AEGIS DEFENDER PRO

Blocks 99% of Malicious Traffic Instantly, Hourly Updates

www.aegiscds.com

Aegis Cyber Defense System (ACDS) provides cybersecurity software and services developed to safeguard every server and network endpoint from reported hackers, spammers, and botnets worldwide. **Aegis Defender Pro (AEGIS)** acts like a sentry at the front gate checking all ID's and proactively denying entry to all known malign IP Addresses that have ever attacked *anyone*, blocking up to 99% of cyberattack attempts. AEGIS installs ACDS' **Master Blocklist (MBL)** of over *770 million IP addresses* as Native Firewall Rules in minutes.

The Problem

Public-facing servers are under constant attack from millions of compromised web servers and computers, known as Botnets or "Zombie Armies". AbuseIPDB.com reported 2 million cyberattacks in 2016; this number grew to over 220 million cyberattacks in 2022. It is estimated that **cyberattacks compromise up to 30,000 computers and devices per day** adding to the Zombie Armies.

Introducing Aegis Defender Pro – A Shield of Protection

Aegis Defender Pro (AEGIS) software installs Firewall Rules directly into the Native Windows Defender Firewall and Native Linux Server Firewalls and updates rules hourly. The rulesets are the AEGIS Master Blocklist consisting of the malign IP Addresses curated over nearly a decade. Aegis Defender Pro is not a unique operating system and does not require additional hardware. AEGIS was originally designed for MSFT Azure / Windows server and operates seamlessly as a Windows service, with only a tray icon to indicate its active status. AEGIS utilizes Windows Firewall default "Silent Drop" setting for incoming packets from IP Addresses on the Master Blocklist and collaborates with existing 3rd party server software to notify ACDS/MBL Services of security incursions and the offending IP Addresses. The Master Blocklist is amassed from reported cyber-attacks since 2016, consolidated into 53 Firewall Rulesets for minimal performance impact. AEGIS has expanded this capability to be applied it to support Linux server firewalls.

Aegis Defender Pro **MBL Services (MBLS)** has cataloged over 770 million known malign IP Addresses to the Master Blocklist since 2016 with the sole purpose of blocking "bad traffic" while allowing "good traffic" to access subscribers' servers. MBLS monitors subscribers' security incursions, cybersecurity watchdog groups and the web for major cyberattacks, collects, and researches the IP Addresses, adds them to the MBL and then updates all subscribers hourly around the clock. As attacks grow in number and complexity, Aegis Defender Pro adapts in real-time to keep all subscribers safe, even against rapidly evolving threats.

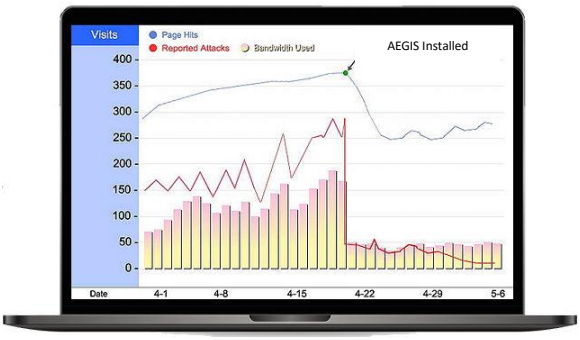
Aegis Defender Pro drastically increases the protection and resilience of all critical infrastructure endpoints including Office, Web and Email Servers. Aegis Defender Pro stops up to 99% of malicious traffic *instantly* on any Windows or Linux machine. By eliminating this nefarious traffic, the SIEMs, WAFs and other Cyber Security measures become more efficient, reducing traffic attacking the server. All endpoint firewalls synchronized with hundreds of millions of reported IPs, all reporting new attacks and all receiving that attack data in minutes.

THE MORE THEY ATTACK US, THE STRONGER WE ALL BECOME

Aegis Defender Pro Operations Benefits

Subscribers have documented network and operational benefits upon installing AEGIS. Network cybersecurity measures take up substantial processing and memory power, but with the significant reduction in attacks with AEGIS, CPU usage reduces from greater than 90% to less than 5% on average. Efficient CPU usage can lead to lower heat output and less equipment wear, effectively lowering equipment, cooling and energy costs. Network-wide performance and bandwidth increases are common, improving network operations, increasing workforce productivity, and allowing IT personnel to maintain the network instead of constantly defending against new cyberattacks.

Real World Performance – Case Studies



Case Study – Web Server Client X

- Before installing Aegis Defender Pro, website received over 40,000 hits/day, including attacks that overloaded the server and caused slow page loads and site crashes.
- With installation of AEGIS, traffic dropped by 50% instantly. Analytics data revealed *all stopped traffic originated in Russia, China, and dozens of other hacker-friendly countries* and *thousands of SMTP and SSHD attacks.*
- Upon installing AEGIS, over 80,000 attacks were blocked.

Over 80,800 Attacks Registered

iptables firewall

Listed by source hosts:

Logged 80835 packets on interface eno2

From 1.2.165.115 - 6 packets to tcp(465)
From 1.11.62.185 - 32 packets to tcp(25,465)
From 1.12.37.144 - 5 packets to tcp(465)
From 1.22.228.147 - 4 packets to tcp(25)
From 1.28.86.66 - 1 packet to tcp(465)

99% Attacks Blocked

SSHD

Failed logins from:

16.16.97.8 (ec2-16-16-97-8.eu-north-1.c
20.101.108.165: 27 times
24.199.110.179: 27 times
35.186.156.47 (47.156.186.35.bc.googleu
35.200.52.181 (181.52.200.35.bc.googleu
40.115.63.169: 28 times
49.0.71.48 (49-0-71-0.24.fixed-public.k

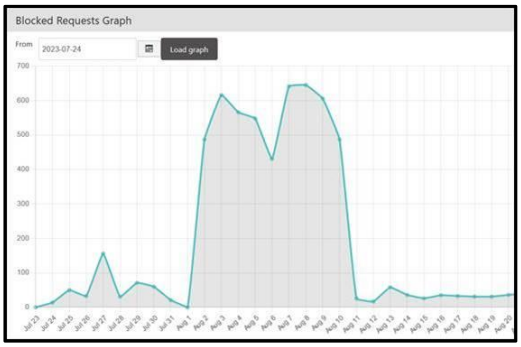
<1% Successful Probes

httpd

A total of 43 sites probed the server

103.219.154.220
104.143.83.241
106.75.166.179
107.170.226.12
109.237.97.180

Case Study – Web Server Client Y



- Client Y agreed to deactivate Aegis Defender Pro on an old website server that was being upgraded by ACDS.
- Initial Deactivation – validated that within hours of deactivating AEGIS, the WAF software recorded 150 attacks (up from 25/day baselined average). With this validation, we scheduled a 10-day test.
- Ten Day Test – Within 24 hours of the AEGIS deactivation the WAF registered 500 attacks. By Day 2 the attacks surpassed 600 per day. The attacks then became more serious, changing from simple fake logins and DoS attacks to SQL Injection and File Upload attacks, *a noticeable pattern of increasingly dangerous attacks.*
- **Without Aegis Defender Pro, attacks jumped 4,233% within 48 hours**.
- AEGIS was reactivated on the 10th day and attacks dropped back to 25 per day, a **97% decrease**.

When attack data was analyzed, 99% of attacking IP addresses were in the Master Blocklist, some have been known for many years.

Real World Protection

The FBI and the Cybersecurity and Infrastructure Security Agency (CISA) issued a warning on September 20, 2023, regarding the SNATCH Ransomware Gang who recently attacked South Africa's Defense Department and the city of Modesto California, USA. Aegis Cyber Defense Systems researched the IP Addresses used by this criminal organization and confirmed Aegis Defender Pro has been blocking these IP Addresses on the Master Blocklist since 2020. AEGIS will continue to add malign IP to the MBL for the ongoing protection of our software subscribers from threat actors like SNATCH.

For More Information

Visit our website at https://www.aegiscds.com

Charles Triglianos
AegisCDS CEO, Founder
800-626-3520
ctrig@aegiscds.com

Mark Whitman
GSS Federal, Managing Partner
202-280-8936
mwhitman@gssfederal.com

About Aegis Cyber Defense Systems

Aegis Cyber Defense Systems (ACDS) began in 2006 as Trig Web Design (TWD) a Web Hosting and Development Services Company. Trig began developing its Cyber Defense System in 2016 in response to the increasing number of cyberattacks causing network delays and offline servers. Trig renamed to Aegis Cyber Defense Systems and is marketing their novel solution **Aegis Defender Pro** which combines AEGIS' exclusive Software Native Firewall Updating System and MBL Services to instantly blocks over 770 million IP Addresses used for cyber-attacks, detect, and report new attacks and update every hour from the ACDS Cyber Security Operations Center.

GSA Contract Holder
Contract # 47QTCA22D00BJ