

Yazata Threat Shield

Teknisk reference for netværksansvarlige, sikkerhedsarkitekter og driftsteams. Dokumentet beskriver det offentliggjorte design og gør uafklarede specifikationer synlige.

SYSTEMROLLE

Yazata beskriver en transparent Layer 2-enhed placeret mellem router/firewall og switch. Den bruger trusselsindikatorer til at vurdere DNS-opslag og forbindelser til kendte risikoadresser i den trafik, der faktisk passerer enheden.

Formålet er et ekstra kontrolpunkt i LAN-datapathen.

LÆSENØGLE FOR TEKNISKE UDSAGN

D / Dokumenteret

Fremgår af Yazatas produkt- eller privatlivstekst. Det er en leverandørbeskrivelse, ikke en uafhængig måling.

V / Visualiseret

Fremgår af det leverede skærbillede af Yazatas dataflow. Grafiske tal og logs er ikke valideret driftstelemetry.

T / Skal testes

Værdier, mekanismer eller adfærd, som kræver teknisk specifikation, leverandørsvar eller lokal pilot.

DOKUMENTETS GRÆNSE

Denne reference kan bruges til arkitekturreview, pilotplan og indkøbsdiallog. Den angiver ikke certificeret throughput, failover, krypteringsdesign, SLA eller kompatibilitet med en bestemt kundes netværk. Sådanne forhold står som åbne verifikationspunkter.

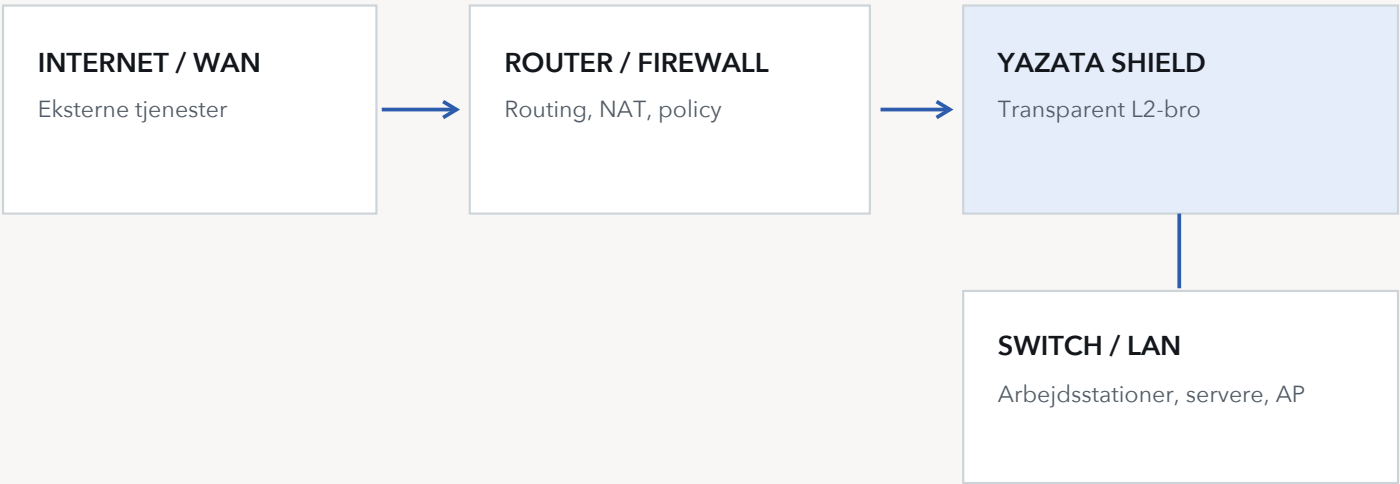
KILDESTATUS

D: Yazatas danske produkt- og privatlivssider. V: skærbillede fra yazatasec.com/#adaptability, 19.09.2026. T: specifikation og pilot påkrævet.

Placering og trafikvej

Inline placering skaber et klart dækningsområde: kun rammer, som krydser enhedens forbindelser, kan påvirkes af dens lokale filtrering.

LOGISK NETVÆRKSDIAGRAM



DÆKNINGSREGEL

Wi-Fi direkte på routeren, alternative uplinks, mobilnet og VPN- eller tunneltrafik uden for den synlige datapath kræver særskilt analyse. Placering alene giver ikke fuld netværksdækning.

KONTROLGRÆNSER

Lag / funktion	Ansvar og afgrænsning
Router / firewall	Terminerer WAN, håndterer routing og eksisterende firewallpolitik. Trafik, der afvises eller termineres her, når ikke Shield.
Yazata Shield	Påstået transparent L2-passage og indikatorbaseret vurdering. Præcis pakke- og blokeringsteknik kræver leverandørdokumentation.
Switch / endpoints	Videresender lokal trafik. Endpoint, segmentering, patching og backup forbliver selvstændige kontroller.

Beslutninger i datapathen

Yazatas materiale omtaler DNS-domæner og kendte IP-adresser. Her er flowet udtrykt som tekniske beslutningspunkter, med åbne spørgsmål markeret.

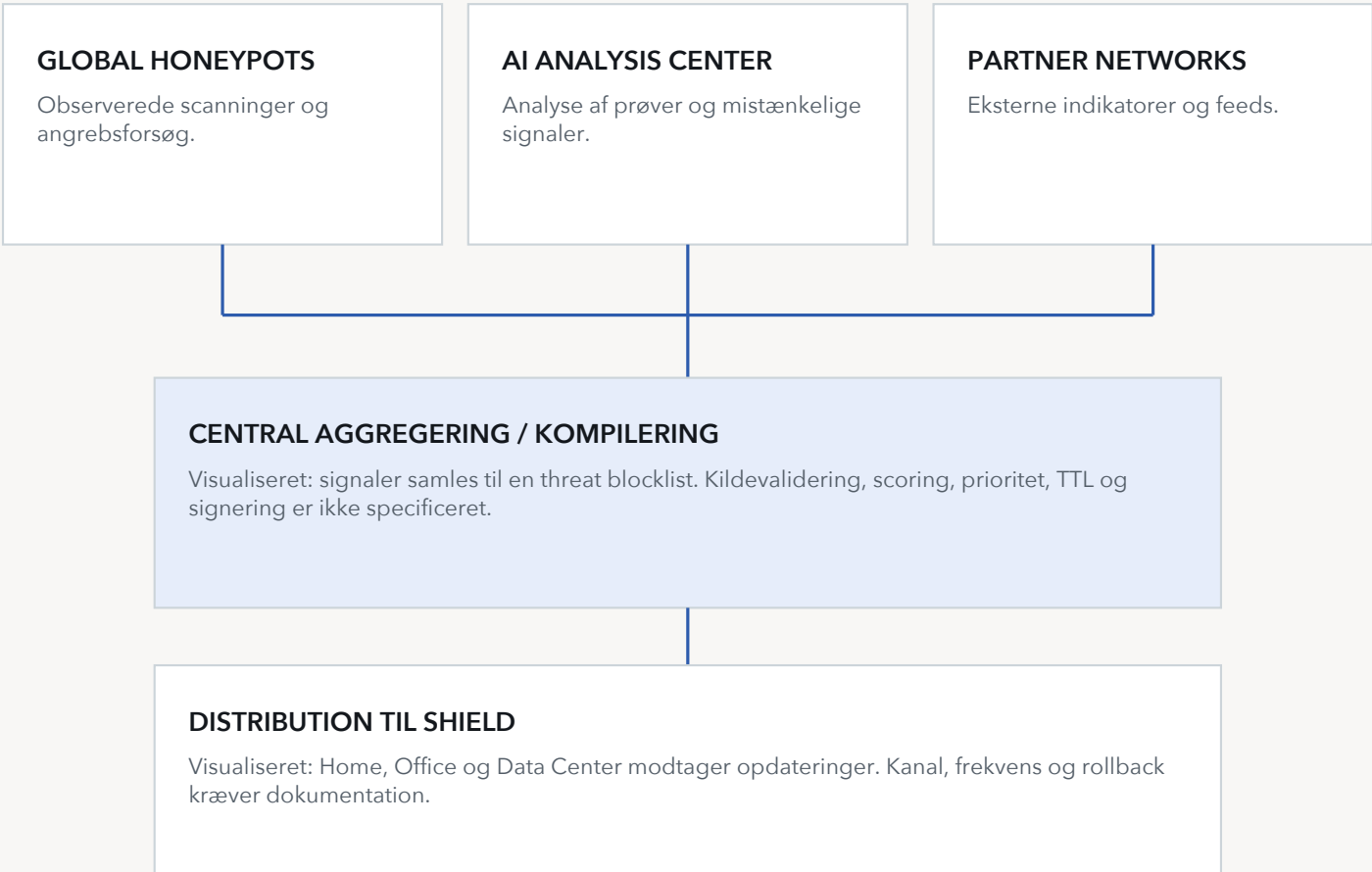
Trin	Hændelse	Kontrol / nødvendig verifikation
1. Passage	Klientens trafik går via router, Shield og switch.	Bekræft begge retninger, VLAN-tags, MTU og bridge-adfærd i faktisk topologi.
2. DNS	En klient eller resolver slår et domæne op.	Afklar hvilke DNS-stier Shield ser, og om blokering sker via svar, drop eller anden mekanisme.
3. IP	En forbindelse søger en kendt risikoadresse.	Afklar matching, IPv4/IPv6, prioritet i forhold til firewall og håndtering af delt hosting.
4. Hændelse	Et match udløser en lokal beslutning.	Indsaml logfelter, tidsstempel, indikator-ID, policy, handling og eksportmulighed.
5. Undtagelse	En legitim tjeneste rammes muligvis af filteret.	Dokumentér allowlist, udløb, godkendelse, auditspor og tilbageførsel.

VIGTIG BEGRÆNSNING

Indikatorbaseret filtrering er afhængig af synlig trafik og aktuelle indikatorer. Den dokumenterer ikke inspektion af krypteret indhold, TLS-dekryptering eller detektion af ukendte angreb. En pilot skal måle både detekterede matches og fejlagtige blokeringer.

Fra kilder til lokal regel

Yazatas dataflow-grafik viser tre inputklasser, central aggregering og distribution til Shield-enheder. Den viser ikke hele kvalitets- eller sikkerhedskæden.



LIVSCYKLUS, DER SKAL DOKUMENTERES

Fase	Spørgsmål til leverandøren
Indtag	Hvilke feedkilder og licenser? Hvordan verificeres oprindelse og dubletter?
Beslutning	Hvilke tærskler, menneskelig kontrol og falsk-positiv processer anvendes?
Udgivelse	Hvordan signeres, versionsstyres, distribueres og rulles regler tilbage?

V: De viste 15,2k+ IP/s, 42,5k+ prøver/s og 8,4k+ feeds/s er ikke verificerede kapacitetstal.

Hvad kan enheden se?

Synlighed afhænger af klientens rute, resolvervalg og tunneler. Testmatrixen nedenfor er en kravliste til piloten, ikke et løfte om understøttelse.

Trafiktype	Afklar i teknisk pilot	Bevis
Klassisk DNS	Lokal resolver, ekstern resolver, UDP/TCP og faktisk passage gennem boksen.	Pakkespor + log
Krypteret DNS	DoT og DoH skjuler forespørgslen på transportvejen; afklar styring eller understøttet integration.	Konfiguration + test
IP-trafik	IPv4, IPv6, UDP/TCP, retning og destination bag NAT eller proxy.	Pakkespor + log
L2-integration	802.1Q VLAN, trunk/access, DHCP, ARP/ND, MTU, LACP og redundante links.	Topologi + test
Omgåelsesveje	AP på router, sekundær router, gæstenet, VPN, mobilnet og direkte uplinks.	Rutediagram

RFC 7858 definerer DNS over TLS; RFC 8484 definerer DNS over HTTPS. Heraf følger, at en on-path DNS-kontrol ikke automatisk kan læse domænenavnet i krypteret DNS. Yazatas konkrete håndtering er ikke dokumenteret i kilderne.

Driftsmodel og ændringskontrol

Før produktion bør ejerskab, opdateringssti og fejltilstand være fastlagt. Disse punkter kan ikke udledes af et arkitekturdiagram.

Område	Minimumskrav til dokumentation	Ejer
Opdateringer	Endpoint, transport, autentificering, signatur, frekvens, version og stale-feed alarm.	Leverandør + IT
Strøm / link	Fail-open eller fail-closed, bypass, boot-tid, linkflap og konsekvens for drift.	Leverandør + netværk
Administration	Adgangsroller, MFA hvis relevant, lokale credentials, firmware og ændringslog.	IT sikkerhed
Telemetri	Logfelter, tidskilde, retention, SIEM-eksport, alarmer og hændelsesworkflow.	SOC / drift
Rollback	Kabel- og konfigurationsplan for kontrolleret bypass og tilbageførsel.	Netværk

FEJLSCENARIER I PILOTEN

Test afbrudt strøm, WAN-tab, tabt feedforbindelse, ugyldig opdatering og genstart under belastning. Registrér observeret datapath, alarmer, genopretningstid og hvem der kan beslutte bypass. Intet standard-failovermønster antages her.

Pilot og accepttest

Brug en afgrænset netværkszone og godkendte testindikatorer. Mål normal drift før og efter indsættelse, og gem evidens til driftsoverdragelse.

ID	Test og fremgangsmåde	Acceptkriterium / evidens
P01	Kortlæg kabling, VLAN, routing, DNS og alternative uplinks.	Godkendt diagram; dækningsområde og omgåelsesveje markeret.
P02	Indsæt enheden i godkendt zone; sammenlign latens, tab og throughput.	Ingen uacceptabel påvirkning mod fastsat lokal baseline.
P03	Prøv godkendt DNS- og IP-testindikator samt legitim kontroltrafik.	Beslutning, log og undtagelse svarer til dokumenteret policy.
P04	Test IPv4/IPv6, VLAN, lokal/ekstern DNS og eventuel krypteret DNS.	Støttede og ikke-støttede stier er registreret.
P05	Afbryd strøm, uplink og feedadgang efter change-plan.	Observeret fejltilstand og genopretning svarer til godkendt driftsdesign.
P06	Udfør bypass og rollback efter skriftlig procedure.	Tilbageført forbindelse, konfiguration og logevidens er verificeret.

Produktionsbeslutning: sikkerhedsansvarlig og netværksejer godkender først dækning, acceptmålinger, alarmer, supportvej og rollback.

Leverandørens evidenspakke

Følgende oplysninger bør følge produktet som datablad, sikkerhedsdokumentation eller svar i et teknisk review.

Prioritet	Dokumentationskrav
Kritisk	Præcis hardwarevariant, portantal, linkhastigheder, strømforbrug, termiske krav, certificeringer og supportlevetid.
Kritisk	Fail-open/fail-closed, fysisk bypass, HA-design, maksimal throughput, latens og metode for måling.
Kritisk	DNS/IP-matchlogik, IPv6, VLAN, DoH/DoT, undtagelser, falsk-positiv proces og politikrækkefølge.
Høj	Feedkilder, proveniens, kvalitetskontrol, TTL, signering, opdateringsinterval og rollback af regler.
Høj	Administrationsflade, identitet/roller, firmwareopdatering, sårbarhedshåndtering og logeksport.
Høj	Præcise dataflows ud af kundens net, datakategorier, lagring, retention og databehandlerforhold.

KILDER OG NORMATIV KONTEKST

[1] Yazatas danske produkt- og privatlivssider, lokalt gennemgået 19.09.2026. [2] Skærbillede fra yazatasec.com/#adaptability leveret af kunden, 19.09.2026. [3] RFC 7858, DNS over TLS: rfc-editor.org/info/rfc7858. [4] RFC 8484, DNS over HTTPS: rfc-editor.org/info/rfc8484. Referencer [3]-[4] beskriver protokoller; de dokumenterer ikke Yazatas implementering.