

# DarkShield

Cloak | Intercept | Contain

## The Invisible First Line of Defence for Modern Networks

In today's landscape, cyberattacks don't start with an exploit—they start with reconnaissance. Tools like Shodan, Censys, and mass scanners are constantly mapping exposed services across the internet, indexing every accessible port, protocol, and banner. Within hours, your network can be catalogued into a global attack database—long before any intrusion detection system gets triggered.

DarkShield breaks this cycle by making your infrastructure invisible. It's not a firewall, an IPS, or another noisy tool bolted onto your SIEM. Instead, it acts as a cloaking layer—deployed silently at the network edge, ahead of your firewall, intercepting malicious reconnaissance and command-and-control (C2) communications before they reach your defences.

Unlike traditional perimeter technologies that rely on static rules, signatures, or reactive alerts, DarkShield is autonomous, adaptive, and stealthy. It does not replace your existing firewalls or security stack—it fortifies them by stopping attacker traffic upstream. Recon is dropped. Callbacks are killed. Breaches are contained before they begin.

You can't attack what you can't see. DarkShield ensures attackers never even know your infrastructure exists.

With zero configuration changes, no tuning, and no alerts to manage, DarkShield delivers instant protection with measurable impact—reducing firewall load, lowering SIEM event volume, and freeing up your SOC to focus on real threats, not false positives.

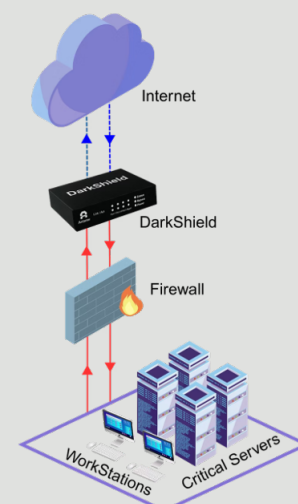


### Key Highlights

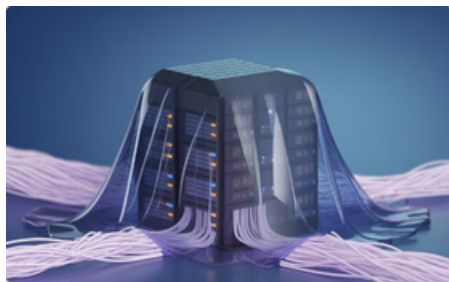
- ▶ **No configuration changes** – Deploy without tuning or modifying firewall rules
- ▶ **Inline deployment** – Precedes perimeter devices to stop threats at the edge
- ▶ **Bidirectional inspection** – Analyses inbound scans and outbound callbacks
- ▶ **Zero noise** – Drops malicious packets silently, with no alerting footprint
- ▶ **C2 disruption** – Cuts active malware connections in real time
- ▶ **Digital invisibility** – Removes your infrastructure from attacker scanners

### How Does It Works

- 1 Deployed before the firewall or router**  
Intercepts threats at the edge, before they enter the network.
- 2 Plug and play**  
Installs seamlessly like a network appliance, no tuning required.
- 3 Zero configuration change**  
No need to modify existing firewall rules, routing, or network policies.
- 4 Bidirectional traffic inspection.**  
Analyses both inbound and outbound traffic to stop command and control callbacks and external scans.

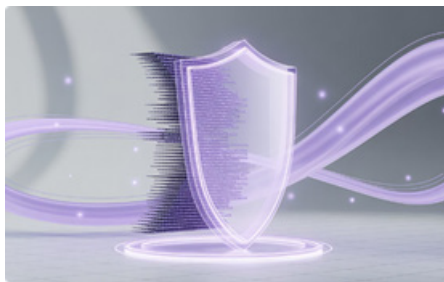


## How DarkShield Stops Attack



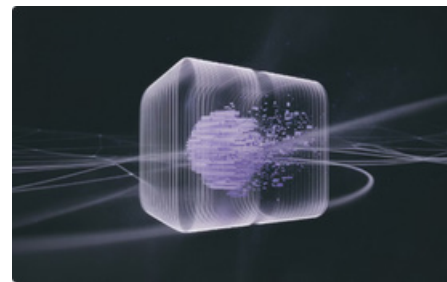
### Cloak – Make your network invisible

- ▶ No exposed IPs, MACs, or services — total digital disappearance
- ▶ Defeats Shodan, Censys, and internet-wide scans
- ▶ Eliminates attack surface before detection can occur



### Intercept – Stop threats in-flight

- ▶ Inline traffic filtering blocks scanners and C2 connections
- ▶ Threat intel-enriched matching via global + honeypot feeds
- ▶ No threat signals left behind — stealth rejection



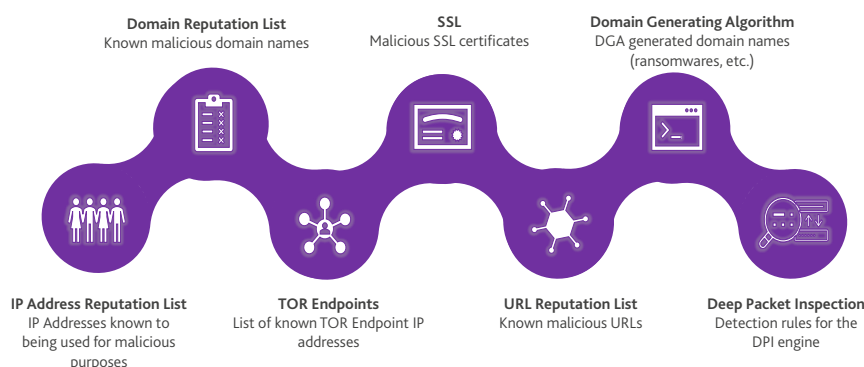
### Contain – Break the breach cycle

- ▶ Auto-isolates infected hosts and C2 channels
- ▶ Prevents lateral movement inside the LAN
- ▶ Triggers alerting workflows for SOC response

## DarkShield Multi-Layer Threat Defence Engine

One layer is not enough. DarkShield uses a multi-layered detection model to block advanced threats that evade traditional firewalls and reactive security tools. Each layer is purpose-built to target a specific vector of reconnaissance, command-and-control (C2), and lateral movement.

This layered design ensures that even if one indicator is missed—like an unlisted IP—other characteristics (such as DGA domain behavior, SSL anomalies, or deep packet patterns) will trigger silent, autonomous mitigation.



## About BDO Singapore

BDO Singapore, established in 1972, is a full-service professional firm catering to a diverse clientele that ranges from small and medium-sized enterprises (SMEs) to multinational corporations. With a team of over 600 professionals, BDO delivers a comprehensive suite of services, including audit, tax, advisory, and business services outsourcing. As an independent member of BDO International, the world's fifth-largest professional services network, the firm combines deep local expertise with global insights. In today's digitally driven landscape,

**BDO's Digital Advisory** practice helps organisations to reshape their value delivery and growth strategies by leveraging advanced technologies such as Robotic Process Automation (RPA), Artificial Intelligence/Machine Learning, and smart enterprise applications like ERP and WMS. Their key offerings encompass the development of tailored digital strategies and transformation roadmaps, optimisation of intelligent business applications, and unlocking the value of data through effective analytics and AI integration. Additional services include automation technologies, cloud deployment, ERP implementation, and project management.

**BDO's Cybersecurity** practice provides a comprehensive, turnkey solution for managing IT risks and digital threats. Their core services include cyber risk assessments, security testing, and developing cybersecurity frameworks aligned with enterprise risk management. Additionally, we offers digital forensics and investigation services, as well as compliance and controls reviews against established regulations. Notably, BDO holds prestigious credentials such as a CREST membership, along with accreditations for cybersecurity assessments, reinforcing its commitment to safeguarding client interests in the digital realm.

## Contact Our BDO Team:



**Gerard Seng**  
Executive Director  
gerardseng@bdo.com.sg  
+65 6990 2645



**Cecil Su**  
Director  
cecilsu@bdo.com.sg  
+65 6990 2846