seer box
by Pluribus One

DATASHEET

Seer Box: a new way of protecting Web Applications and APIs

The challenge of protecting Web Applications and APIs

In contemporary digital landscapes, Web Applications are the primary target for approximately 40% of cyber-attacks. This statistic isn't surprising given their inherently public exposure, making them continuously accessible for low-cost and fully automated vulnerability scans. Such accessibility poses a significant threat to application security and the integrity of hosted data, especially considering that an average of 85% of software vulnerabilities remain unaddressed.

The primary approach to mitigate these attacks involves eliminating the vulnerability, thereby eradicating the root problem, wherever possible (e.g. if it doesn't compromise the application functionalities). However, this process typically requires some time, as software suppliers may need to provide updates. During this interim period, a window of exposure exists wherein attackers can exploit the vulnerability.

Additionally, it's important to recognize that security issues in Web Applications and APIs aren't always attributable to specific vulnerabilities. For instance, to combat malicious bot activity performing content scraping, it's imperative to focus on discerning the overarching behavior of clients rather than solely addressing individual requests.

Why WAFs are not the best fit for SOC & MSSPs?

The cybersecurity market has significantly moved in the last years toward managed services, with customers relying increasingly on Security Operation Centers and Managed Cybersecurity Service Providers to quickly mitigate the risk without having to handle technologies directly.

According to the SANS SOC Survey 2023, among the almost 50 cybersecurity technologies most commonly adopted by modern SOCs, WAFs are the only ones with specific capabilities for the detection and blocking of attacks against Web Applications and APIs.

In fact, they are the solution commonly used to mitigate the exploitation of application layer vulnerabilities and to keep away malicious bots from exposed applications and services.

Nevertheless, besides being used to send alert notifications to a SIEM wherever a WAF is already present, WAFs tend typically to remain outside the perimeter of the solutions directly managed by the SOCs. The two main causes are 1) that WAFs are part of the infrastructure (so there is a point connected with the responsibility to manage it) and 2) that configuring application layer rules requires specific knowledge of the applications and services to be protected. Both these aspects go beyond the primary purposes of detection and first response which are the primary goals of a SOC. And when a WAF is not already there, deploying a component that requires a change to the infrastructure and that is priced also for its capability to block the attacks, might be not the most convenient choice. Additionally, like all the perimetral devices, WAFs are effective only against attacks that arrive from outside the perimeter.

In circumstances when the threat actor has the chance to reach directly the protected services because he is already within the perimeter or because of a WAF misconfiguration that allows him to reach the origin server's direct IP address directly, WAFs can not provide visibility of the malicious activity which is effectively targeting the Web Application or the APIs.

SEER BOX®: a unique point of view on Web Applications and APIs

SEER BOX® by PLURIBUS ONE is a product for the monitoring and protection of Web applications and APIs that, when compared against traditional Web Application Firewalls, aims to offer a broader perspective on the security of the monitored services.

Whilst it can enable "Web Application Firewall - like" functionalities, in PLURIBUS ONE we prefer to define it as a Web Application Security Manager since it is designed to be the cornerstone of a defensive end-to-end strategy for protecting Web Applications and Services. SEER BOX® can operate as a primary Web Application Firewall but can also complement WAFs already in the infrastructure representing the last line of security in the protection of Web Applications and APIs. Unlike traditional WAFs SEER BOX® is designed to be non-invasive during deployment, integrating natively with the solutions already present both for the observation of traffic in transit and the application of traffic-blocking policies. As for traffic reading, SEER BOX® is natively integrated with the most widely used solutions on the market, such as Web Server/Reverse Proxy/Load Balancer, Application Delivery Controller, Firewall and WAF, and SIEM, both commercial and open-source among the most widely used on the market. It has also been certified by NGINX as a fully compatible dynamic NGINX+ module.

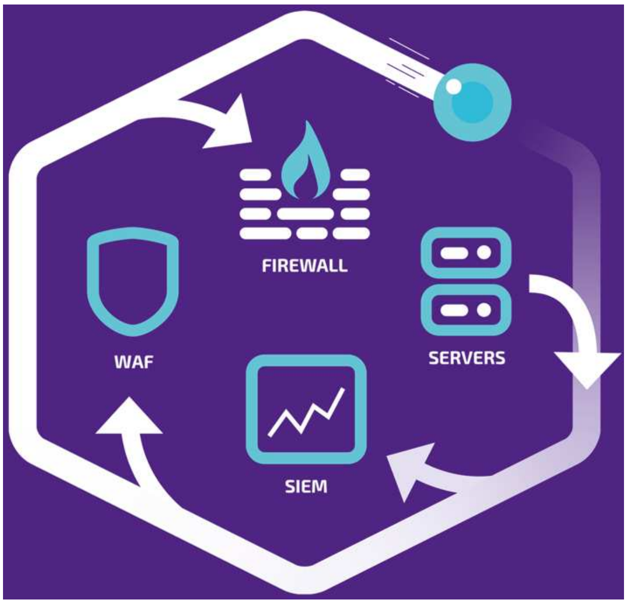

Figure 1. SEER BOX is fed by servers, ADC, and reverse proxies, can control FW and WAF to increase their protection capabilities, and can notify externally the alers for instance sending them to a SIEM platform.

Natively supported traffic sources

- HA Proxy
- NGINX
- APACHE
- Oplon ADC
- Cloud Load Balancers or equivalent with ad-hoc logging formats already available in Seer Box®

Check more on https://docs.seerbox.it/category/log-sources-and-

From a protection perspective, any solutions with blocking capabilities (L3, L7) already in the infrastructure can be leveraged and instrumented by SEER BOX® to enforce traffic-blocking policies that the SEER BOX® GUI allows to define easily through a guided procedure.

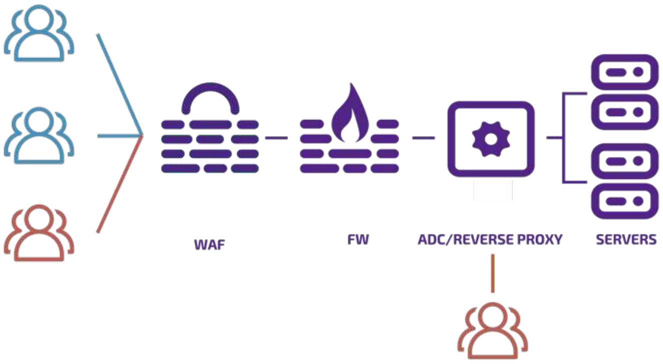

Figure 2. Reading the traffic directly from the servers, ADCs, or reverse proxies, and thus being really close to the applications, SEER BOX® can offer visibility on what is actually going on on the Web Applications and APIs that traditional WAFs, because of their deployment model, can not guarantee.

Besides being noninvasive, which makes the solution suitable also for environments where traffic rewriting rules that could be negatively impacted by an inline WAF have been configured, the offline deployment of SEER BOX offers the possibility to have increased visibility on what the Web Applications and APIs are effectively receiving, for instance in cases where the FW or WAFs have been bypassed and the attacker is reaching the services laterally.

In essence, SEER BOX can be easily deployed to add visibility and protection to what is going on the Web Applications and Services, making automatically available the information useful to block the attack, thus operating like an XDR for Web Applications and APIs.

The SEER BOX® technology stack

> **"Do you plan to continue using Elixir for future projects?**
>
> "According to the Stack Overflow Survey Elixir has been among the top two most loved or admired programming languages (alongside Rust, which), and it did it for a good reason. The result of this question is pretty clear - the community loves Elixir, and they're here to stay."
>
> **STACK OVERFLOW SURVEY, 2023**

When the development of SEER BOX® started, PLURIBUS ONE committed itself to deliver to the market an innovative web application security solution. The Engineering and Development team at PLURIBUS ONE decided to invest in the latest technologies to design a product striving for the highest standards of security, efficiency and reliability, distributed as a modular and containerized system.

SEER BOX® relies on a highly concurrent and scalable architecture implemented in **Elixir** in order to orchestrate its management components, running on the trusted and well-known *BEAM/OTP* platform and empowered by its robust set of dedicated frameworks, resulting in an extremely resilient and fail-safe system.

At the core of its data processing components, **Rust** is employed to ensure security and efficiency, taking full advantage of the language's groundbreaking strengths in terms of speed, memory safety and reliability. The functional approach and the innovative character derived from these leading edge technologies with the support of their thriving, and modern ecosystem, allowed the PLURIBUS ONE engineering team to build a system providing first class protection of web services and secure handling of sensitive data, all while guaranteeing efficiency, availability and ease of use.

Finally, we adopted a **fully containerized** design, which makes it possible to **deploy** the solution easily (**directly from Dockerhub[1] or Quay.io[2]** and with the greatest flexibility, on private, public and even hybrid environments, ensuring the possibility to scale from low traffic up to enterprise installations with the maximum possible cost-effectiveness in terms of resource allocation.

SEER BOX® Versions & Features

Seer Box® is licensed and priced based on the number of hits (HTTP/HTTPS requests toward the monitored services) collected on a monthly basis. All the versions of SEER BOX® feature an extended set of APIs, to enable and support Security Orchestration, Automation, and Response.

Version	Hits/Month (Millions)
MSSP-LIGHT	20
MSSP-SMALL	45
MSSP-PREMIUM	90
MSSP-BUSINESS	180
MSSP-ENTERPRISE	>180

The deployment of Seer Box consists of two components: a ***Sentinel***, which is a (minimal) sensor designed to operate in distributed environments, and it is responsible for the parsing of the access logs and for a first layer of detection; a second component, the ***Engine***, is the main Seer Box component responsible to gather data from the Sentinels, extending the analysis the Sentinel(s) did (e.g. adding, for instance, a temporal dimension) and providing all the basic Seer Box services like the GUI or the persistence.

Depending on their policies (e.g. for the customer data management), MSSPs and SOCs, might decide to deploy at the customer premise only the Sentinel (keeping the Engine on their premise) or to make a full installation of Seer Box for each customer they serve.

SEERBOX® KEY FEATURES	
INSTALLATION	Either on the SOC/MSSP or on the customer premises. The ENGINE (main GUI and all the essential services are provided free-of-charge. Payment occurs as long as the customers are onboarded. Pricing is based on the table above.
DETECTION MODULES	All enabled
THREAT INTELLIGENCE	Enabled. Seer Box installations continuously receive external data feeds that support the detection capabilities.
PROTECTION - LAYER 3 BLOCKING	Yes
PROTECTION - LAYER 7 BLOCKING	Ad-hoc quotation
AUTOMATED RESPONSE	Yes. Layer 3 blocking can be configured on a domain/group basis, deciding also for which attack categories it should be enabled.

[1] https://hub.docker.com/u/pluribusone
[2] https://quay.io/organization/pluribus_one

AUTOMATED REPORTING	Yes. Possibility to create separate report for specific domains or domain groups, configuring the reference period. Reports are available via the interface or can be automatically sent by email.
CUSTOMIZED REPORT (e.g. partner or customer logo)	Ad-hoc quotation
SIEM INTEGRATION	Yes
APIs for INTEGRATION & AUTOMATION	Yes. Documented at https://docs.seerbox.it

Want to try SEER BOX®?

PLURIBUS ONE makes available a BASIC license of SEER BOX®, provided as a **freemium** version and thus completely free of charge.

Scan the QR code or go directly to **www.seerbox.it** and register, to have your **free** copy of SEER BOX® up and running in minutes.

The company

PLURIBUS ONE Is a European cybersecurity vendor. The company is headquartered in Cagliari (ITALY) and it is built on 20 years of expertise in building machine Learning and AI solutions for computer security. The company serves customers from both the public and private sectors, covering the areas of banking, insurance, transportation, healthcare, water management, and e-commerce.

The company has been awarded with the "Cybersecurity Made in Europe" acknowledgement by ECSO, the **European Cyber Security Organization.**

PLURIBUS ONE is ISO 27001 certified for the security of the software development process. The DevSecOps approach at PLURIBUS ONE is fueled by OWASP frameworks and tools, like the Software Component Verification Standard and OWASP Dependency - Track for identifying and reducing risk in software supply chains.

CYBERSECURITY
MADE IN EUROPE

Contacts:

PLURIBUS ONE S.R.L.
Via Emilio Segrè 19

info@pluribus-one.it

seer box

by Pluribus One