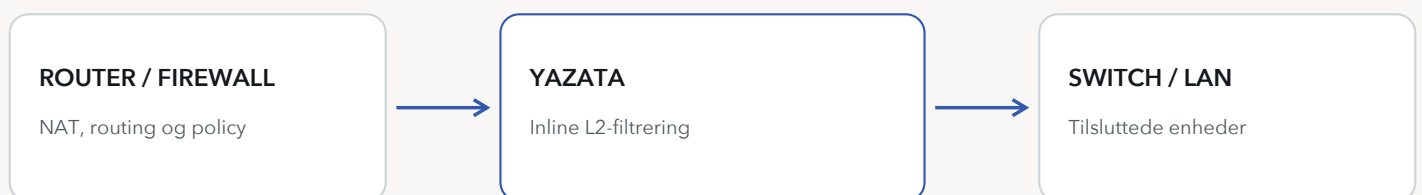


01 · PLACERING OG FUNKTION

Et filter i datapathen.

Yazata Threat Shield beskrives som en transparent Layer 2-bro mellem router/firewall og switch. Den kan kun vurdere den trafik, som faktisk passerer dens to netværksporte.



Routerens LAN-port forbindes til boksens indgang; udgangen går til switchens uplink. Enheder på parallelle veje, herunder Wi-Fi direkte på routeren, ligger uden for denne datapath.

TRE TYPER BESLUTNINGER

01

DNS-domæner

Et opslag til et kendt skadeligt domæne kan afvises, når DNS-trafikken passerer boksen.

02

IP-forbindelser

Udgående forbindelser til kendte C2- eller botnet-adresser kan blokeres.

03

Indgående trafik

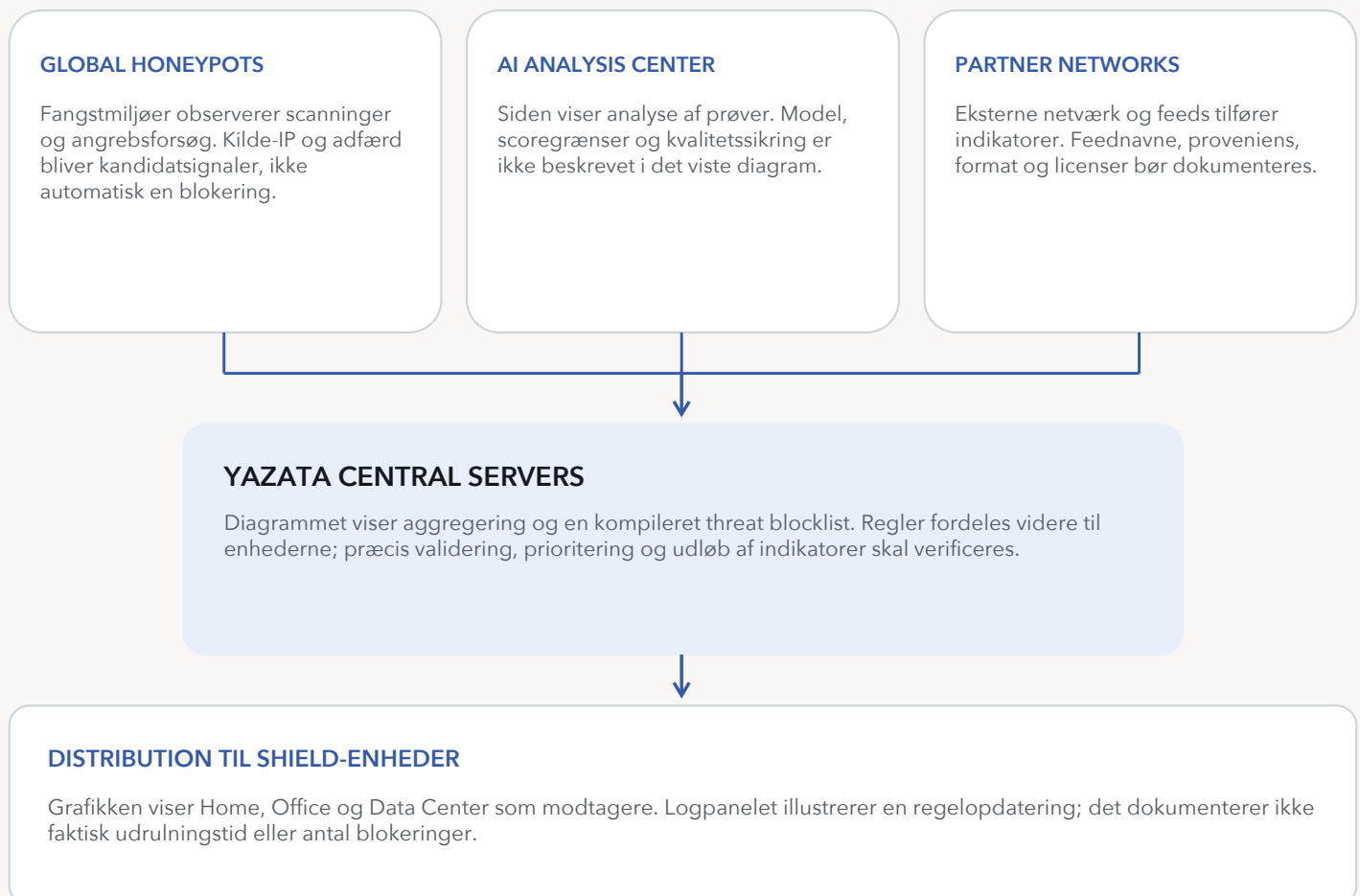
Kun trafik, som router/firewall videregiver gennem boksen, kan vurderes her.

L2-placeringen ændrer ikke i sig selv firewall, routing eller endpoint-beskyttelse. Det konkrete samspil skal testes i kundens topologi.

02 · TRUSSELSEFTERRETNING

Tre kilder. Ét regelsæt.

Yazatas diagram viser tre typer input til centrale servere. Serverne aggregerer signalerne og distribuerer en kompileret trusselsliste til Shield-enheder.



LOKAL EFFEKT I TRAFIK, DER PASSERER BOKSEN

Domæner

Kendte skadelige navne kan indgå i DNS-filtrering.

IP-adresser

Kendte risikoadresser kan indgå i forbindelsesfilteret.

Hændelser

Test logfelter, undtagelser og eksport i en pilot.

OM TALLENE I DIAGRAMMET

Websiden viser 15,2k+ IP/s, 42,5k+ prøver/s og 8,4k+ feeds/s samt en live-lignende systemlog. Behandl dette som en produktvisualisering, indtil leverandøren dokumenterer målemetode, periode og driftstal.

03 · PILOT OG AFKLARING

Dokumentér adfærden.

En teknisk pilot bør vise præcis, hvilke veje boksen ser, hvad den blokerer, og hvad den ikke kan afgøre. Nedenstående punkter bør verificeres før produktion.

Datapath og VLAN

Tegn faktisk kabling. Test trunk, VLAN-tags, DHCP, IPv4/IPv6 og trafik via access points og sekundære routere.

DNS-stier

Test både lokal resolver, ekstern DNS og eventuel krypteret DNS. Fastlæg hvilke forespørgsler der passerer boksen.

Blokeringsadfærd

Test en godkendt indikator for DNS og IP; dokumentér svar, logpost, mulighed for undtagelse og risiko for falske positive.

Drift og fejl

Afklar strømudfald, fail-open/fail-closed, opdateringssvigt, genstart, rollback og hvem der kontaktes ved fejl.

Feeds og data

Få dokumenteret feednavne, proveniens, kvalitetskontrol, indikatorers udløb, opdateringskanal, logfelte og hvilke data der forlader lokationen.

Kapacitet

Mål throughput og latens i jeres trafikprofil. Leverandøropgivne tal er ikke en erstatning for en lokal test.

ROLLE I SIKKERHEDSARKITEKTUREN

Yazata er et supplerende filter for kendte domæner og adresser. Firewall, endpoint-beskyttelse, patching, backup, segmentering og hændelseshåndtering forbliver selvstændige kontroller. Ukendte eller målrettede angreb kan passere et indikatorbaseret filter.

KILDEGRUNDLAG

Yazatas dataflow-grafik (yazatasec.com/#adaptability, skærmbillede 19.09.2026) og Yazata Danmarks produkt- og privatlivssider. Feednavne og driftstal kræver leverandørdokumentation.