

Facilitate extended detection and response (XDR). The XDR is configured for you, with our secure cloud as the hub. You get rapid updates of intrusion detection and response functionality across your endpoints and cloud workloads. Partner with us to roll out versatile advanced security over existing infrastructure and in rapid development environments. Our advanced endpoint protection fortifies you with AV/antimalware protection, file integrity monitoring (FIM), vulnerability detection and management, crowdsourced global threat intelligence, rapid response, and security and compliance performance reporting for today's hybrid cloud computing architectures.

Gain strong support for securing your digital operations and business initiatives. Atomic OSSEC SaaS is a one-year renewable ongoing partnership for experienced implementation, configuration and security management across major clouds, applications, OSs, and your favorite legacy systems. The service includes software use, professional support and security engineering expertise. You don't have to configure the XDR features yourself. Reinforce security across growing IT and business services; be able to correlate all the logs from your servers, systems, and APIs and actively respond.

Repel malicious code and achieve compliance with advanced FIM. Powerful Atomiccorp FIM boosts strong visibility and control over your files, systems, applications, and code, so your data and systems are used for their intended purposes. Understand when file and system details have changed and rapidly respond if these changes are malicious or could lead to risk or data compliance violations. Atomic OSSEC SaaS brings deep file inspection and strong audit capabilities to fortify secure access control over private and personal data. Be able to detect and respond to threats and vulnerabilities through global threat intelligence and response automation. Protect private and sensitive data through FIM and other advanced file-level protections while addressing auditing and reporting requirements for standards and regulatory compliance (CIS, GDPR, HIPAA, JSIG, NIST 800-53 and 800-171, PCI DSS, and more).

Overcome technical challenges at a low cost point. Get timely answers to questions in a cost-effective manner. Our software development expertise will empower you to get better at configuring for secure access and optimum system performance using Linux, VMware, and apps such as Ping. We'll also help you to more easily scale, secure, and manage TCP/IP web channels and hosted web properties. Atomiccorp OSSEC SaaS provide cost advantages over on-premise (e.g., Atomic OSSEC SaaS is ½ the cost of running endpoint protection software from an on-prem hub), and you get dedicated expert configuration and custom inquiry support toward orchestrating the security to your endpoints and cloud workloads.

Triage smartly with security data aggregation. Atomic OSSEC SaaS leverages more than 400 out-of-the-box connectors to collect log data. The Atomic OSSEC engine analyzes, tags, and ranks security events. Atomic OSSEC parses this disparate data like a SIEM for active response, threat and pattern identification, vulnerability management, and systematic compliance and reporting, and it can also route critical events to any SIEM system or other operational monitoring system. All other log data can be sent to cost effective cold storage, with zero data loss.

Excel at log correlation and management. Monitoring the logs on a system for malicious activity is not enough. You need to be able to correlate events across multiple systems and be able analyze the activity for patterns and cross-system vulnerabilities. This is a crucial capability because coordinated attacks are not on a single system; they are network-wide, multi-stage, and across multiple systems. Atomic OSSEC SaaS powers thousands of advanced detection rules, including file integrity monitoring (FIM), global threat intelligence, and response automation that make sense of logs and SIEM data coming from myriad devices and software sources. It recognizes anomalies and seemingly disparate events as connected, groups those incidents, and the automated rules take action to stop the coordinated attack. Atomic OSSEC SaaS also captures log records and other artifacts for management and compliance reporting (PCI DSS, NIST 800-171).

Make sense of the data with security event analysis. Be able to expand deployments to non-CLI (non-command line interface) users with a graphical user interface (GUI). Capture information for analysts or for analysis by security and compliance stakeholders. These security stakeholders can leverage built-in event search and reporting interfaces, and visually manage agents, servers, FIM settings, vulnerability management reports, NIST, PCI DSS and other compliance checks, rollbacks, and integrations with third-party systems.

Stay in control with expert professional support. The Atomiccorp professional service team provides accredited credentials and service in CDPSE, CISA, CISSPA, ComTIA, CSX, and INFOSEC. We host the security hub and serve as an invested partner in your optimum installation, configuration and reconfiguration, log management, FIM, vulnerability management, pen testing, and more. You get detection, response, and reporting at a better use of staff-hours and overall cost than if you configure and manage security servers and agent updates yourself. We're available to start when you are to ensure ease of use, and provide expert configuration and training, with leading knowledge of OSSEC.

Figure 1. Atomic OSSEC FIM – Detect File and System Changes for Security and Compliance

Date/Time	Source	Level	Rule	Event
2022-08-01 03:13:12	app.atomiccorp.com	7	553	File /usr/bin/mysql_tinfo_to_sqi#prelink#par73f was deleted.
2022-08-01 03:13:12	app.atomiccorp.com	5	554	File /usr/bin/mysql_tinfo_to_sqi#prelink#par73f was added.
2022-08-01 03:13:12	app.atomiccorp.com	7	553	File /usr/bin/mysql_plugin#prelink#0vrm2ky was deleted.
2022-08-01 03:13:12	app.atomiccorp.com	7	560	File /usr/bin/mysql_plugin#prelink#0vrm2ky checksum changed. Size changed fra...
2022-08-01 03:13:12	app.atomiccorp.com	5	554	File /usr/bin/mysql_plugin#prelink#0vrm2ky was added.
2022-08-01 03:13:12	app.atomiccorp.com	7	553	File /usr/bin/mysiamog#prelink#Af8Kcj was deleted.
2022-08-01 03:13:12	app.atomiccorp.com	5	554	File /usr/bin/mysiamog#prelink#Af8Kcj was added.
2022-08-01 03:13:12	app.atomiccorp.com	7	553	File /usr/bin/mysiamochk#prelink#2g7um8 was deleted.
2022-08-01 03:13:12	app.atomiccorp.com	5	554	File /usr/bin/mysiamochk#prelink#2g7um8 was added.
2022-08-01 03:13:11	app.atomiccorp.com	7	553	File /usr/bin/resolveip#prelink#L1YQj was deleted.
2022-08-01 03:13:11	app.atomiccorp.com	5	554	File /usr/bin/resolveip#prelink#L1YQj was added.
2022-08-01 03:13:11	app.atomiccorp.com	7	553	File /usr/bin/perror#prelink#gC1a1W3 was deleted.
2022-08-01 03:13:11	app.atomiccorp.com	5	554	File /usr/bin/perror#prelink#gC1a1W3 was added.
2022-08-01 03:13:10	app.atomiccorp.com	7	553	File /usr/bin/mysql_upgrade#prelink#Bm2wM was deleted.

[Atomic OSSEC SaaS](#) is a 1-year commitment with a monthly subscription price based on the number of endpoints connected. Find out more about the Atomiccorp OSSEC centrally managed XDR solution.

Get a demo. Take advantage of an Atomic OSSEC [free trial](#) period.

Get FedRAMP certification and compliance in your hosted data facilities. Atomiccorp OSSEC SaaS comes in a standard service, or in a FedRAMP SOC 2. Talk with us about the high compliance [Atomic OSSEC SaaS](#) offering through Atomiccorp's certified managed security provider partners.

Contact [Sales](#) with questions about pricing.