



ATOMICORP

## Solution Overview | Atomic OSSEC

### Atomic OSSEC

Your business is running far, fast, and furious, harnessing distributed computing and the cloud, and deploying apps, servers, VMs, and containers. As you roll out services, enterprise security and compliance efforts struggle to keep up with the pace of change and with the growing threat from cybercriminal activities.

For these challenges, many have turned to the free, agile and flexible Open Source Security (OSSEC). A community-based security development platform like OSSEC gives you a solid toolset of security and privacy capabilities such as intrusion detection, log management, file integrity monitoring, and active response, for any environment including legacy systems that still require protection.

But there remains a largely untapped efficiency and value progression for OSSEC and OSSEC+ users. Additional real-time rules are needed to orchestrate advanced security on the latest apps and legacy systems. Real-time data and a management console are required to see where attacks are occurring, and the means to mitigate the threats needed as well. Experience the power of Atomic OSSEC's extended rules and management interface. See in real-time where and how attacks are occurring, mitigate threats automatically and view trends over time to better understand attack readiness. Gain confidence in your security posture and leverage our expertise for support. Knowledge is power and Atomic OSSEC puts that at your

fingertips. One click access to support, instant pdf reports, CIS and SCAP benchmarked scans with auto-updates. Explore the value of Atomic OSSEC's rules and tools, leverage the powerful OSSEC engine and gain real insight into your Linux, Windows, or other computing environments, including legacy platforms. Atomic OSSEC brings the additional functionality, expertise, and support needed in today's changing environments.

## Atomic OSSEC

**Device integration.** Centrally configure and manage deployments – including for tens of thousands of monitored devices across hundreds of device types.

**File integrity monitoring (FIM).** Atomiccorp OSSEC provides advanced FIM, which is essential toward keeping your data systems clean, making sure data reaches intended recipients only, and generating artifacts to respond to regulatory requirements.

**Cross platform security.** You need to be able to orchestrate security detection rapidly out to the assets you want to protect, whether you're using multiple cloud, public to private cloud, or cloud-to-premises workloads or as part of a hybrid environment that may include legacy systems. Flexible Atomic OSSEC works across AWS, Azure, and Google, and also integrates with Cloudflare toward securing web entities.

**Vulnerability scanning.** If you don't know it exists, how can you protect it? For example, anything that touches anything else that touches cardholder data is part of your state of security, and it must be included in your security program. If you don't know your state, you can't ensure PCI and other forms of regulatory compliance. Know the state of your servers, data, and touchpoints through frequent vulnerability scans, so legacy apps and dark data don't come back to haunt you.

**Reporting and compliance.** Real-time reports with sufficient detail about changes provided by your security information management (SIM) and FIM system(s) are a requirement. Without these reports, you might miss critical file changes or attacks. Atomic OSSEC supports OpenSCAP and CIS, and can be set for PCI-DSS, HIPAA, and GDPR. It provides a SIEM dashboard from which you can easily and accurately assess and report key security indicators such as KPIs, KCIs, and KRIs as part of SLAs and compliance audits.

**SIEM integration.** Atomic OSSEC provides native SIEM integration with ELK, Splunk, Arcsight, and others. This adds a true SIEM function to your OSSEC management dashboard capability.

**Operating systems supported.** Linux OS, Windows, Mac OSX, AIX

Available on premises and/or as part of cloud-based SaaS.

## Figure 1: Compliance Scoring and Reporting



## Figure 2: Vulnerability Scanning and Management

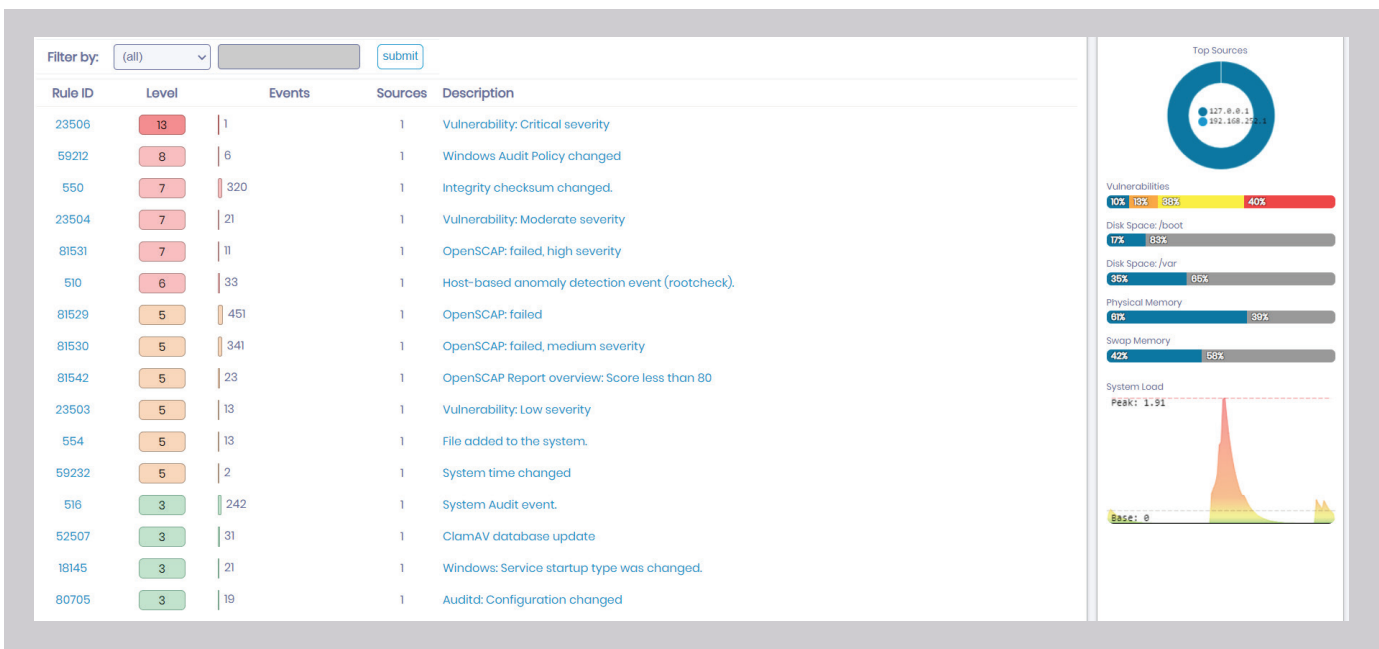


Table 1. The Atomic Advantage

Capability	OSSEC	OSSEC+	Atomic OSSEC	The Atomic Advantage
Enterprise support	No	No	Yes	Available on premises and/or as part of cloud-based SaaS
File integrity monitoring	Yes	Yes	Advanced	The ability to monitor more than just files, keeping your databases, servers, cloud environments clean. Automatic log management that discovers discrepancies and mitigates false alarms.
Vulnerability scanning	No	No	Yes	Assess the vulnerabilities of files and their hosting environments, including directories, servers, and clouds.
Active response	No	No	Yes	Be prepared for unknown attacks, as well as known, with machine learning and built-in seclusion capabilities.
2FA and hardware security key integration	No	No	Yes	Integration with YubiKey and Google Titan.
OSSEC rules	1,000	1,000s	5,000	5x the number of OSSEC+ rules.
Threat Intelligence	No	No	Yes	Global community threat data supporting your protection and active response.
Visualization dashboards	No	Yes	Advanced	Several thousand additional rules and community threat intel data form the analytical basis for graphics.
Reporting and compliance	Not integrated	Not integrated	Yes	OpenSCAP, Center for Internet Security, PCI-DSS, HIPAA, GDPR.
SIEM	Not integrated	Not integrated	Yes	Out-of-the-box integration with Splunk, Arcsight, ELK, and others
Service support	No	No	Yes	Dedicated expertise to help you get the most out of your advanced OSSEC implementation.
Support for all major cloud platforms	No	No	Yes	AWS, Azure, GCP

## Atomic OSSEC Benefits

**Security agility and visibility.** Don't let visibility and policy over network and data computing get lost in the cloud. Your organization requires automatic and easily orchestrated detection and response capabilities because it's still your data (and your customers' data) that you have to protect to and from these clouds. Monitor, scan and visualize files and other digital assets and drill down using Atomiccorp OSSEC cross-platform security and SIEM capabilities.

**SecDevOps capabilities and expertise.** The ability to orchestrate, automate and respond with security (SOAR), early detection, vulnerability scanning, and risk management are all crucial pieces of the security component of best practice DevSecOps. These approaches, experience, and capabilities from Atomiccorp OSSEC enable a security operations center (SOC) to keep up with the business and network sides' pace of IT service delivery.

**Versatility.** Today's hybrid cloud reality requires securing and achieving compliance across a multiplatform computing landscape. Atomic OSSEC provides support for the major cloud providers and others. The cloud workload protection platform is prebuilt but customizable so your security can be as agile as your business.

**Compliance.** Atomic OSSEC provides strong real-time forensic file integrity monitoring. It includes the security and privacy safeguards, as well as CIS and SCAP benchmarks, needed to comply with standards such as PCI-DSS, HIPAA, Hitrust, NIST 800-53, NIST 800-171, CIS, and GDPR.

**Support of Different Roles.** Atomic OSSEC expands deployments to non-CLI users. These users can visually manage their areas of focus and leverage event search and reporting interfaces to get at and present data.

**High Availability and Disaster Recovery.** Atomic OSSEC delivers advantages when managing large environments via clustering functionality, with the management console enabling you to group data instances by type, group, division or any other criteria versus in one obscure, monolithic block of heterogeneous resources. This makes it easier for security managers and analysts to discern patterns, secure and control resources, and optimize performance, by equipment type, OS, container, application, etc. This cluster management facilitates high availability and disaster recovery.

**Cost Savings.** The Atomic OSSEC deployment saves money by reducing agent fatigue (product redundancy and confusion) on your servers and other network endpoints and cutting alarm fatigue in your SOC. Savings can also come in SIEM through upfront analysis and prioritization of incidents and the reduction of noise, including false positives. Last, Atomic OSSEC integrates with major cloud providers without bringing additional egress or API fees.