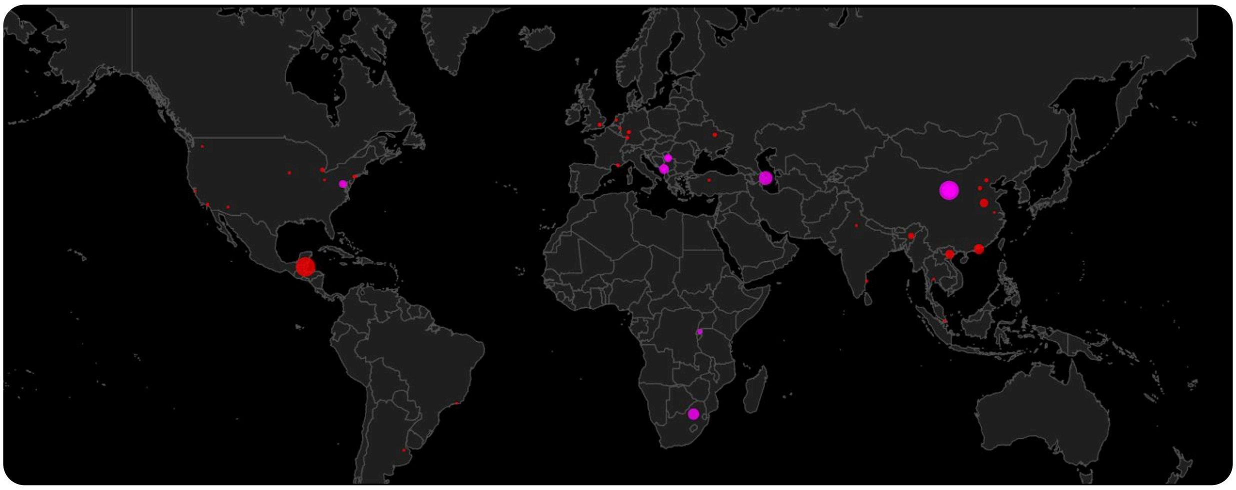
GUIDE

Understanding Shield Matrix

GFI Software™

Introduction

Shield Matrix is a cutting-edge security feature designed to protect networks from emerging threats by automatically identifying and blocking malicious IP addresses. Shield Matrix works with the Intrusion Prevention System (IPS) and antivirus components to deliver comprehensive, multi-layered security.



live map of sources (IPs) of attackers targeting one or more honeypots scattered across the globe.

The Evolving Threat Landscape: *Why Traditional Methods Fall Short*

Traditional security measures, using periodic updates and signature-based detection, are no longer sufficient to protect against the rapidly evolving threat landscape. Zero-day attacks, which exploit previously unknown vulnerabilities, can spread quickly and cause significant damage before traditional security measures can respond. Shield Matrix addresses this gap by providing real-time, zero-day threat protection.

How Shield Matrix Works

Shield Matrix employs a sophisticated, multi-stage process to identify and neutralize threats efficiently, without impacting your GFI KerioControl appliance's performance.

A Threat Intelligence Engine: Global Data Collection and Continuous Analysis

Shield Matrix leverages a vast, global network of honeypots and traps. These systems are designed to attract and identify malicious activities and IP addresses involved in attack attempts worldwide.

- **Data Collection:** IP addresses exhibiting suspicious or hostile behavior are continuously gathered from this distributed sensor network.
- **Dynamic Database:** This intelligence feeds into a constantly updated global threat database, forming the backbone of Shield Matrix's protective capabilities.

B AI-Powered Threat Assessment: *Offloaded Processing and Confidence Scoring*

Once potential threat data is collected, it undergoes rigorous analysis:

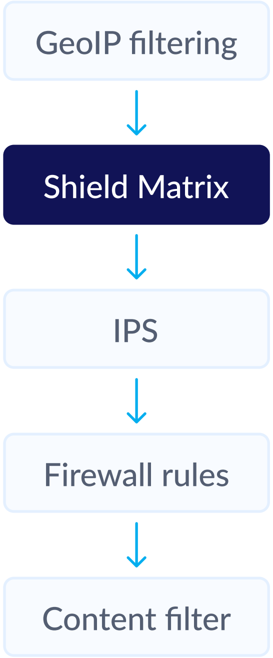
1. **Artificial Intelligence (AI) Analysis:** Every attack attempt and associated IP address is analyzed by sophisticated AI algorithms. This AI evaluates various factors to determine the likelihood and severity of the threat.

2. **Confidence Levels:** Based on this analysis, each potential threat is assigned a confidence level: Low, Medium, or High. Factors influencing this score include:

   - Attacker IP unknown to integrated third-party threat intelligence.
   - Aggressive attack patterns detected against a trap.
   - Continuous attacks originating from the same C-segment IP range.
   - Detection of activity likely indicating a human attacker (as opposed to automated bots).
   - Fuzzing attacks or country-specific targeted attacks.

3. **Resource Efficiency:** All this intensive analysis is performed on update servers, **not** on your local GFI KerioControl appliance; your machine gets only relevant or processed data.

C Real-Time Protection for Your Network: *Updates, Traffic Processing, and Action*



- **Database Updates:** The list of malicious IP addresses is pushed to your GFI KerioControl appliance through updates. These updates occur every 15 minutes.

- **Traffic Processing Order:** Shield Matrix operates early in the traffic inspection pipeline. It processes incoming network traffic immediately after GeoIP filtering checks, making it the second engine to analyze connections.

- **Action Taken:** When an incoming connection originates from an IP address flagged by Shield Matrix, GFI KerioControl can instantly drop the connection based on your configured policy, effectively neutralizing the threat before it can interact with your network.

Key Features and In-Depth Benefits

Shield Matrix offers a compelling suite of features and benefits designed for modern network security:

Proactive Zero-Day Defense:

- **Rapid Threat Response:** By updating its threat database every 15 minutes, Shield Matrix significantly reduces the exposure window to newly identified threats.
- **Blocks Emerging Threats:** Defends against threats that haven't yet been classified by traditional IPS signatures.

Intelligent Threat Prioritization & Customizable Responses:

- **Confidence-Based Actions:** Administrators can configure distinct actions based on the AI-assessed confidence level of a threat (High, Medium, Low). Options include:
    - **Log and Drop:** Blocks the connection and records the event.
    - **Log Only:** Records the event but allows the connection.
    - **No Action:** Ignores the threat.
- **Granular Control:** This flexibility allows businesses to tailor the aggressiveness of Shield Matrix to their specific risk tolerance and operational requirements.

Resource Efficient & Seamless Integration:

- **No Performance Impact:** As all heavy AI analysis is offloaded to GFI's cloud infrastructure, your GFI KerioControl appliance's performance remains unaffected.
- **True Integration:** Shield Matrix is built directly into GFI KerioControl. There's no extra hardware to deploy, no complex configuration, and no separate management interface to learn.

Complementary and Enhanced Security:

- **Multi-Layered Approach:** Strengthens GFI KerioControl's existing IPS and antivirus capabilities, creating a more resilient defense-in-depth strategy.

Enterprise-Grade Security with SMB Simplicity:

- **Advanced Protection:** Provides access to sophisticated threat intelligence and AI-driven analysis previously found only in enterprise-level solutions.
- **Ease of Use:** Managed through GFI KerioControl's intuitive interface, renowned for its ease of use (rated 4.9/5 stars), making advanced security accessible without requiring specialized security personnel.

Ideal Use Cases & Beneficiaries

Shield Matrix delivers significant value to a wide range of organizations:

1. **Regulated Industries and Compliance-Focused Organizations:** Helps meet security compliance and regulations such as NIS-2, HIPAA, PCI DSS, and GDPR.
2. **Managed Service Providers (MSPs):** Enables MSPs to differentiate their security offerings, provide superior protection to clients, and reduce incident response overhead. Centralized management can be achieved via GFI AppManager.
3. **Organizations with Remote Workforces:** Robust protection for all users, including those connecting remotely via VPN, by securing the network perimeter against real-time threats.
4. **Small to Medium-Sized Businesses (SMBs):** Offers enterprise-grade protection without the associated complexity or high cost.

Shield Matrix empowers organizations to:

- **Minimize Exposure:** Drastically reduce the window of vulnerability to new and emerging threats.
- **Prevent Breaches:** Proactively block malicious IPs, measurably reducing the risk of costly security incidents.
- **Reduce Management Overhead:** Automate threat response, potentially reducing security management time by 30-40%.
- **Achieve Compliance:** Meet and exceed regulatory requirements with advanced, demonstrable security measures.

Shield Matrix is more than just a feature; it's a strategic enhancement that closes the critical gap left by traditional security update cycles, offering peace of mind and robust protection in an increasingly hostile digital world.

Strengthen your network security today. Contact your GFI reseller to activate Shield Matrix and experience real-time threat protection for your GFI KerioControl system.

GFI Software™