KYGnus

SICHER, EFFIZIENT, NACHHALTIG

Product Catalog 2025

KYGnus Security Catalog

Protecting Infrastructure with Transparency and Power

KYGnus – Inspired by the resilience of the Gnu. Cooperative protection. Open Source strength.

About KYGnus

- KYGnus develops enterprise-grade, open-source security solutions designed to protect infrastructure, networks, and endpoints with transparency and efficiency. Our tools are built for organizations that value both strong defense and the freedom to audit, adapt, and extend their security systems.
- We specialize in creating modular security platforms ranging from malware detection to intrusion prevention and centralized server management. All KYGnus products are designed to be scalable, reliable, and easy to integrate into existing IT environments.

Why Open Source?

- Transparency: Source code can be audited.
- Security: No hidden backdoors.
- Flexibility: Customizable for enterprise needs.
- Cost-efficiency: No vendor lock-in, long-term sustainability.

Our mission is to deliver powerful, open-source security solutions that organizations can trust, audit, and adapt to their needs.

KYGnus Security Solutions
Product Portfolio

Our open-source security tools are designed for enterprises, research institutions, and professionals who value transparency and robust protection.

Loa-AMD

Android Malware Detection Tool

A Linux-powered malware detection engine for Android devices, developed under the LoA Project to provide deep, transparent protection against mobile threats.

ClamAV

Open Source Antivirus Engine

A web-based frontend for ClamAV enabling local and remote malware scanning with a simple UI.

Honeypots

Controlled decoy environments that attract and monitor attackers to study their methods and provide early threat detection for enterprise networks.

Hermes Security Manager

A web-based platform for Linux server security, combining monitoring, malware detection, and IDS/IPS in one interface.

Guardix IDS/IPS Server

A high-performance, pre-configured IDS/IPS solution built on enterprise hardware with Suricata and Zeek for advanced network intrusion detection and prevention.

Loa-AMD – Advanced Android Malware Detection

Loa-AMD is a next-generation malware detection tool for Android devices. Built as part of the LoA Project (Linux on Android), it integrates the stability and transparency of Linux security modules to provide deep and reliable malware protection.

The LoA Project aims to close critical gaps in Android security by introducing a secure Linux layer to the Android OS. This integration allows for low-level scanning, advanced detection techniques, and protection against sophisticated mobile threats

Loa-AMD – Advanced Android Malware Detection

Key Features:

- Multi-engine malware scanning
- Deep system analysis using Linux security modules
- Real-time detection and alerts
- Lightweight, optimized for mobile devices
- 100% open source for auditability and trust

Why Loa-AMD is Different:

Traditional antivirus apps operate at the user level of Android, leaving deeper layers unchecked. Loa-AMD leverages Linux-level access to analyze files, detect hidden malware, and block privilege escalation attempts more effectively.

Use Cases:

- Securing enterprise Android devices
- Research labs analyzing mobile malware
- Individual users seeking transparent, open-source protection

Hermes Security Manager – Centralized Linux Server Protection

All-in-one security dashboard for administrators and cybersecurity teams.

Hermes Security Manager is a web-based platform designed to remotely monitor, manage, and secure Linux servers over SSH. It combines real-time monitoring, malware detection, firewall management, and IDS/IPS integration into a single interface for complete server protection.

Key Features:

- Dashboard: Unified view of security status and server health
- Antivirus Scanning: Integrated ClamAV, RKHunter, chkrootkit, YARA
- Process Monitoring: Detect and manage suspicious activity
- Network Monitoring: Identify malicious IPs and ports in real time
- File Integrity Monitoring: Track and quarantine altered files
- Log Management: Centralized access to security logs
- Firewall Management: Configure rules and integrate Fail2Ban
- Kernel Module Analysis: Detect vulnerable or malicious modules
- IDS/IPS: Built-in Suricata integration

Hermes Security Manager – Centralized Linux Server Protection

Why Hermes is Unique:

- Combines multiple security layers in one open-source platform.
- Enables remote, centralized management via secure SSH connections.
- Designed for enterprise scalability and transparency.

Use Cases:

- Enterprise Linux server security
- Research networks requiring centralized monitoring
- System administrators managing multiple servers

Honeypots – Proactive Cyber Defense

KYGnus Honeypots are controlled, isolated systems designed to attract cyber attackers and collect valuable information about their techniques. By mimicking real assets, they provide early warning signals and critical insights into emerging threats.

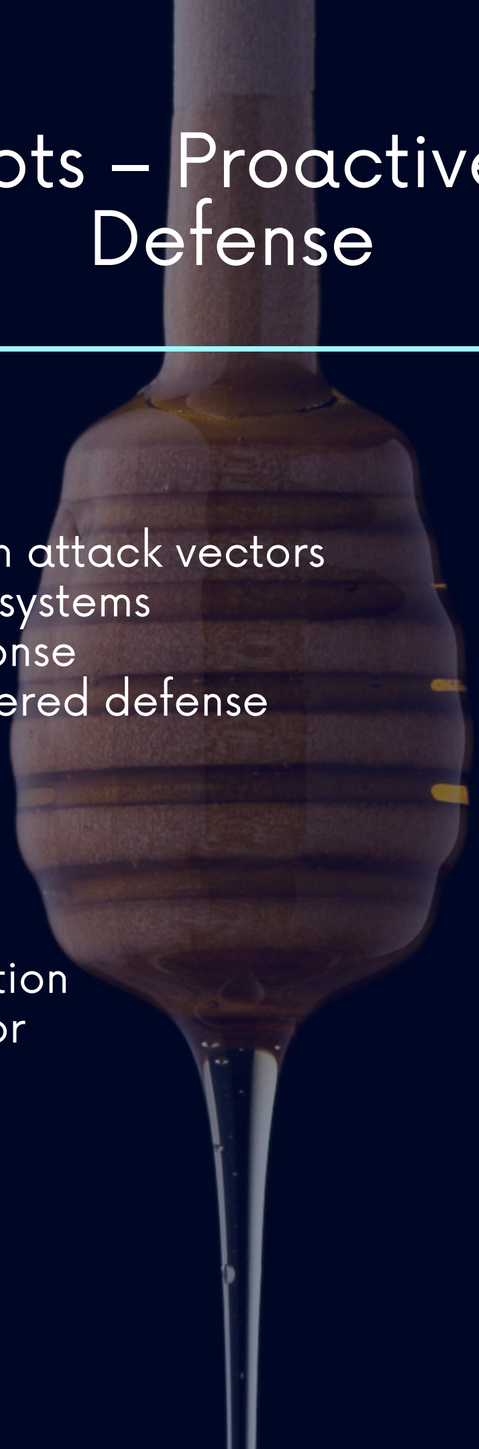
What is a Honeypot? (short explanation):

- Decoy System: A fake but realistic target that attracts attackers.
- Monitored Environment: Every interaction is logged and analyzed.
- Data Collection: Provides intelligence on attack patterns and tools.
- Early Warning: Alerts the security team to intrusions before real systems are compromised.

Why KYGnus Honeypots are Unique:

- Designed for seamless integration with KYGnus' other security tools (Hermes, Guardix).
- Open source for full auditability and customization.

Honeypots – Proactive Cyber Defense



Key Benefits:

- Identifies zero-day exploits and unknown attack vectors
- Diverts attackers away from production systems
- Provides forensic data for incident response
- Integrates with SIEM and IDS/IPS for layered defense

Use Cases:

- Enterprise networks seeking early detection
- Research labs studying attacker behavior
- Critical infrastructure defense

Guardix IDS/IPS Server – Enterprise Network Defense

Real-time intrusion detection and prevention for high-performance networks

Guardix is a pre-configured, high-performance Intrusion Detection and Prevention System (IDS/IPS) built on enterprise-grade hardware. Combining Suricata, Zeek, and advanced monitoring tools, Guardix provides comprehensive network protection against sophisticated threats.

Key Features:

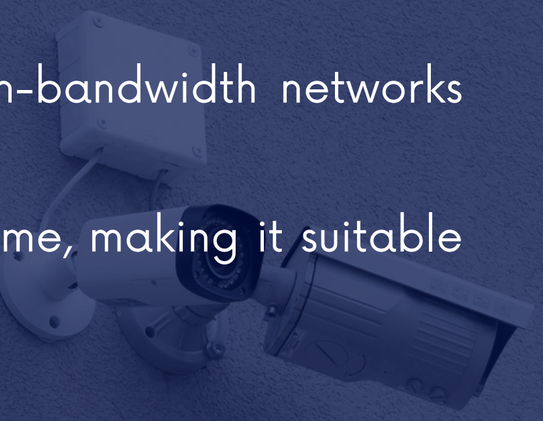
- Real-time threat detection & prevention
- Behavioral network analysis
- Pre-configured and ready to deploy
- Scalable for large enterprise environments
- Open-source core for auditability and customization

Guardix IDS/IPS Server – Enterprise Network Defense

Hardware – Built for Enterprise Performance
Guardix runs on HP ProLiant DL360 G8 4LFF enterprise hardware, chosen for reliability and scalability in demanding environments:

- CPU: 2× Intel Xeon E5-2697 v2 processors (24 cores / 48 threads) for parallel traffic analysis.
- Memory: 128 GB DDR3 RAM to handle large rule sets and high-throughput network traffic without bottlenecks.
- Storage: 2 TB SSD for fast log storage and system responsiveness.
- Networking: 10 Gb Ethernet support ensures Guardix can operate in modern high-bandwidth networks without packet loss.

This configuration allows the system to monitor and filter gigabit-level traffic in real time, making it suitable for both enterprise and data center environments.



Guardix IDS/IPS Server – Enterprise Network Defense

Software Stack – Proven Open Source

Guardix is powered by Debian Linux with integrated enterprise security tools:

- Suricata for intrusion detection & prevention.
- Zeek for deep network analysis and logging.
- Maltrail for detecting malicious traffic.
- CSF Firewall & Fail2Ban for layered defense.

Using open-source components makes Guardix auditable, secure, and customizable for different environments.

Use Cases – Where Guardix Fits Best

- Enterprise networks needing proactive intrusion prevention.
- Data centers managing high-volume traffic.
- Healthcare or research facilities protecting sensitive data.
- Organizations looking for a ready-to-deploy IDS/IPS solution with minimal setup.

ClamNET – Web-Based Malware Scanning

Cross-platform ClamAV management for local and remote systems.

ClamNET is a web-based frontend for ClamAV that allows IT administrators to scan files and directories on both local and remote systems via SSH. Designed for simplicity and speed, it supports Windows and Linux environments with real-time scan results.

Key Features:

- Web interface – no need for CLI commands
- Supports both local and SSH remote scans
- Real-time streaming results in the browser
- Auto-detects OS and adapts settings
- Clean, log-style output for easy review

ClamNET – Web-Based Malware Scanning

Use Cases:

- Enterprise environments with mixed OS infrastructure
- Research labs and servers needing quick integrity checks
- System administrators requiring a simple web-based scanning too

Why clamNET Stands Out:

- Brings ClamAV to a user-friendly web interface while maintaining full power and flexibility.
- Completely open source for audit and customization.

How It Works:

- Local Scan: Enter a file or directory path and scan instantly using ClamAV.
- Remote Scan (SSH): Connect to remote Linux or Windows systems to scan files securely over SSH.

Why KYGnus Security Solutions?

🔓 Open Source:

- Every product is transparent and auditable. Clients can verify the code themselves, ensuring full trust and compliance with strict security regulations.

🛡️ Safe & Privacy-Focused:

- All tools are designed to prevent data leaks and prioritize local processing. Sensitive information never leaves the client's environment.
- ⚙️ Extendable & Modular:
- We build security platforms that can adapt. Whether you need custom integrations or new features, KYGnus products are designed to grow with your needs.

💻 Easy to Use:

- Despite the powerful features, all tools have intuitive interfaces. From web-based dashboards to plug-and-play appliances, deployment is quick and efficient.

🌍 Cross-Platform:

- Many solutions work on Windows, Linux, macOS, and integrate into mixed infrastructures without reconfiguration.

With KYGnus, you don't just get individual tools—you get a comprehensive, transparent, and adaptable security ecosystem designed for modern enterprises.

KYGnus

SICHER, EFFIZIENT, NACHHALTIG

Get in Touch with KYGnus

IRequest a demo today and see how our open-source, enterprise-grade tools can enhance your security infrastructure.

Contact Information:

📧 Email: kygnus.innovation@gmail.com

🌐 Website: www.kygnus.github.io

📞 Phone: +49 (0) 1768208646