Upgrade your Open Source Firewall to a Next Generation Firewall in seconds!

Next Generation Firewall,
Manageable from the Cloud

zenarmor

THOMAS KRENN®

Zenarmor 19925 Stevens Creek Blvd. Suite 100, Cupertino CA 95014, USA www.zenarmor.com

Zenarmor® NGFW Plug-in

Software extension providing next-generation firewall (NGFW) functionality to your open-source OS.

Zenarmor is appliance free and includes Zenconsole, SVN's cloud based solution for managing all your Zenarmor NGFW instances

Supported Platforms

OPNsense	Ubuntu
Centos	Debian
FreeBSD	PFsense

Red Hat
Certified Technology
Red Hat®

Why Open Source Firewalls?

Area	Benefit
For L2-L4, more powerful than commercial competitors	**Compared to commercial legacy firewall, and is Free!**
Same core OS used in the Commercial competitors	**Confidence in OS firewall as also being ready for enterprise use.**
Unprecedented level of extendability via Plug ins & packages	**Flexibility to add your preferred related extensions when and if needed. (Snort, Suricata, etc.)**
Frequent scrutinized code base	**Better Security**
Frequent software updates	**Typically 2 major and 8-10 minor update per year keeps the functionality at the leading edge**
Bug fixes	**Shipped fast**
User interface	**Easy to use - Intuitive**
No Hardware lock-in	**Use what's available and/or Migrate to the latest H/W on your schedule**

Legacy Firewall vs. NGFW

Area	Legacy	NGFW
Traffic Filtering (Port, IP, Protocol)	Supported	Supported
Intrusion Prevention System (IPS)	Not Supported	Supported
Network Address Translation (NAT)	Supported	Supported
Virtual Private Networking (VPN)	Supported	Supported
Application Level awareness and control	Not Supported	Supported
Network Layers	L2- L4	L2- L4
Reporting	Standard Reports	Highly Customized Reporting
Threat Intelligence	Not Supported	AI Based
Deep Packet Inspection	Not Supported	Including TLS

Legacy firewalls are unable to protect the enterprise from modern threats

Why Open Source Firewalls?

Area	Benefit
Performance	A ~$300 x86 64 bit bare metal server can easily support 1Gbps
Reliability	with 10's of thousands of devices deployed worldwide the open source software is broadly used for everything from home users to government agencies
Support	Provided by the community or by companies supporting the stack
Documentation	High maintained and Freely available to everyone on the web

Open source Firewalls are also Free!

Which Open Source Firewall?

The Rising Star

OPNsense®

The Famous

pfsense®

Open source Firewalls are already protecting over 1M networks worldwide

Why Zenarmor® ?

The best way to prevent modern day cyber attacks using an open source firewall

- The only NGFW that offers the best of the two worlds (Open source + Commercial)
- Industry's best Network Analytics and Reporting
- AI-powered cloud based threat intelligence providing protection against zero-day malware
- Powerful Application Controls
- Enterprise-grade web securi+ ty & filtering covering over 300 M active sites as well as 200 M passive domains

OS Firewalls + Zenarmor

OPN/pfSense	Zenarmor	Both	Feature
✓			Packet Filtering: Access control lists (ACLs) that filter based on TCP/IP connections.
✓			Network access control (NAT): IP address translation service for one-to-one or one-to-many translations.
✓			Stateful Packet Inspection: Access control policy logic that tracks TCP/IP state such as three-way handshake and other TCP/IP flags, which are used to defeat various packet crafting and replay attacks.
✓			Virtual Private Network (VPN): LAN-to-LAN and remote access VPN (IPsec or TLS-based).
	✓		Application Layer Gateway Service: The ability to inspect parent protocol sessions and dynamically open secure pin holes for secondary child connections (for example, inspecting a Session Initiation Protocol [SIP] control channel so that Real-Time Transport Protocol [RTP] channels for voice traffic can be opened and closed dynamically).
✓			Basic Routing and Switching Support: Firewalls need to be able to route packets and participate in routing protocol domains (OSPF, BGP, etc.), and they need to be able to understand common Layer 2 techniques (VLAN and EtherChannel).
✓			Advanced Networking Support: Integrations with WAN acceleration, SD-WAN interoperability (API level), IPv6 features, app-based quality of service (QoS) and app-based performance routing.
	✓		Real-Time TLS Decryption: The firewall platform must have the capability to decrypt and encrypt TLS traffic at line rate so that encrypted threats can be inspected, identified and blockedDeep Packet Inspection

OS Firewalls + Zenarmor

OPN/pfSense	Zenarmor	Both	Feature
		✓	Integrated IDPS: Intrusion detection and prevention systems (IDPSs) detect threats based on network traffic analysis; this feature should be integrated with the rule base such that alerts are correlated with individual rules, and recommendations for remediation should be provided automatically without the need for manual log analysis
	✓		Virtualization/Public Cloud Support: Enterprise firewall platforms must support network function virtualization (NFV) with full feature and management parity between virtual and appliance versions. Amazon Web Services (AWS), Microsoft Azure and Google Cloud must be explicitly supported at the IaaS level and should have support for PaaS on their roadmaps.
	✓		Application Awareness/Control: The firewall needs to be able to inspect and block individual application subcomponents/services. For example, the firewall should be able to filter Facebook Messenger while still allowing users to browse general Facebook pages.
	✓		Integration With External Identity Store: Identity (user or workload)-based policies and access control must be supported and integrated with application-level control.
			Cloud or On-Premises Sandbox/Detonation Capability: In order to protect the enterprise from emerging zero-day threats, a sandbox/detonation capability is required for large organizations.
		✓	External Threat Intelligence Feeds: The ability to ingest third- and first-party threat intelligence feeds can greatly increase the efficacy of blocking decisions.

Gartner®

Enterprise firewalls should support the following functional (product feature) requirements

OS Firewalls + Zenarmor

OPN/pfSense	Zenarmor	Both	Feature
	✓		Manageability: Enterprise firewall platforms must support a centralized management platform that can support configuration management, event/log correlation, software version management, threat management and report generation across multiple (thousands of) distributed firewall instances. This management platform should be common across on-premises and public cloud instances.
		✓	High Availability: Enterprise firewall platforms must support high availability if a single instance of the platform malfunctions; active/standby and active/active failover models should be supported at the physical appliance level and the virtual appliance level. Cloud-based instances must clearly state failover and failback times, which may be impacted by underlying cloud infrastructure limitations.
	✓		Scalability: Physical appliances need to scale to line rate with all common features and TLS decryption enabled, while virtual appliances should scale to meet demand with all common features enabled. Cloud-based instances should support native cloud scale-out groups, which dynamically spin up new resources if traffic throughput increases. Scale out and scale up should be addressed.
		✓	Usability: Ease of use and simplicity of operation are important factors. Most enterprise organizations have limited numbers of trained firewall engineers, and thus automation support (programmability and API support) coupled with SDN integration is critical criterion for the operationalization of enterprise firewall platforms.
		✓	Supportability: Vendor support and the ability to troubleshoot problems on a firewall platform are critical because firewall downtime directly correlates to business downtime for the vast majority of organizations.

Together Zenarmor® + OPNsense/pfSense® provides both the functional and nonfunctional requirements defined by Gartner® for Enterprise firewall platforms

Industry-first Technology

Extending open-source firewall functionality through:

TRADITIONAL APPLIANCE PRODUCTS

TLS Decrypt / Encrypt

3rd PARTY APPLIANCE

FORWARD HTTP(S) PROXY

REVERSE HTTP(S) PROXY

DNS FILTER APP

OS NETWORK STACK

OS APPS

DPI ENGINE

IPS ENGINE

VENDOR APPLIANCE

VS

zenarmor

an

ALL IN ONE

lightweight application delivering
the whole SASE stack

Zenarmor Key Features

Key features that extend open-source firewall functionality:

- AI based Threat Intelligence backed Cybersecurity with Complete Application Visibility & Control
- Industry's best Network Analytics with drill-down Network Visibility
- User/Group based filtering & reports
- Centralized & Granular Policy based filtering across all firewalls
- Encrypted Attacks Protection with Lightweight TLS Inspection

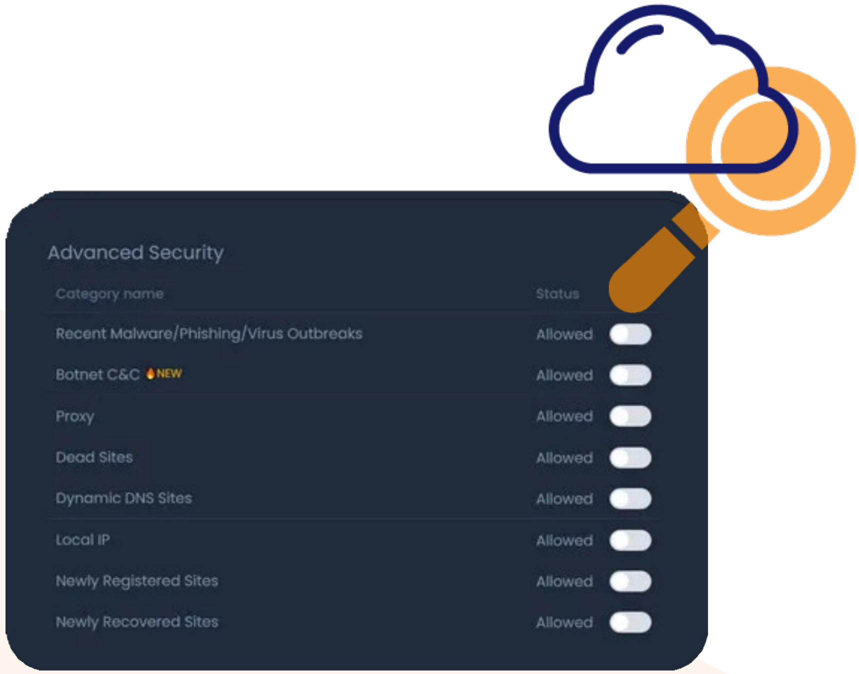
Industry-first Technology

Extending open-source firewall functionality through:

- **One of the most efficient packet inspection technologies**
  (In the world.)
- **The first engine which offers native TLS inspection**
  (Regardless of the port numbers.)
- **It's fully transparent**
  (Other products rely on a "proxy" method, which cannot protect the whole TCP/UDP port spectrum.)
- **All-in-one, Software only. Use the hardware you prefer**
  (w/o custom ASICs.)
- **Best in class native network analytics and reporting**
  (Providing the richest set of analytics and reporting for the Unified Threat Management (UTM) class of products.)
- **No more proxies**
  (The industry's best packet processor with native Lightweight TLS inspection across all ports.)
- **RESTful API**
  (Enables easy integration to your existing toolset.)
- **Flexible, plug-in architecture**
  (Extends the power of your Open Source Firewall to make it a NGFW!)

Zenarmor Key Benefits

Get real-time protection against advanced 0-day attack campaigns



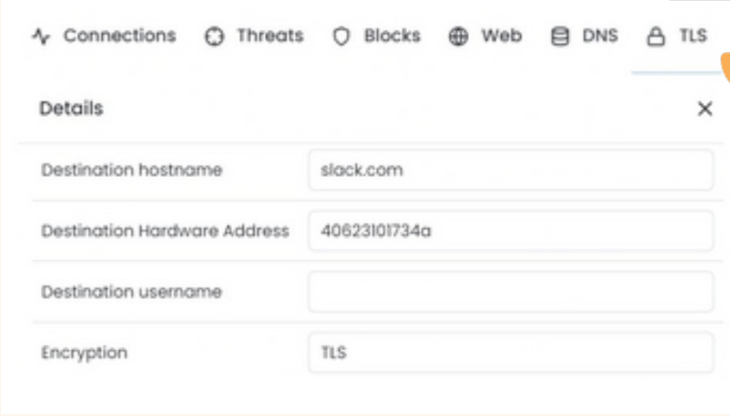
Advanced Security

Category name	Status
Recent Malware/Phishing/Virus Outbreaks	Allowed
Botnet C&C NEW	Allowed
Proxy	Allowed
Dead Sites	Allowed
Dynamic DNS Sites	Allowed
Local IP	Allowed
Newly Registered Sites	Allowed
Newly Recovered Sites	Allowed

- Realize the power of AI-based Cloud threat intelligence.
- Stop zero-day malware and phishing attacks in real-time
- Detect and block new botnets in an instant
- Leverage Deep Content Inspection to prevent evasive threats that otherwise would bypass IP, Port and DNS based filtering

Zenarmor Key Benefits

TLS Inspection



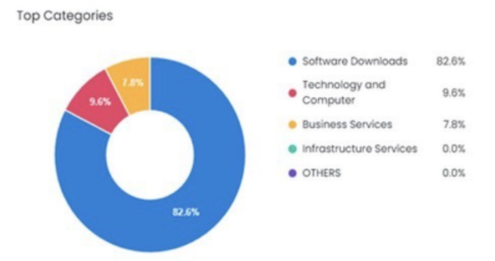
Destination hostname	slack.com
Destination Hardware Address	40623101734a
Destination username	
Encryption	TLS

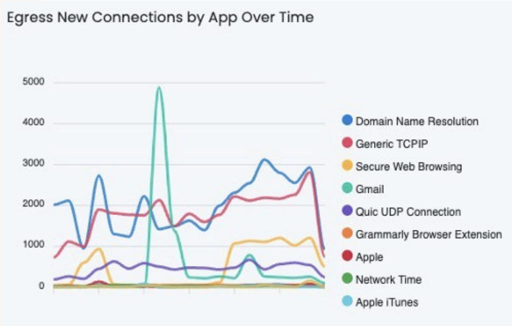
Prevent evasive threats with TLS Inspection

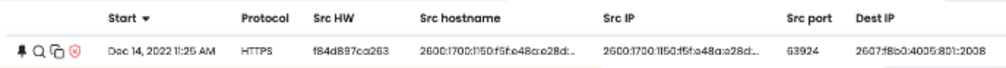
- Sophisticated L7 Enterprise-grade content filtering technology
- Detects and Blocks Threats using encryption
- Stop bad guys from using encryption
- Enable certificate-based or full TLS Inspection to protect against encrypted threats (*Planned for late 2023)

Zenarmor Key Benefits

Industry's best reporting


Top Categories


Egress New Connections by App Over Time



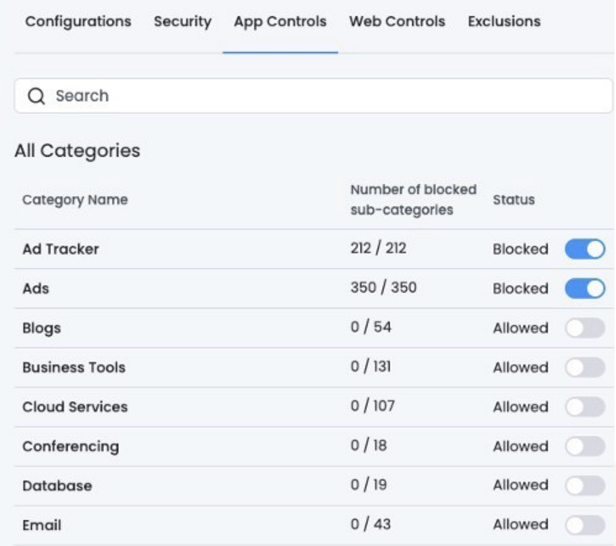
	Start ▾	Protocol	Src HW	Src hostname	Src IP	Src port	Dest IP
	Dec 14, 2022 11:25 AM	HTTPS	f84d897ca263	2600:1700:1150:f5f:e48a:e28d:..	2600:1700:1150:f5f:e48a:e28d:..	63924	2607:f8b0:4005:801::2008

Always be in-the-know with Industry's best reporting

- Be on top of everything that's going on in your network.
- Create scheduled reports that deliver a clear picture of what's happening across all your networks.
- Delegate reporting on a need-to-know basis
- Spot anomalies visually and as they occur
- Start from the big picture, drill down to per-connection details

Zenarmor Key Benefits

Powerful Application Controls



All Categories

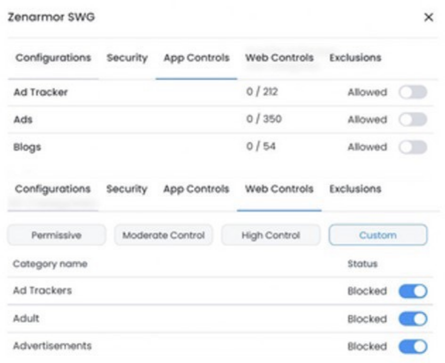
Category Name	Number of blocked sub-categories	Status
Ad Tracker	212 / 212	Blocked
Ads	350 / 350	Blocked
Blogs	0 / 54	Allowed
Business Tools	0 / 131	Allowed
Cloud Services	0 / 107	Allowed
Conferencing	0 / 18	Allowed
Database	0 / 19	Allowed
Email	0 / 43	Allowed

Improve Business Productivity with Application Control

- Block or control unauthorized applications
- Rich application database identifies thousands of applications
- L7 identification regardless of port numbers

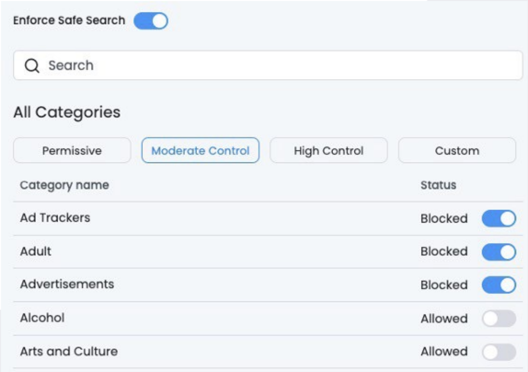
Zenarmor Key Benefits

Enterprise-grade web filtering & security



Ad Tracker	0 / 212	Allowed	○
Ads	0 / 350	Allowed	○
Blogs	0 / 54	Allowed	○

Category name	Status	
Ad Trackers	Blocked	●
Adult	Blocked	●
Advertisements	Blocked	●


Enforce Safe Search ●

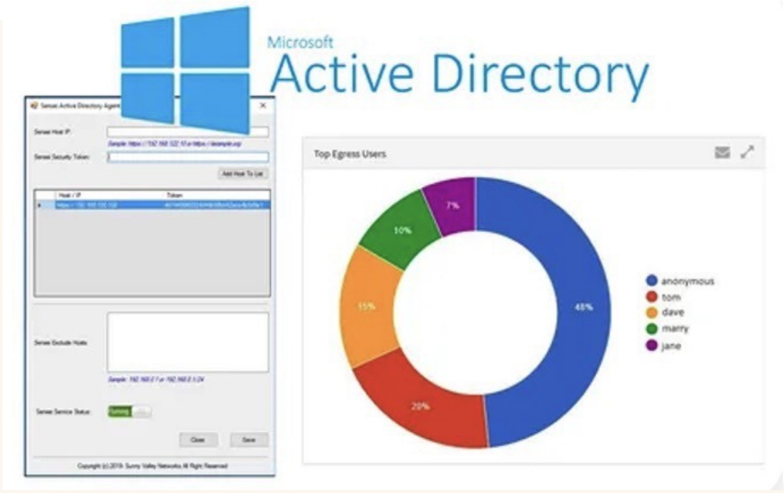
Category name	Status	
Ad Trackers	Blocked	●
Adult	Blocked	●
Advertisements	Blocked	●
Alcohol	Allowed	○
Arts and Culture	Allowed	○

Enforce Corporate Policies Across All Networks

- Apply policies for more than 300 Million web sites under 60 different categories
- Create custom categories to blacklist or whitelist sites

Zenarmor Key Benefits

Identity, Device and Location aware policies

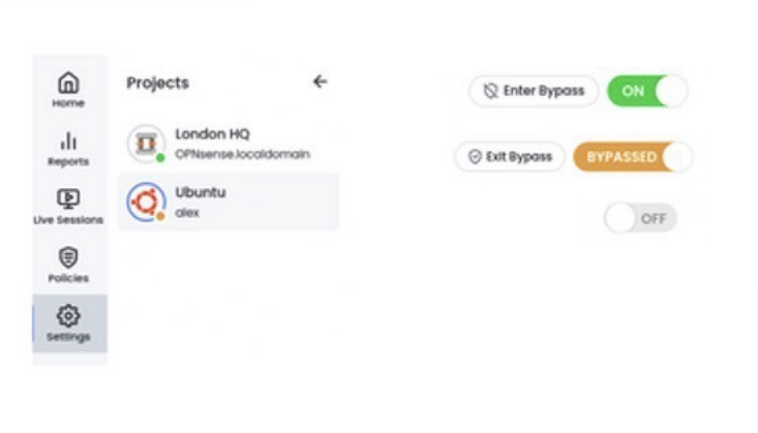


Enforce Corporate Policies Across All Networks

- Forget about trying to manage IP addresses
- Easily enforce policies for individual users and groups to enable granular access controls
- Integrate with popular User directory databases like Microsoft Active Directory or LDAP

Zenarmor Key Benefits

Centrally manageable through the Cloud

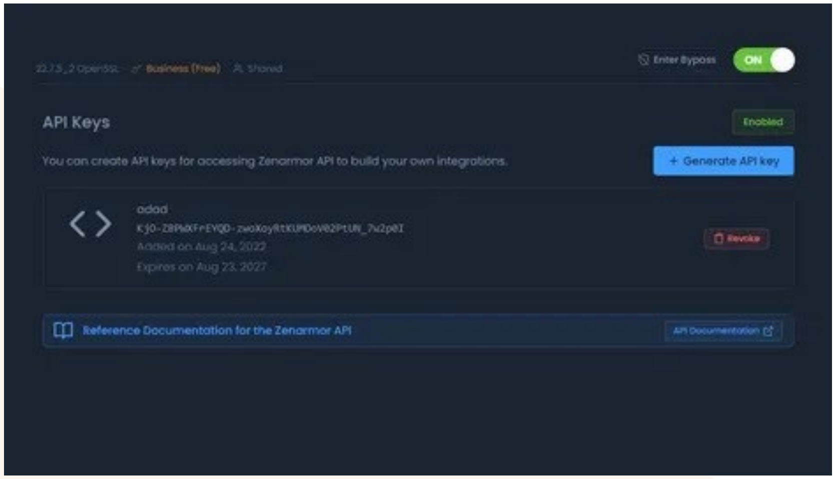


Manage from Anywhere!

- Easily manage all your firewalls from the Cloud and in a single pane of glass
- Create centralized, location independent policies
- Enforce your policies across all IT environments
- Share firewall management with your team

Zenarmor Key Benefits

Extend via RESTful API



22.7.5_2 OpenSSL · Business (Free) · Shared

API Keys

You can create API keys for accessing Zenarmor API to build your own integrations.

adad

```
KjO-Z8PWXFrEYQD-zwoXoyRtKUMDoV82PtUN_7w2p0I
```

Added on Aug 24, 2022

Expires on Aug 23, 2027

Reference Documentation for the Zenarmor API

Automate with RESTful API and operate at scale!

- Create automations to operate at scale!
- Complete Zenarmor functionality is available through the RESTful API

Zenarmor Key Benefits

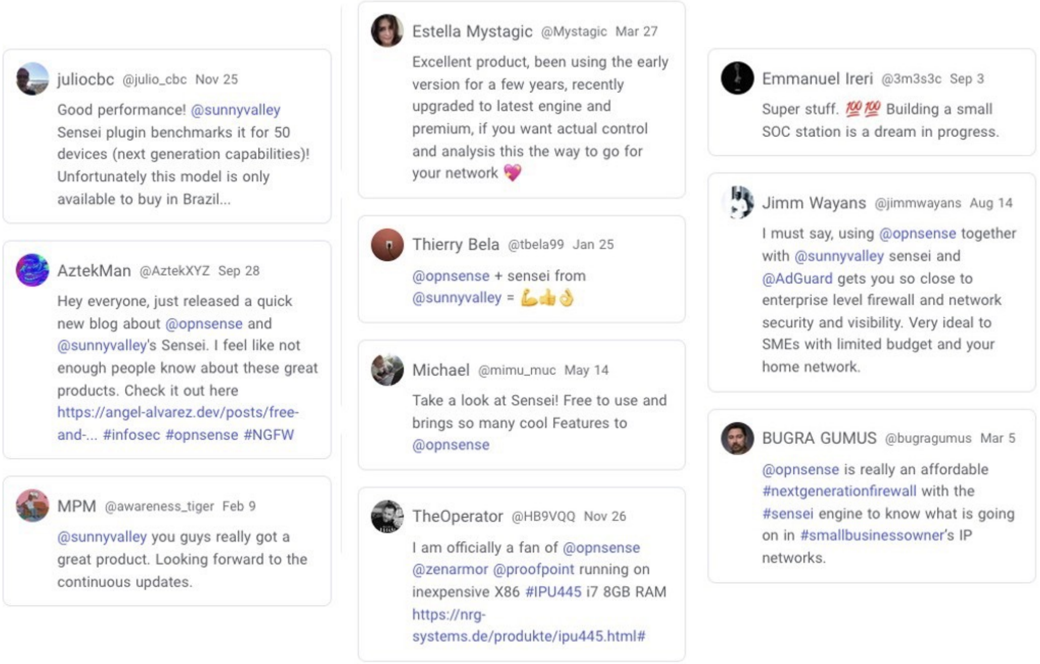
Seamless Integrations

Seamlessly integrate with your existing security tools

- Stream Zenarmor's rich security telemetry to your favorite SIEM
- Further integrate with Microsoft Active Directory, Elasticsearch, Splunk, Wazuh, Syslog etc. to boost your enterprise detection context.

Loved by the Best!

Zenarmor has been developed by thousands of OPNsense® and pfsense® users worldwide.



juliocbc @julio_cbc Nov 25

Good performance! @sunnyvalley Sensei plugin benchmarks it for 50 devices (next generation capabilities)! Unfortunately this model is only available to buy in Brazil...

AztekMan @AztekXYZ Sep 28

Hey everyone, just released a quick new blog about @opnsense and @sunnyvalley's Sensei. I feel like not enough people know about these great products. Check it out here https://angel-alvarez.dev/posts/free-and-... #infosec #opnsense #NGFW

MPM @awareness_tiger Feb 9

@sunnyvalley you guys really got a great product. Looking forward to the continuous updates.

Estella Mystagic @Mystagic Mar 27

Excellent product, been using the early version for a few years, recently upgraded to latest engine and premium, if you want actual control and analysis this the way to go for your network 💖

Thierry Bela @tbela99 Jan 25

@opnsense + sensei from @sunnyvalley = 💪👍👌

Michael @mimu_muc May 14

Take a look at Sensei! Free to use and brings so many cool Features to @opnsense

TheOperator @HB9VQQ Nov 26

I am officially a fan of @opnsense @zenarmor @proofpoint running on inexpensive X86 #IPU445 i7 8GB RAM https://nrg-systems.de/produkte/ipu445.html#

Emmanuel Ireri @3m3s3c Sep 3

Super stuff. 💯💯 Building a small SOC station is a dream in progress.

Jimm Wayans @jimmwayans Aug 14

I must say, using @opnsense together with @sunnyvalley sensei and @AdGuard gets you so close to enterprise level firewall and network security and visibility. Very ideal to SMEs with limited budget and your home network.

BUGRA GUMUS @bugragumus Mar 5

@opnsense is really an affordable #nextgenerationfirewall with the #sensei engine to know what is going on in #smallbusinessowner's IP networks.

It's protecting over a million endpoints, including home users, academic institutions, large enterprises and even government agencies.

Technology Partner

Open Source core OS platform Partnership

Zenarmor and OPNsense teams are working together closely in ,bringing the \A technology to the reach of OPNsense community as well as collaborating on improving the advanced networking and security capabilities of the FreeBSD Operating System.

OPNsense®

Working very closely with Deciso B.v. Deciso is the founder of **OPNsense**

zenarmor In Numbers

14,000+

Active deployments in 140+ countries

11.K+

Customers across all verticals

A single deployment secures up to 8,000 devices

Lithuanian Government tested and recommended for nation-wide academic institutions

French schools region-wide deployment covering 170+ locations

100+

Partners from all around the world including ISPs, MSPs and Consultants

800,000+

Endpoints protected globally

10M+

Threat Intelligence Queries processed daily

Government and Military deployments around the globe

Wrapping Up

Delivers High performance Next Generation Firewall Capabilities

- Software only: No Expensive Custom Hardware Needed
- Easy to Deploy and Manage

You will love Zenarmor because it delivers

- Cloud Based Threat Intelligence covering 300m+ sites
- Great performance on x86 64bit H/W
- Stability and Rich Feature-set including Lightweight TLS Inspection
- Industry Leading Reporting
  Exceptional TCO
- Zenconsole Cloud based Management Included
- Coexists nicely with other Open Source tools running on your firewall

Scales from Home use to Enterprise NGFW deployments

- Easily managed from the Cloud

Strategic partnership

Between Zenarmor and Thomas-Krenn

- Thomas-Krenn hardware
  - Rackserver
  - LES devices
- OPNsense open source software
- Zenarmor for NGFW features

Thomas-Krenn + OPNsense + Zenarmor = perfect match

Where to find

Licenses and prices

- Zenarmor in the Thomas-Krenn online shop
- Ready to purchase versions
  - Soho Edition (up to 100 devices)
  - Business Edition (up to 2000 devices)
  - HA Licenses with Business Edition
- Custom solution also possible
  - More devices
  - Longer terms (up to 5 years with discount)
  - Special offers for special organizations

Hardware sizing

Common configurations with Zenarmor

- Up to 50 users and ~350 Mbit/s WAN (with VPN) connection
  - Xeon-D systems
  - RI1102D-F
  - 16GB RAM with Zenarmor

- 50 up to 150 users and 1 Gbit/s WAN (with VPN)
  - Xeon-E systems
  - 16GB RAM with Zenarmor

- 150+ users and >1 Gbit/s WAN (with VPN)
  - New Xeon-E RI1101-SMXEFH with Xeon E-2334
  - RA1208-AIEPN with CPU Epyc 72F3
  - 32GB RAM with Zenarmor (>250 Users)

Information

About Zenarmor

- Zenarmor User Guide
- How to decide which subscription plan is right for you
- Zenarmor OPNsense Plugin
- Zenarmor Plans
- Information in the Thomas-Krenn-Wiki

Q&A

zenarmor

Next Steps?

Thank You!

zenarmor

- http://www.zenarmor.com
- sales@zenarmor.com
- (650) 288 4488
- 19925 Stevens Creek Blvd. Suite 100, Cupertino CA 95014, USA