How e-Lock WebALARM Complement Web Application Firewall to Provide a Complete Security Solution

Both products, e-Lock WebALARM and Web Application Firewall, an example will be FortiWeb, provides different types of protection and fully complements each other in providing the user with a complete security solution. Below are the areas that are protected by WebALARM and Web Application Firewall.

A. Protection By WAF

	Web Application Firewall
Application Layer Vulnerability Protection	Most WAF provides box protection for the most complex attacks such as SQL Injection, Cross Site Scripting, CSRF and many others. This is usually performed by using behavioral analysis and also signature based checks.
Denial of Service (DoS)	They also provide multiple protection policies for network and application layer denial of service threats with sophisticated mechanism helps identify and block automated attacks but usually with the use of behavioral analysis again.
HTTP RFC Compliance Validation	Most WAF can also blocks any attacks manipulating the HTTP protocol by maintaining strict RFC standards to prevent attacks such as encoding attacks, buffer overflows and other application specific attacks.

B. Protection by WebALARM

	e-Lock WebALARM
Specialized Data-Level Solution	WebALARM is a mission-specific specialized solution focusing only on data-level protection, hence offering unsurpassed accuracy, reliability and performance on file integrity monitoring and protection.
Why Is It Important To Focus Only On Server's Data-Level Protection?	In general, servers are already well protected by existing enterprise firewalls and network-level intrusion detection systems. Hence, data-level protection becomes the single most important security focus on the servers, minimizing the server's resource burden and also the administrative workload.

	e-Lock WebALARM
File Integrity Monitoring Optimization	WebALARM is optimized to perform file integrity monitoring. Firstly, it provides highly efficient real-time change detection which consumes little system resource. Secondly, it provides flexible grouping of files and folders for different monitoring requirements, notification methods and reactive measures.
Accurate Tamper Detection	WebALARM works on the principle of protecting what is known to be good. It operates based on detecting file change events and comparing the current file state and content against a known trusted baseline to ensure reliability of error detection without false positives.
Automatic Recovery	WebALARM's main value proposition is its ability to perform automatic recovery to enforce data integrity protection. Any unauthorized change detected will be repaired immediately to minimize the time window of non-compliance. This feature is fully automated without human intervention. This automatic recovery is fully built-in by default and can be used out-of-the-box without configuration.
Data Change Workflow Integration	WebALARM provides multiple methods to integrate with customer's data change operation workflow. Data update can be authorized based time-window or based on secure updates from trusted secure staging servers. WebALARM also allows easy integration with content management systems (CMS).
Independent Standalone Operation	WebALARM allows standalone operation without any requirements for constant updates. Once configured, the WebALARM allows hassle-free "install and forget" operation. The management console is only required during the initial configuration and not required for operation.