CRYPTONET LABS

La sicurezza dell'endpoint e l'accesso sicuro alle proprie applicazioni

Fulcro della Digital Transformation

Treviso, 23/5/2019

Relatore

Edoardo Montrasi

- IT/OT Senior Security Consultant
- Technical Pre-sales & Delivery
- PCI QSA – ISO 27001 LA

CRYPTONET LABS

COMPLIANCE

CONSULENZA

OFFENSIVE SECURITY

DEFENSIVE SECURITY

AGENDA

1 Digital Transformation

EVOLUZIONE DELLO SCENARIO ICT
POSSIAMO ANCORA PARLARE DI PERIMETRO?

2 Internet diventa rete aziendale

SECURITY STACK ON-PREMISES: LIMITAZIONI
ESIGENZE DEGLI UTENTI E REQUISITI DI SICUREZZA

3 Accesso sicuro dall'endpoint

- ALLE PROPRIE APPLICAZIONI, CON ZSCALER PRIVATE ACCESS
- A INTERNET, CON ZSCALER INTERNET ACCESS

4 Protezione dell'endpoint

- DA MINACCE MALWARE EVOLUTE, CON SENTINEL ONE

5 Benefici e cost savings

AGENDA

1 Digital Transformation

EVOLUZIONE DELLO SCENARIO ICT
POSSIAMO ANCORA PARLARE DI PERIMETRO?

2 Internet diventa rete aziendale

SECURITY STACK ON-PREMISES: LIMITAZIONI
ESIGENZE DEGLI UTENTI E REQUISITI DI SICUREZZA

3 Accesso sicuro dall'endpoint

- ALLE PROPRIE APPLICAZIONI, CON ZSCALER PRIVATE ACCESS
- A INTERNET, CON ZSCALER INTERNET ACCESS

4 Protezione dell'endpoint

- DA MINACCE MALWARE EVOLUTE, CON SENTINEL ONE

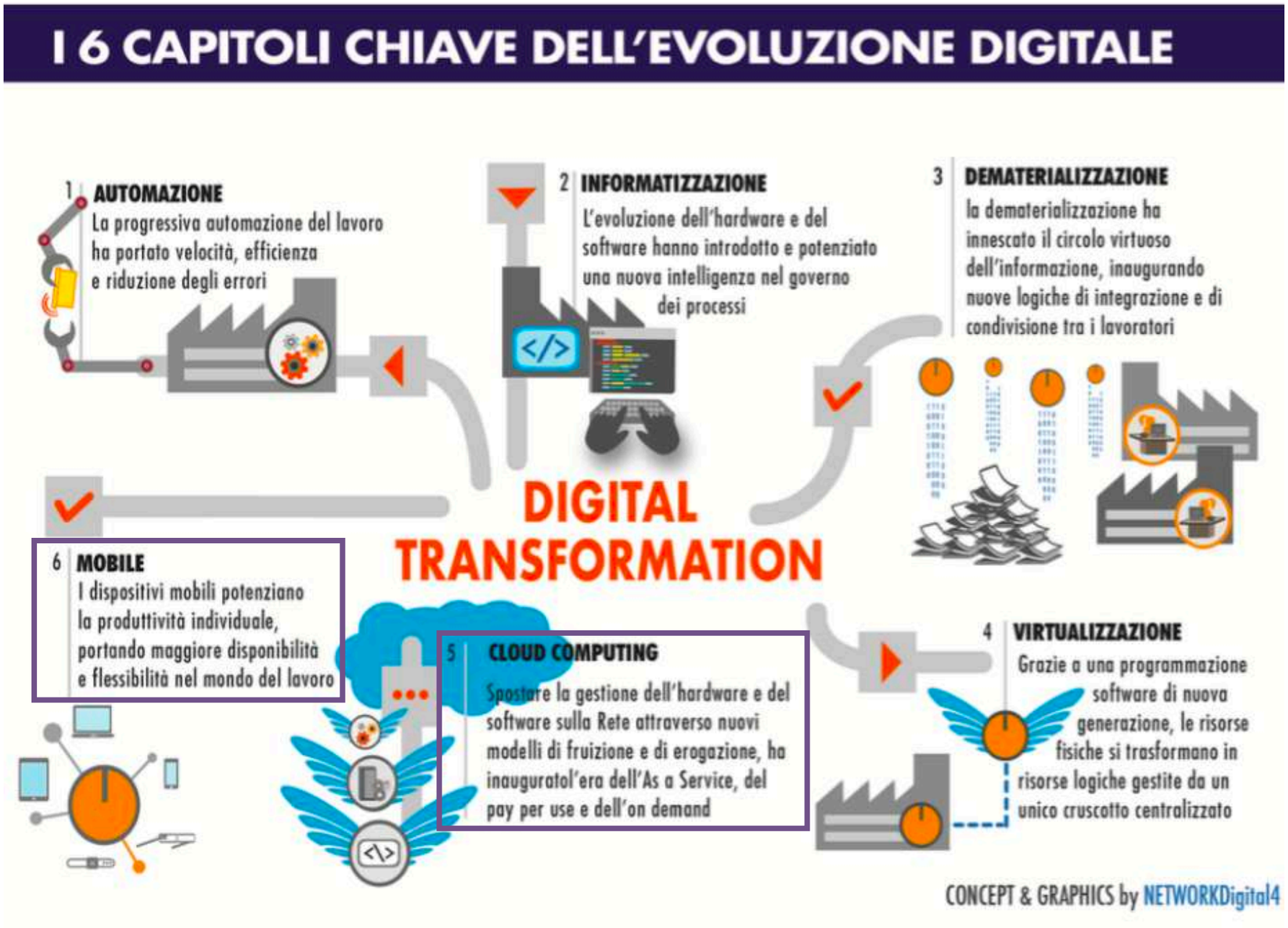
5 Benefici e cost savings

Digital Transformation

La trasformazione digitale è l'opportunità
di ridisegnare e migliorare i processi
che governano il business,
utilizzando una combinazione
di diverse soluzioni tecnologiche,
riducendo le ridondanze e gli errori legati
*ad attività manuali non strategiche**

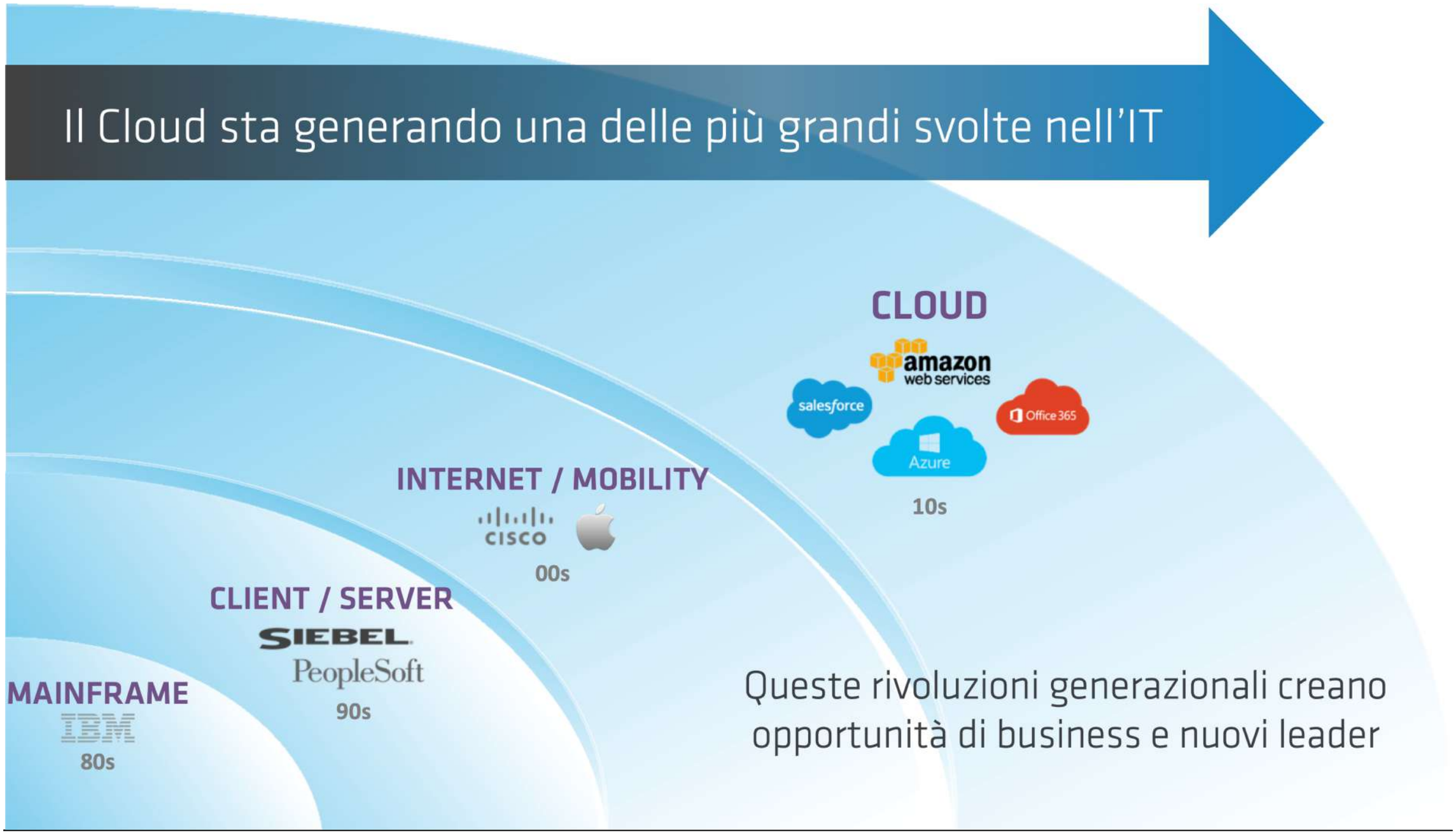
** Da https://www.startupbusiness.it/cose-la-digital-transformation-e-i-suoi-6-pilastri/89908/*

La trasformazione digitale



Da https://www.startupbusiness.it/cose-la-digital-transformation-e-i-suoi-6-pilastri/89908/

Come sta evolvendo lo scenario ICT?



E i nostri utenti? Smart working

Esiste ancora il perimetro aziendale?

AGENDA

1 Digital Transformation

EVOLUZIONE DELLO SCENARIO ICT
POSSIAMO ANCORA PARLARE DI PERIMETRO?

2 Internet diventa rete aziendale

SECURITY STACK ON-PREMISES: LIMITAZIONI
ESIGENZE DEGLI UTENTI E REQUISITI DI SICUREZZA

3 Accesso sicuro dall'endpoint

- ALLE PROPRIE APPLICAZIONI, CON ZSCALER PRIVATE ACCESS
- A INTERNET, CON ZSCALER INTERNET ACCESS

4 Protezione dell'endpoint

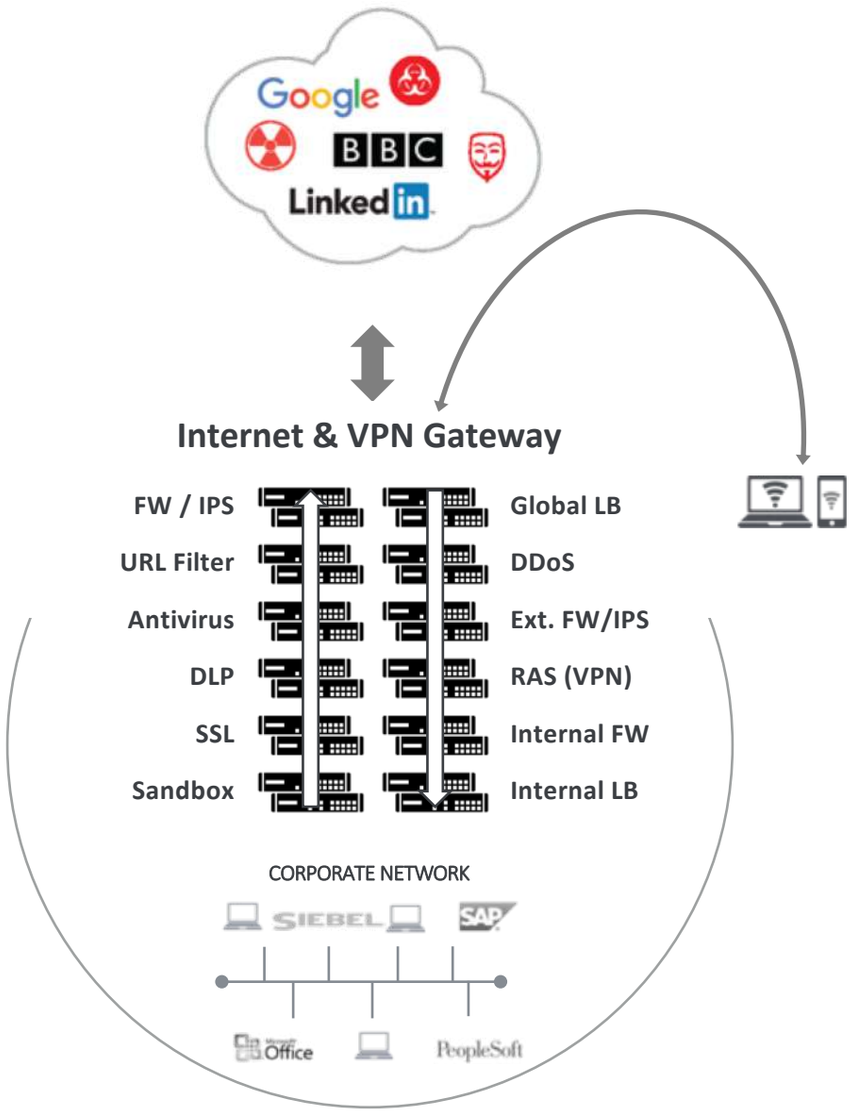
- DA MINACCE MALWARE EVOLUTE, CON SENTINEL ONE

5 Benefici e cost savings

Approccio tradizionale

ALLA SICUREZZA PERIMETRALE

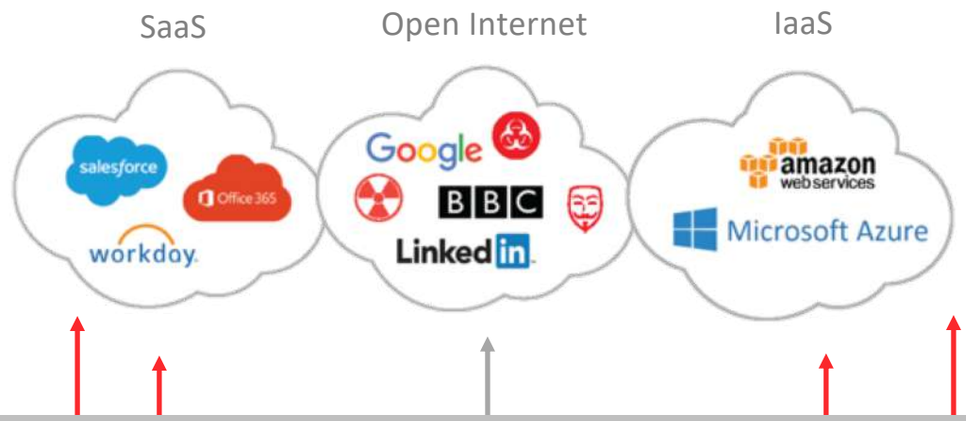
Internet gateways
Secure access to the Internet



VPN gateways
Remote access to DC apps

Circa 1987 – 1994– 1999 – 2000 – 2004

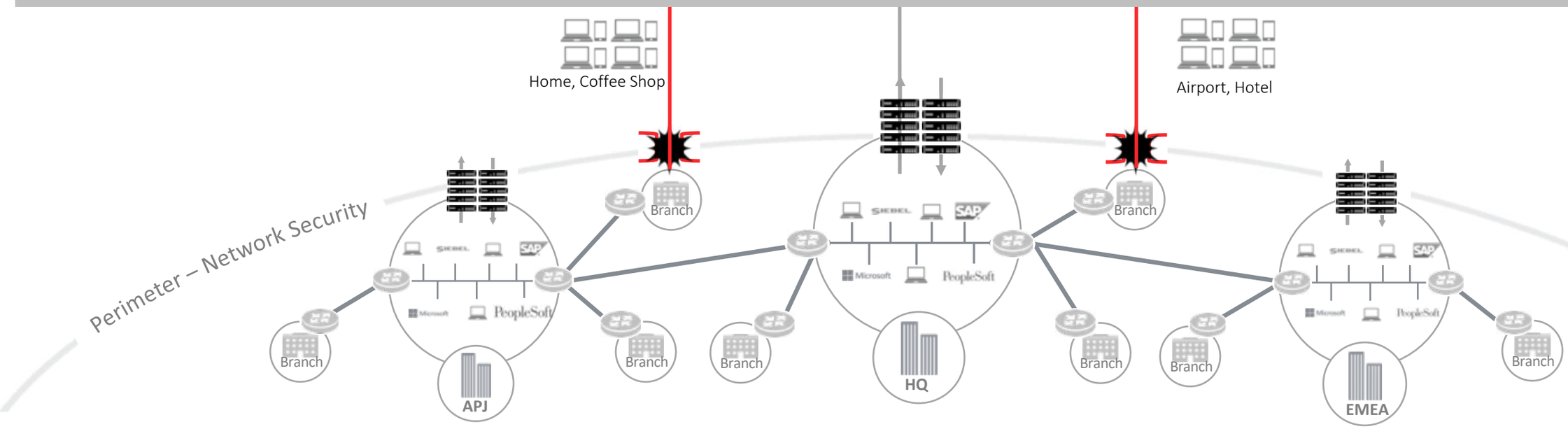
Cloud e mobilità: la logica cambia



Microsoft

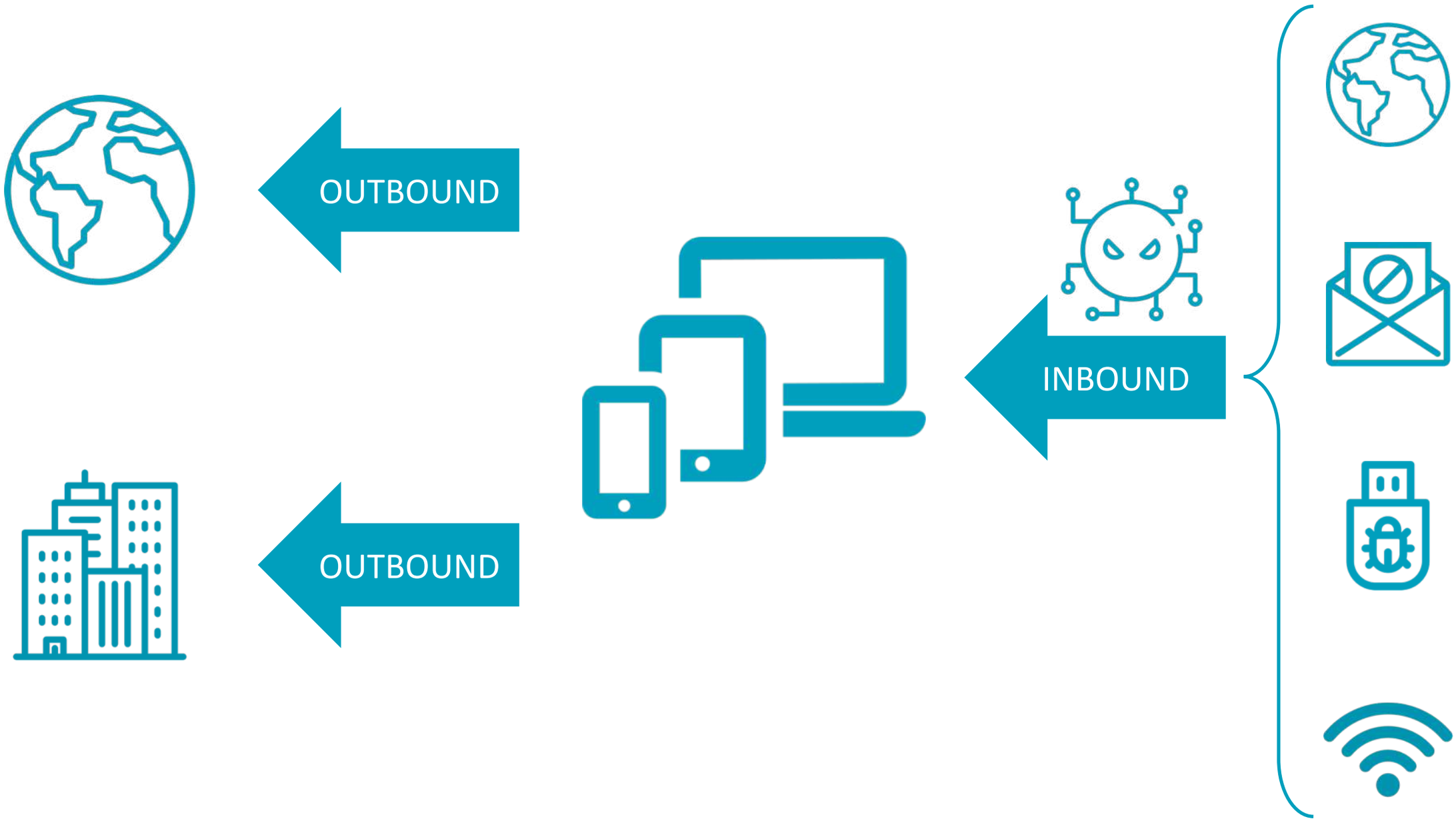
“Office 365 was built to be accessed via direct Internet connection”

How do you secure a network (Internet) you don’t control?



Endpoint: fulcro della trasformazione

SCENARI DI SICUREZZA



Compliance

UN ULTERIORE DRIVER PER L'ENDPOINT SECURITY

Art. 32 – Sicurezza del trattamento
1. […] il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: […]
- b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare […] dall'accesso, in modo accidentale o illegale, a dati personali […]

ISO 27001

A.6.2.1 e A.6.2.2 – A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices [… and] to protect information accessed, processed and stored at teleworking sites.
A.12.2.1 - Detection, prevention and recovery controls to protect against malware shall be implemented, […]

PCI

Req. 5 - Protect all systems against malware and regularly update anti-virus software […]
Req. 1.4 – Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network […], and which are also used to access the CDE.

AGENDA

1 Digital Transformation

EVOLUZIONE DELLO SCENARIO ICT
POSSIAMO ANCORA PARLARE DI PERIMETRO?

2 Internet diventa rete aziendale

SECURITY STACK ON-PREMISES: LIMITAZIONI
ESIGENZE DEGLI UTENTI E REQUISITI DI SICUREZZA

3 Accesso sicuro dall'endpoint

- ALLE PROPRIE APPLICAZIONI, CON ZSCALER PRIVATE ACCESS
- A INTERNET, CON ZSCALER INTERNET ACCESS

4 Protezione dell'endpoint

- DA MINACCE MALWARE EVOLUTE, CON SENTINEL ONE

5 Benefici e cost savings

Accesso verso Internet

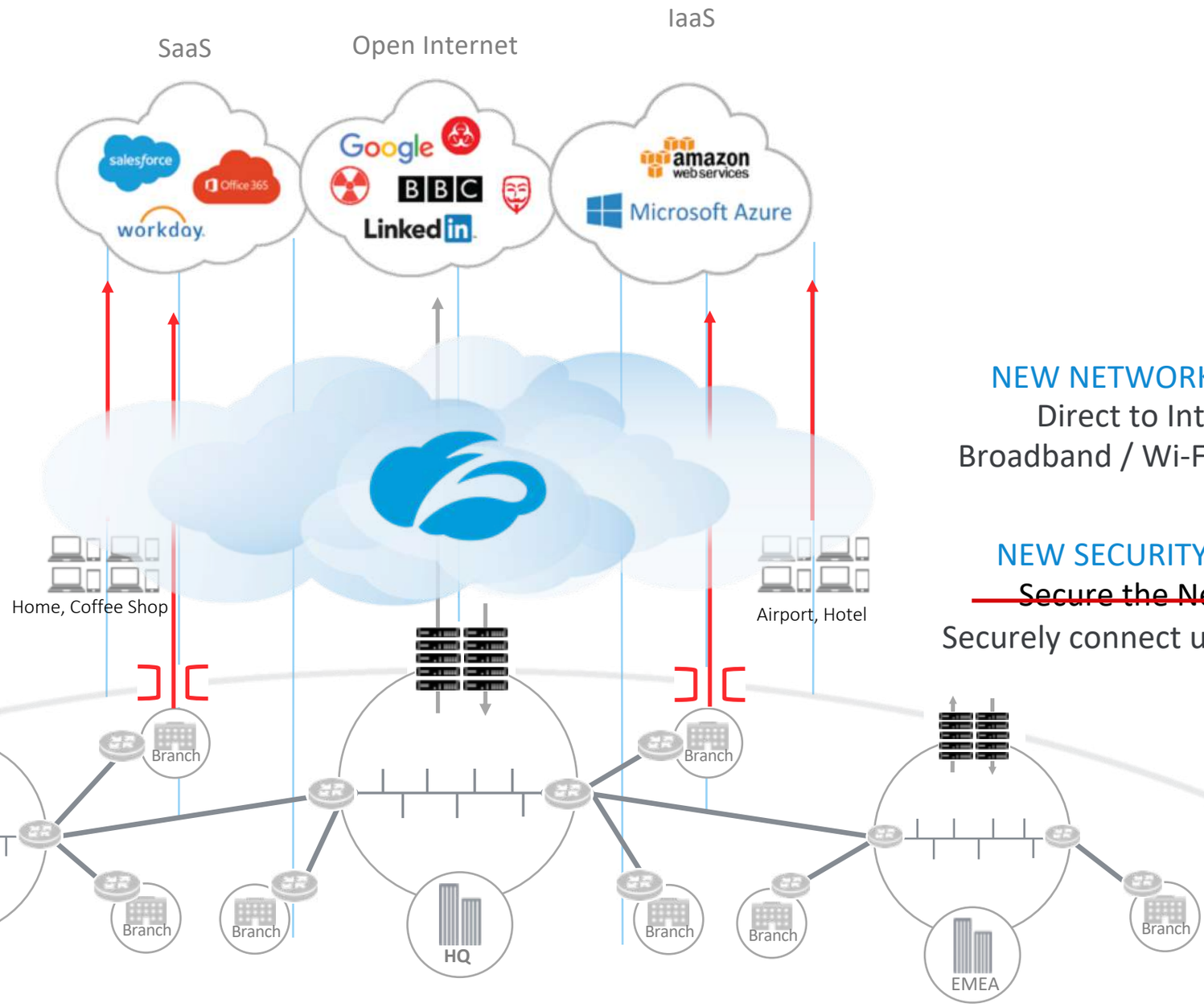
SCENARI DI SICUREZZA

Dall'endpoint verso Internet

ACCESSO SICURO VERSO CIO' CHE E' UNTRUSTED

OLD NETWORK MODEL
Hub-and-Spoke
MPLS / VPN

OLD SECURITY MODEL
Secure the Corporate Network



NEW NETWORK MODEL
Direct to Internet
Broadband / Wi-Fi / LTE / 5G

NEW SECURITY MODEL
~~Secure the Network~~
Securely connect users to apps

Zscaler Internet Access

Consolidate and simplify point appliances

ACCESS CONTROL

- CLOUD FIREWALL
- CLOUD APPS (CASB)
- URL FILTERING
- BANDWIDTH QOS

THREAT PREVENTION

- ANTI-VIRUS
- INTRUSION PREVENTION
- ADVANCED PROTECTION
- CLOUD SANDBOX

DATA PROTECTION

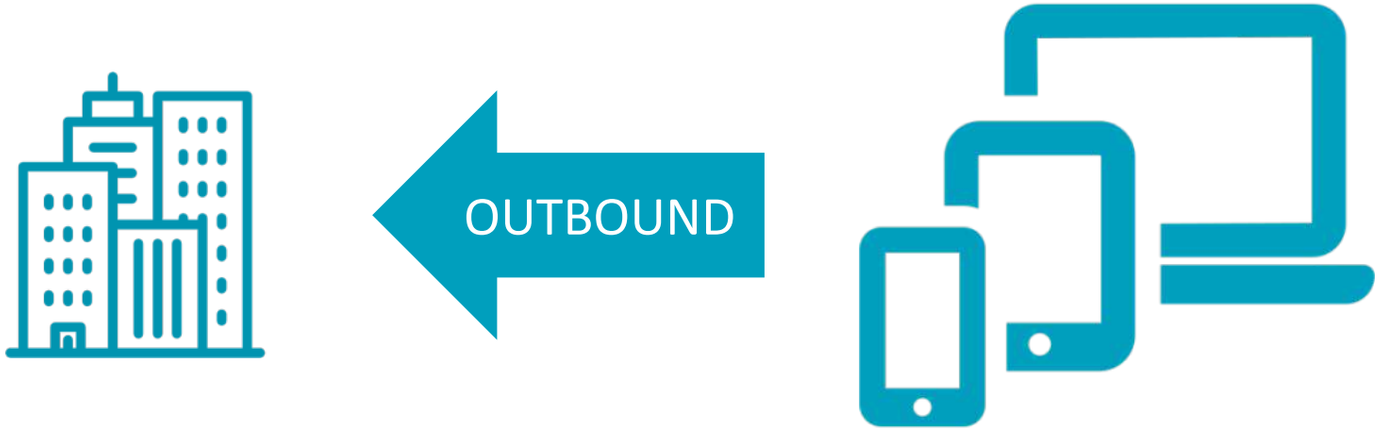
- FORENSICS
- DLP INTERNAL DATA
- DLP CLOUD DATA

CLOUD SECURITY PLATFORM

100+	35B+	125M+	120K+
data centers worldwide	transactions processed every day	threats blocked every day	security updates every day

Accesso alle applicazioni in DC

SCENARI DI SICUREZZA



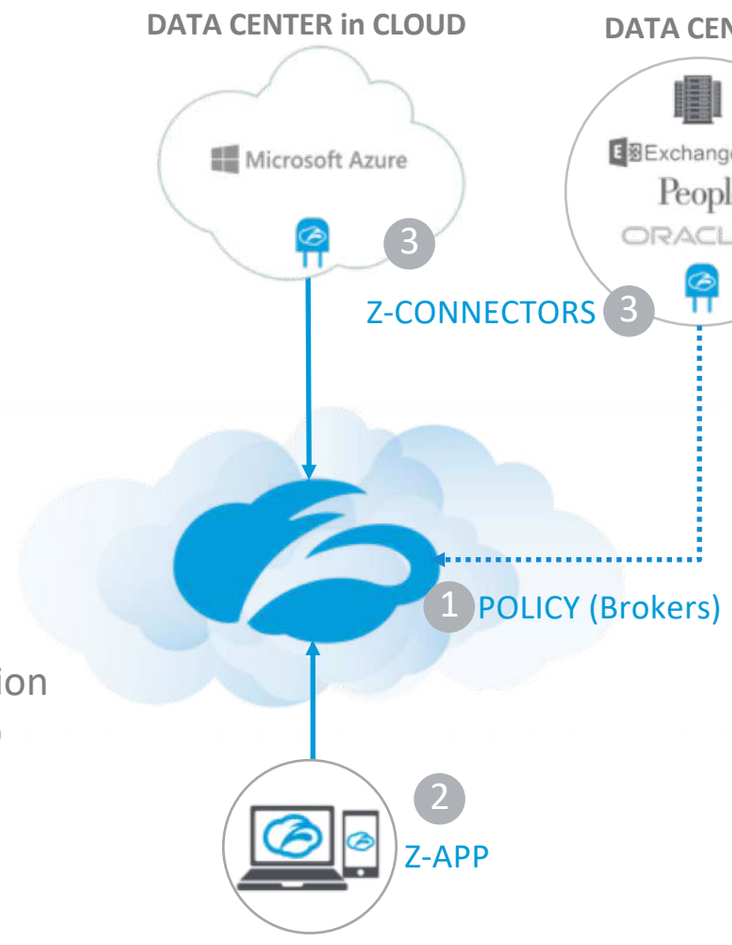
Dall'endpoint verso le applicazioni in DC

RAGGIUNGIAMO CIO' CHE E' TRUSTED

Innovative design

1. Cloud policy engine – define user app access rights (auth before access)
2. Z-APP – Request access to app
3. Z-Connectors – sits in front of apps. Starts inside out connection

Zscaler cloud brokers a secure connection between the Z-Connector and Z-App



Secure App Access without VPN and NGFWs

Access Control

User to App Policies
Multifactor Auth. – Private Certificates

Threat Prevention

Users never on the network
DDoS Prevention – apps not exposed to the Internet
App Micro Segmentation – not network segmentation

Data Protection

App Discovery (CASB for Internal Apps)
App and User Monitoring (DLP with Zscaler Internet Access)

ZPA replaces the entire inbound gateway/DMZ - not just a VPN replacement
Reduced cost and complexity; better security and user experience

Zscaler Private Access

1. **Users not on the corporate network**

   App access shouldn't require network access

   Policies are app-centric, not network IPs & ACLs

   If users aren't on your network, your network isn't extended to thousands of locations and attack surface is minimized. Hence better security.

2. **Apps invisible, not exposed to Internet**

   Internal apps can't be discovered or exploited

   App access only after authentication & policy

   No inbound connections, no public IP addresses. Darknet – apps are dark to the Internal and unauthorized users. Hence better security.

3. **Use Internet as a secure network without a VPN**

   End-to-end encryption, double TLS tunnels

   Bring your own keys, impossible to intercept

   Customer-controlled client & server certificates. Zscaler handles brokering, but traffic remains completely private.

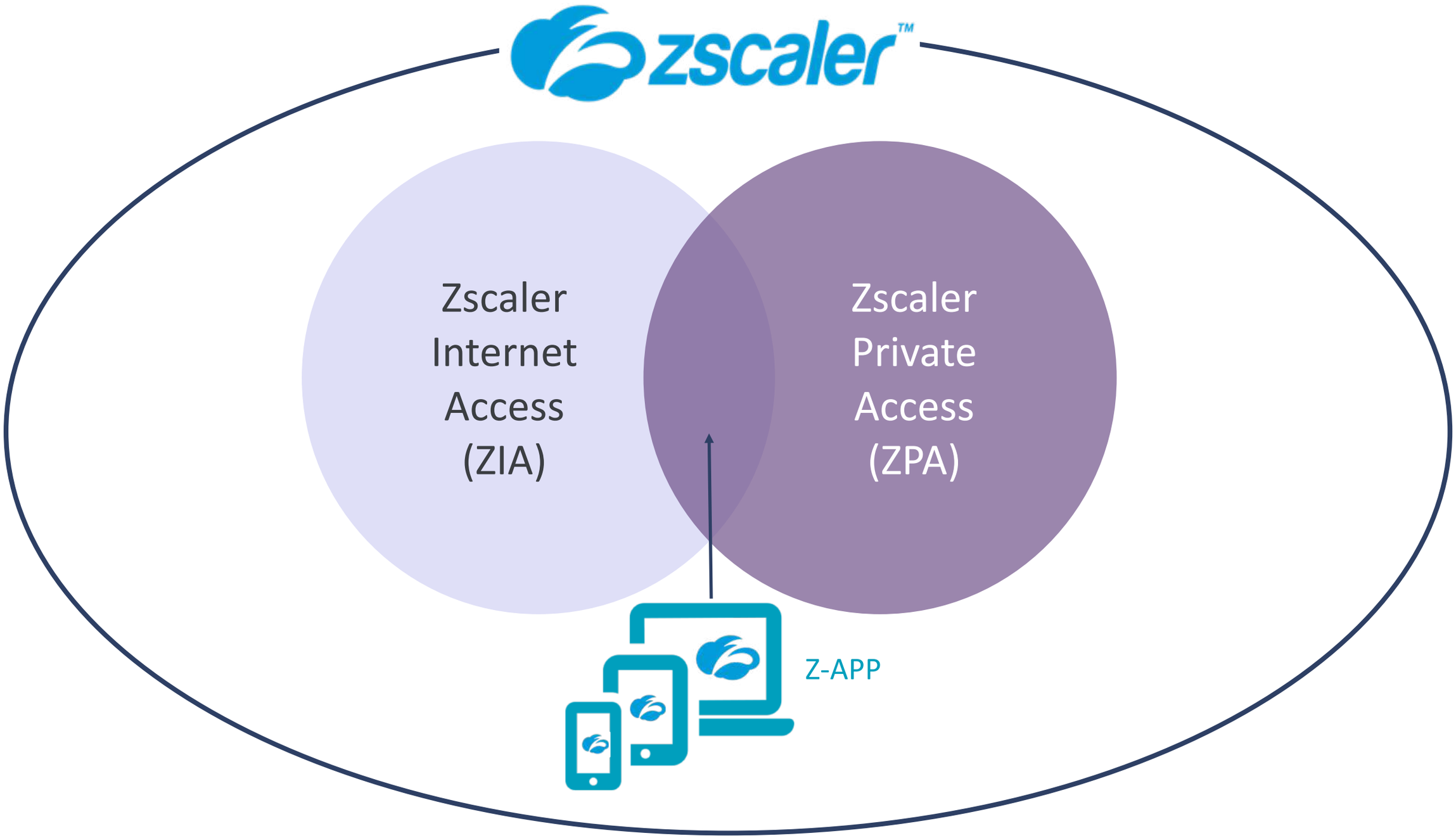
4. **App segmentation without network segmentation**

   User connection to a specific app

   Each app is segmented, no lateral movement

   Not network-to-network connection, but user-to-app. Connection is made to a specific app with a per-session user-to-app micro-tunnel.

Outbound security: Zscaler



AGENDA

1 Digital Transformation

EVOLUZIONE DELLO SCENARIO ICT
POSSIAMO ANCORA PARLARE DI PERIMETRO?

2 Internet diventa rete aziendale

SECURITY STACK ON-PREMISES: LIMITAZIONI
ESIGENZE DEGLI UTENTI E REQUISITI DI SICUREZZA

3 Accesso sicuro dall'endpoint

- ALLE PROPRIE APPLICAZIONI, CON ZSCALER PRIVATE ACCESS
- A INTERNET, CON ZSCALER INTERNET ACCESS

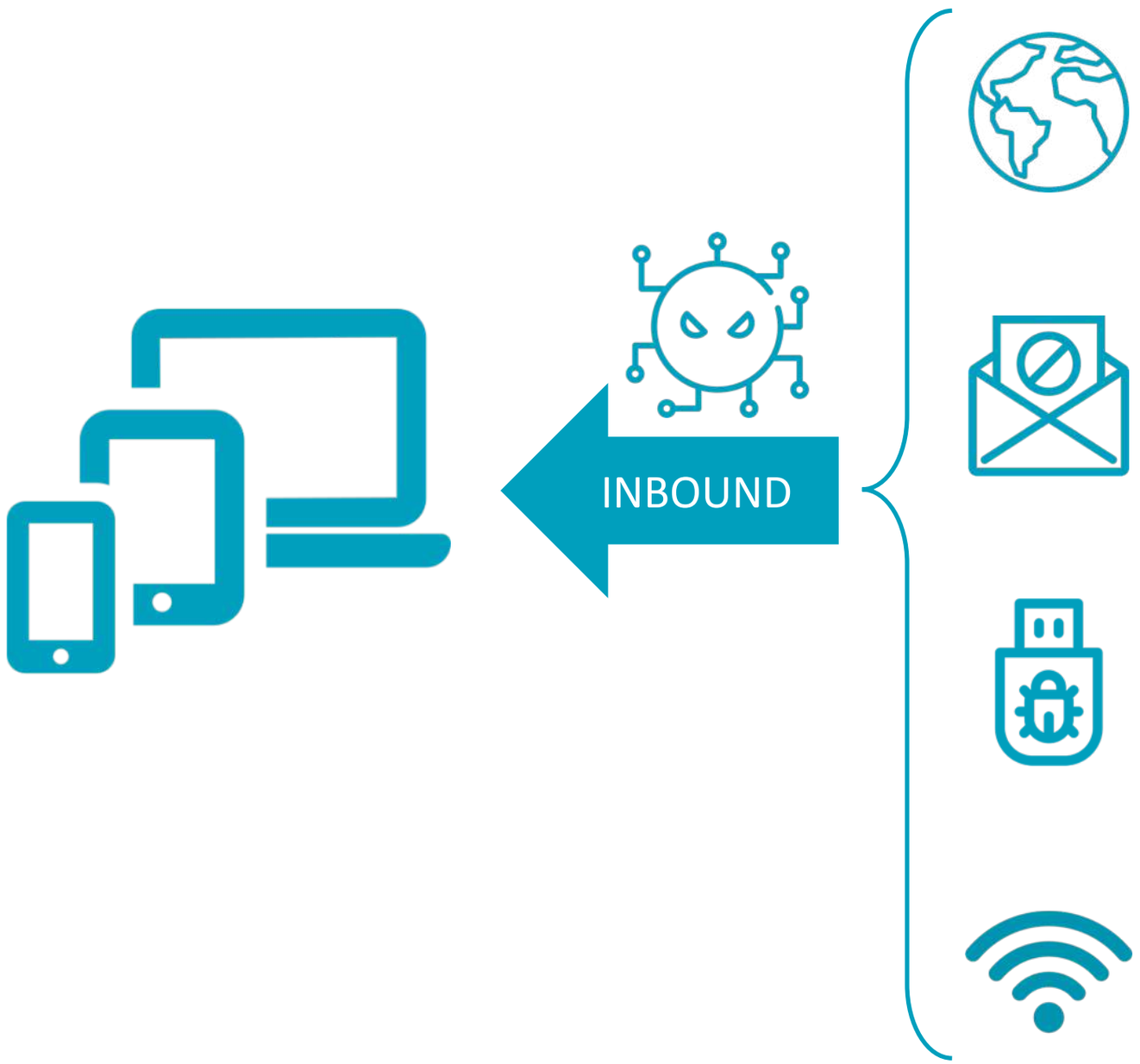
4 Protezione dell'endpoint

- DA MINACCE MALWARE EVOLUTE, CON SENTINEL ONE

5 Benefici e cost savings

Protezione in ricezione

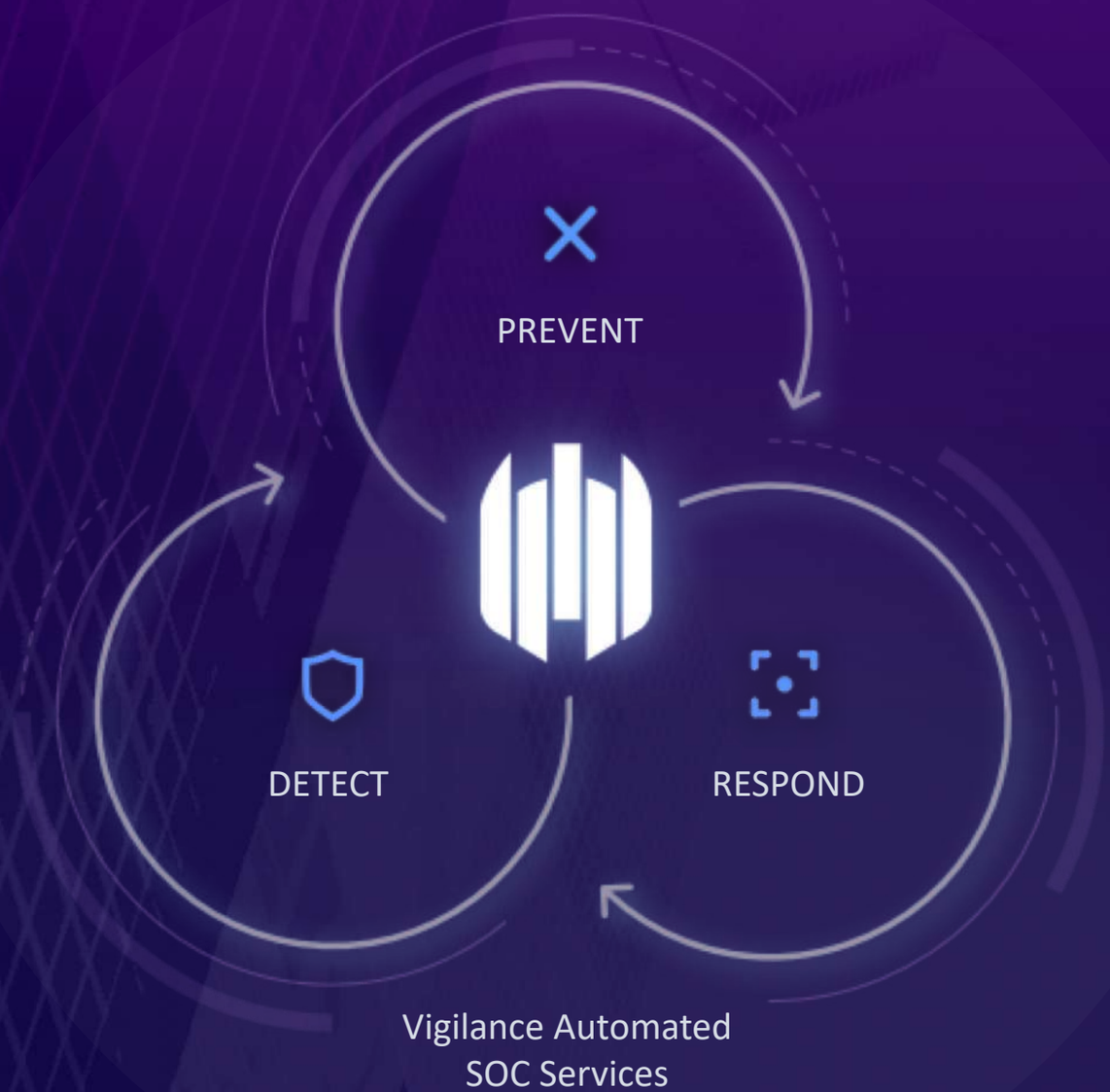
SCENARI DI SICUREZZA



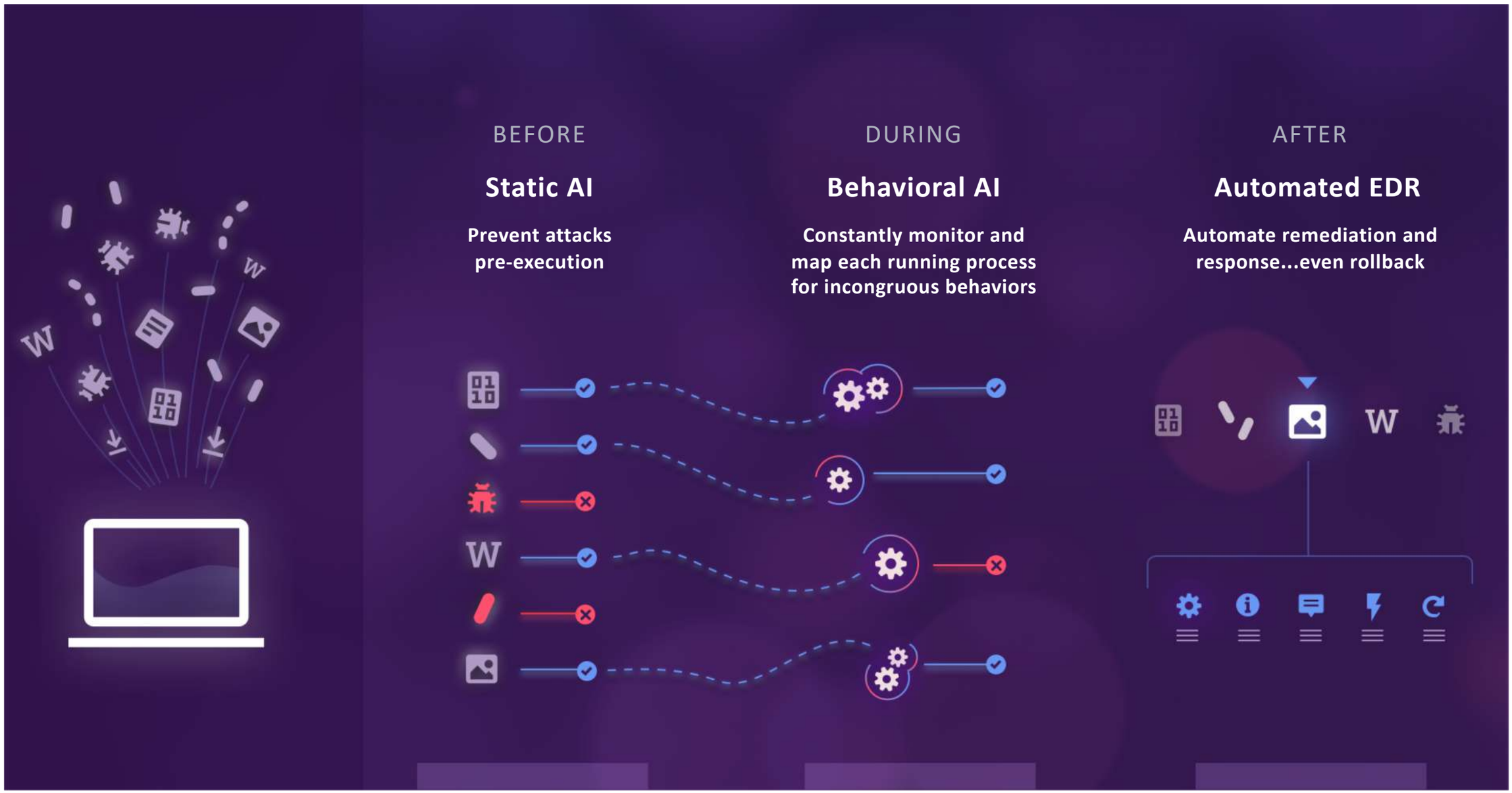
SentinelOne: approccio multi-strategy

SentinelOne

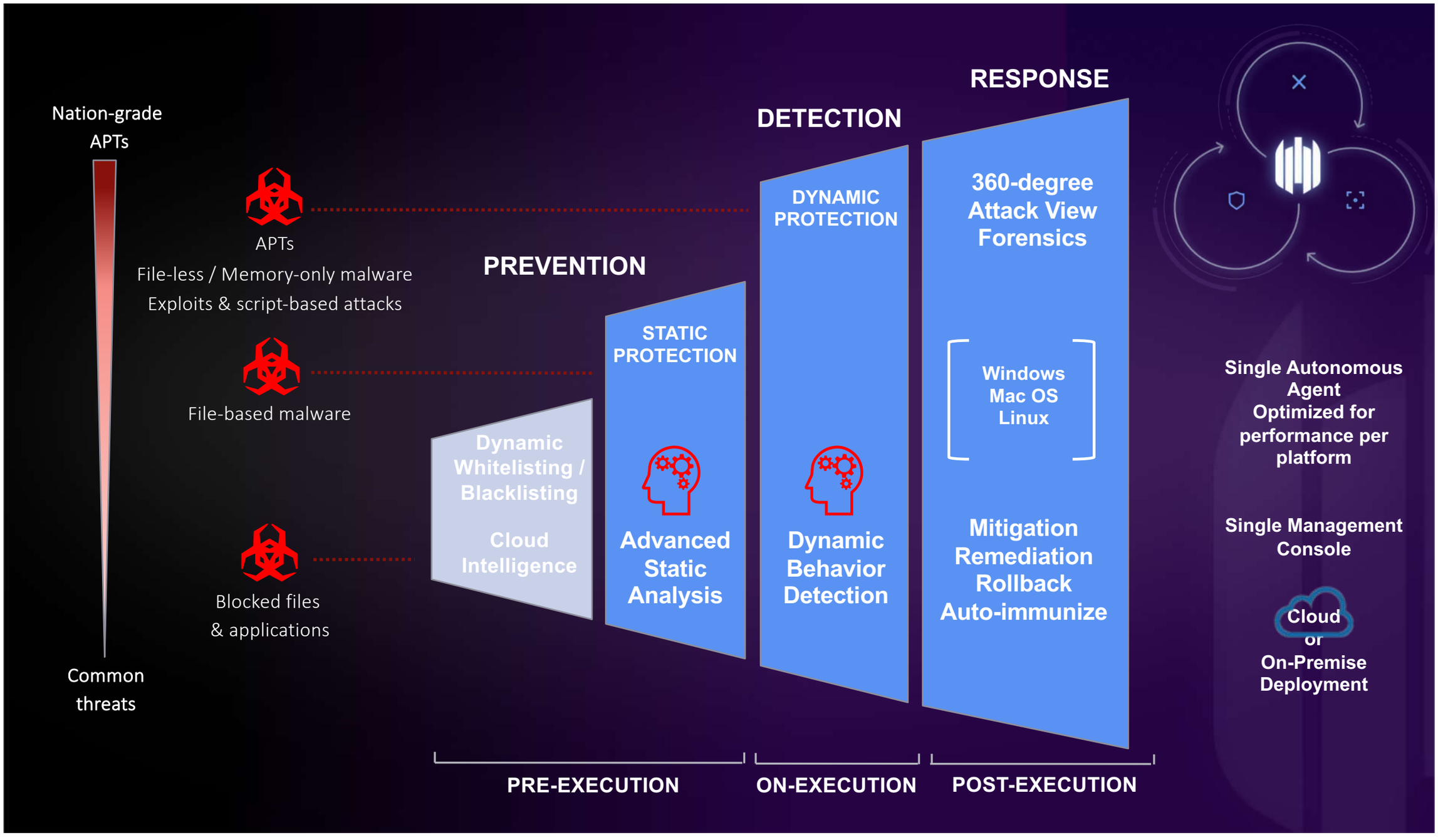
Autonomous Next-Generation Endpoint Protection



SentinelOne e malware lifecycle



SentinelOne: meccanismi di analisi



AGENDA

1 Digital Transformation

EVOLUZIONE DELLO SCENARIO ICT
POSSIAMO ANCORA PARLARE DI PERIMETRO?

2 Internet diventa rete aziendale

SECURITY STACK ON-PREMISES: LIMITAZIONI
ESIGENZE DEGLI UTENTI E REQUISITI DI SICUREZZA

3 Accesso sicuro dall'endpoint

- ALLE PROPRIE APPLICAZIONI, CON ZSCALER PRIVATE ACCESS
- A INTERNET, CON ZSCALER INTERNET ACCESS

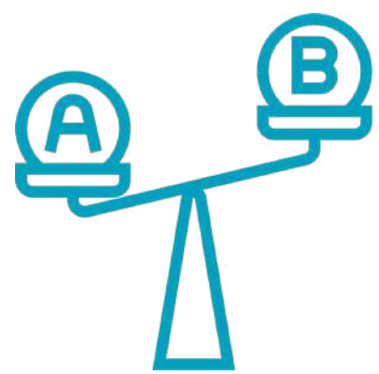
4 Protezione dell'endpoint

- DA MINACCE MALWARE EVOLUTE, CON SENTINEL ONE

5 Benefici e cost savings

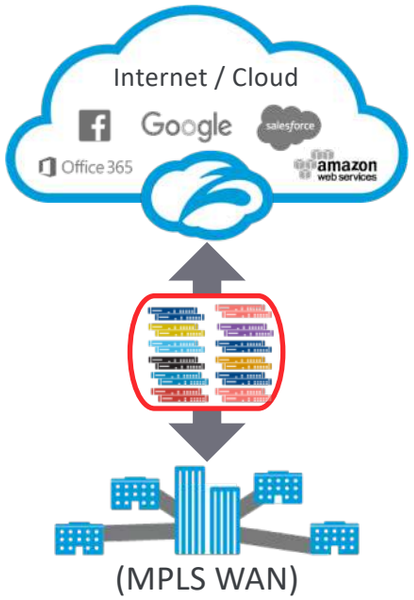
Benefici

1. Copertura delle esigenze di sicurezza dell'endpoint con un approccio basato su soluzioni complementari
   - sia in outbound sia in inbound
2. Le policy di protezione o di accesso sicuro sono associate all'utente e ai suoi dispostivi e lo «seguono» ovunque si sposti
3. Protezione estesa anche alle applicazioni:
   - sono pubblicate agli utenti non «a Internet»
   - segmentazione a livello applicativo
4. La cloud garantisce vantaggi in termini di scalabilità e manutenzione (aggiornamento), non solo dell'infrastruttura ma anche dei controlli di sicurezza
5. Si possono introdurre opportuni cost savings



Cost savings

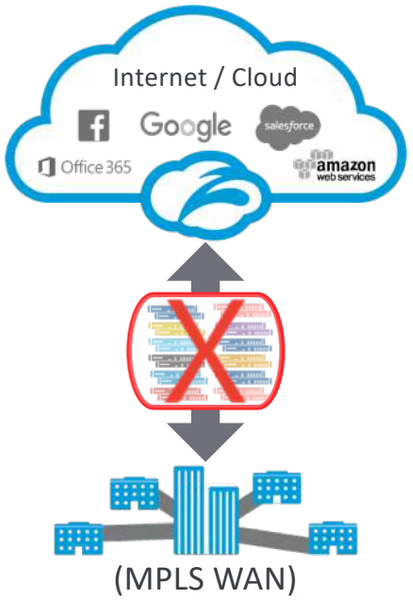
SECURE
Up-level your security



Make Zscaler your next hop to the Internet

Fast to deploy. No infrastructure changes required.

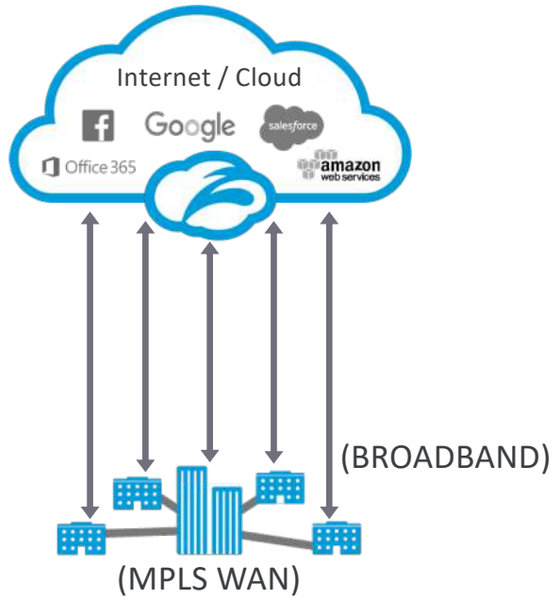
SIMPLIFY
Remove point products



Phase out gateway appliances at your own pace.

Reduce cost and management overhead

TRANSFORM
Cloud-enable your network

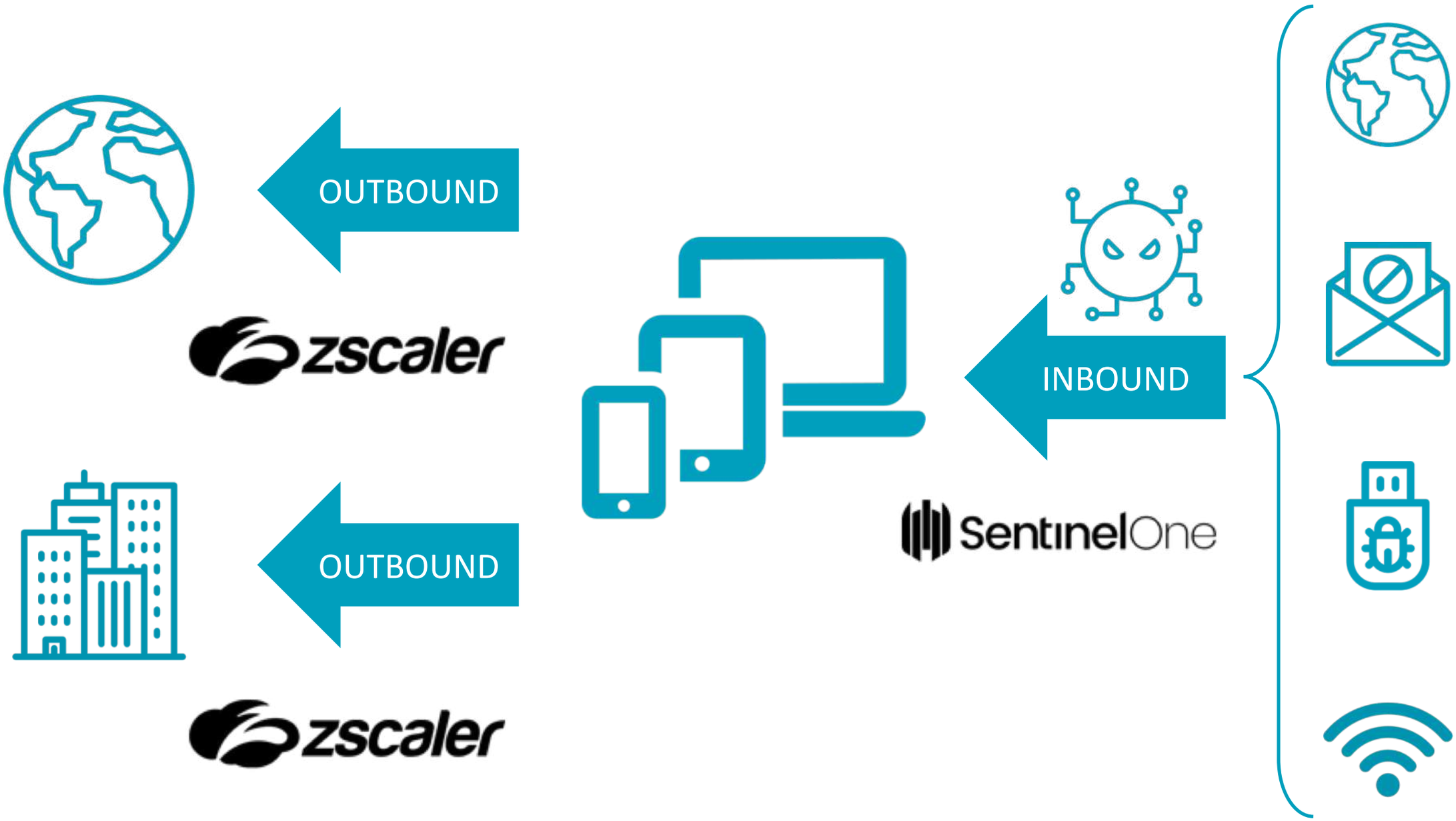


Enable local breakouts for Internet traffic – no backhaul

Deliver a secure and better user experience

Endpoint security: il nostro approccio

«BIG PICTURE»



Grazie per l’attenzione

Vi aspettiamo allo stand

Edoardo Montrasi

edoardo.montrasi@cryptonetlabs.it

