AI SHIELDNET

AIShieldNet LLM Zero-Day EndPoint Protection

AI ShieldNet: Your AI-Powered Guardian Against Evolving Zero-Day Threats

About AI ShieldNet

AI ShieldNet is a cybersecurity solution that combines an agent and a SaaS platform to detect, block zero-day attacks.
It uses advanced LLM and AI algorithms to analyze threats and malware in real time, identifying suspicious activity and protecting users from falling victim to zero-day threat.

10+

Over 10 AI edge cutting technology

1000+

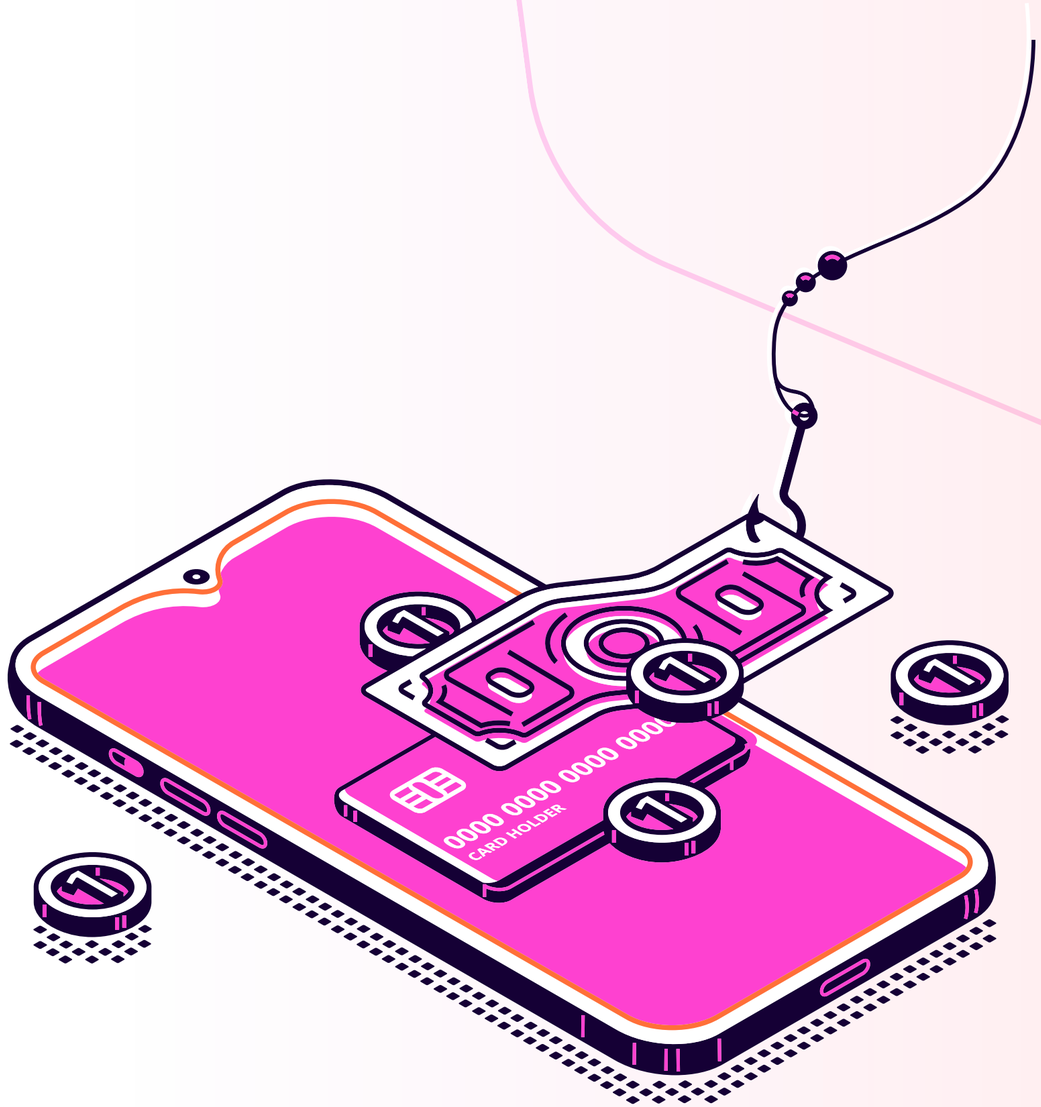
Detect and Prevent 1K Zero Day Malware and Phishing

80%

Zero Day Detection Accuracy

1-2 Response Time

Fast real-time AI analysis within 1-2 seconds



Our AI solutions

LLM EndPoint Protection

AI ShieldNet takes aim at endpoints, unlike traditional Anti-Virus.

Phishing Endpoint Protection

AI ShieldNet protects users against Phishing attacks.

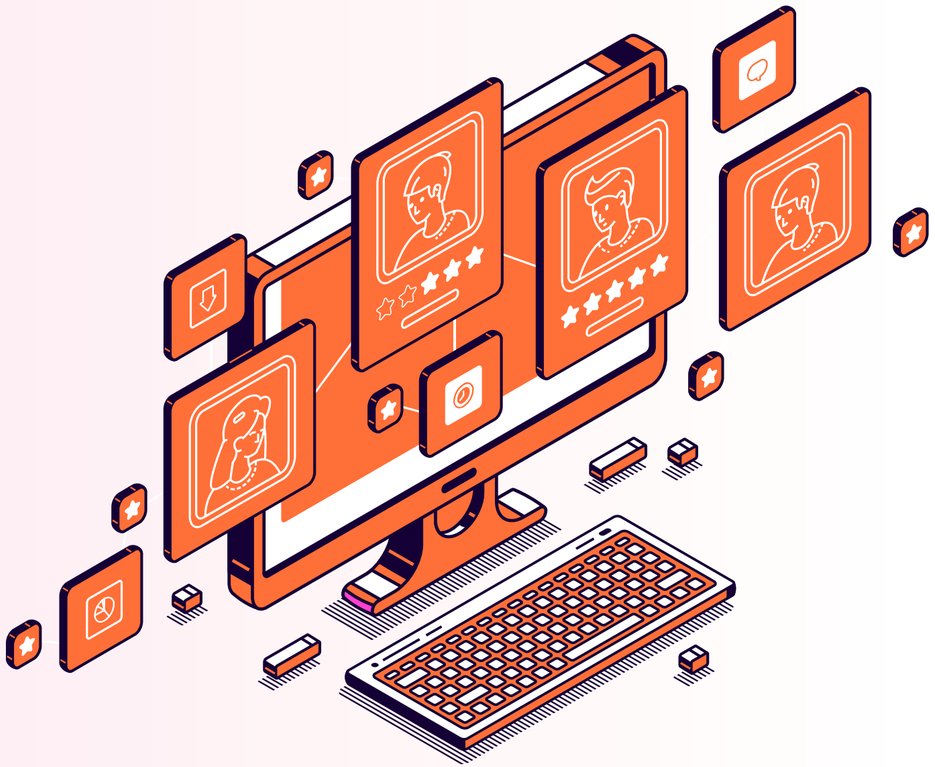
SaaS Platform

The SaaS provides a business overview of various trends and tracking.

AI Zero Trust File Analysis

Real-time Malware and URL analysis is now possible with dual AI, taking only 10 seconds to process.

Why choose AI ShieldNet



Beyond Detection: AI ShieldNet doesn't just sound the alarm, it provides invaluable intel. Its AI engine learns from every encounter, constantly refining its defenses and providing actionable insights to strengthen your overall security posture.

- **Dual AI Driven Malware and Phishing Detection**
- **EndPoint Protection**
- **24/7 Real Time Protection**
- **Comprehensive Dashboard and Logs**

AI SHIELDNET

AI Driven Cyber Security

Zero Day Phishing Detection

SaaS Platform

Protect your organization from Zero Day Attacks

We provides comprehensive AI security solutions

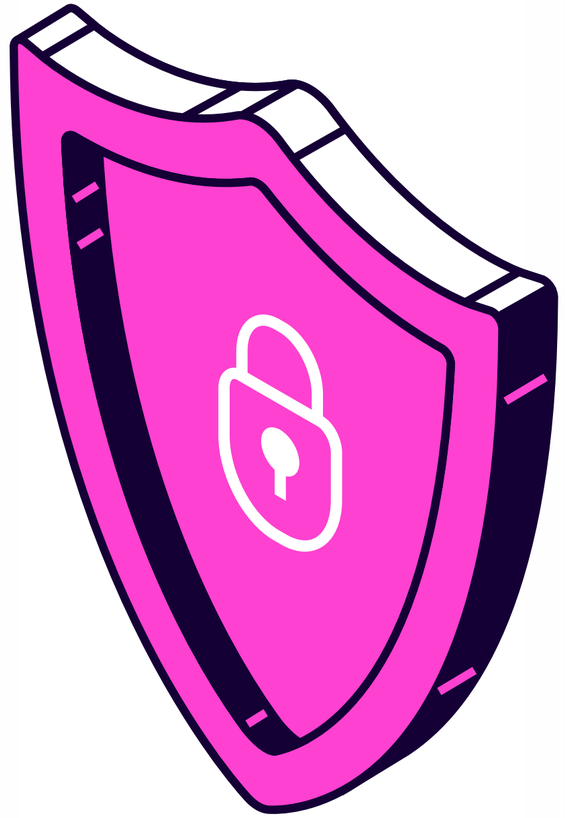
Endpoint & Browser Extension

Zero Trust File AI Analysis

Cryptocurrency Protection

Safeguard your assets

AIShieldNet is your intelligent defense layer, designed to protect your critical digital assets from evolving cyber threats. Leveraging advanced AI and real-time analytics, AIShieldNet ensures continuous monitoring, threat detection, and rapid response—so your data, systems, and operations remain secure and resilient. Stay ahead of risks with smart, adaptive protection.



01.

Risk reduction

Give a detailed description of the header being provided here.

02.

Increase Security

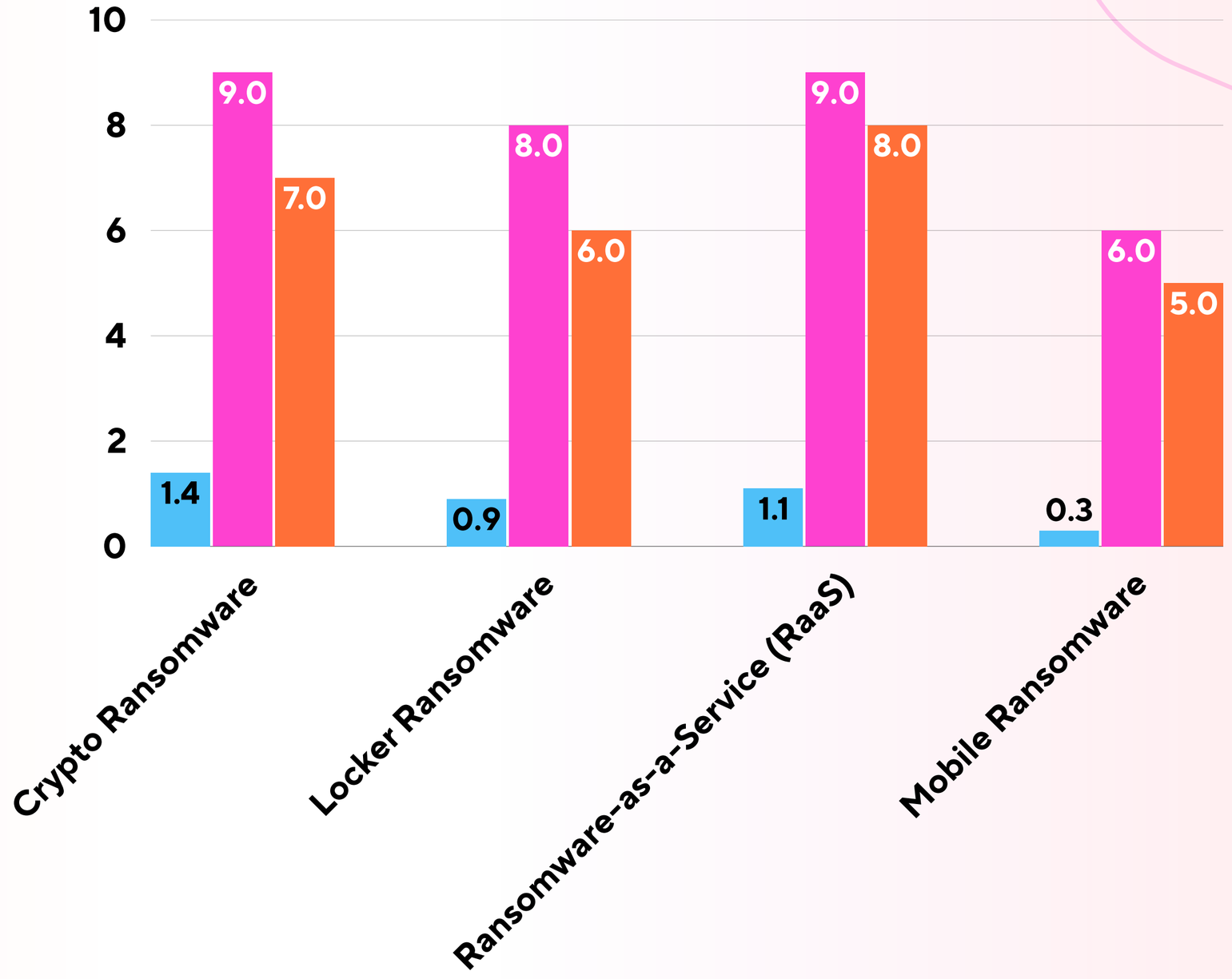
Give a detailed description of the header being provided here.

03.

Data Loss Prevention

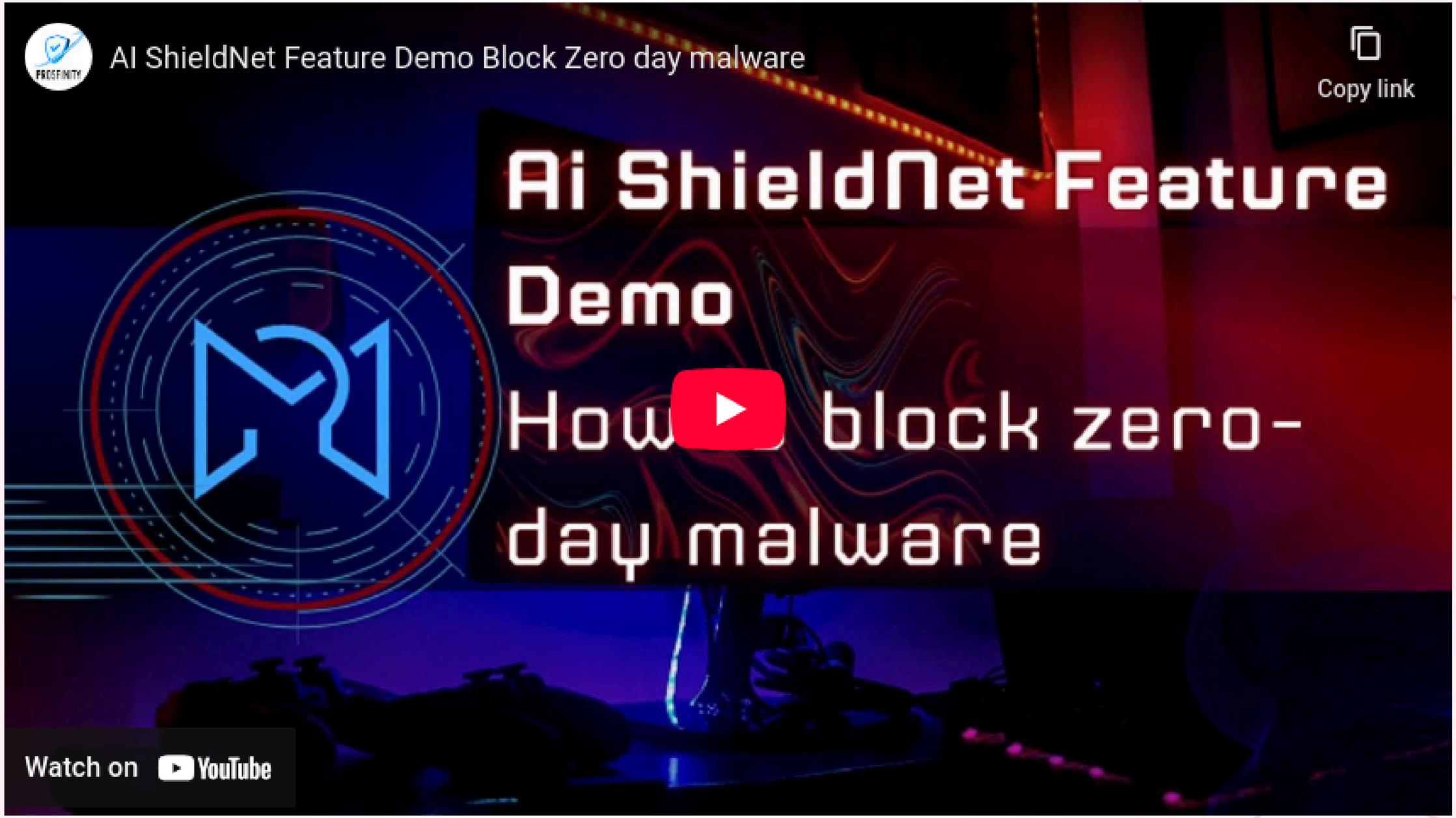
Give a detailed description of the header being provided here.

Ransomware Threat Report



- **Total Projected Losses (In billions USD)**
- **Severity (1-10)**
- **Success Rate (1-10)**

Effective mitigation strategies are in place, with high or medium mitigation levels across incidents.



Click here to watch video

Features Used for AI Detection

LLMs & Netrual Network AI

Zero-Trust AI Analysis of Execute, Excel, Word

AI EndPoint Anti-Phishing

AI Category

The AI detection system uses powerful LLMs and neural network AI for real-time threat identification and adaptive learning. With zero-trust analysis, it carefully inspects all executable, Excel, and Word files for signs of malicious behavior, categorizing threats by risk for fast response.

The platform combines advanced AI techniques—like anomaly detection and contextual analysis—to maximize protection. Integrated endpoint anti-phishing AI further blocks suspicious URLs and phishing attempts, delivering fast and reliable cybersecurity for modern threats.

Zero Trust AI Analysis

AIShieldNet introduces an innovative zero trust approach to AI-powered file analysis that fundamentally changes how processes are allowed to run on a user's system. With this design, when a user attempts to open a file or run a process, the AIShieldNet agent immediately intercepts and kills the process—by default, nothing is trusted.

The suspicious file or process is then sent to a secure cloud-based AI engine for real-time analysis. Only after the cloud AI determines the process is safe does the agent allow it to resume; if the analysis is inconclusive or malicious, the process remains blocked. This strict "never trust, always verify" policy, combined with advanced cloud AI analytics, shifts security from a reactive to a proactive stance, significantly reducing the risk of zero-day attacks and unknown threats—ensuring that no process is ever allowed to run without thorough, real-time scrutiny.

About AIShieldNet LLM

AIShieldNet Endpoint Detection and Response (EDR) solution introduces a groundbreaking approach to endpoint security by leveraging real-time cloud AI analysis of Windows process events.

LLM Engine

Management Dashboard & Integration APIs

LLM Analysis

Cloud Update without waiting for a full client software update

Beyond MITRE Patterns – Zero-Day Threats

Contextual and Narrative Understanding

Behavioral Analysis vs. Signatures

AI SHIELDNET

LLM Data Flow From Endpoint to Cloud and Back

1. Process Capture (Endpoint)
2. Real-Time Forwarding to Cloud
3. LLM Analysis (Cloud AI Engine)
4. Risk Scoring & Decision
5. Response Action (Endpoint Enforcement)
6. Alerting & Reporting Feedback & Learning

Detection Logic with LLM Intelligence

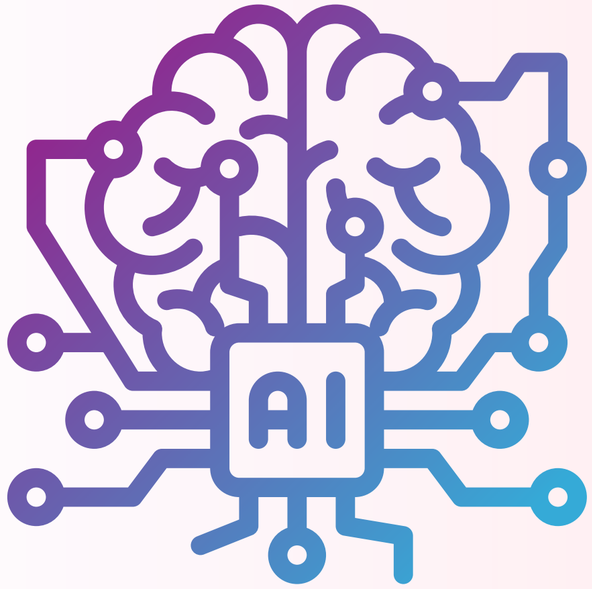
01.
Behavioral Analysis vs. Signatures

02.
Contextual and Narrative Understanding

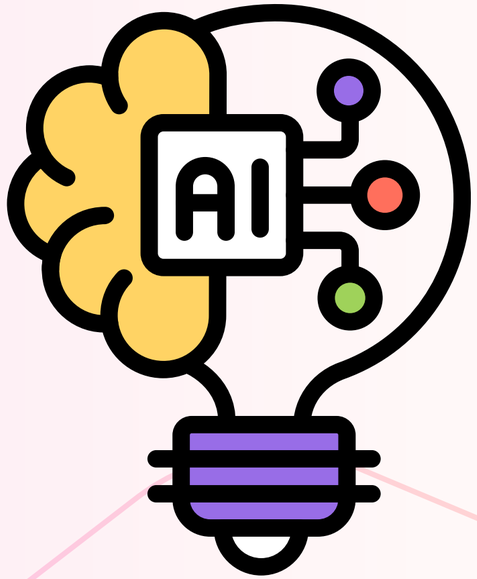
03.
Beyond MITRE Patterns – Zero-Day Threats

04.
Reducing False Positives via Reasoning

05.
The detection logic is not static



Unique Differentiators of AIShieldNet LLM-Powered Approach



01.
First-of-its-Kind LLM-Integrated EDR

02.
Unmatched Zero-Day Threat Detection

03.
Comprehensive Visibility (No Gaps in Monitoring)

04.
Context-Driven Precision (Fewer False Alarms)

05.
Collective Intelligence & Cloud Scale

06.
Augmented Analyst Experience

Use Cases and Benefits

01.
Zero-Day Ransomware Prevention

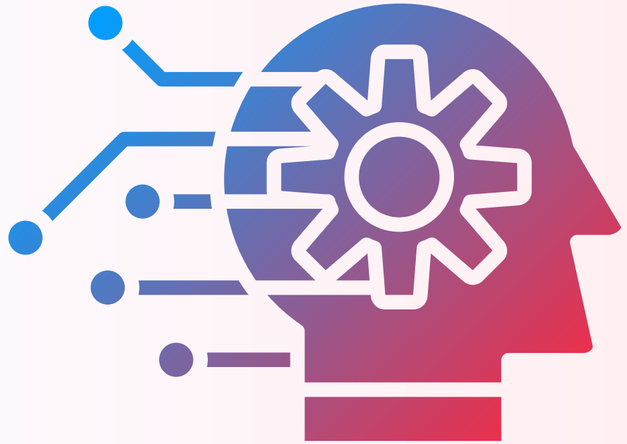
02.
Insider Threat Detection

03.
Fileless Malware and Living-off-the-Land Attack Blocking

04.
Hands-on-Keyboard" Human Attacker Detection

05.
Advanced Persistent Threat (APT) and Lateral Movement Visibility

06.
Operational Benefits and ROI



Security plan for your security needs

AI SHIELDNET ENDPOINT PROTECTION

From $9.9 HKD

per month

Comprehensive protection
for mid-sized enterprises.

What you will get:

- LLM’s Behaviour Analysis
- Zero Day Malware and Phishing Detection & Response
- Free Trial
- MDR SaaS Portal

Get Protected Today!

Contact info

+852 98319379

nathanlau@prosfinity.com

marketing@prosfinity.com