ATOMICORP®

Extend the Power of OSSEC with Atomic Enterprise OSSEC

Intro on OSSEC

Open Source Security (OSSEC) is a powerful engine for the collection and analysis of system data but it is lacking a lot of functionality that makes it practical for laymen use. Atomicorp has invested 14 years contributing to OSSEC and have leveraged that expertise to provide users with *Atomic Enterprise OSSEC (AEO)* to make OSSEC more powerful and much easier to use and configure. Our CTO Scott Shinn runs the OSSEC project and has been using it for more than a decade to protect both commercial and government systems.

Security

Atomic Enterprise OSSEC provides a set of OSSEC specific add-ons that are necessary to protect systems as well as manage deployment. *AEO* includes advanced malware protection, automated hardening, advanced web protection engines, machine learning and more that enable servers, devices and endpoints to protect themselves from both common and targeted attacks. *AEO* also provides advanced real-time rootkit protection and detection, vulnerability scanning, memory protection, vulnerability shielding, network intrusion protection, and self-healing.

The Fastest And Most Efficient Way To Protect Your OSSEC Installation From Cyber Attacks

Realtime Malware Protection

AEO integrates directly with Virustotal, allowing users to protect themselves from malware using every malware product simultaneously, without having to install any of them. Fast, light and the most comprehensive malware protection system available.

Automatic Compliance Auditing and Alerting

AEO automatically monitors the compliance of systems, sends alerts when they are not in compliance, and automatically enforces compliance.

Unrivaled Web Protection

AEO protects against SQL injection, cross-site scripting, cross-site request forgery, encoding abuse, protocol abuse, Unicode and UTF-8 attacks, HTTP smuggling, path recursion, web spam, shells, spam tools, mailers, malicious iFrames and more.

Vulnerability Shielding

AEO provides real-time vulnerability shielding to protect systems form zero-day threats before vendors release patches for their products.

Portable Media and USB Device Control

AEO allows you control over what portable media and USB devices can be used with endpoints, devices and servers. This enables full control ensuring only trusted devices are used with specific systems.

Real-Time Actionable Threat Intelligence

AEO protects against bad actors with automatically updated machine-actionable threat intelligence as new threats, methods of attack and sources are identified.

Real-Time Malicious Domain and Source Blocking

AEO's real-time global cloud identifies malicious activities from domains and sources that are attacking one customer and automatically uses that data to protect all other AEO protected customers before they are hit.

> “ *AEO* enables OSSEC to integrate with all major SIEMs. ”

Role-Based Management Interface

Atomic Enterprise OSSEC includes a purpose-built Management Interface for OSSEC to meet common enterprise needs including: log and event visualization, event detail analysis and investigation, and system configuration and maintenance. *AEO's* Management Interface enables you to more quickly analyze attacks, manage OSSEC and your agents and take actions where needed. You have the ability to not only see your events, but to manage the systems that OSSEC is monitoring. This gives you true control over your security posture.   In addition, *AEO's* Management Interface has role-based-access-control for heightened security.

Compliance

File Integrity Monitoring (FIM) has become integrated into a host of industry standards including PCI DSS, FISMA, and NERC-CIP. In addition, FIM has key features required for HIPAA and SOX compliance. OSSEC has offered FIM capabilities for more than a decade. *Atomic Enterprise OSSEC* includes a set of OSSEC specific add-ons that build on OSSEC's foundational tools such as FIM, including advanced encryption to meet new file hashing requirements in these standards. As is, OSSEC only meets 6 of the 179 software related PCI DSS requirements. By installing and configuring *Atomic Enterprise OSSEC*, you can meet over 100 of the 3.2 requirements.

Ease of Use

OSSEC is robust and flexible but it is also complicated and can get expensive without expert configuration help. In addition to making OSSEC easier to use via the Management Interface, *Atomic Enterprise OSSEC* has one step auto key set-up and one step installation as well as automatic remote agent upgrades. And, Atomicorp has the expertise and experience to ensure OSSEC is deployed and configured properly and performs at scale so that you are getting exactly what you need from your installation, and can rely on it to meet your ongoing security and compliance needs.

Integrations

AEO enables OSSEC to automatically integrate with all major SIEMs in their proprietary formats. Apps like Splunk, Arcsight (CIS), eOrchestor, and QRadar (LEEF) are all supported out of the box. *AEO* also integrates automatic long-term storage options like Amazon's Glacier to save you money when storing years of data for compliance. In addition, *Atomic Enterprise OSSEC* supports hundreds of application integrations including all major security vendors (McAfee, Palo Alto, Cisco, Cloudflare, etc.) and can orchestrate and automate all of these applications and vendor products.

Unrivaled Support

AEO includes built-in support features that allow customers to directly communicate with Atomicorp support engineers in real-time. For example, the Management Interface includes a simple one-click button to report a false positive that includes all the information necessary to duplicate the event and get immediate support from Atomicorp.

Additional Features

AEO includes remote log retention settings in the interface, advanced machine learning, newly integrated advanced NoiseSocket cryptography from Virgil Security, integrated advanced threat intelligence collected by thousands of honeypots and systems and mined and updated by Atomicorp's machine learning systems, and a robust custom report generator. None of which are included in standard OSSEC.

> “ *AEO* is the fastest and most efficient way to protect your OSSEC installation from cyber attacks. ”

Visualize All of Your OSSEC Events	Use AEO's Management Interface to see, react and manage system events in real-time.
Search All of Your OSSEC Events	Quickly search your systems using a long list of parameters to precisely locate and make adjustments to any event.
Manage All of Your Agent Systems	Centrally manage all of your agents and rules and drill down and manage rules on individual agent systems.
Manage Your File Integrity Monitoring System	Configure what you want to monitor, add, delete, update or ignore. Set base policies and create custom notifications for system events.
Make OSSEC an Endpoint Detection, Protection and Response System	Turn OSSEC into an Endpoint Detection, Protection and Response system giving you a fully-automated playbook.
Achieve Long-Term Archiving	Use storage solutions like Amazon Glacier, Simple Storage, or Azure for built-in, long term log archiving.
Meet Security Compliance Requirements	Meet security compliance requirements including HIPAA, PCI DSS, SOX, DoD and more using AEO's turn-key Management Interface.

About Atomicorp

Atomicorp eliminates the complexity and burden of cybersecurity and compliancy across cloud infrastructures through its comprehensive, multi-layered cloud and server protection platform. Harnessing the power of Open Source Security (OSSEC) and proprietary machine learning, Atomicorp aggregates and correlates data across the enterprise to automatically provide high fidelity active response and recovery. And, Atomicorp enables organizations to maximize their cybersecurity resources to better address today's rapidly evolving threat environment. From end-of-support to cutting edge systems, Atomicorp has the flexibility to provide security and compliancy to any organization. Atomicorp protects thousands of customers within retail, media, healthcare, insurance, and government institutions worldwide.

Headquarters:
15049 Conference Center Drive
Suite 180
Chantilly VA 20151

(703) 299-6667
www.atomicorp.com
info@atomicorp.com