Brought to you by 5th Mountain Networks (Pty) Ltd

South Africa's trusted specialist in secure, ethical, non-intrusive network visibility and managed cyber services.

Dōgen has been developed locally by 5th Mountain Networks as a privacy-respecting encrypted-traffic visibility layer designed specifically for regulated environments such as banking, financial services, education and distributed enterprises. Dogen is powered by the Zenarmor inspection engine for metadata-based threat detection and encrypted-traffic behavioural analytics.

Dōgen – Visibility Into Encrypted Threats (Without Decryption)

1. The Strategic Challenge

Business environments increasingly rely on encrypted traffic, cloud platforms, remote access, and distributed environments. While necessary, this shift has created a volume of encrypted communication that traditional firewalls cannot properly interpret without full TLS decryption—an approach that is often impractical, expensive, operationally disruptive, or undesirable in highly regulated environments.

This results in a new class of risk: attack behaviour that is technically present inside encrypted flows, but operationally invisible to traditional inspection methods.

Most modern attacker techniques now assume that traffic will be encrypted, and therefore deliberately hides inside encrypted channels and cloud infrastructure rather than attempting to bypass the firewall directly.

2. The Role of Dōgen

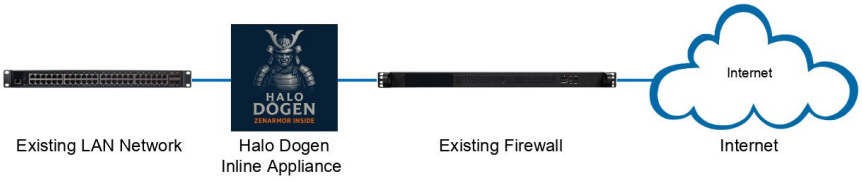
Dōgen provides a specialised visibility layer that interprets encrypted traffic behaviour without decrypting the traffic and without changing routing or architecture.

It does not replace the firewall, but instead:

- reveals areas the firewall cannot interpret,
- identifies hidden attacker behaviour,
- validates security assumptions, and
- quantifies risk that would otherwise remain unknown.

Dōgen essentially shows what is actually happening inside encrypted traffic, while the firewall continues performing its enforcement function.

Dōgen therefore operates as a dedicated encrypted-visibility overlay designed to coexist with, rather than replace, your existing investment in NGFW architecture.

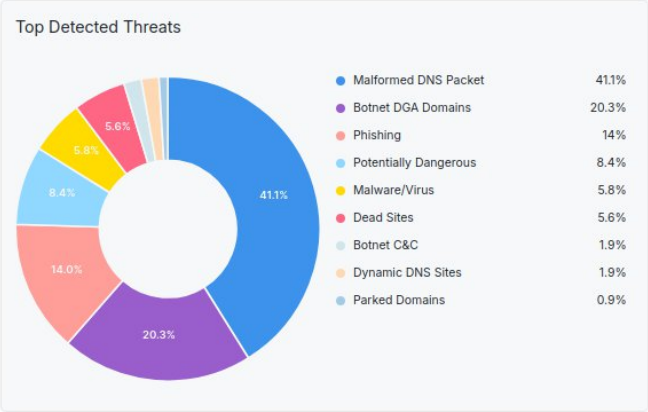


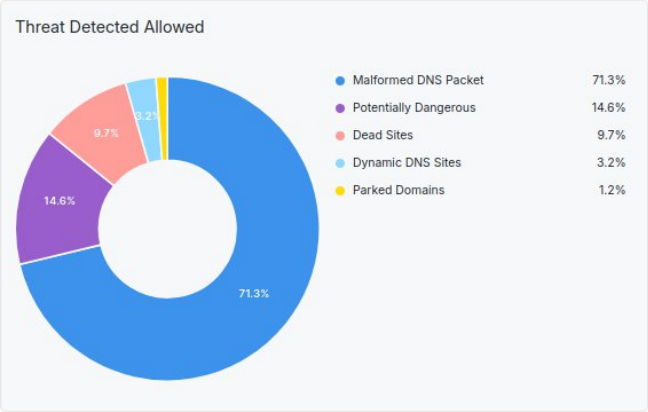
3. What Dōgen Reveals

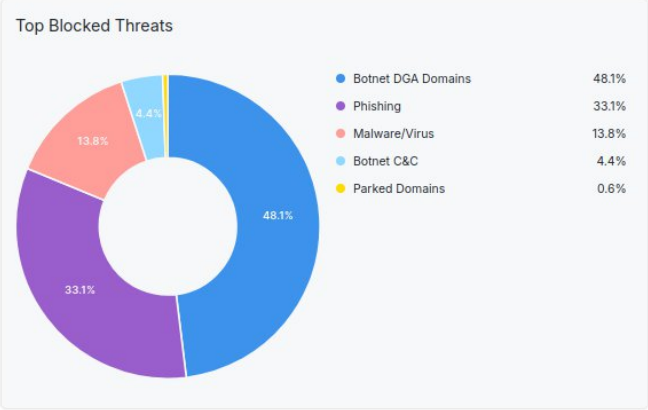
Dōgen focuses on behavioural indicators inside encrypted sessions, including:

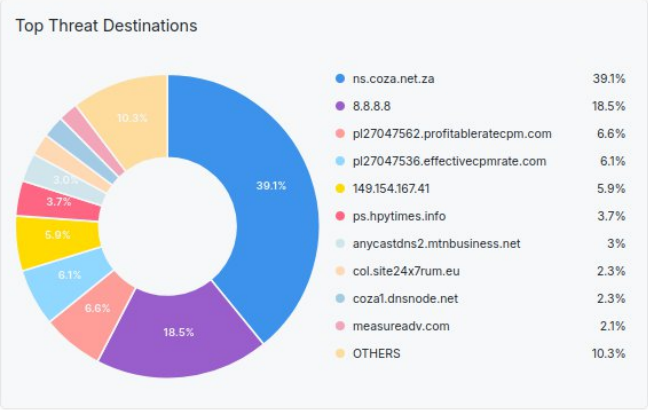
- command-and-control communication patterns,
- suspicious encrypted tunnels,
- unauthorised remote administration tools,
- compromised IoT devices attempting external communication,
- hidden exfiltration behaviours,
- encrypted flows associated with known malicious infrastructure, and
- internal attacker movement after initial compromise.

These are all recognised phases of modern intrusions—not isolated alerts. These are visible even when payloads are fully encrypted.









4. Why Firewalls Struggle (and Why Dōgen Still Sees More)

Modern encryption (TLS 1.3, ECH, QUIC, DoH/DoT, certificate pinning) removes the telemetry that firewalls have historically used for classification.

Even fully licensed and correctly configured NGFWs legitimately lose visibility into application intent inside encrypted sessions—this is an architectural limitation, not a configuration failure.

Dōgen restores that lost visibility by analysing encrypted behaviour through advanced ML/AI models and global threat intelligence, allowing it to risk-score encrypted flows, detect covert movement, and surface malicious intent **without decrypting the payload**.

In short: Dōgen sees what encryption conceals—not by breaking encryption, but by interpreting risk and intent at global threat-intelligence scale.

BrightCloud Global Learning & Scale

Dōgen's visibility is powered by **BrightCloud's continuously learning global threat intelligence**, which analyses billions of security events across worldwide networks every day. This provides real-time reputation scoring, category intelligence, malicious infrastructure tracking, and behavioural correlation at a scale no single organisation could achieve independently.

By leveraging BrightCloud's global telemetry, Dōgen translates encrypted activity into meaningful security insight—even when payloads remain fully private and unread.

BrightCloud is a globally recognised threat-intelligence platform used across major enterprise security products worldwide.

This global intelligence acts as the behavioural baseline Dōgen uses to detect attacker progression inside encrypted sessions.

5. Why Behaviour Matters

Modern intrusions rarely begin with obvious signatures. Instead, attackers follow a staged process: obtain a foothold,

- quietly explore the network,
- move internally, and
- exfiltrate slowly,

all while encrypted.

Each step is encrypted by design. Traditional inspection methods seldom see these stages.

Dōgen identifies the behavioural footprints associated with these stages without touching the encrypted payload.

6. Examples of Encrypted Risk Made Visible

With no decryption at all, Dōgen can identify:

- suspiciously persistent encrypted sessions,
- outbound traffic to malicious infrastructure,
- encrypted tunnels used for data extraction,
- compromised IoT devices communicating externally,
- unauthorised remote administration tools
- encrypted communications inconsistent with the device profile, and
- encrypted flows deliberately designed to hide intent.

These are all active behaviours, not theoretical patterns.

7. Security Outcome

Dōgen enables:

- accurate security posture assessment by identifying encrypted activity currently not inspected by existing controls
- clear visibility into behaviours the firewall cannot interpret, revealing hidden risk inside encrypted sessions
- earlier identification of advanced intrusion phases, even when fully encrypted
- reduced attacker “dwell time” — the period an intruder remains inside the environment before being detected, which is strongly correlated with lowering breach impact and preventing data loss in modern encrypted attacks
- enhanced SOC threat-hunting capability through evidence-based encrypted-traffic analytics
- closer alignment to Zero Trust principles by identifying hidden behaviour rather than relying only on session allow/block decisions
- POPIA-aligned encrypted-traffic inspection, since no decryption or content analysis is performed

8. What Dōgen Does NOT Do

Dōgen:

- does not decrypt traffic,
- does not replace the firewall,
- does not intercept user sessions,
- does not alter network routing,
- does not require endpoint agents, and
- does not interfere with privacy.

All analysis is done on metadata only, and no sensitive content is inspected or handled.

9. Designed for Regulated Contexts

Highly-regulated sectors face three simultaneous pressure points:

- increased encryption,
- increased cloud dependency, and
- increasingly sophisticated threat actors using encrypted delivery and control channels.

Full decryption may introduce architectural risk, privacy challenge, operational complexity, and POPIA considerations.

Dōgen sidesteps these challenges by providing visibility based on encrypted-traffic behaviour rather than decrypted content.

10. Positioning

Dōgen provides the ability to:

- quantify real encrypted risk,
- validate current firewall effectiveness,
- strengthen SOC decision-making, and
- provide actionable encrypted-behaviour intelligence,

without redesigning the network or compromising user privacy.

Dōgen ultimately improves visibility and reduces risk exposure in a modern encrypted environment—exactly where traditional controls are least able to operate.

Executive Summary

- Encrypted traffic is now the dominant transport layer for modern attacks.
- Traditional firewalls cannot interpret encrypted behaviour without full TLS interception.
- Dōgen identifies hidden threat behaviour inside encrypted traffic without decryption.
- This provides risk visibility, earlier detection, and reduced attacker presence.
- All while maintaining privacy and POPIA-aligned encrypted-traffic *visibility*.

Dōgen was developed specifically to provide encrypted-traffic visibility in distributed and highly regulated South African enterprise environments—without decryption, without architectural change, and without privacy compromise.