PANTAU // ENTERPRISE SERVER SECURITY PLATFORM

SECURITY THAT WORKS AT THE KERNEL.

Zero-DNS Kernel WAF (eBPF/XDP) • Active Cyber Deception (Honeypot) • Anti-Deface • Backdoor Forensics

ZERO-FRICTION ONE-LINE AGENT DEPLOYMENT (TANPA UBAH DNS)

PANTAU bukan penyedia sewaan VPS, sebaliknya merupakan platform pertahanan siber peringkat kernel yang dipasang terus ke dalam server sedia ada melalui pautan agen berenkripsi. Daftar di portal PANTAU, salin pautan pendaftaran unik, dan jalankan pada terminal server untuk mengaktifkan perlindungan eBPF/XDP dalam masa 60 saat tanpa risiko *downtime* atau perubahan trafik DNS.

```
curl -sSL https://enroll.pantau.security/agent/register?token=ENT_KEY | sudo bash
```

JADUAL PELESENAN TAHUNAN KORPORAT & GLC

Struktur pelesenan direka khusus untuk melindungi infrastruktur kritikal, syarikat telekomunikasi, e-dagang berskala besar, dan agensi kerajaan dengan perlindungan menyeluruh peringkat kernel.

	COMMERCIAL / MID-MARKET **PANTAU CORE WAF**	MOST POPULAR • GLC / ENTERPRISE **PANTAU DECEPTION MATRIX**	TELCO / PERBANKAN / KERAJAAN **PANTAU SOVEREIGN SHIELD**
Kontrak Lisensi Tahunan	**RM 48,000** setahun (Kontrak Korporat)	**RM 145,000** setahun (Kontrak Korporat)	HARGA BERMULA **RM 290,000** setahun (Mengikut Saiz Pusat Data)
Kuota Link / Server Agent	Sehingga **10 Server Agents** (Salin & pasang di 10 server)	Sehingga **30 Server Agents** (Salin & pasang di 30 server)	**Unlimited Server Agents** (Liputan Pusat Data Penuh)
Yuran Integrasi & Onboarding (One-Off)	**RM 5,000** Baseline Hardening & Penalaan Awal	**RM 18,000** Custom WAF Policy & Honeypot Grid	**Harga Bermula RM 50,000** On-Premise / Air-Gapped & SIEM Setup
Kaedah Pemasangan	One-Line Encrypted Link (60-Saat)	One-Line Link + Penalaan Polisi Khas	Repositori Persendirian / On-Premise Control

	COMMERCIAL / MID-MARKET **PANTAU CORE WAF**	MOST POPULAR • GLC / ENTERPRISE **PANTAU DECEPTION MATRIX**	TELCO / PERBANKAN / KERAJAAN **PANTAU SOVEREIGN SHIELD**
Tapisan Trafik & DDoS	eBPF/XDP Kernel Firewall (L4 & L7) + DDoS Mitigation	eBPF/XDP Kernel Firewall + AI Behavioral Bot & API Shield	Dedicated High-Throughput eBPF Filtering + Global Blacklist Sync
Perlindungan Eksploitasi & Imbasan	Anti-Web Scanner (Stealth Mode), Brute-Force Halt & Core WAF (SQLi/XSS)	Semua dalam Core WAF + Sekatan Bot Transaksi & Anti-Scraping	Semua dalam Deception Matrix + Custom Virtual Patching (Sistem Legasi)
Integriti Fail & Perangkap Siber	Pemantauan Kerentanan Mingguan & Patch Berjadual	**Kernel-Lock Anti-Deface (Auto-Heal) + Active Honeypot Traps**	**Multi-Layer Deception Grid + Immutable Kernel File Lock**
Jejak Backdoor & Forensik	Log Sekatan Serangan & Papan Pemuka Keselamatan	**Real-Time Backdoor & Webshell Hunter** (Kuarantin Automatik)	**Kill-Chain Forensics, Jejak Asal Backdoor & C2 Sinkholing**

PERINCIAN KEUPAYAAN MENGIKUT PAKEJ

1. PANTAU CORE WAF — Essential Kernel Defense — RM 48,000 / Tahun (10 Server Agents)

Perlindungan asas berkelajuan tinggi pada peringkat kernel untuk menghentikan serangan web dan cubaan pemindaian sebelum trafik mencecah aplikasi utama.

- **eBPF/XDP Layer 4 & Layer 7 Kernel WAF:** Menyekat serangan SQL Injection (SQLi), Cross-Site Scripting (XSS), Remote Code Execution (RCE), dan banjir trafik DDoS terus pada kad rangkaian (NIC) dengan penggunaan CPU di bawah 1%.
- **Zero-Reconnaissance Anti-Scanner Engine:** Membutakan alatan pengimbas kerentanan automatik (Nmap, Acunetix, Nikto, WPScan, SQLMap, BurpSuite). Server kelihatan tertutup rapat kepada penggodam tetapi beroperasi normal untuk pengguna sah.
- **Automated Brute-Force & Credential Stuffing Halt:** Memutuskan serta-merta cubaan meneka kata laluan pada SSH, cPanel, halaman pentadbir, dan titik akhir (*endpoint*) API.
- **Automated Security Patch Workflow:** Pengurusan tampalan keselamatan berkala dengan aliran kerja pengesahan dari papan pemuka pusat.

2. PANTAU DECEPTION MATRIX — Proactive Traps & Anti-Deface — RM 145,000 / Tahun (30 Server Agents)

Direka untuk organisasi yang memerlukan pertahanan aktif, perlindungan perubahan kod sumber secara haram, dan pengesanan kod hasad tersembunyi.

- **Merangkumi semua keupayaan PANTAU CORE WAF, ditambah:**
- **Kernel-Lock Anti-Deface & Auto-Heal Engine:** Mengunci fail teras aplikasi web pada peringkat kernel. Sekiranya penceroboh berjaya mengubah suai laman utama (*web defacement*) atau menyuntik skrip haram, agen PANTAU membatalkan perubahan tersebut dan memulihkan fail asal secara automatik dalam masa milisaat.
- **Built-In Honeypot & Cyber Deception Traps:** Membina umpan tiruan secara automatik (port pangkalan data palsu, direktori pentadbir bayangan, dan titik akhir API umpan). Sebarang IP yang menyentuh perangkap ini disenaraihitamkan serta-merta merentas semua server dengan kadar *0% False Positive*.
- **Real-Time Backdoor & Webshell Tracker:** Mengimbas memori dan sistem fail secara berterusan untuk mengesan *webshell* tersembunyi (C99, B374K, Alfa), *reverse shell*, dan proses haram sebelum mengasingkannya (*quarantine*).
- **AI-Assisted Behavioral Bot & API Protection:** Melindungi transaksi perniagaan dan aliran API daripada bot pintar, penipuan automatik, dan kecurian data berterusan.

3. PANTAU SOVEREIGN SHIELD — Deep Forensics & Data Center Control

Harga Bermula RM 290,000 / Tahun (Unlimited Agents)

Penyelesaian kedaulatan siber penuh untuk infrastruktur kritikal negara, syarikat telekomunikasi, institusi kewangan, dan pusat data berskala besar.

- **Merangkumi semua keupayaan PANTAU DECEPTION MATRIX, ditambah:**
- **Backdoor Origin & Kill-Chain Forensics:** Menjejaki punca sebenar kemasukan *backdoor* (vektor serangan, fail yang ditembusi, rentetan arahan yang dijalankan oleh penggodam) serta memutuskan komunikasi keluar ke pelayan *Command & Control (C2)* penceroboh (*C2 Sinkholing*).
- **One-Click Emergency Host Quarantine & Anti-Tamper Agent:** Keupayaan mengasingkan server yang diceroboh dengan satu klik dari pusat kawalan, serta perlindungan agen peringkat kernel yang menghalang penggodam (walaupun dengan akses `root`) daripada mematikan agen PANTAU.
- **Custom WAF Virtual Patching:** Kejuruteraan peraturan keselamatan khusus untuk menutup celah kerentanan pada aplikasi legasi tanpa perlu mengubah kod sumber asal.
- **Full SIEM, SOAR & SOC Integration:** Penghantaran telemetri masa nyata ke sistem Splunk, IBM QRadar, Elastic, Webhook, serta sokongan laporan pematuhan audit (ISO 27001, BNM RMiT, dan NACSA) dengan jaminan SLA khusus 24/7.

KELEBIHAN SENI BINA AGEN PANTAU

Komponen Sistem	WAF Berasaskan Cloud / DNS Lama	PANTAU Kernel Agent (eBPF/XDP)
Pemasangan & Integrasi	Perlu tukar rekod DNS, sijil SSL, dan halakan trafik ke pelayan luar.	**Salin & tampal 1 pautan arahan** di terminal server; aktif dalam 60 saat tanpa ubah DNS.
Kedaulatan Data & Privasi	Trafik sensitif dinyahsulit di pelayan pihak ketiga luar negara.	**100% Dalam Server Sendiri:** Semua penapisan berlaku di dalam kernel server pelanggan.
Pengesanan Backdoor & Deface	Buta terhadap aktiviti dalaman server dan perubahan fail tempatan.	**Kawalan Penuh Dalam Server:** Mengesan *webshell*, mengunci fail web, dan memasang *Honeypot*.

WHY PANTAU DELIVERS VALUE — SENI BINA & SPESIFIKASI TEKNIKAL

Lebih daripada sekadar tembok api (*More Than A Firewall*). PANTAU menggabungkan enam lapisan pertahanan aktif secara terus di dalam kernel Linux untuk memberikan perlindungan menyeluruh terhadap serangan moden tanpa membebankan prestasi server.

01 // KERNEL-LEVEL DEFENSE & DDoS MITIGATION (eBPF / XDP) — Layer 3, Layer 4 & Layer 7

Berbeza dengan WAF tradisional yang beroperasi di lapisan aplikasi (*user-space*) dan memperlahankan pelayan web ketika diserang, PANTAU menggunakan teknologi **Extended Berkeley Packet Filter (eBPF)** dan **eXpress Data Path (XDP)**. Paket serangan DDoS (SYN Flood, UDP Amplification, HTTP/2 Rapid Reset) digugurkan terus pada pemacu kad rangkaian (NIC) dalam masa kurang daripada **1 milisaat** sebelum sempat menggunakan memori RAM atau CPU aplikasi.

02 // ZERO-RECONNAISSANCE & ANTI-WEB SCANNER ENGINE — Stealth Perimeter Cloaking

Setiap pencerobohan bermula dengan fasa pengimbasan (*reconnaissance*). Enjin Anti-Imbasan PANTAU mengenal pasti cap jari (*fingerprints*), corak permintaan, dan tandatangan pengimbas kerentanan automatik seperti **Nmap, Acunetix, Nikto, WPScan, SQLMap, BurpSuite, dan Nessus**. Sebaik sahaja imbasan dikesan, PANTAU memutuskannya pada peringkat kernel—menjadikan server kelihatan "mati" atau tertutup kepada penggodam sementara pengguna sebenar melayari web tanpa gangguan.

03 // APPLICATION WAF & AUTOMATED BRUTE-FORCE HALT

OWASP Top 10 & API Shield

Pemeriksaan muatan mendalam (*Deep Payload Inspection*) menyekat serangan **SQL Injection (SQLi), Cross-Site Scripting (XSS), Local/Remote File Inclusion (LFI/RFI), dan Remote Code Execution (RCE)**. Pada masa yang sama, modul *Brute-Force Halt* memantau semua titik pengesahan (SSH, FTP, cPanel, halaman log masuk CMS/Admin, dan API *endpoint*) untuk menyekat serangan tekaan kata laluan dan *credential stuffing* secara automatik.

04 // IMMUTABLE KERNEL ANTI-DEFACE & AUTO-HEAL ENGINE

Real-Time File Integrity Lock

Walaupun penggodam berjaya mencuri kata laluan pentadbir atau menembusi celah kod aplikasi pihak ketiga, mereka tetap tidak boleh mengubah tampilan laman web. PANTAU mengunci direktori kod sumber utama pada tahap sistem fail kernel. Sebarang cubaan mengubah fail indeks, menyuntik halaman *deface*, atau memasukkan skrip haram (seperti pautan spam/judi) akan **dihalang serta-merta dan dipulihkan kepada fail asal secara automatik (Auto-Heal)** dalam masa milisaat.

05 // ACTIVE CYBER DECEPTION (BUILT-IN HONEYPOT GRID)

Zero False-Positive Trapping

Sebaik sahaja pautan agen dipasang, PANTAU secara automatik menjana perangkap siber (*Honeypot*) yang terdiri daripada port pengurusan palsu, laluan direktori pentadbir bayangan (contoh: `/wp-admin-bak`, `/.env.prod`), dan titik akhir API tiruan. Kerana tiada pengguna sah yang akan mengakses laluan umpan ini, sebarang trafik yang menyentuhnya disahkan 100% sebagai penceroboh, direkodkan teknik serangannya, dan disenaraihitamkan merentas seluruh kluster server.

06 // DEEP BACKDOOR HUNTER & KILL-CHAIN FORENSICS

Webshell Detection & C2 Sinkhole

PANTAU memantau panggilan sistem (*syscalls*) dan memori server secara masa nyata untuk mengesan *backdoor* yang sudah tertanam seperti **C99, B374K, Alfa Shell, IndoXploit, Crypto-Miner, dan Reverse Shell**. Modul forensik menjejaki *Kill-Chain* penuh: daripada IP mana *backdoor* dimuat naik, fail mana yang dieksploitasi, apakah arahan terminal yang telah dijalankan oleh penceroboh, serta memutuskan terus sambungan keluar ke pelayan *Command & Control (C2)* penggodam.

MATRIKS PERBANDINGAN KEUPAYAAN TEKNIKAL MENGIKUT PAKEJ

	PANTAU CORE WAF RM 48,000 / TAHUN	**PANTAU DECEPTION MATRIX** RM 145,000 / TAHUN	**PANTAU SOVEREIGN SHIELD** BERMULA RM 290,000 / TAHUN
Kuota Server Agent	10 Server Agents	30 Server Agents	Unlimited (Satu Pusat Data)
Pemasangan One-Line Link	Termasuk (Self-Enrollment)	Termasuk + Assisted Tuning	On-Premise / Air-Gapped Repo

	PANTAU CORE WAF RM 48,000 / TAHUN	PANTAU DECEPTION MATRIX RM 145,000 / TAHUN	PANTAU SOVEREIGN SHIELD BERMULA RM 290,000 / TAHUN
eBPF/XDP L4 & L7 DDoS Shield	Termasuk (Standard Filtering)	Termasuk (AI Traffic Profiling)	Termasuk (Multi-Node Sync)
Anti-Scanner (Stealth Mode)	Sekatan Pengimbas Automatik	Sekatan + Pemalsuan Tandatangan	Sekatan + Global Threat Sharing
Brute-Force & SQLi/XSS WAF	Perlindungan Penuh (SSH & Web)	Perlindungan Penuh + API & Bot Shield	Perlindungan Penuh + Custom Virtual Patch
Anti-Deface & File Lock	Pemantauan Integriti Mingguan	**Kernel File Lock + Auto-Heal**	**Immutable Kernel Lock + Audit Trail**
Sistem Perangkap Honeypot	—	**Active Web & Port Honeypot**	**Custom Deception Grid & Decoy DB**
Jejak Backdoor & Forensik	Amaran Aktiviti Mencurigakan	**Webshell Hunter & Auto-Quarantine**	**Kill-Chain Forensics & C2 Sinkholing**
Integrasi SOC & Pematuhan	Papan Pemuka & Laporan PDF	Webhook, Slack, Telegram & API	**Full SIEM/SOAR + ISO/BNM RMiT/NACSA**

Nota Komersial: Semua harga yang dinyatakan adalah dalam Ringgit Malaysia (MYR) tidak termasuk cukai perkhidmatan semasa. Bagi pakej **PANTAU SOVEREIGN SHIELD**, harga akhir ditentukan berdasarkan jumlah kluster pusat data, keperluan penempatan *On-Premise / Air-Gapped*, dan tahap sokongan SLA yang dipersetujui.