Wazuh Case Study

Groupon deploys Wazuh to protect and monitor Amazon Web Services (AWS)

Groupon is an experiences marketplace where consumers discover fun things to do and local businesses thrive. It offers customers a wide selection of experiences at great values, and merchants a reach to millions of consumers around the world.

For Groupon, security is vital. Its security team has been operating a full stack of security products to protect and monitor Amazon Web Services (AWS) and enhancing the security of the company.

Martin Petracca, the Information Technology Security Manager at Groupon, was seeking an open source solution that could provide high customization and scalability in order to meet their needs.

After conducting an extensive evaluation of security solutions, Groupon selected the Wazuh platform. “Wazuh is the most comprehensive open source security solution, providing a wide range of capabilities and integrations with other products and technologies like AWS and VirusTotal,”, said Martin.

In 2018 the Groupon security team started using Wazuh, gaining visibility and improving their security metrics while reducing costs. Furthermore, Wazuh has become their intrusion detection system of choice to comply with the Payment Card Industry Data Security Standard (PCI DSS).

> “These wonderful open source tools, such as Wazuh, allow us to obtain telemetry from multiple technologies, correlate events, and run investigations from a central management interface. Their customization capabilities and seamless integration with various tools are among the key advantages they offer.
>
> Martín Petracca,
> Information Technology Security Manager”

The challenge

A key challenge for Groupon has been protecting and monitoring a very high volume of data from Amazon Web Services without incurring prohibitive costs and allowing the solution to scale as necessary. The Groupon team sought clear security metrics, with good visibility and real-time monitoring in case of security incidents.

To accomplish this, they searched for an open source SIEM solution that allowed integration with other tools, particularly AWS. In Martin’s words, “there are multiple variables to verify before adopting an open source software, such as the existence of an active repository, the possibility of high customization, and professional support”.

Martín Petracca
IT Security Manager
Groupon

"Wazuh is the most comprehensive open source security solution, as it provides a wide range of capabilities, as well as integrations with other products and technologies."

Key benefits

- Easy integration with other tools
- Increased security metrics
- Enhanced visibility
- Support
- Scalability
- Reduced Costs

Groupon deploys Wazuh to protect and monitor Amazon Web Services (AWS)

Solutions

Wazuh is a free, open source, and enterprise-ready security monitoring solution that offers integration with multiple tools.

> “The integration of new solutions and its central monitoring tool makes Wazuh the perfect fit.
>
> Martín Petracca,
> Information Technology Security Manager”

Furthermore, due to their scope of work, they required a solution that would allow high scalability, since “the number of agents needed could increase rapidly”.

For all these reasons they opted for Wazuh, which also allowed them to save costs, as “usually, SIEMs and other commercial cybersecurity products are very expensive”.

As a result, the Groupon security team has been able to achieve their goal of protecting and monitoring AWS services and improving their environment visibility with the Wazuh monitoring options, and all at a minimal cost.

Beyond this, Martin remarks that “not paying for a license is not the biggest advantage of using an open-source tool.
It’s the customization, no vendor lock-in, source code available, scaling, community & support, and more.”

Along with Wazuh, Groupon chose other open source tools such as ELK, AWS native services, Prowler, and Cloud Custodian to achieve their goal, leveraging the high integration potential of Wazuh.

Top Wazuh capabilities used by Groupon

- Regulatory Compliance
- Vulnerability Detection
- File Integrity Monitoring
- Log Data Analysis
- Intrusion Detection

About Wazuh

Wazuh is a free, open source, and enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response, and compliance. Wazuh protects workloads across on-premise, virtualized, containerized, and cloud-based environments. Used by thousands of organizations around the world, from small businesses to large enterprises, the Wazuh solution is used to collect, aggregate, index and analyze security data, helping organizations detect intrusions, threats, and behavioral anomalies.

Wazuh consists of an endpoint security agent, deployed to monitored systems, and an intelligent management server, which provides the threat intelligence vand performs the data analysis.

As cyber threats are becoming more sophisticated, real-time monitoring and security analysis are needed for fast threat detection and remediation. Our lightweight agent provides the necessary monitoring and response capabilities, while our server component provides the security intelligence and performs data analysis.