Rethinking Cyber Security: Stopping SSH Botnets While Saving CPU and Energy

Green Active Defence stops automated SSH botnets at the kernel layer, reclaiming server CPU and cutting carbon emissions from home VPSs to global data centres.



Green Active Defence by OrionEye v4.0: Conceptual representation of kernel-level SSH botnet blocking, CPU optimization, and carbon reduction across global server infrastructure.

HATTENHOFEN, BAVARIA, GERMANY, October 15, 2026 /EINPresswire.com/ -- Hattenhofen, Germany – Cybersecurity is no longer just a technical or defensive challenge; it is fast becoming a critical cost factor and a pressing environmental issue. Every single day, millions of automated botnets execute relentless SSH brute-force attacks against servers worldwide. While IT teams focus primarily on data breach risks, a massive hidden cost goes largely unnoticed: the enormous waste of server CPU capacity, escalating cloud hosting fees, and avoidable carbon emissions.

> Rethinking cyber security means stopping attacks at the kernel level before they waste CPU capacity, server energy, and carbon emissions."
>
> *Samuel La Manna, Lead Architect at Lowegate Studio*

The Real Cost of Cyber Attacks: From Home VPS to Enterprise Data Centres

When a server processes thousands of malicious login attempts, its CPU operates under continuous strain. This parasite workload directly impacts operating budgets across all tiers of digital infrastructure:

• Individual Developers & Home VPS Users: Malicious traffic consumes compute cycles that could be used for actual application workloads, forcing users to upgrade to higher, more expensive server tiers simply to maintain performance.

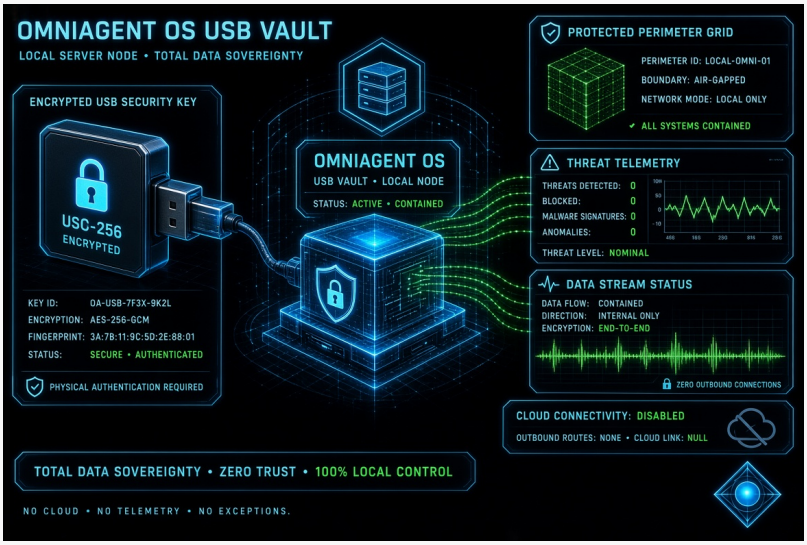
• Small & Medium Enterprises (SMEs): Infrastructure costs compound rapidly when multiple server nodes are continuously handling botnet chatter, increasing monthly cloud hosting bills and system latency.

• Enterprise Data Centres: High CPU utilization demands greater electrical power and forces cooling systems to work harder, driving up Power Usage Effectiveness (PUE) metrics and operational expenditure.

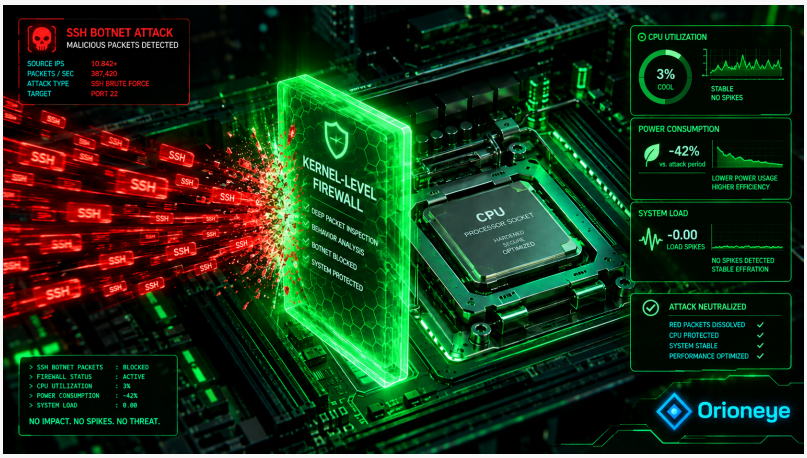
Rethinking Defence: Green Active Defence

Traditional security mechanisms often handle attack traffic late at the application layer, allowing malicious connections to consume significant system resources before being blocked. OrionEye introduces the concept of Green Active Defence to change this paradigm. By analyzing threat telemetry and using AI model correlation, repeated attack attempts are identified as coordinated campaigns and blocked directly at the kernel layer, before they can strain system processes.

By stopping attack traffic at the lowest possible layer, server CPU usage drops instantly. This simple architectural shift restores processing capacity for legitimate workloads while noticeably reducing power consumption, cooling demand, and hosting overhead across connected nodes.



OmniAgent OS USB Vault integration by OrionEye: On-premises threat telemetry and encrypted security records with 100% local data sovereignty and zero cloud dependency.



Green Active Defence in action: Automated SSH botnet attacks are intercepted directly at the kernel layer, preventing CPU load spikes and reducing server power consumption.

Quantifying the Impact: Recovering Wasted CPU and Cutting CO2

To put this in perspective, real-world telemetry measured on live infrastructure shows that relentless SSH brute-force attempts consume roughly 540 seconds of continuous 100% CPU time every single day per server. Multiply this across a deployment of 10,000 servers over a single year, and the energy wasted processing hostile traffic translates into tons of unnecessary carbon emissions and tens of thousands of Euros in wasted hardware allocation.

By eliminating this parasite workload at the kernel level, widespread adoption of Green Active Defence enables organizations to optimize their current hardware investment—saving energy equivalent to driving tens of thousands of kilometres in a standard passenger vehicle—without

needing to purchase expensive proprietary security hardware.

Data Sovereignty and AI Orchestration
Unlike traditional enterprise security solutions that force clients to stream sensitive server telemetry to external cloud vendors, OrionEye, paired with OmniAgent OS, prioritizes local data sovereignty. Telemetry and security records remain on-premises or secured inside an encrypted local vault. Furthermore, the platform integrates multi-engine OSINT aggregation and multi-LLM orchestration, allowing operators to run threat investigations in natural language while maintaining total control over their data perimeter.

By aligning cyber security with financial cost-efficiency and energy sustainability, Green Active Defence proves that protecting digital infrastructure and reducing operational overhead can go hand in hand.

For further information, technical documentation, and interactive live demonstrations, please visit: https://orioneye.io

Company Contact / Press Contact:
Lowegate Studio
Contact Person: Samuel La Manna
E-Mail: contact-orioneye@lowegatestudio.de
Website: https://orioneye.io

Samuel La Manna
Lowegate Studio
contact-orioneye@lowegatestudio.de
Visit us on social media:
LinkedIn
YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/949765798

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.