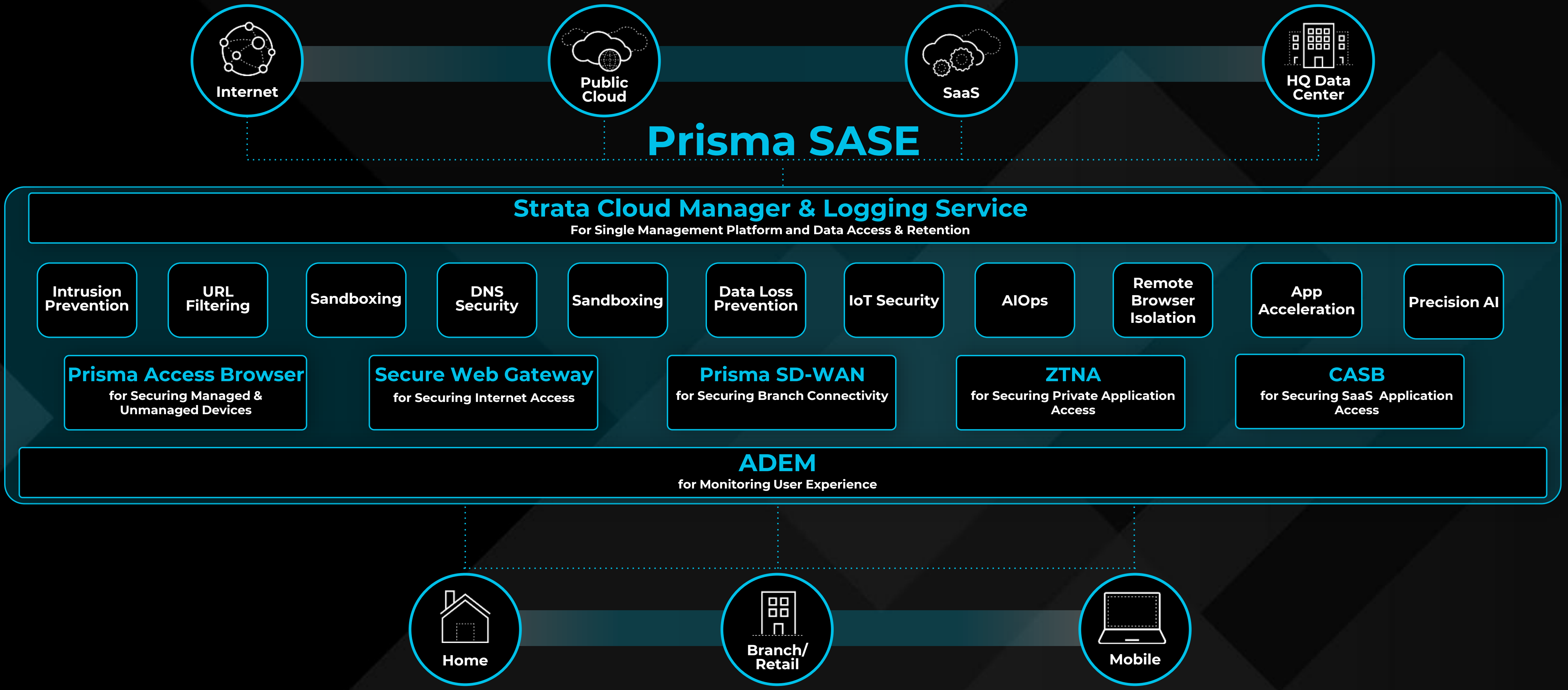
Prisma Access
for Securing Devices, Internet Access, SaaS & Private Applications

Prisma SD-WAN
for Securing Branch Connectivity

Prisma Access Browser
for Securing Managed & Unmanaged Devices

Autonomous Digital Experience Management
for Monitoring User Experience & Ensuring Connectivity & Access Performance

Prisma SASE is the Industry Leader for Single Vendor SASE



Internet

Public Cloud

SaaS

HQ Data Center

Prisma SASE

Strata Cloud Manager & Logging Service

For Single Management Platform and Data Access & Retention

Intrusion Prevention

URL Filtering

Sandboxing

DNS Security

Sandboxing

Data Loss Prevention

IoT Security

AIOps

Remote Browser Isolation

App Acceleration

Precision AI

Prisma Access Browser

for Securing Managed & Unmanaged Devices

Secure Web Gateway

for Securing Internet Access

Prisma SD-WAN

for Securing Branch Connectivity

ZTNA

for Securing Private Application Access

CASB

for Securing SaaS Application Access

ADEM

for Monitoring User Experience

Home

Branch/ Retail

Mobile

Prisma SASE : Securing Work Where it Happens

Prisma Access Browser

Data Security

App Acceleration

ADEM

Prisma SASE : Securing Work Where it Happens

Prisma Access Browser

Data Security

App Acceleration

ADEM

A web first world has transformed the way we work

The Browser is the Primary Hub of Productivity

85%-100%

of a worker's day is spent in the browser.

Palo Alto Networks/Omdia Forrester

But Browsers are Vulnerable

95%

of organizations reported a security incident originating in the browser.

Palo Alto Networks/Omdia

328

vulnerabilities were found in the browser in 2024.

CVE Details

Widespread Use of SaaS, Web, & GenAI apps via the Browser

~10,000

SaaS and web apps organizations use today, on average.

Venasolutions.com

But Organizations Lack Visibility & Control in SaaS, Web, & GenAI Apps

65%

of organizations have limited to no control into what data is shared in AI tools.

Palo Alto Networks/Omdia

Employees & Third Parties Leverage Unmanaged Devices to Get Work Done

~90%

of organizations enable employees access to corporate applications with personal devices.

Palo Alto Networks/Omdia

But Unsecure Devices Compromise Top Organizations

~85%

of successful ransomware compromises originate from unmanaged devices.

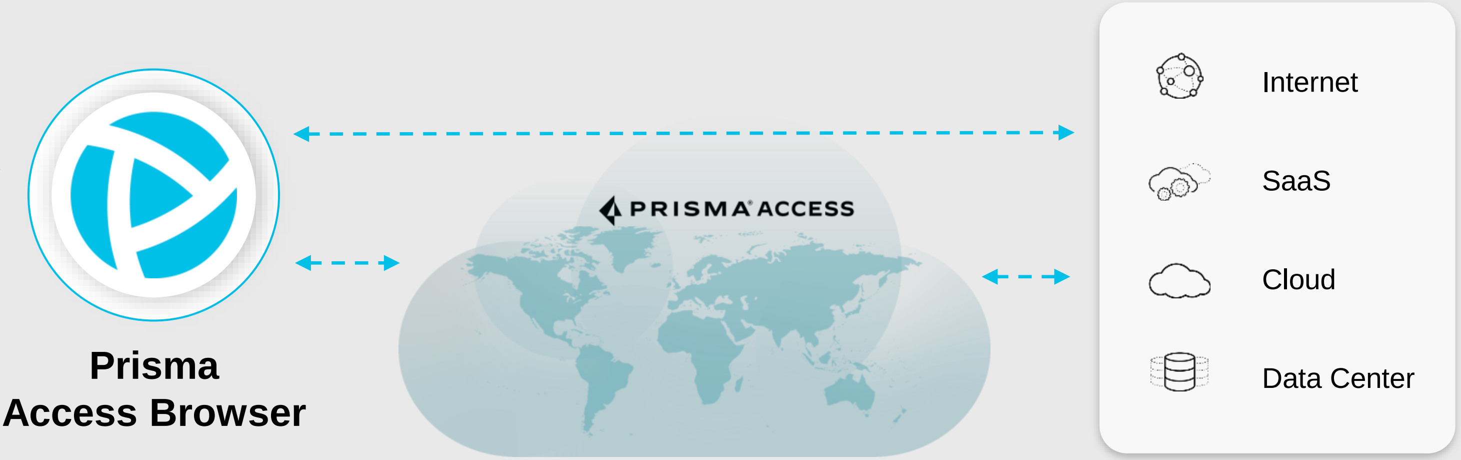
Microsoft

Prisma Access Browser

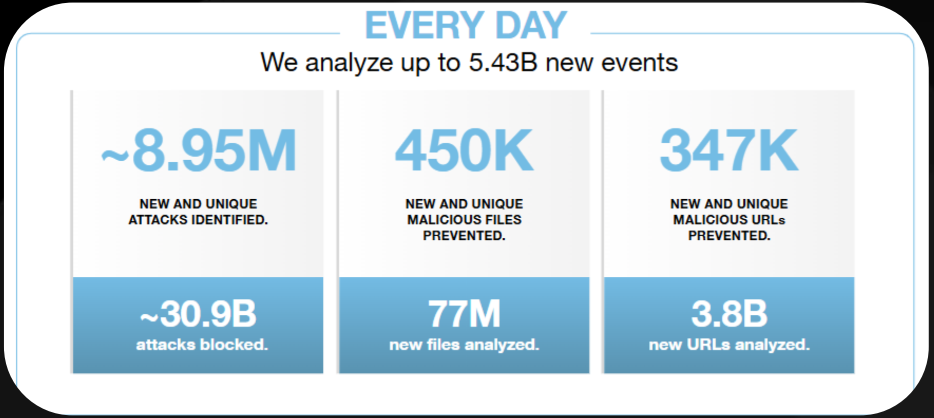
- Any - User, Device, Location, Application
- Based on Chromium
- Secure work in the browser
- Powered by Palo Alto Networks Security

Available on

iOS



Prisma Access Browser



EVERY DAY

We analyze up to 5.43B new events

~8.95M NEW AND UNIQUE ATTACKS IDENTIFIED.	450K NEW AND UNIQUE MALICIOUS FILES PREVENTED.	347K NEW AND UNIQUE MALICIOUS URLs PREVENTED.
~30.9B attacks blocked.	77M new files analyzed.	3.8B new URLs analyzed.

By **2030** enterprise browsers will be the **core platform** for delivering workforce productivity and security software on managed and unmanaged devices for a seamless hybrid work experience.

Gartner

Prisma Access Browser Use Cases

Third Parties and Contractors

- M&As
- Call Centers
- Frontline and Field Workers
- Lower Cost of Shipping Laptops
- Reduce VDI

BYOD

- Workforce Agility
- Device Freedom
- Enable Mobile
- After Hours

Anything you can think of..

- Support Undecryptable Traffic
  (e.g., QUIC, Microsoft 365 SLA, and more)
- Last-Mile Data Protection
- Enable secure usage of GenAI
- Business Continuity Plan
- Secure Privileged Users
- Insider Threats and Browser Hunting
- Forensics and Compliance
- Access to Non-Managed Accounts
  (e.g., Virtual Deal Room, Financial Services)

Prisma SASE 3.0: Securing Work Where it Happens

Prisma Access Browser

Data Security

App Acceleration

ADEM

Every company is digital, fueled by data

CLOUD SERVICES

Enterprise data is decentralized and dispersed across **PaaS** and **IaaS**

SAAS APPLICATIONS

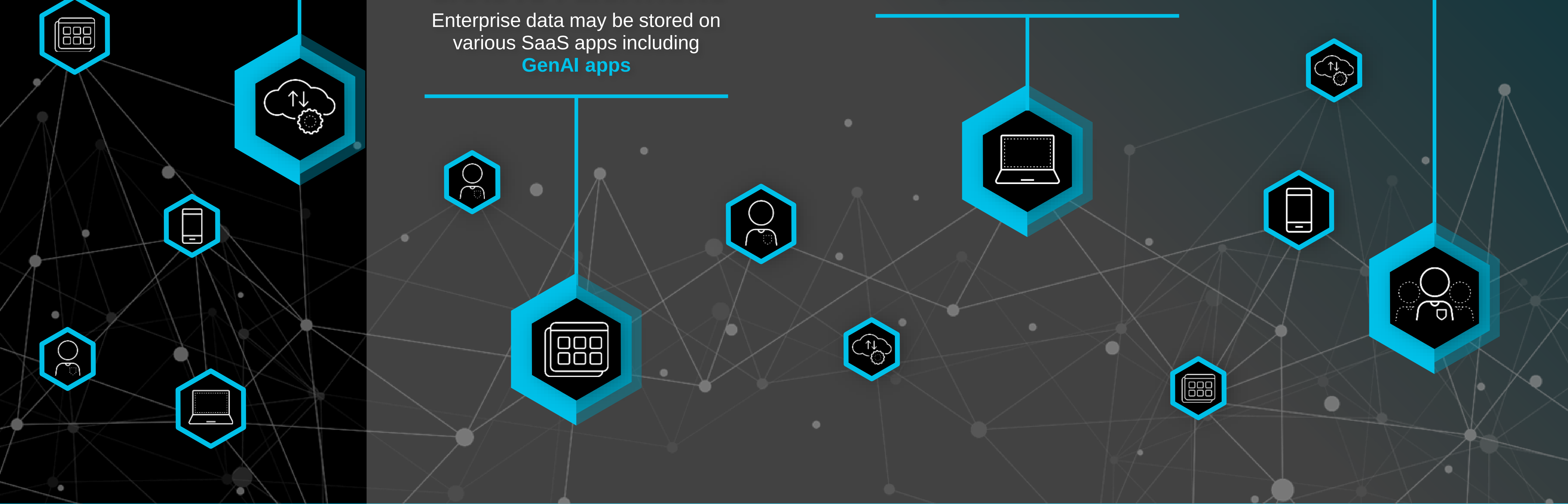
Enterprise data may be stored on various SaaS apps including **GenAI apps**

DEVICES

Company data can be stored on both managed and **unmanaged personal devices**

USERS

Employees, **third-party contractors** and **partners** access data from various locations (HQ, branch, home, remote)



Protecting this data has become challenging

130+

Number of **SaaS applications** an enterprise typically purchases

40%

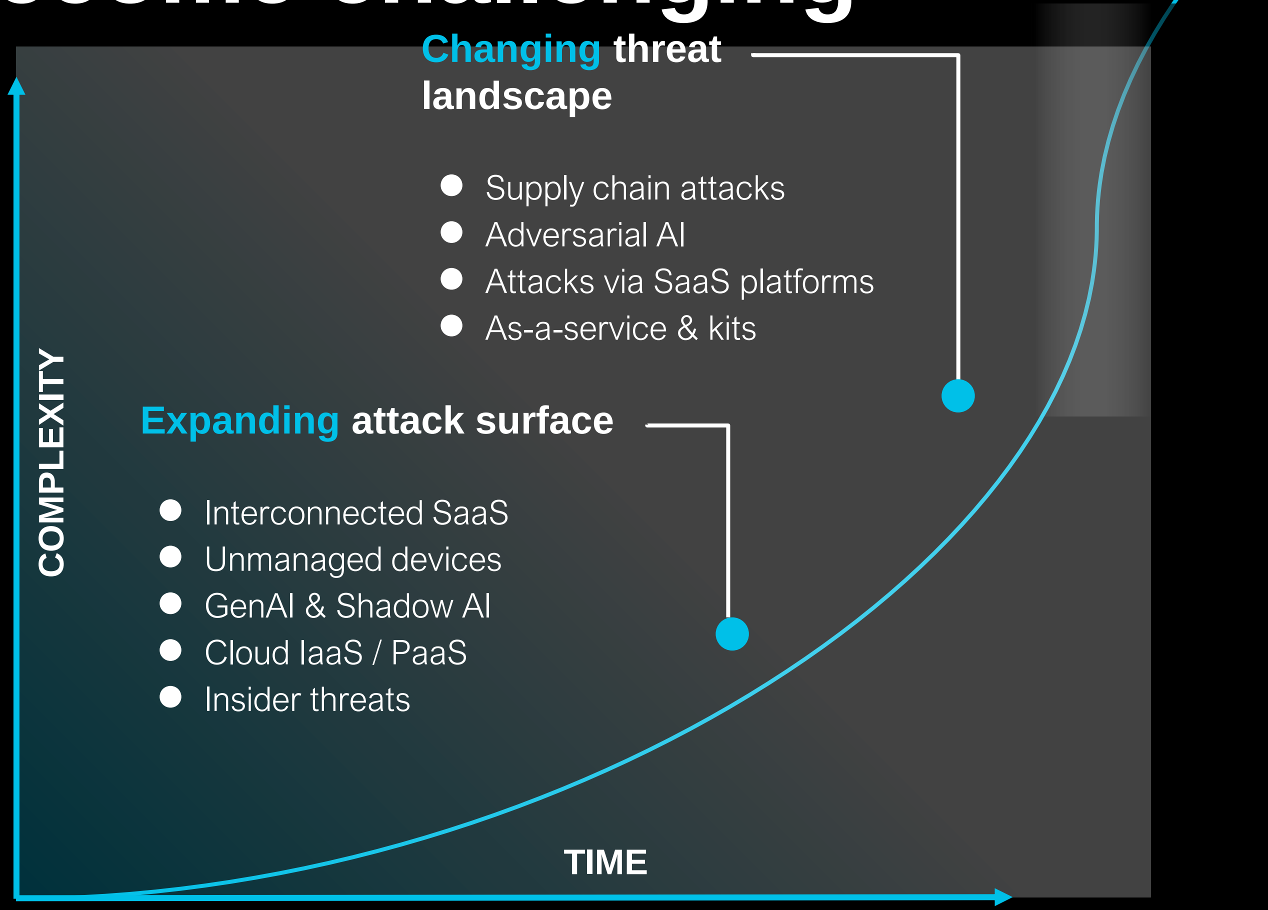
of organizations experienced a security incident from **unmanaged devices**

55%

of employees have used **unapproved GenAI tools** at work

81%

of organizations have **exposed sensitive SaaS data**



Changing threat landscape

- Supply chain attacks
- Adversarial AI
- Attacks via SaaS platforms
- As-a-service & kits

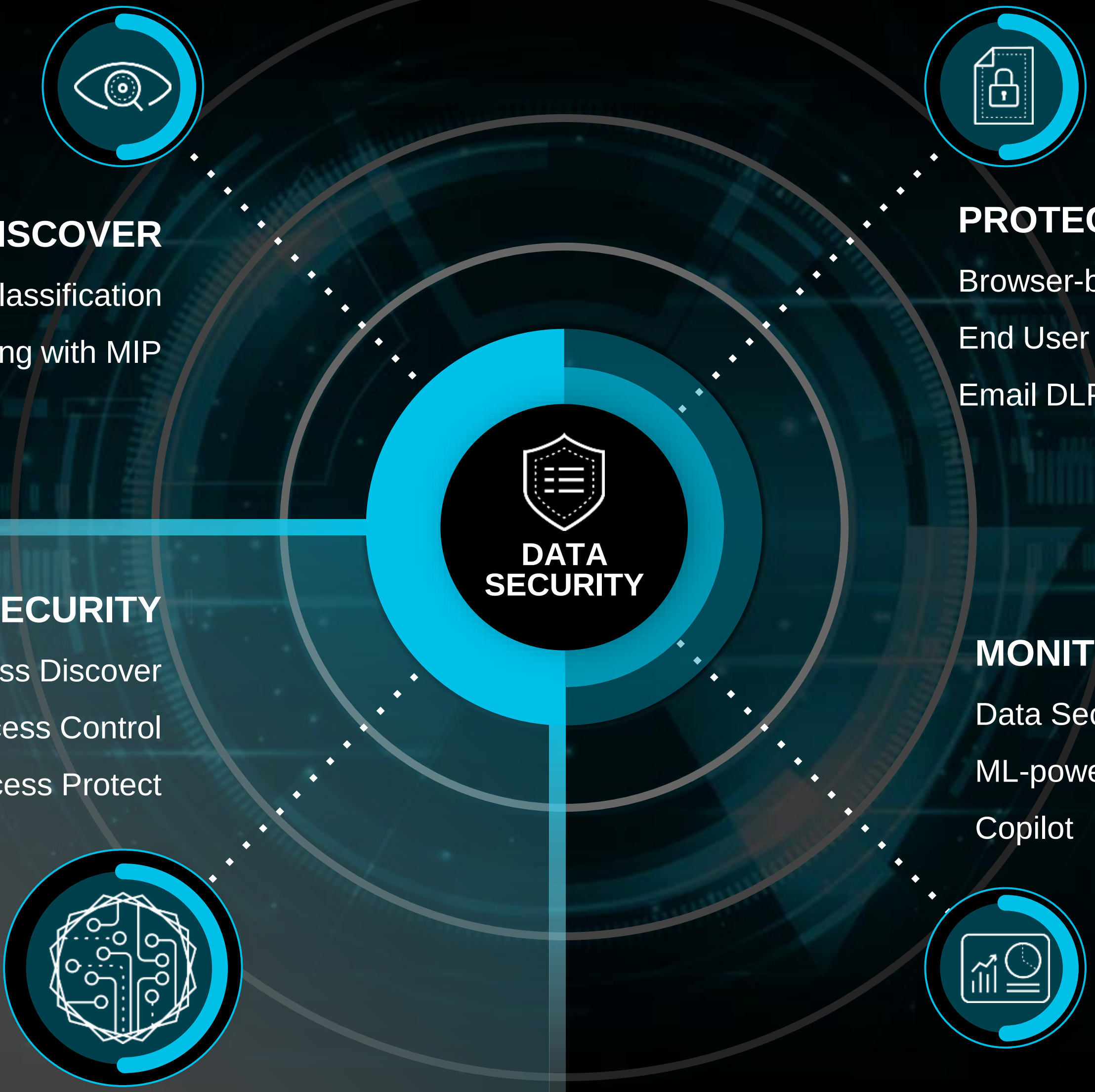
Expanding attack surface

- Interconnected SaaS
- Unmanaged devices
- GenAI & Shadow AI
- Cloud IaaS / PaaS
- Insider threats

THIS TRANSFORMATION CREATES UNIQUE SECURITY CHALLENGES

Sources: Salesforce, Nov. 2023; Device Security Study, Omdia 2024

Introducing NEW AI-powered capabilities to protect data



DISCOVER

LLM-powered Data Classification

Data Labeling with MIP

PROTECT

Browser-based DLP

End User Coaching

Email DLP

GEN AI SECURITY

AI Access Discover

AI Access Control

AI Access Protect

MONITOR

Data Security Dashboard

ML-powered Behavior Threats

Copilot

Prisma SASE 3.0: Securing Work Where it Happens

Prisma Access Browser

Data Security

App Acceleration

ADEM

Slow app performance drains productivity and frustrates users

Slow downloads of large files

Delayed load times of Business Apps

Choppy video quality due to poor connectivity

The average worker loses

46 minutes per day

to slow technology.

Individualized optimization further boosts throughput

Custom packet shaper for each user individually to compensate for:

Network Context

WiFi, Cellular, intermittent lossy connectivity, etc.

Device Context

Hardware and OS differences (e.g., Desktop/mobile, Windows vs. iOS vs. Android)

App Context

Live vs. near live, bandwidth-sensitive vs. latency-sensitive apps

Prisma SASE : Securing Work Where it Happens

Prisma Access Browser

Data Security

App Acceleration

ADEM

Distributed Apps and Hybrid Workforces Lead to Op

Users Everywhere

77% of employees choose hybrid work.

Gartner

Apps Everywhere

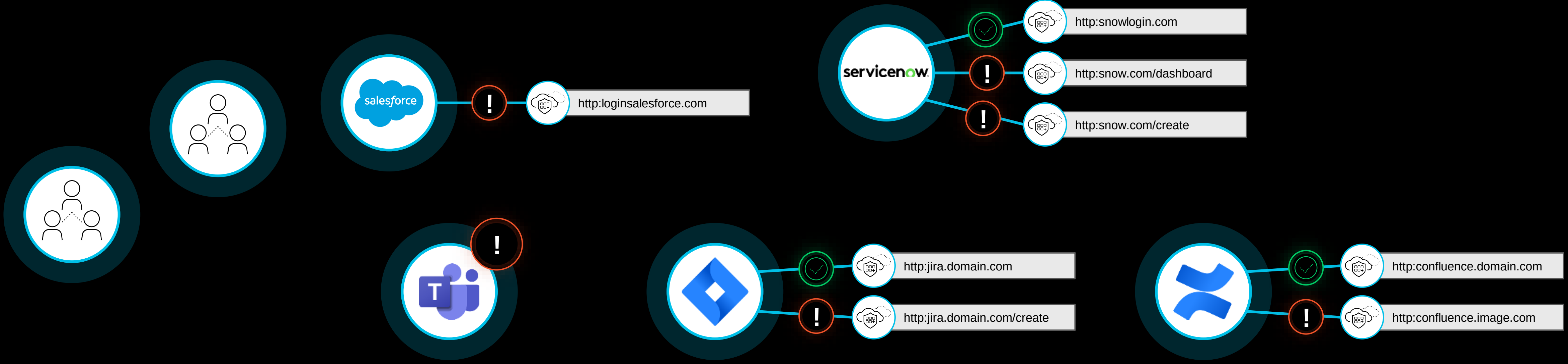
Organizations maintain an average of over 110 SaaS apps.

Gartner

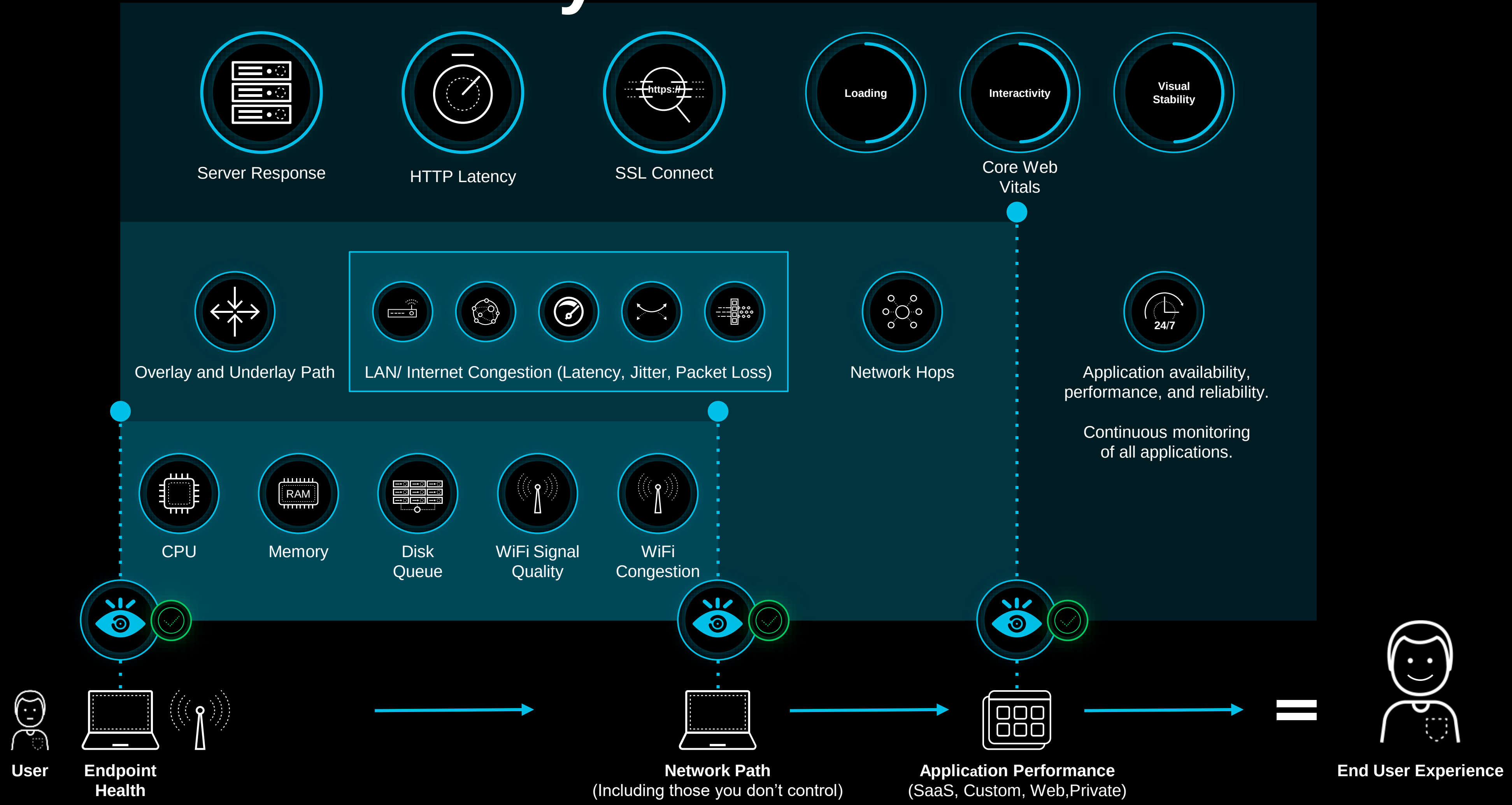
App Interdependencies Everywhere

56% of IT Managers do not have a complete view of dependencies between applications

Forrester



Maintain Full Visibility to Keep Employees Productive From Anywhere



paloalto NETWORKS | PRISMA

Thank You

paloaltonetworks.com

www.pwc.dk

Together we succeed…

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.