



ATOMICORP



Solution Overview

Atomic Protector

Atomic Protector for endpoint security and cloud workload protection

Once cyberattacks breach an endpoint they can spread and do deeper damage, so an understanding of what 'endpoint' security entails is more critical today than ever. You need to establish your perimeter, know what's connected to what, and which pathways are vulnerable to widely used lateral attacks, which spread malware and deceptive instructions from one endpoint to another.

Atomic Protector, a cloud workload protection platform, provides a wide and defense-in-depth approach where you're not only securing your perimeter, but also shoring up your lateral portals and processes.

Why is the cloud so important in endpoint security? The cloud is the ubiquitous piece that rounds out endpoint and edge access security, which is particularly important in today's decentralized and distributed workforces. A cloud protection platform is a workload-centric security protection solution category in which the most comprehensive provide vitally needed agent-based capabilities. According to Gartner, the solution type addresses "the unique requirements of server workload protection in modern hybrid data center architectures that span on-premises, physical and virtual machines (VMs) and multiple public cloud infrastructure as a service (IaaS) environments." Containers, too, we might add.

Atomic Protector for Crucial System Protection and Compliance

Endpoint and cloud workload protection platform Atomic Protector provides advanced security and tools for comprehensive endpoint security and lateral protection that empower you to:

1. Know your assets. How can you protect something if you don't know it exists or what its security state is? The answer is security software agents and network registration that discover your assets and quickly assess them for any security or compliance issues. Gain control over access and privileges. Extend visibility, access and privilege gradually with the push of a button.

2. Inspect endpoints in real time with system and file integrity monitoring. Controls can fail due to user mistakes, insider threats, superior adversaries, zero days, etc. Being able to detect when a control fails is necessary to a robust and correct response. A good tool should monitor more than just the files and data stores containing sensitive data. It should also monitor configuration information and software native to the operating system, like registries, applications, drivers, and libraries, as well as infrastructure components such as the configuration of network and cloud devices, web servers, and firewalls. All this should be monitored in real-time.

3. Protect your endpoints and cloud workloads. Endpoints are servers, laptops, routers, firewalls, VMs, containers and more. Defend these assets with end-user protections such as strong malware protection, device hardening, multi-factor authentication (MFA), intrusion detection and prevention, and vulnerability shielding. Realize that endpoint protection must include cloud workload protection. A cloud workload protection platform scans hybrid cloud data center architectures, including on-premises, physical and virtual machines (VMs), public cloud IaaS, and containers, to secure processing and more easily segment the workload according to security and law.

4. Secure access control with protected servers. How do attacks spread laterally? They compromise a less important system and use that to hop to a more important one. Don't let default security options allow bad actors to beat you. Easily configure your server environment with the security to prevent spread. Deploy a defense-in-depth strategy that protects your endpoints from lateral access attacks.

5. SOAR with active response. Be able to identify infected endpoints and isolate them rapidly, without manual intervention. Inject advanced security rules into your computing environment and employ rules that are flexible enough to allow authentic access but that prohibit rapid privilege escalation or abuse. Once the bad guys have gained a foothold, they look for links to further exploit. Detect these vulnerable desktops, laptops, and end users and automatically protect them.

6. Prevent DoS attacks. Stop service on assets where a suspicious volume of activity is being requested. When a threshold is reached, the agent quarantines the end device. Get alarms so you can look into the transactions without first sustaining a knockout blow.

7. View alerts of unusual system and network activity in an integrated SIEM console. Display data in visualizations on a management console that allows you to drill in, isolate and respond. Use it for security performance, for compliance, for reporting, for forensic analysis, and more.

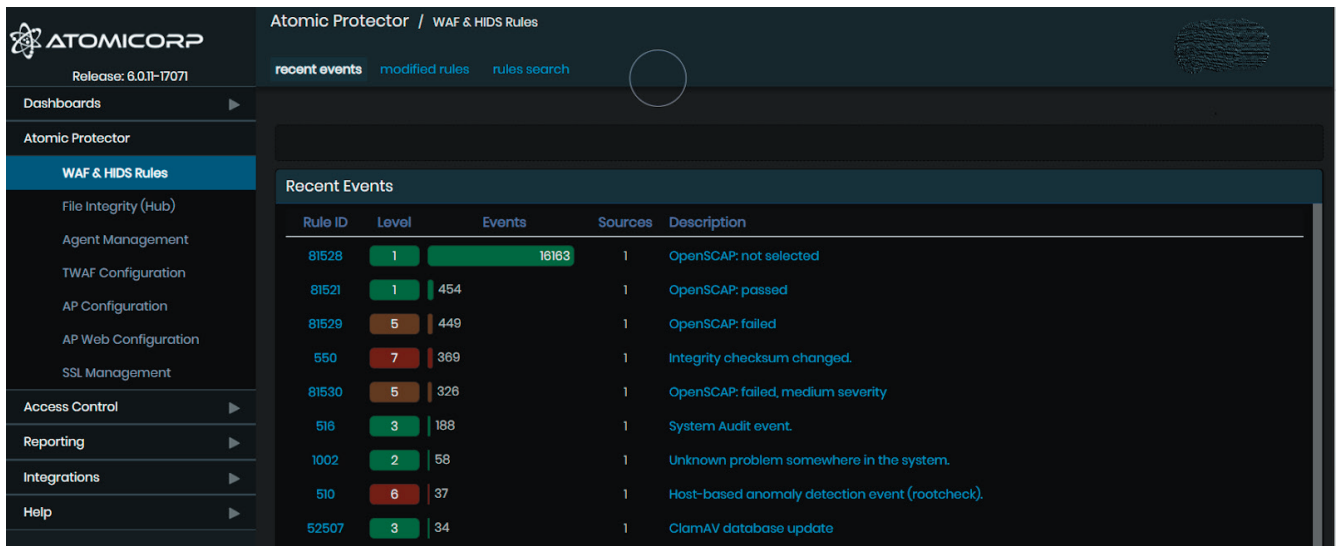
Atomic Protector, previously "Atomic Secured Linux (ASL)," is the most widely distributed full-stack security solution for Linux servers today. Atomiccorp customers withstand 65 billion daily attacks. This volume has become the norm because attackers have proliferated and many now employ automation. The only way to combat this escalation is to automate defense. That is why Atomic Protector includes everything from a secure kernel for your host Linux OS to intrusion detection and prevention systems and everything in between.

Atomic Protector Capabilities

Atomic Protector relieves the complexity of managing holistic endpoint security through intelligence and automation, and is ideal for managed security service providers (MSSPs) who offer software as a service. It provides:

- » Workstation protection
- » File integrity monitoring
- » Vulnerability scanning and management
- » SOAR- and DevSecOps-inspired simple and secure automation
- » Compliance, reporting and analysis
- » Exploit prevention
- » Memory protection
- » System hardening
- » Application control
- » Cloud workload protection and microsegmentation
- » Supports Linux, Mac OS, Windows.
- » Additional features

Figure 1. Intrusion detection across devices and by device state



The screenshot shows the Atomic Protector interface for WAF & HIDS Rules. The left sidebar contains navigation options: Dashboards, Atomic Protector (with sub-items: WAF & HIDS Rules, File Integrity (Hub), Agent Management, TWAF Configuration, AP Configuration, AP Web Configuration, SSL Management), Access Control, Reporting, Integrations, and Help. The main content area displays a 'Recent Events' table with columns for Rule ID, Level, Events, Sources, and Description.

Rule ID	Level	Events	Sources	Description
81528	1	16183	1	OpenSCAP: not selected
81521	1	454	1	OpenSCAP: passed
81529	5	449	1	OpenSCAP: failed
550	7	369	1	Integrity checksum changed.
81530	5	326	1	OpenSCAP: failed, medium severity
516	3	188	1	System Audit event.
1002	2	58	1	Unknown problem somewhere in the system.
510	6	37	1	Host-based anomaly detection event (rootcheck).
52507	3	34	1	ClamAV database update

With Atomic Protector, you can monitor and control time-based activities, suspicious activities, and location-based events, honeypot for testing, and even trick the bad guys with fake responses to make them think their attacks have failed. Atomic Protector dynamically defangs attacks. This type of defense traditionally involved forensics, but forensics takes time. Our method strips malicious code as it's being sent to the user, without the risks associated with traditional quarantining or defanging solutions.

You don't need to put a firewall in front of every web server. The system detects by itself, protects itself, and protects serving endpoints. You want to stop an attack and let the security team know about it. Automation has to occur for this to happen.

It's time to automate defense against automated attacks, and reduce the time spent troubleshooting security incidents and preventing hard-to-detect attacks.

Hosting providers, enterprises and midsize businesses all use Atomic Protector to automate their defenses, reduce the time spent troubleshooting security incidents, and prevent and stop the spread of these increasingly sophisticated attacks. Isn't it time to evaluate Atomic Protector?

Atomiccorp Benefits

Get Comprehensive Security in a Single Agent

- » A single self-contained on-premise security solution that incorporates file integrity monitoring, policy enforcement, system hardening, vulnerability scanning, intrusion detection, log management, and more.
- » Real-time automated compliance alerting and enforcement.
- » Monitoring millions of files distributed across tens of thousands of systems in real-time with full tracking and capture of system file changes.

Streamline Compliance Monitoring And Remediation

- » Support for all major compliance protocols including PCI-DSS, CMMC, NIST, HIPAA, GDPR, JSIG, and more.
- » Automatically addresses over 100 PCI DSS 3.2 technical requirements.
- » Continuous compliance monitoring and remediation ensure relief from costly non-compliance fines.

Automate Intrusion Prevention and Adaptive Security

- » Adaptive security based on global real-time threat intelligence.
- » Automatically interfaces with every open source software provisioning, configuration management and application deployment tool including Puppet, Chef and Ansible.
- » Automated protection of cloud workloads ensures that DevOps can operate at the speed required to deploy new, valuable features.

Simplify Security Operations While Reducing SOC Costs

- » Continuous compliance monitoring and automated compliance remediation.
- » SIEM log filtering ensures that only actionable SIEM alerts are generated, making cyber security analysts and engineers more effective and efficient.
- » Reduces SIEM costs by up to 80%, dramatically reducing SOC costs without sacrificing fidelity.

Run It Anywhere

- » Automated security that provides detection, protection and analytics for any environment (Linux, Microsoft Windows, OSX, FreeBSD, OpenBSD, AIX, Solaris, etc.).
- » Provides automated protection for workloads in multi-cloud, on-premise or hybrid environments, eliminating the need for multiple solutions.
- » Enables system security for legacy systems including Solaris, HP-UX, and IBM AIX.

Figure 2. PCI-DSS Compliance Reporting

