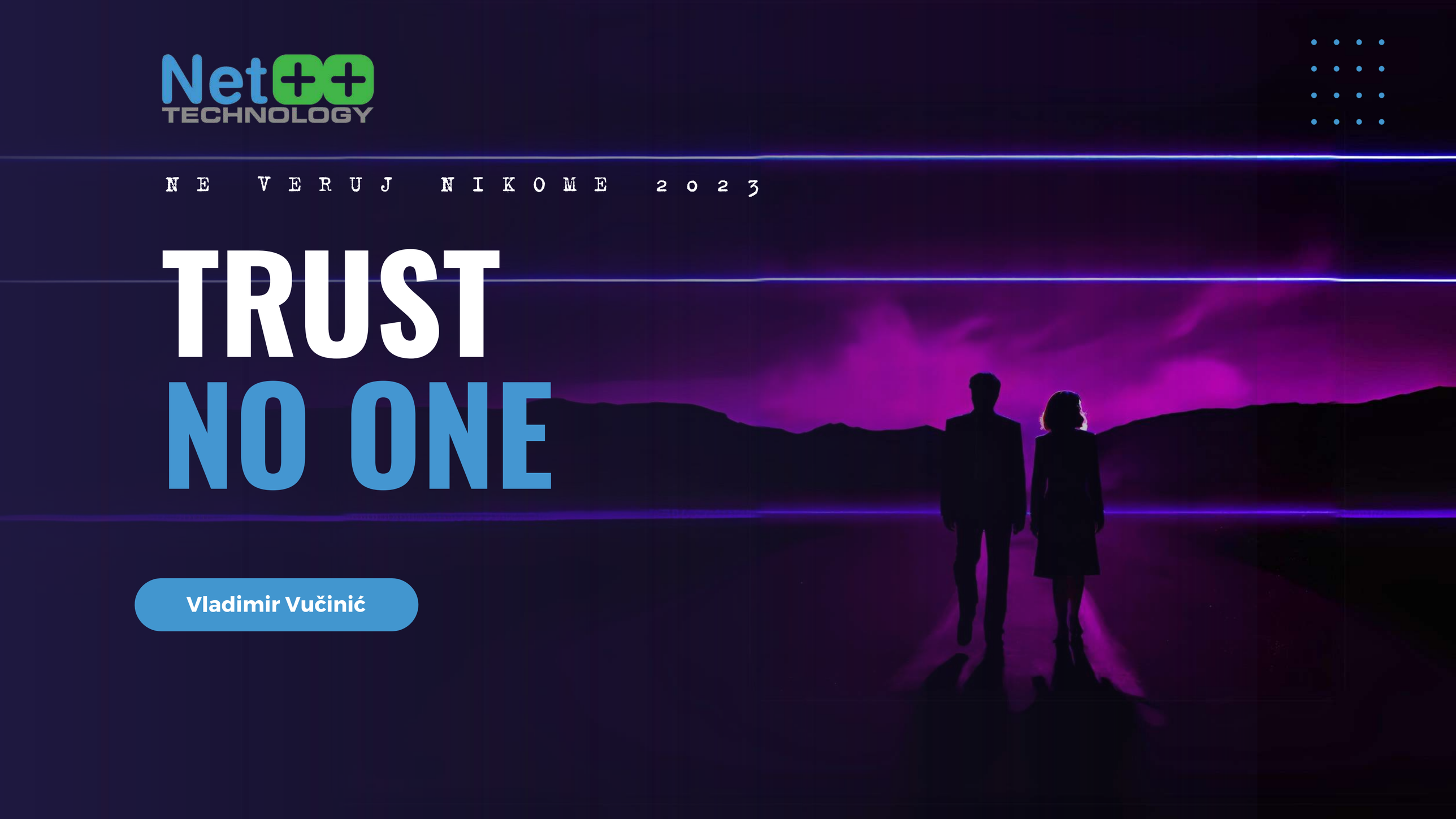
NE VERUJ NIKOME 2023

TRUST NO ONE



Vladimir Vučinić

GOVORIĆE DANAS

VLADIMIR VUČINIĆ

Net++ technology

DUBRAVKO HLEDE

MBCOM Technologies

DIMITRIJE VELIČANIN

Net++ technology

DAVOR PERAT

MBCOM Technologies

SRĐAN VRANIĆ

Co.Next

Agenda

10:00 Trust no 1 (Vladimir Vučinić)	**30 min**
10:30 Trust no network traffic (Dimitrije Veličanin)	**30 min**
11:00 ZTNA by Symantec (Dubravko Hlede)	**30 min**
11:30 Kafe pauza	**30 min**
12:00 Zero Trust - iz X files u stvarnost (Srđan Vranić)	**30 min**
12:30 DLP u Zero Trust okviru (Davor Perat)	**30 min**
13:00 Nije sve SF (Vladimir Vučinić)	**30 min**

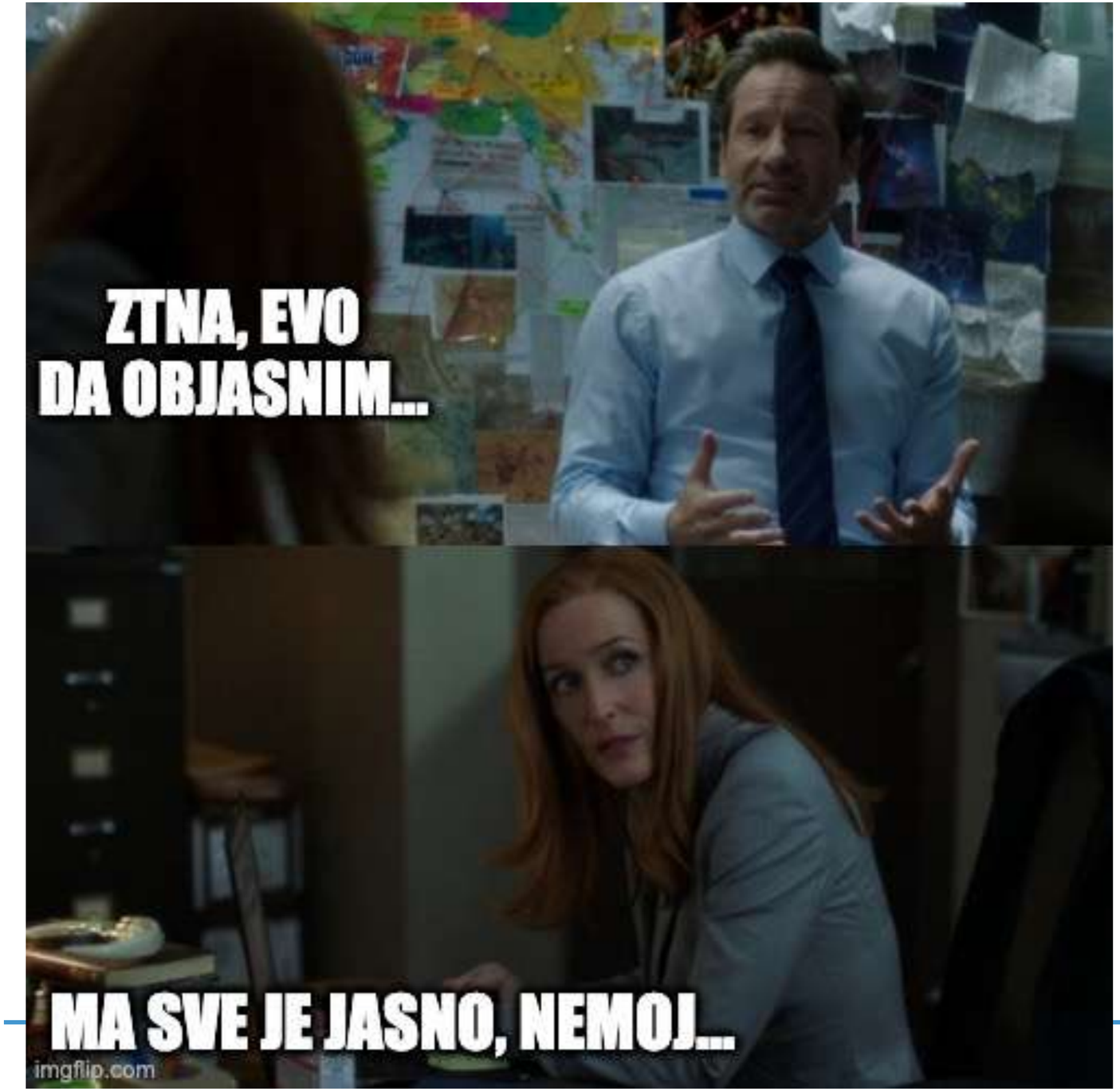
13:30 Pitanja i odgovori	**15 min**
13:45 Nagradna igra	15 min
14:00 Ručak (sala u prizemlju)	

NetPlus TECHNOLOGY

Trust no 1

ZTNA

Vladimir Vučinić, Net++ technology


ZTNA, EVO
DA OBJASNIM...
MA SVE JE JASNO, NEMOJ...
imgflip.com

Malo istorije

- Zero trust je termin koji je osmislio **John Kindervag**, 2010.g., kao Forrester-ov istraživač (sada CTO u Netscope)

- Prolaze godine... (skoro decenija), po neka firma i organizacija (Google, NIST, NCST) se igraju sa ZT (Zero Trust) arhitekturom

- Gartner-ov analitičar Steve Riley se bavio ZT konceptom i napravio koncept “continuous adaptive risk and trust assessment” (CARTA), srećom nekom je rekao da ne zvuči idealno, te je 2019.g. Gartner objavio izveštaj tržišta za ZTNA (umesto CARTA), mada je postojala i ideja da se zove ZTAA (Zero Trust Application Access)

- Ostaje ipak pitanje ”Šta je zapravo ZTNA?”


ZTNA?
ZNA LI KO ŠTA JE ZTNA?
imgflip.com

?

ZTNA – Zero Trust Network Access

ZTNA – Zero Trust Network Access

Gartner: ZTNA su proizvodi i servisi koji kreiraju logičku granicu za pristup baziranu na identitetu i kontekstu koja obuhvata korisnika i internu aplikaciju ili skup aplikacija. Aplikacije su sakrivene, a pristup je ograničen kroz broker poverenja (trust broker) ka skupu imenovanih entiteta, koji ograničava bočna (lateral) kretanja kroz mrežu.

Forrester: ZTNA je specifična tehnologija koja koristi Zero Trust principe kako bi omogućila pristup mreži i aplikacijama. ZTNA menja virtual private network (VPN), posebno za one koji rade “od kuće”, tj. udaljene radnike.

Trust broker

- najvažnija komponenta, nalazi se van mreže;

- autentifikuje korisnike;

- dodeljuje odgovarajući nivo poverenja korisniku;

- omogućava pristup samo potrebnim aplikacijama.

U čemu je razlika u odnosu na VPN?

- VPN prvo omogući pristup, pa autentifikuje korisnika!

- broker može prvo da proveri uređaj, lokaciju sa koje se povezuje, biometriku, da dodeli ocenu (trust score), pa tek onda da omogući pristup i to samo onim aplikacijama kojima taj korisnik sme da pristupi!

ZTNA vs VPN

“VPN je stvar koja sedi sa jednom nogom u Internetu, a sa drugom u lokalnoj mreži” – Riley

VPN koncentratori i agenti se retko ažuriraju, stalno u upotrebi

Bez VPN agenta nema pristupa

VPN access liste i upravljanje, često pristup celoj mreži

vs

Trust broker je pod kontrolom vendora od poverenja, sa dobrom istorijom i timom koji ga nadgleda, sa cybersecurity veštinama obično boljim od onih sa kojima raspolažu preduzeća

Često i bez agenta

ZTNA iz ugla vendora

SYMC: ZTNA je SaaS (Software as a Service) rešenje koje omogućava sigurno i granularno upravljanje pristupom bilo kom korporativnom resursu hostovanom on-premises ili u cloud-u. Koristi Zero Trust Access principe za pružanje point-to-point povezivanja, bez agenata ili uređaja, eliminišući pretnje na mrežnom nivou. Sakriva korporativne resurse, potpuno izolujući datacentar od korisnika i Interneta. Izloženost mrežnog nivoa napadima je potpuno uklonjena, bez mogućnosti lateralnog kretanja i bez mrežnih pretnji

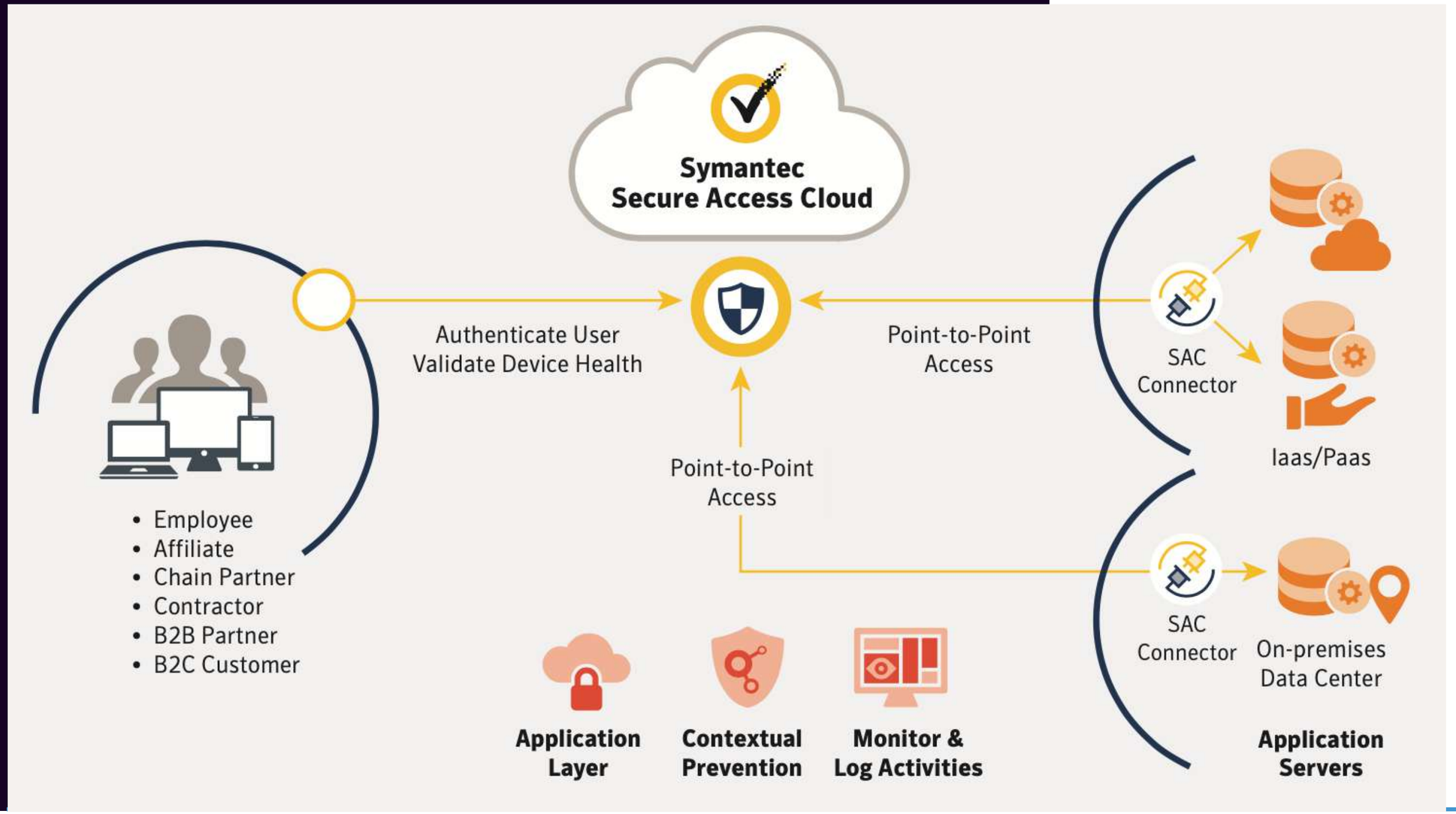
PANW: ZTNA je kategorija tehnologija koje omogućavaju siguran udaljeni pristup aplikacijama i servisima na osnovu definisanih pravila za kontrolu pristupa. Za razliku od VPN-ova, koji omogućavaju pristup celoj mreži, ZTNA rešenje podrazumevano zabranjuju pristup, omogućavajući pristup samo onima kojima je eksplicitno dozvoljen.

Symantec™
A Division of Broadcom

paloalto®
NETWORKS

Net++ TECHNOLOGY

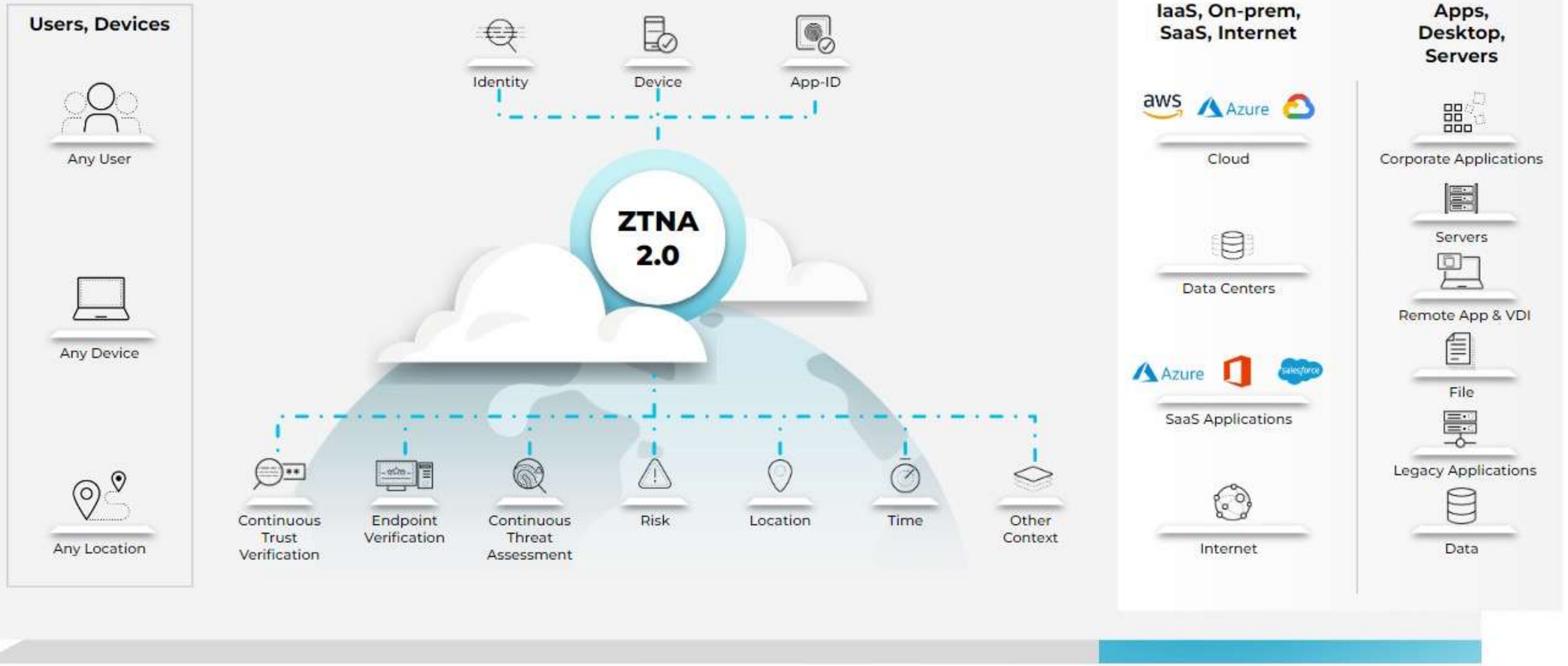
Symantec
A Division of Broadcom



NetOne TECHNOLOGY

paloalto NETWORKS

ZERO TRUST NETWORK ACCESS 2.0 DIAGRAM



NetOO TECHNOLOGY

Zašto ZTNA?

- rad sa udaljenih lokacija (od kuće), hibridni rad, konsultanti, spoljni saradnici

- lakše i bolje upravljanje pristupom, bolja kontrola

- veća sigurnost

- veća dostupnost

- lakše skaliranje

- DLP cloud integracija

Mane?

- ipak je to neki tuđi računar/server (cloud)

Symantec™
A Division of Broadcom

paloalto®
NETWORKS

Net++ TECHNOLOGY

NE VERUJ NIKOME 2023

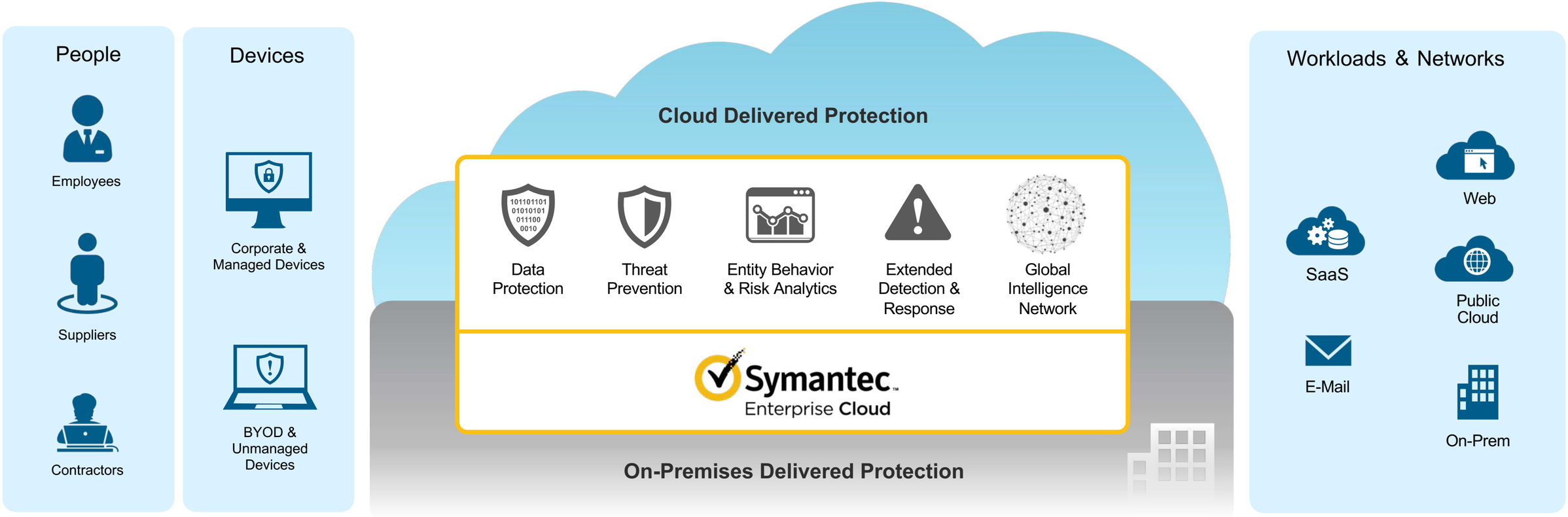
HVALA NA PAŽNJI

Email: office@netpp.rs

Telefon: 011 3699 967

Web: www.netpp.rs

Symantec Enterprise Cloud: Data-Centric Hybrid Security



Endpoint Security	Network Security	Information Security	Email Security

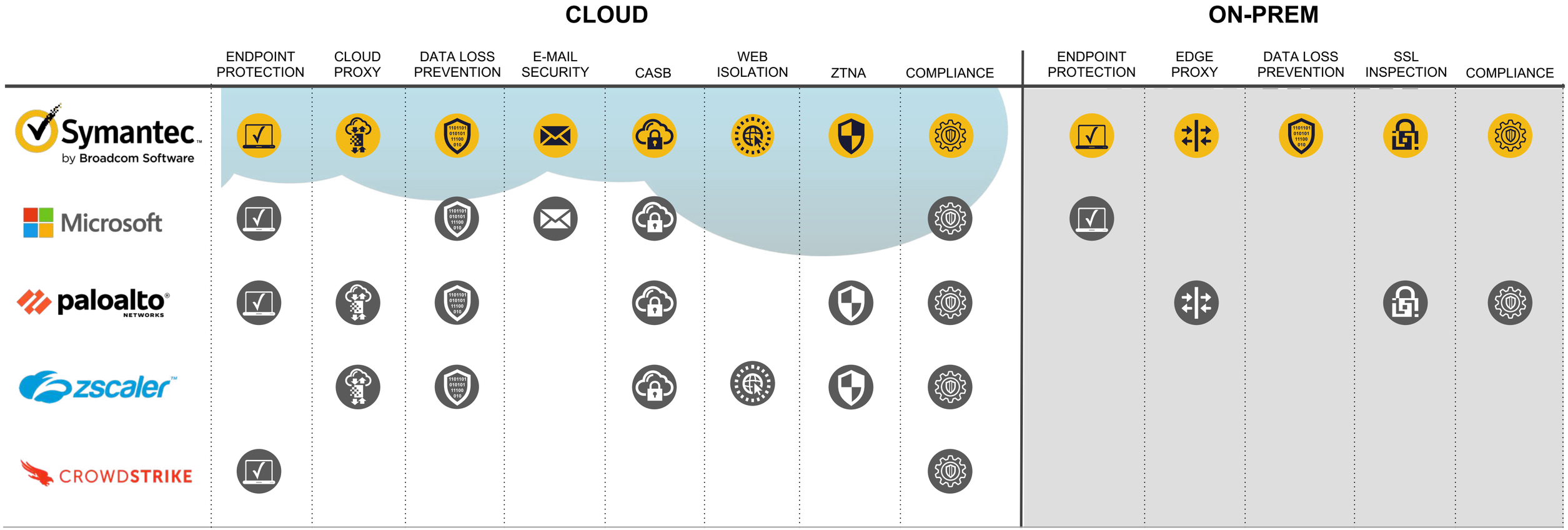
CONSISTENT **COMPLIANCE**

ENABLE **REMOTE WORK**

DATA & THREAT **SECURITY EVERYWHERE**

Symantec by Broadcom Software

Only Symantec Addresses Hybrid Enterprise Security Holistically



Microsoft: https://www.microsoft.com/en-us/microsoft-365/enterprise/e5?activetab=pivot%3aoverviewtab

Palo Alto Networks: https://www.paloaltonetworks.com/

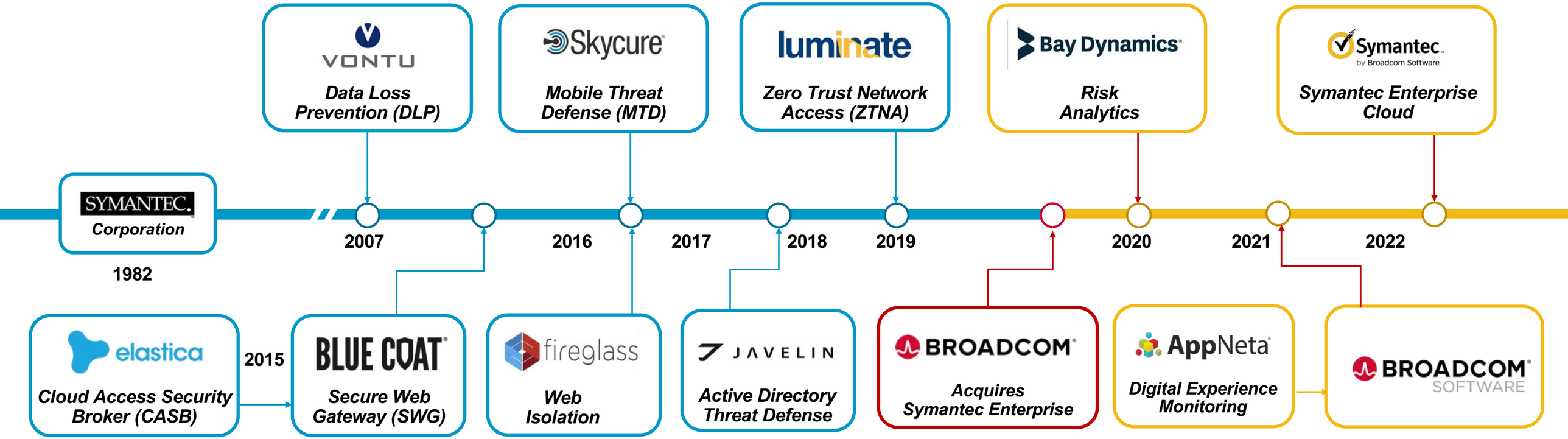
Zscaler: https://www.zscaler.com/

Crowdstrike: https://www.crowdstrike.com/endpoint-security-products/

Symantec by Broadcom Software

The launch of a unified enterprise solution

Broad and deep capabilities built and optimized over years



1,400 ENGINEERS | **300+** SECURITY RESEARCHERS

~2,000+ PATENTS | **11 TRILLION** ELEMENTS OR LINES OF TELEMETRY

Symantec by Broadcom Software

HVALA NA PAŽNJI

+381 11 36999 967
www.netpp.rs
Otokara Keršovanija 11/39, Beograd