OLPEMI

Secure Every Click

Creating a Safer World

PotatoNet Co., Ltd.

We detect malicious URLs from the visible web to the invisible deep and dark web — so every click your users make is a safe one.

Address 120, Neungdong-Ro, Gwangjin-Gu, Seoul, Republic Of Korea

TEL +82-2-468-0118 **Email** sales@potatonet.ai

AI-Powered Malicious URL Detection Solution Based on Deep Web Threat Intelligence

OLPEMI

Korea Innovative Procurement Product (2026-2029)

AI deep-web malicious-URL threat intelligence — seeing what hides in the dark, before the click lands.

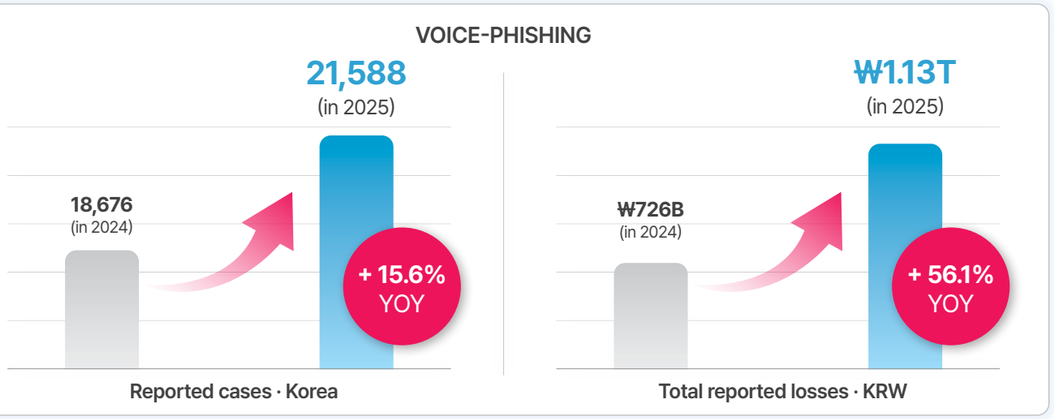
2026 Innovative Procurement Prototype Product — Selected
2024 Information-Security Products for SMEs — Designated Supplier
2024 Technology Development Pilot Program — Selected
2023 Information-Security Growth Program — Supported

PotatoNet

CYBER ATTACK OVERVIEW

SURGE IN SOCIAL ENGINEERING ATTACKS EXPLOITING HUMAN PSYCHOLOGY

Cyberattacks start with a URL

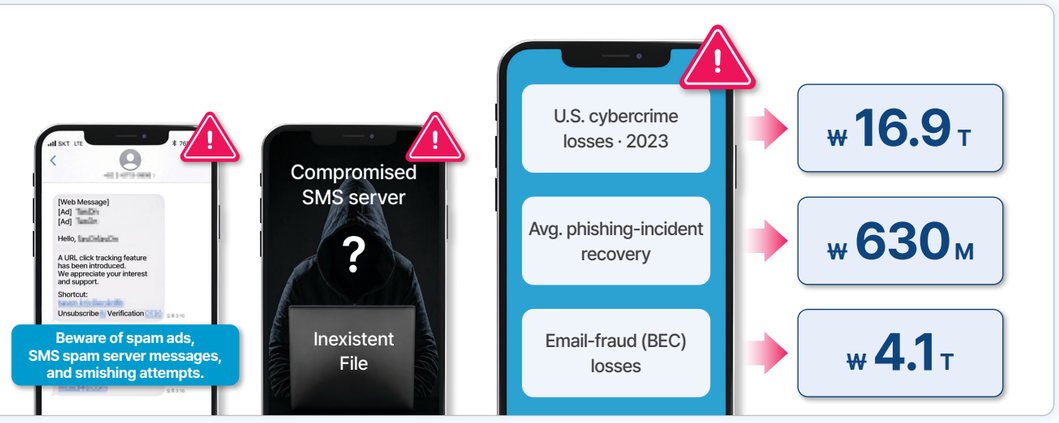


Google, Apple & Facebook account records leaked on the dark web (Jun 2025) **16 billion**

Telecom SIM-card records exposed in carrier breaches **26.95 million**

Online-retail & guarantee-insurance providers hit by infections **Ransomware**

Source · Phishing Landscape 2024



CYBER ATTACK OVERVIEW

MOST THREATS GO UNDETECTED THEY LOOK AS IF THEY DON'T EXIST

WHY COLLECTION MATTERS

Hidden URLs

Built from subdomains, ports, sub-paths and parameters — links that can't be identified from the domain alone. Detection must start from the exact URL the target was sent.

Detection-evasion URLs

A site that's inactive or refuses to serve content can't be analysed. Attackers tune delivery to the victim's device, time and location — so collection itself must adapt.

- Attacks Leveraging the Deep Web's Non-Indexable Structure
- A Large Proportion of Malicious URLs Are Hidden Within the Deep Web
- Limitations of Blacklists and Domain-Based Defense Systems

CHARACTERISTICS OF DEEP-WEB URLS

No login required

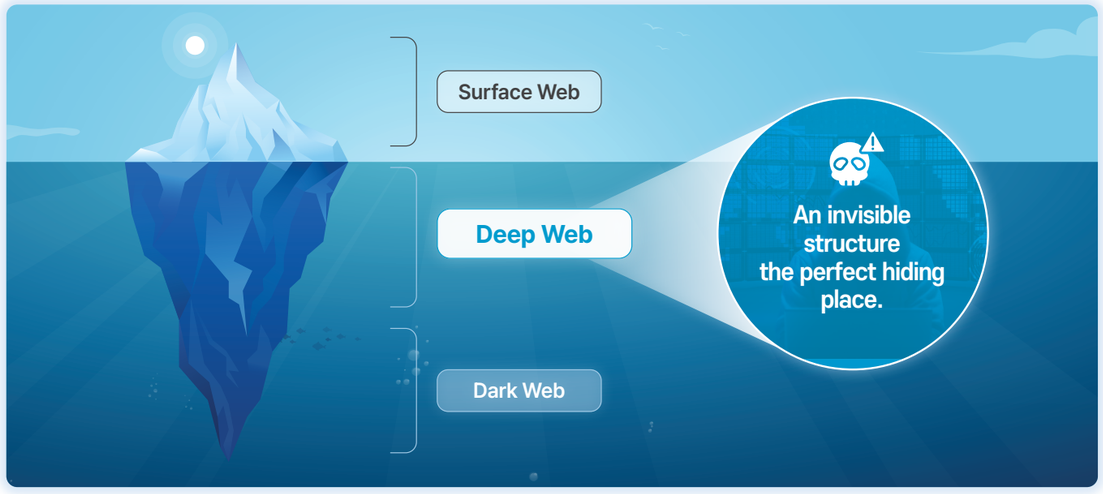
Reachable without any authentication — unlike the legitimate deep web.

Looks like the surface web

Visually identical to ordinary sites and opens in a standard browser.

Disconnected paths

No internal pages or links point to it, so the URL can't be found by crawling.



AI-POWERED DEEP WEB URL DETECTION

What is Olpemi URL Threat Intelligence?

Leveraging AI and deep web threat intelligence to detect malicious URLs.

Proactive cyber defense before malware infection occurs.

World's First Deep Web Detection Technology / Protected by Over 10 Patents.

Selected as a 2026 Innovative Procurement Product.

Differentiation

Detecting Across Both the Surface Web and the Deep Web.

Detection of Unknown and Newly Emerging URL Threats.

Specialized in detecting attacker C2 servers and web shells.

AI-POWERED DEEP WEB URL DETECTION

01

Innovation in deep-web concealment detection

- Identify malicious deep-web content & detect C2 servers
- Counter inactive, no-activity evasion systems
- Detect web shells & malware on compromised servers
- Catch new malicious URLs via real-time monitoring

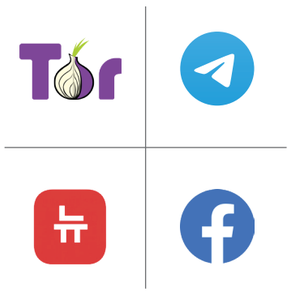
02

State-of-the-art vulnerability detection platform

- BERT, sLM, VLM & multi-agent (generative) models
- Cascading decision processing with sLM reports
- Dynamic rendering & malware analysis
- Asynchronous processing on Docker + AI big-data
- Image- and code-based attacker profiling

03

Internet-wide URL threat hunting



INTRODUCE OLPEMI - LINE UP

ONE PLATFORM, FOUR WAYS TO DEPLOY IT

- Detects deep-web-based threats
- Real-time new-threat detection
- Innovative procurement prototype

OLPEMI TI
Analysis & Validation

OLPEMI URL Threat intelligence
Malicious URL Threat Detection

—

Crawls suspicious URLs flagged by other security tools on a separate network and verifies whether they are malicious.

OLPEMI SWG
Secure Web Gateway

OLPEMI SWG
Detection of Malicious URLs and Insider Data Leakage

—

Inspects inbound and outbound traffic at the network gateway to catch malicious activity and internal data leaks.

OLPEMI WALL
Detection Firewall

OLPEMI WALL
Deep Web Intelligence Firewall

—

Protects web and cloud servers by detecting and blocking malicious deep-web requests at the server.

OLPEMI MOBILE
PC/Mobile

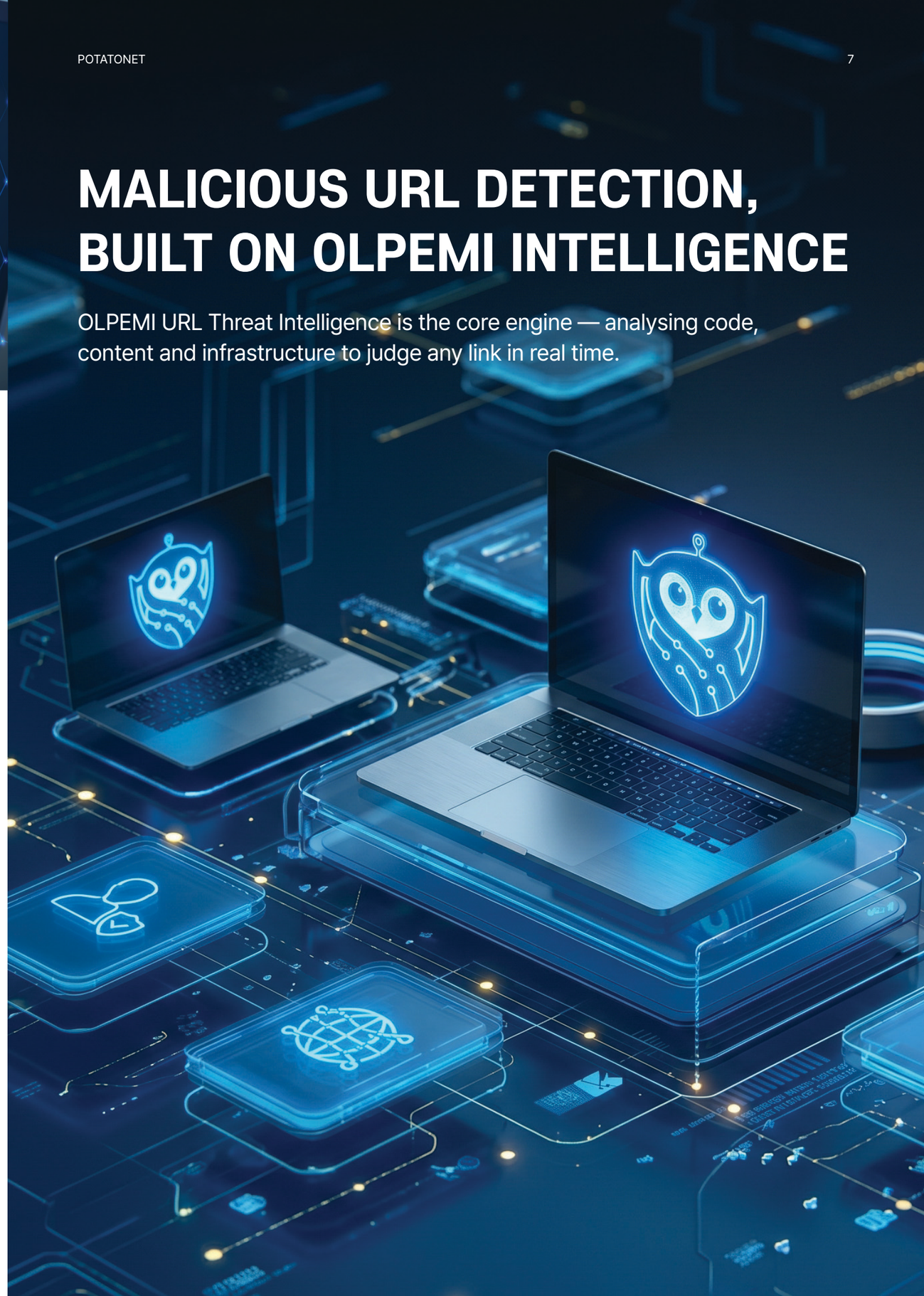
OLPEMI Mobile, Browser Extension
Malicious URL Detection on PC & Mobile

—

A mobile app and browser extension that block access to malicious URLs on phones and PCs.

MALICIOUS URL DETECTION, BUILT ON OLPEMI INTELLIGENCE

OLPEMI URL Threat Intelligence is the core engine — analysing code, content and infrastructure to judge any link in real time.



OLPEMI URL THREAT INTELLIGENCE(TI)

01 ANALYSIS DATA

URLs, web metadata, JavaScript-tuned language models and a vast reference dataset — ten dimensions analysed for every link.

01 URL structural features
Length, special characters, entropy, IDN/Punycode, DGA.

02 Web code & resources
HTML, JavaScript, iframes, external scripts, text.

03 Web content & images
Rendered content, screenshots, favicons, logos, link structure.

04 Redirect chain
URLs, IPs, status codes & rendered content for every hop.

05 Downloaded files
File type, size, hash.

06 HTTP communication metadata
Request/response headers, cipher suites.

07 Domain & certificate ops
WHOIS/RDAP, CT logs, passive DNS, newly-registered domains.

08 Servers & hosting infra
HTTP status codes, web server, IP, ASN, reverse DNS.

09 Time & lifecycle
Activity period and lifecycle signals.

10 Attacker infrastructure
Bulk registrations, hosting/cloud providers, registrars, certificates.

OLPEMI URL THREAT INTELLIGENCE(TI)

02 AI ANALYSIS OF CODE CONTEXT & STRUCTURE

An integrated detection system that reads code structure and context at the same time.

01 AI for code analysis

GraphCodeBERT
- Reads code context & data flow; identifies and classifies malicious behaviour.

sLLM
- Analyses code behaviour & logic, then extracts the risk.

RAG
- Vector-DB search; compares against known attack patterns.

02 AI analysis

Phishing detection

Malware detection engine
- Code-based malicious-behaviour detection.

Phishing detection engine
- Image / text / brand -based detection.

Multidimensional engine
- Combines code, image & infra reputation plus external signals into one verdict.

03 Response

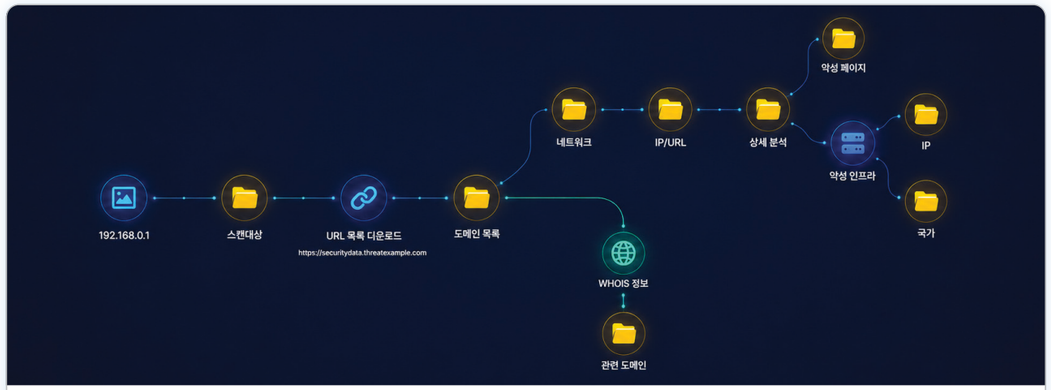
Analysis Results

- Evidence of intent
- AI risk level
- Reputation risk
- Report

03 ATTACKER PROFILING

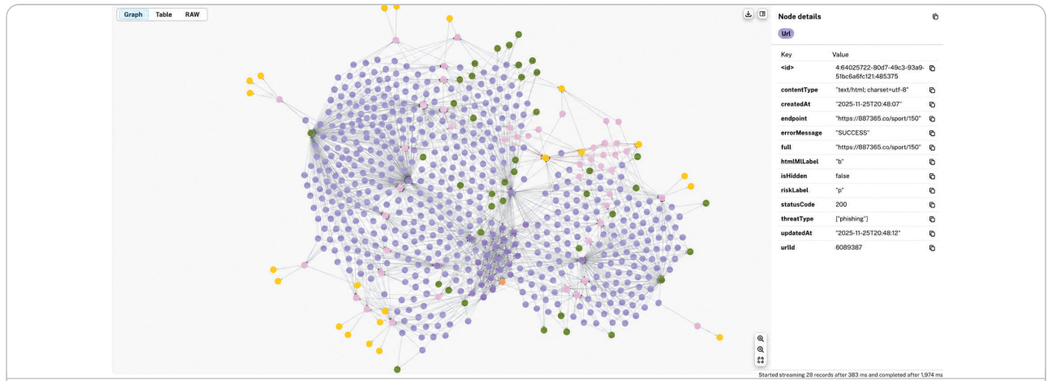
Multidimensional analysis of code, images and infrastructure to map who is behind an attack.

Analysis of high-risk IPs & domains



Multidimensional Analysis Using Code, Images, IP, Domain, and ASN Data

Malware graph-DB correlation analysis



Identifying malware relationships and classifying attack campaigns using contextual and structural information from code blocks.

“We analyse attackers’ tactics and strategies, and uncover the connections between malicious websites.”

04 PHISHING DETECTION

Multimodal phishing detection

AI reads a site’s images and text together to detect phishing in real time.

Screenshot analysis	Brand & image match	Multimodal AI	Brand database
Group identical campaigns by screenshot hash.	Compare a page against the genuine brand site.	Classify with image + text models together.	Live registry of brand domains abused in phishing.

05 HOW TO USE OLPEMI THREAT INTELLIGENCE

Validate suspicious URLs collected from your network, email and security devices.

01 Network equipment
Network Equipment (NDR / Visibility / DPU) → Extraction of URLs → OLPEMI TI → Automated TI Validation & Analysis

02 Email server
Email Server (SMTP) → URL Extraction from Emails → OLPEMI TI → Automated TI Validation & Analysis

03 Security devices
Security Appliances (IPS, UTM, TMS, NGFW, EDR, XDR) → Suspicious URL Collection → OLPEMI TI → Automated TI Validation & Analysis

Network Equipment · Email Server · Security Appliances · OLPEMI TI(API) · Automated TI Validation & Analysis

CORE SERVICES OLPEMI LINE UP

OLPEMI CORE MENU LINE UP

Dashboard

- Weekly Top-5 web screenshots
- Deep / malicious / suspicious URL pie-graph
- Status-code statistics
- Geographic detection map
- Malicious / suspicious status
- Deep-web URL status
- Web risk status
- JS risk status
- Malware web status
- Malicious domain status
- Malicious IP / hosting status
- URL inspection status

Platform management

- URL request (web & files)
- Web management
- Web-screenshot management
- Download-file management
- Deep-web management
- Phishing management
- Bookmark management

Detection engine

- Cross-Engine Analysis
- False Positive Management
- Report Management
- Web Risk Model
- JavaScript Risk Model
- Multi-Classification Model

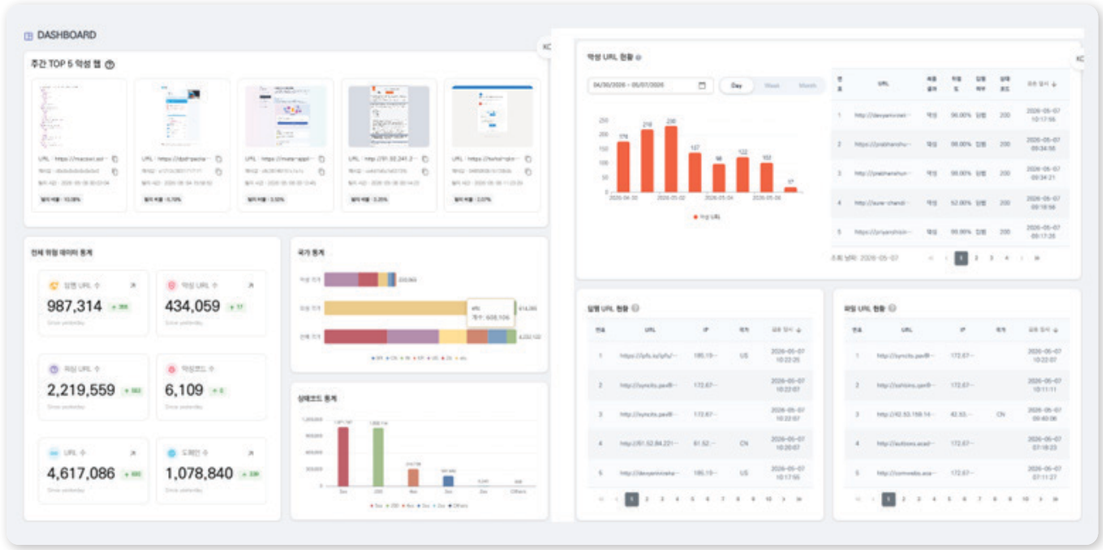
Data management

- Whitelist
- Blacklist
- Hosting / cloud
- Brand database

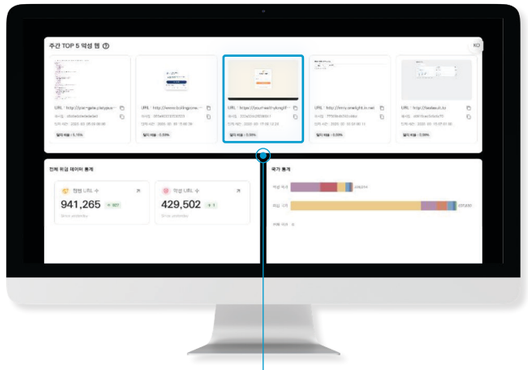
CORE SERVICES OLPEMI LINE UP

The Olpemi dashboard

Malicious-URL, deep-web and file-URL detection status — in one view.



Geographic detection & Top-5 attack screenshots



Main menu

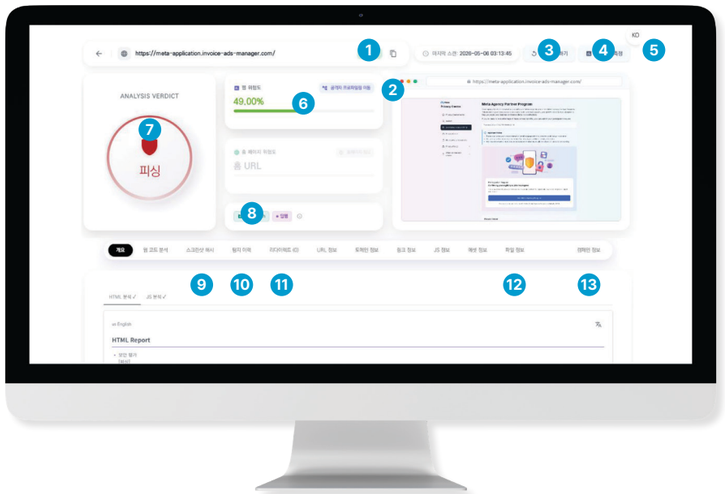
Platform Management	Analysis of Web, File, and Screenshot Detection Results
Detection Engine	Cross-Engine Result Analysis
Data Management	Black/Whitelist URLs, Brand DB, Domain/IP DB

URL, Hash, Detection Time, Detection Rate

CORE SERVICES OLPEMI LINE UP

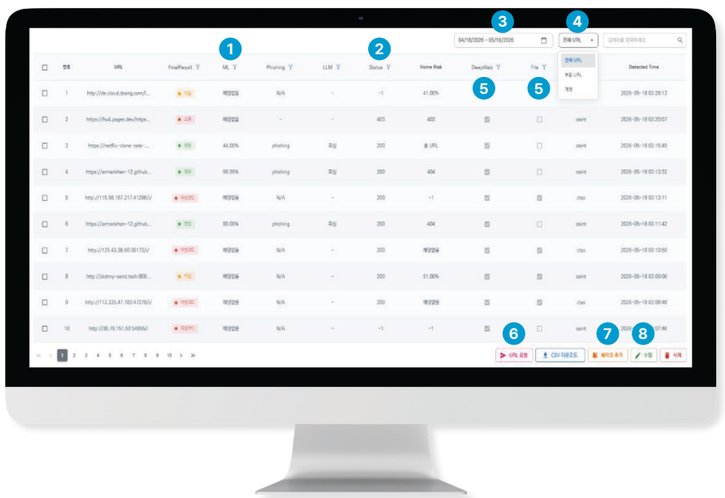
Detailed URL analysis

Attack-similarity analysis through static & dynamic crawling and multidimensional comparison.



1. Connection status codes
2. Copy URL
3. Re-crawl (Data collection)
4. AI risk re-assessment
5. Multilingual support
6. Attacker profiling
7. Final determination
8. Source of collection
9. Visual proof of same attack
10. Similar IP / domain history
11. Transit & distribution moves
12. File malware & hash check
13. JS / screenshot / infra match

URL monitoring list

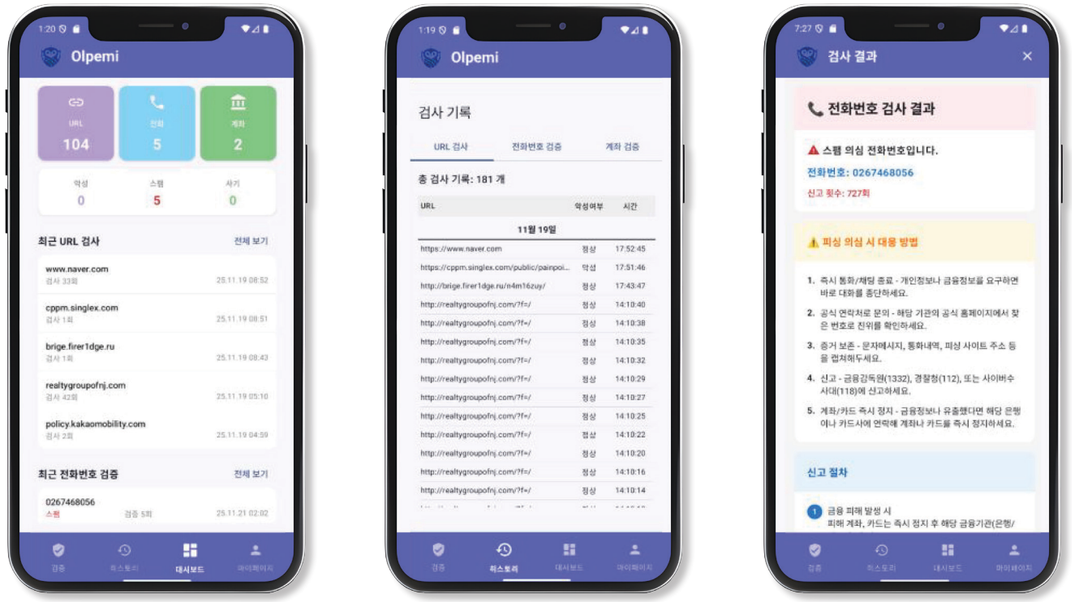


1. Final-result risk filter
2. Status-code filter
3. Date-range search
4. URL & account search
5. Deep-web / file-presence filter
6. URL check
7. Bookmark for further review
8. Risk-level adjustment

OLPEMI MOBILE

SMARTPHONE PROTECTION FOR EVERYONE

Mobile Application for Malicious Web Blocking and Smishing Detection



KEY FEATURES & BENEFITS

Real-time URL checking

Analyses links the moment they're opened and blocks access to malicious sites.

Smart threat analysis

Extends checks to risky URLs related to the one being verified, for higher accuracy.

Smishing defence

Pre-empts fraud by verifying phone numbers and bank-account details.

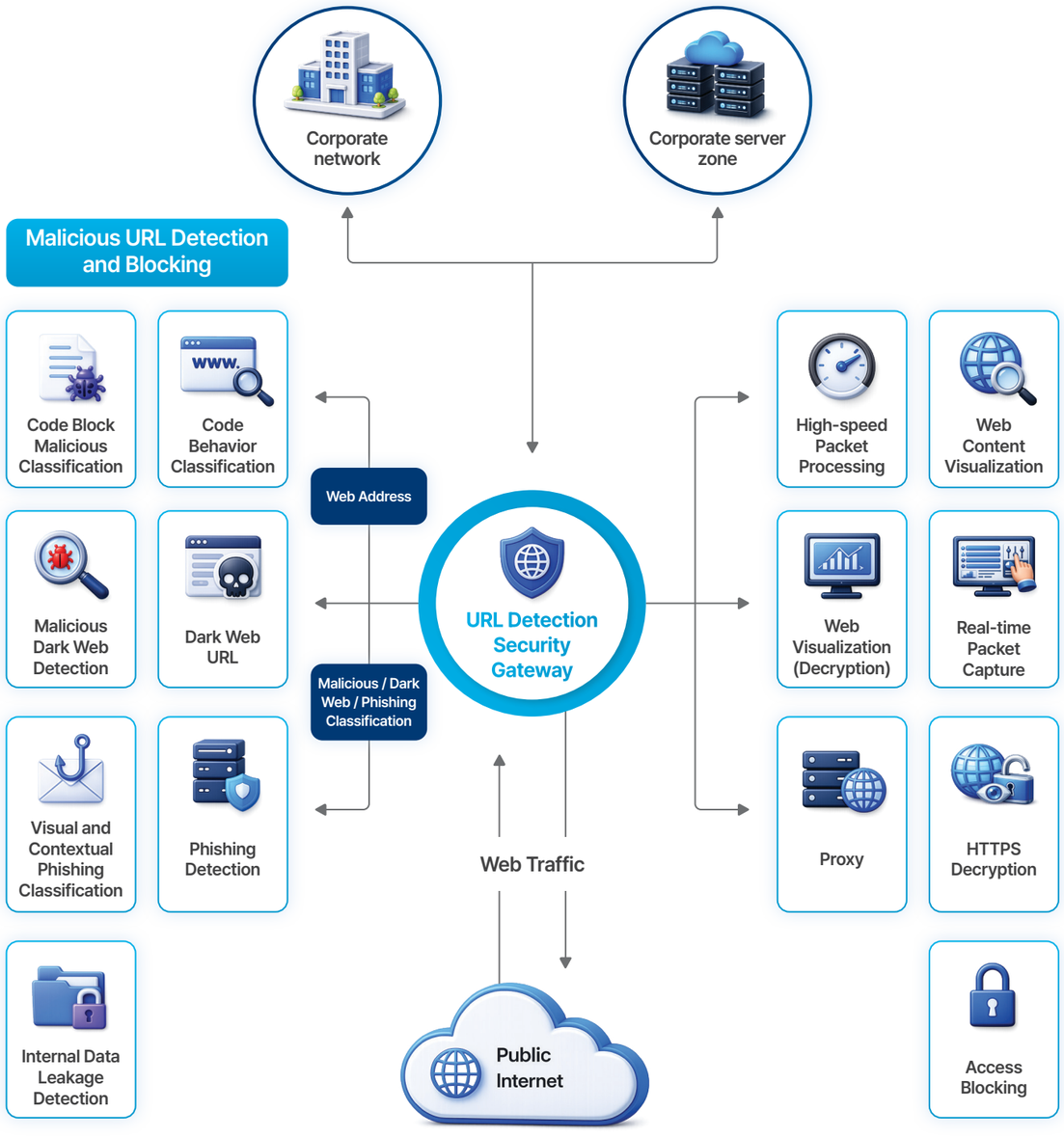
Simple by design

An intuitive, app-based service anyone can use — no expertise required.

OLPEMI SECURITY GATEWAY

DEEP-WEB URL DETECTION AT THE GATEWAY

Inspects web traffic at the point of internet connection to proactively prevent malware infection.



A security solution that precisely analyzes inbound and outbound web traffic within the network to identify and block malicious URLs.

This enables a unified response to security threats, addressing not only external inbound threats but also attempts to exfiltrate internal assets.

OLPEMI SECURITY GATEWAY

WHAT THE GATEWAY DOES

KEY FEATURES

Proactive blocking

Pre-empts threats at the gateway, before they reach users.

Multi-analysis detection

Precise detection by code, context and timing.

Integrated response

Blocks attacks and prevents data leaks at once.

High-speed processing

DPI-based analysis with immediate response.

Reputation lists

Reputation-based whitelisting and blacklisting.

Live monitoring

Real-time view of URL requests and responses.

DIFFERENTIATORS

Behavior-based detection technology

Multidimensional analysis applied

SWG
Olpemi Security Gateway

Covers internal data leaks

Gateway-centric efficient operation

DEEP WEB DETECTION FIREWALL

DEEP-WEB DETECTION FIREWALL

OLPEMI WALL · DEEP-WEB DETECTION FIREWALL

BLOCKING · DEFENSE

Proactive threat prevention

Web-server access control and deep-web webshell detection block malicious attacks and code execution.

01

PROTECTION · INTERNAL

Preventing internal leaks

Blocking unauthorized deep-web access prevents the leakage of internal information.

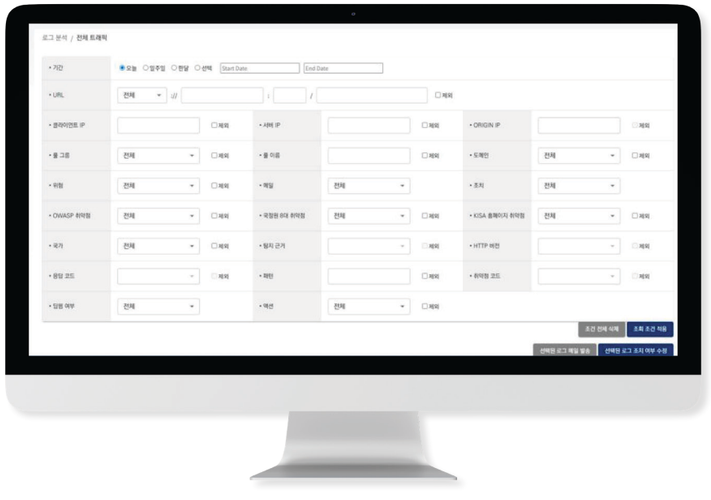
02

ANALYSIS · OPERATIONS

Real-time integrated response

Detects and responds in real time via traffic, URL, IP and behaviour analysis.

03



Block at the source. By stopping the deep web at the web-server level, WALL prevents web-shell and malware execution and blocks internal information leakage.

DEEP WEB DETECTION FIREWALL

THE CASE FOR ATTACK-ORIENTED SECURITY

WHY IT'S NEEDED

01

Respond to phased attacks

Intrusion → internal privilege → exfiltration.
Perimeter blocking alone can't counter the later stages.

02

See stealthy threats

Webshells and deep-web attacks slip past signature tools — hidden paths need deep analysis.

03

Catch traffic in disguise

As attacks mimic normal traffic, defence must shift to behaviour and anomaly detection.

04

Prevent, don't react

Move from reactive cleanup to blocking attacks before they execute.

DIFFERENTIATORS

Beyond simple pattern-based detection

Webshell-detection-centric architecture

WALL
Deep-Web Firewall

Zero-trust security framework

Internal & external integrated response