Building an Affordable Security Operations Model That Is Audit-Ready

Cobus Burgers
Managing Director

18 February 2026

netcb ForumX

Why is it necessary to build a SOC?

Building a cost-effective SOC (Security Operations Center) framework for audit readiness is critical because regulatory and legal landscapes have shifted in such a way that security is no longer just a technical best practice — it's a compliance obligation.

The Legal Context

- Legal Liability and Duty of Care
  - Organisations have a legal obligation to safeguard sensitive data (personal, financial, health, government).
  - Failure to implement reasonable cybersecurity controls — even citing “budget constraints” — can be interpreted as negligence in a court of law.
  - A SOC framework demonstrates due diligence and duty of care, protecting against lawsuits, penalties, and reputational damage.

- Regulatory Mandates
  - Most modern regulations explicitly require security monitoring, logging, and incident response — all SOC functions. Examples:
    - POPIA (South Africa) → requires responsible parties to implement appropriate, reasonable technical and organisational measures to secure personal information. Audit readiness proves compliance.
    - GDPR (EU) → mandates data breach detection, reporting, and accountability. A SOC ensures continuous monitoring and audit trails.
    - HIPAA (US) → demands audit controls and activity review for healthcare data.
    - PCI DSS (Payment Card Industry) → requires log management, intrusion detection, and monitoring, all core SOC functions.
    - ISO 27001 & NIST frameworks → stress audit readiness, evidence-based monitoring, and incident handling.
  - Without a SOC, organisations risk non-compliance fines running into millions of dollars.

The Legal Context

- Audit Readiness = Compliance Evidence
  - Regulators and auditors don’t just want “policies on paper”; they want evidence of ongoing monitoring, detection, and response.
  - A SOC provides real-time logs, incident reports, and remediation evidence — the kind of audit trail regulators demand.
  - Being audit-ready means an organisation avoids reactive, costly fire drills every time an audit comes around.

- Regulatory Focus on Proportionality and Cost-Effectiveness
  - Many laws (e.g., POPIA, GDPR, ISO 27001) phrase security requirements as “reasonable and appropriate measures.”
  - A cost-effective SOC shows that the organisation is applying proportional controls — scaling security to risk and budget — which auditors and regulators recognise as a compliant stance.
  - Over-spending isn’t sustainable; under-spending invites fines. Cost-effectiveness ensures regulatory balance.

The Legal Context

- Incident Reporting and Legal Time-frames
  - GDPR → 72 hours to report a breach.
  - POPIA → "as soon as reasonably possible."
  - Without SOC monitoring and automation, meeting these legal deadlines is impossible.
  - Audit-ready SOC frameworks ensure organisations prove compliance with incident reporting obligations.

- Board Accountability & Personal Liability
  - In many jurisdictions, boards and executives are personally liable for compliance failures (e.g., directors under POPIA, GDPR, Sarbanes-Oxley).
  - A SOC provides the evidence executives need to demonstrate compliance efforts in court or during regulatory review.

The Bottom Line

A cost-effective SOC framework is critical not just for defending against cyber threats, but for meeting legal and regulatory obligations, avoiding fines, and demonstrating compliance during audits. It turns cybersecurity from a "best effort" into a provable, defensible compliance posture — protecting the organisation legally, financially, and reputationally.

Introducing Wazuh – The foundational pillar of your SOC

Security Analytics

Intrusion Detection

Log Data Analysis

File Integrity Monitoring

Vulnerability Detection

Configuration Assessment

Incident Response

Regulatory Compliance

Cloud Security

Containers Security

Endpoint Detection and Response (XDR)

Combines anomaly and signature-based technologies to detect intrusions or software misuse.
Wazuh is also used to monitor user activities, assess system configuration and detect vulnerabilities.

Compliance & Security Management

Wazuh provides necessary security controls, required by standards such as PCI DSS, HIPAA, GDPR, GPG13, NIST, and others.

SIEM I Log Management

Wazuh is used to collect, analyze and correlate data, being able to deliver threat detection, compliance management, and incident response capabilities.

Wazuh facilitates Compliance

- Centralised Log Collection & Audit Trail
  - What regulators require: Continuous recording of security-relevant events, immutable logs, and auditability.
  - How Wazuh delivers:
    - Collects logs from servers, endpoints, firewalls, cloud services, and applications.
    - Stores and correlates events in a central index (Elastic/OpenSearch).
    - Tamper-proofing ensures evidence stands up in an audit.
  - Regulatory tie-ins:
    - POPIA, GDPR, HIPAA, PCI DSS, ISO 27001 → all require audit logging and retention.

- Vulnerability Detection
  - What regulators require: Proactive risk management and patching processes.
  - How Wazuh delivers:
    - Built-in vulnerability scanner compares assets against known CVEs.
    - Integrates with external feeds for real-time updates.
    - Prioritises risk remediation.
  - Regulatory tie-ins:
    - ISO 27001 (A.12, A.14), NIST, PCI DSS, HIPAA → require vulnerability management.

- File Integrity Monitoring (FIM)
  - What regulators require: Detection of unauthorised data or system changes.
  - How Wazuh delivers:
    - Tracks file changes in OS, databases, apps, and critical directories.
    - Alerts when sensitive data or system configurations are modified.
  - Regulatory tie-ins:
    - PCI DSS explicitly mandates FIM.
    - HIPAA, GDPR, POPIA require data integrity assurance.

- Intrusion Detection (IDS) & Threat Intelligence
  - What regulators require: Continuous monitoring for unauthorised access attempts.
  - How Wazuh delivers:
    - Network-based IDS rules + endpoint anomaly detection.
    - Threat intel feeds to correlate malicious IOCs.
    - Detection of brute force, privilege escalation, malware behaviour.
  - Regulatory tie-ins:
    - POPIA, GDPR, HIPAA, PCI DSS → all require monitoring for suspicious activity.

Wazuh facilitates Compliance

- Incident Response & Automation
  - What regulators require: Demonstrated capability to respond and contain breaches quickly.
  - How Wazuh delivers:
    - Active responses (auto-block IPs, quarantine compromised hosts, kill malicious processes).
    - Integration with SOAR/SIEM tools to automate playbooks.
    - Full incident timeline for audit evidence.
- Regulatory tie-ins:
  - GDPR's 72-hour breach reporting, HIPAA breach notification, POPIA "reasonable steps" standard.

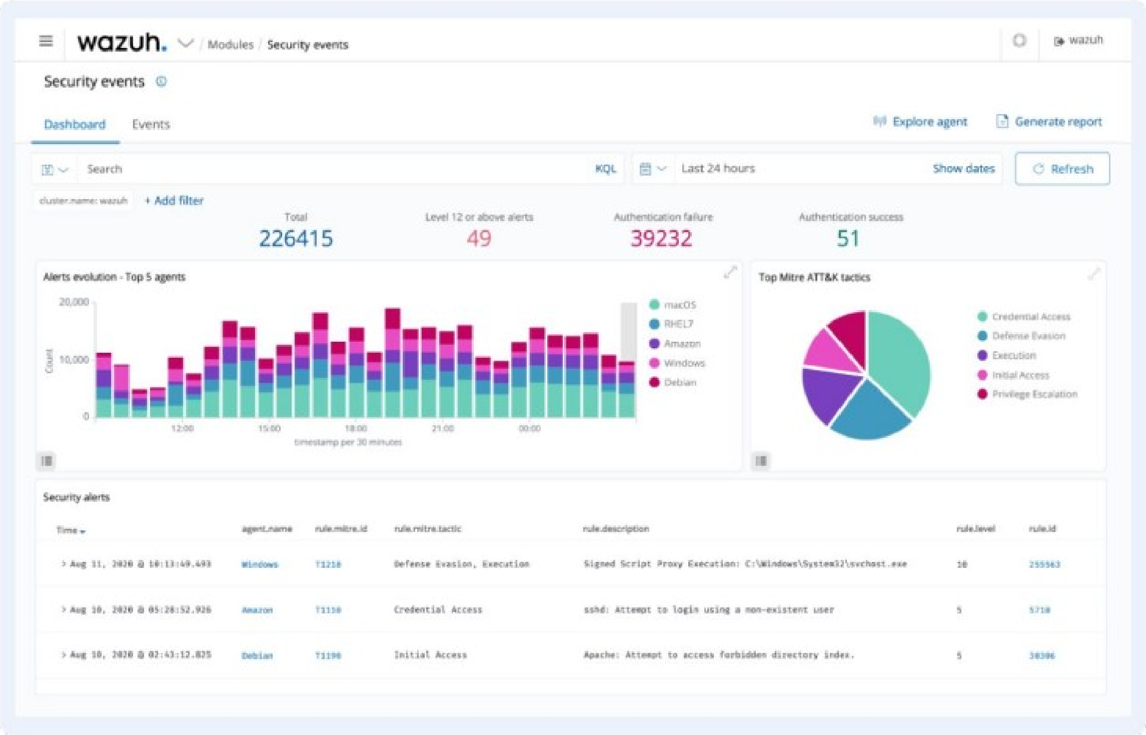
- Compliance Modules & Reporting
  - What regulators require: Proof of compliance during audits.
  - How Wazuh delivers:
    - Prebuilt dashboards and rulesets for PCI DSS, HIPAA, GDPR, NIST, ISO 27001.
    - Generates compliance-focused reports with mapped controls.
    - Provides evidence logs that can be exported directly for auditors.
- Regulatory tie-ins:
  - All major frameworks emphasise "documented evidence" → Wazuh produces exactly that.

- Cost-Effectiveness & SOC Enablement
  - Why this matters legally: Laws require "reasonable and appropriate" controls — not overspending on tools.
  - How Wazuh enables SOC:
    - Open-source core = cost-effective, scales horizontally.
    - Supports hybrid deployments (on-prem + cloud).
    - Forms the backbone for log management, threat detection, and compliance — the three pillars of a SOC.
    - Can integrate with other SIEM, SOAR, and ticketing systems for a full SOC stack.

Wazuh maps directly to regulatory clauses (logging, monitoring, integrity, vulnerability management, incident response, reporting). It provides the evidence auditors demand and the capabilities regulators mandate.

That's why it's often the first foundational layer of a cost-effective SOC — once Wazuh is in place, you can bolt on SIEM dashboards, SOAR automation, and incident response workflows without reinventing the wheel.

Security Analytics



Security events

cluster.name: wazuh

Total	Level 12 or above alerts	Authentication failure	Authentication success
226415	49	39232	51

Security alerts

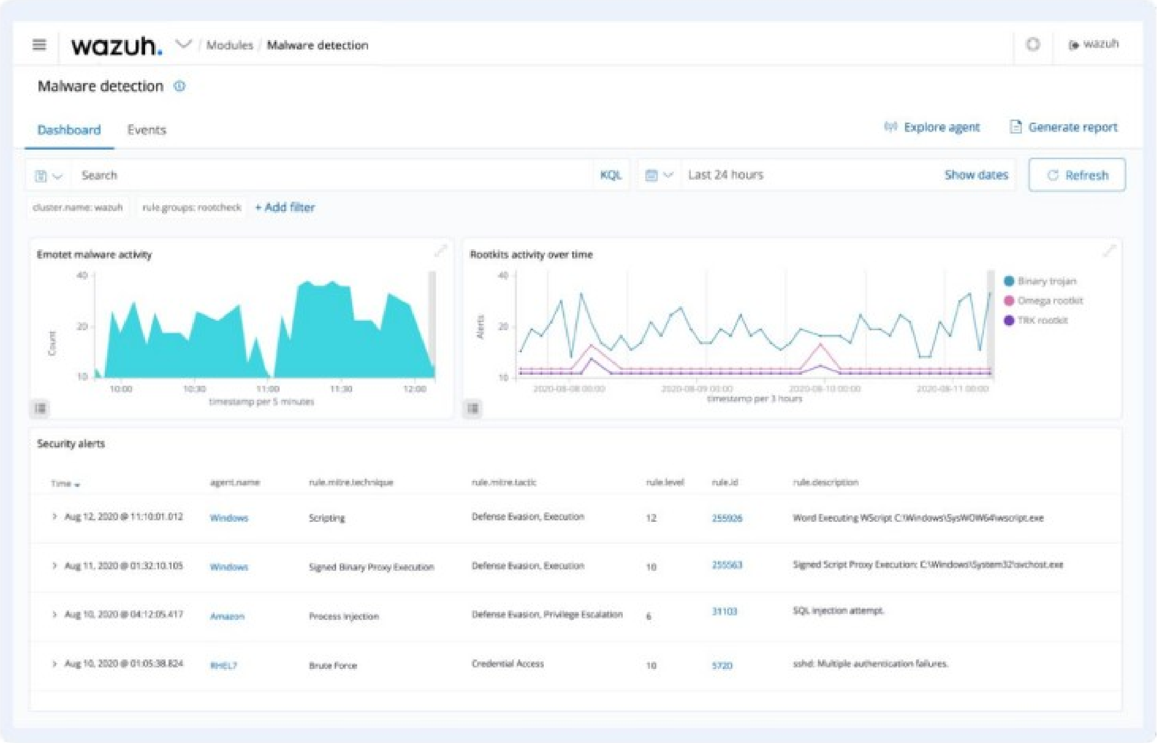
Time	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level	rule.id
Aug 11, 2020 @ 10:13:49.493	Windows	T1216	Defense Evasion, Execution	Signed Script Proxy Execution: C:\Windows\System32\svchost.exe	10	255563
Aug 10, 2020 @ 05:28:52.926	Amazon	T1110	Credential Access	sshd: Attempt to login using a non-existent user	5	5710
Aug 10, 2020 @ 02:43:12.825	Debian	T1190	Initial Access	Apache: Attempt to access forbidden directory index.	5	30306

Wazuh is used to collect, aggregate, index and analyze security data, helping organizations detect intrusions, threats, and behavioral anomalies.

Our lightweight agent provides the necessary monitoring and response capabilities, while our server component provides the security intelligence and performs data analysis.

As cyber threats are becoming more sophisticated, real-time monitoring and security analysis are needed for fast threat detection and remediation.

Intrusion Detection



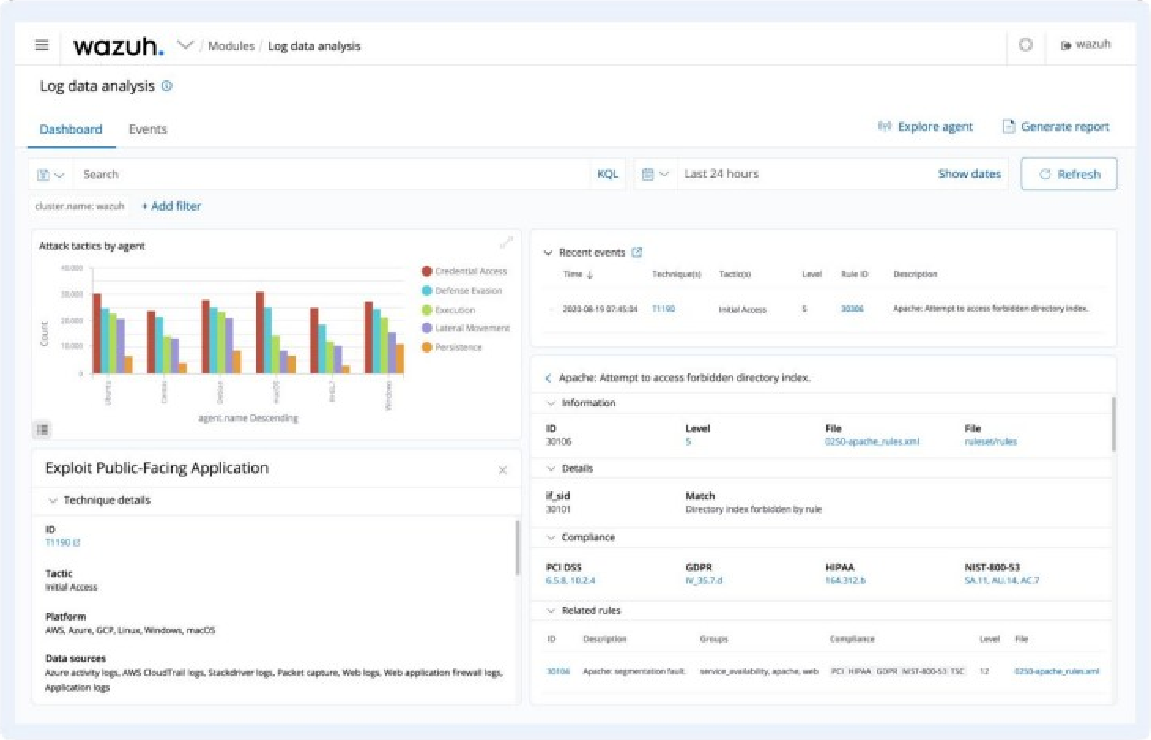
Security alerts

Time	agent.name	rule.mitre.technique	rule.mitre.tactic	rule.level	rule.id	rule.description
Aug 12, 2020 @ 11:10:01.012	Windows	Scripting	Defense Evasion, Execution	12	255926	Word Executing WScript C:\Windows\SysWOW64\wscript.exe
Aug 11, 2020 @ 01:32:10.105	Windows	Signed Binary Proxy Execution	Defense Evasion, Execution	10	255563	Signed Script Proxy Execution: C:\Windows\System32\svchost.exe
Aug 10, 2020 @ 04:12:05.417	Amazon	Process Injection	Defense Evasion, Privilege Escalation	6	31103	SQL injection attempt.
Aug 10, 2020 @ 01:05:38.824	RHEL7	Brute Force	Credential Access	10	5720	sshd: Multiple authentication failures.

Wazuh agents scan the monitored systems looking for malware, rootkits, and suspicious anomalies. They detect hidden files, cloaked processes, or unregistered network listeners, as well as inconsistencies in system call responses.

In addition to agent capabilities, the server component uses a signature-based approach to intrusion detection, using its regular expression engine to analyze collected log data and look for indicators of compromise.

Log Data Analysis



Log data analysis

cluster.name: wazuh

Recent events

Time ↓	Technique(s)	Tactic(s)	Level	Rule ID	Description
2023-08-19 07:45:34	T1190	Initial Access	5	30306	Apache: Attempt to access forbidden directory index.

Apache: Attempt to access forbidden directory index.

Information

ID	Level	File	File
30106	5	0250-apache_rules.xml	ruleset/rules

Details

if_sid	Match
30101	Directory index forbidden by rule

Compliance

PCI DSS	GDPR	HIPAA	NIST-800-53
6.5.8, 10.2.4	IV_35.7.d	164.312.b	SA.11, AU.14, AC.7

Related rules

ID	Description	Groups	Compliance	Level	File
30104	Apache: segmentation fault.	service_availability, apache, web	PCI HIPAA GDPR NIST-800-53 TSC	12	0250-apache_rules.xml

Exploit Public-Facing Application

Technique details

ID
T1190

Tactic
Initial Access

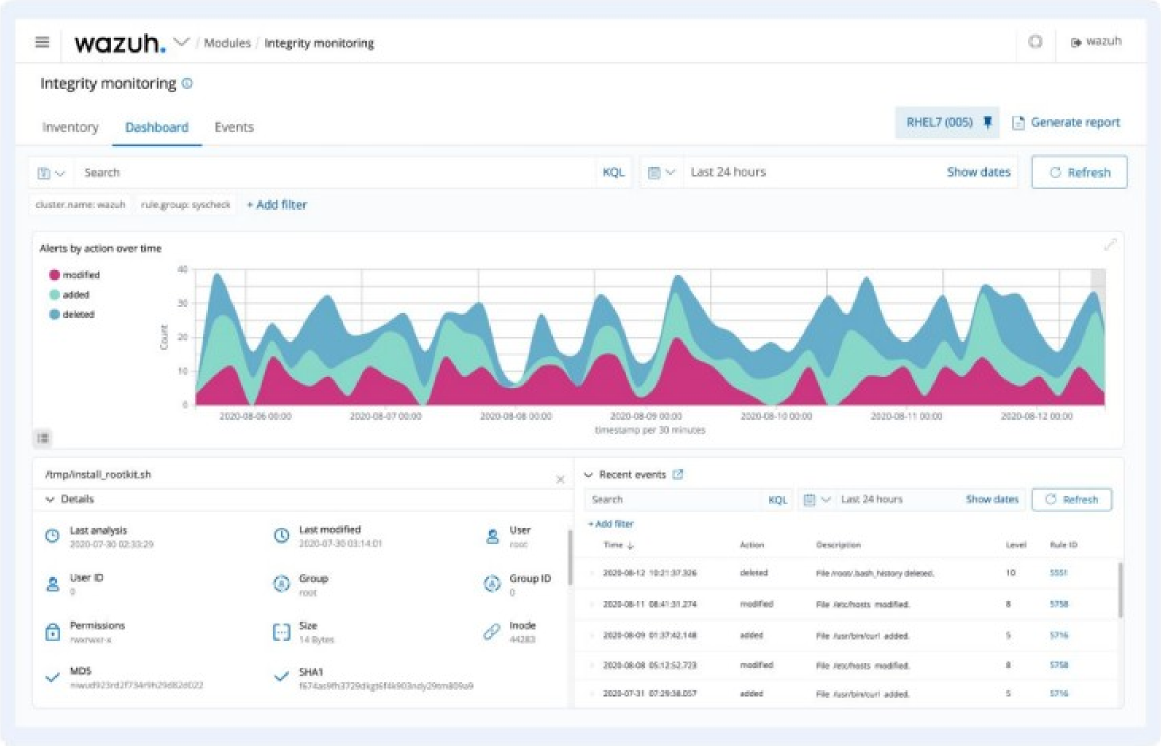
Platform
AWS, Azure, GCP, Linux, Windows, macOS

Data sources
Azure activity logs, AWS CloudTrail logs, Stackdriver logs, Packet capture, Web logs, Web application firewall logs, Application logs

Wazuh agents read operating system and application logs, and securely forward them to a central manager for rule-based analysis and storage.

The Wazuh rules grant awareness of application or system errors, misconfigurations, attempted and/or successful malicious activities, policy violations, and a variety of other security and operational issues.

File Integrity Monitoring



/tmp/install_rootkit.sh

Details

Last analysis: 2020-07-30 02:33:29
Last modified: 2020-07-30 03:14:01
User: root
User ID: 0
Group: root
Group ID: 0
Permissions: rwxrwxr-x
Size: 14 Bytes
Inode: 44283
MD5: niwudf923rd2f734r9h29d82d022
SHA1: f674as9fh3729dkgs6f4k903ndy29m809a9

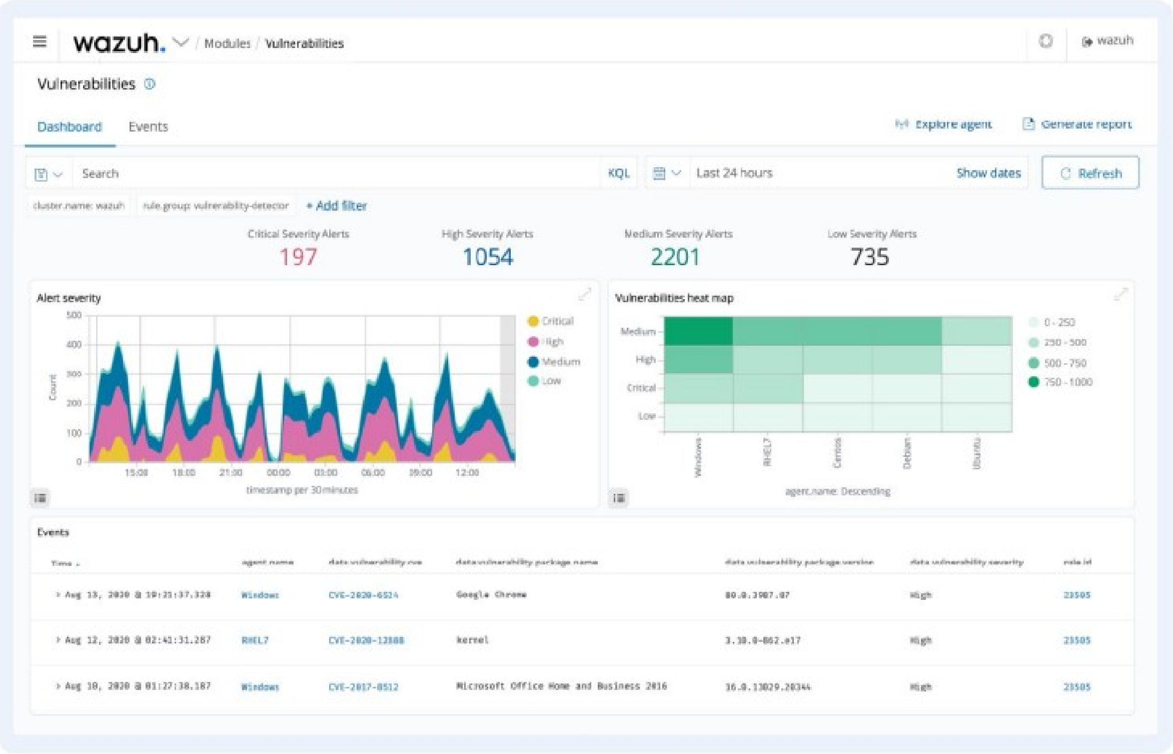
Recent events

Time ↓	Action	Description	Level	Rule ID
2020-08-12 10:21:37.326	deleted	File /root/.bash_history deleted.	10	5551
2020-08-11 08:41:31.274	modified	File /etc/hosts modified.	8	5758
2020-08-09 01:37:42.148	added	File /usr/bin/curl added.	5	5716
2020-08-08 05:12:52.723	modified	File /etc/hosts modified.	8	5758
2020-07-31 07:29:38.057	added	File /usr/bin/curl added.	5	5716

Wazuh monitors the file system, identifying changes in content, permissions, ownership, and attributes of files that you need to keep an eye on. In addition, it natively identifies users and applications used to create or modify files.

File integrity monitoring capabilities can be used in combination with threat intelligence to identify threats or compromised hosts.
In addition, several regulatory compliance standards, such as PCI DSS, require it.

Vulnerability Detection



Critical Severity Alerts	High Severity Alerts	Medium Severity Alerts	Low Severity Alerts
197	1054	2201	735

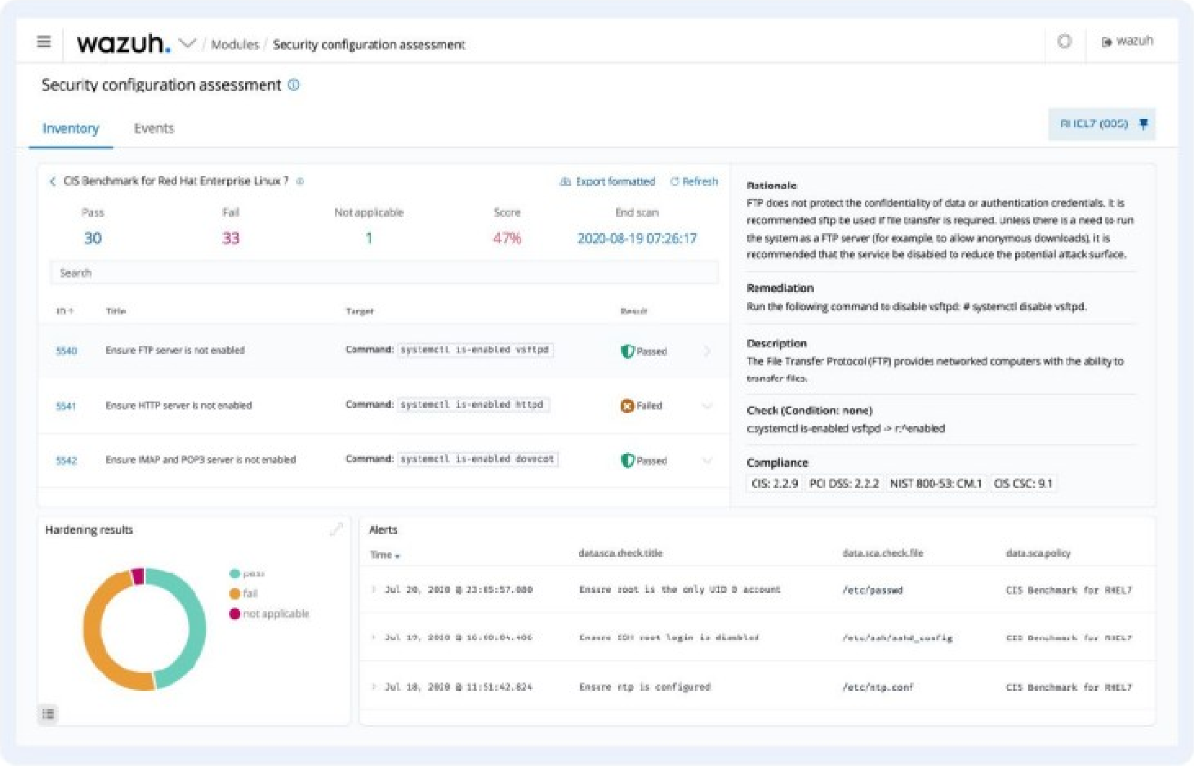
Events

Time ↓	agent.name	data.vulnerability.cve	data.vulnerability.package.name	data.vulnerability.package.version	data.vulnerability.severity	rule.id
› Aug 13, 2020 @ 19:21:37.328	Windows	CVE-2020-6524	Google Chrome	80.0.3987.87	High	23505
› Aug 12, 2020 @ 02:41:31.287	RHEL7	CVE-2020-12888	kernel	3.10.0-862.el7	High	23505
› Aug 10, 2020 @ 01:27:38.187	Windows	CVE-2017-0512	Microsoft Office Home and Business 2016	16.0.13029.20344	High	23505

Wazuh agents pull software inventory data and send this information to the server, where it is correlated with continuously updated CVE (Common Vulnerabilities and Exposure) databases, in order to identify well-known vulnerable software.

Automated vulnerability assessment helps you find the weak spots in your critical assets and take corrective action before attackers exploit them to sabotage your business or steal confidential data.

Configuration Assessment



Security configuration assessment ⓘ

‹ CIS Benchmark for Red Hat Enterprise Linux 7 ⓘ

Pass	Fail	Not applicable	Score	End scan
30	33	1	47%	2020-08-19 07:26:17

ID ↑	Title	Target	Result
5540	Ensure FTP server is not enabled	Command: `systemctl is-enabled vsftpd`	Passed
5541	Ensure HTTP server is not enabled	Command: `systemctl is-enabled httpd`	Failed
5542	Ensure IMAP and POP3 server is not enabled	Command: `systemctl is-enabled dovecot`	Passed

Rationale
FTP does not protect the confidentiality of data or authentication credentials. It is recommended sftp be used if file transfer is required. Unless there is a need to run the system as a FTP server (for example, to allow anonymous downloads), it is recommended that the service be disabled to reduce the potential attack surface.

Remediation
Run the following command to disable vsftpd: # systemctl disable vsftpd.

Description
The File Transfer Protocol(FTP) provides networked computers with the ability to transfer files.

Check (Condition: none)
c:systemctl is-enabled vsftpd -> r:^enabled

Compliance
CIS: 2.2.9 | PCI DSS: 2.2.2 | NIST 800-53: CM.1 | CIS CSC: 9.1

Hardening results

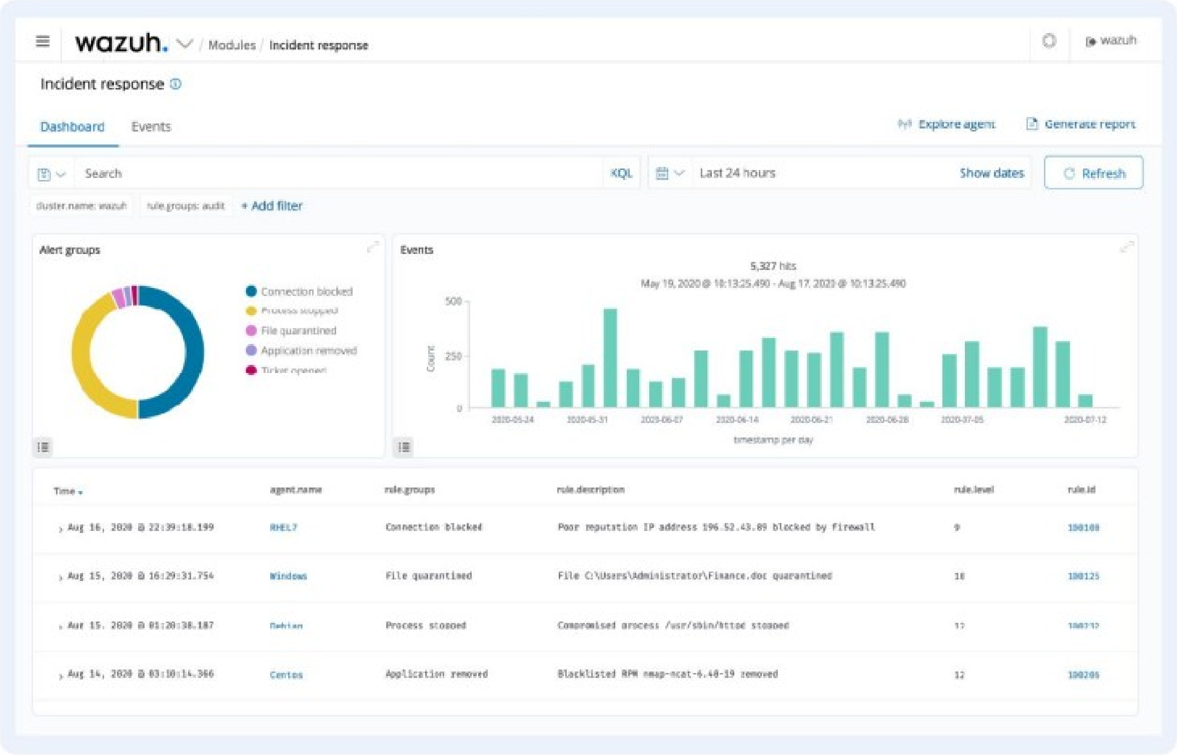
Alerts

Time ▾	datasca.check.title	data.sca.check.file	data.sca.policy
› Jul 20, 2020 @ 23:05:57.080	Ensure root is the only UID 0 account	/etc/passwd	CIS Benchmark for RHEL7
› Jul 19, 2020 @ 16:00:04.406	Ensure SSH root login is disabled	/etc/ssh/sshd_config	CIS Benchmark for RHEL7
› Jul 18, 2020 @ 11:51:42.624	Ensure ntp is configured	/etc/ntp.conf	CIS Benchmark for RHEL7

Wazuh monitors system and application configuration settings to ensure they are compliant with your security policies, standards and/or hardening guides. Agents perform periodic scans to detect applications that are known to be vulnerable, unpatched, or insecurely configured.

Additionally, configuration checks are customizable to properly align them with your organization. Alerts include recommendations for better configuration, references and mapping with regulatory compliance.

Incident Response

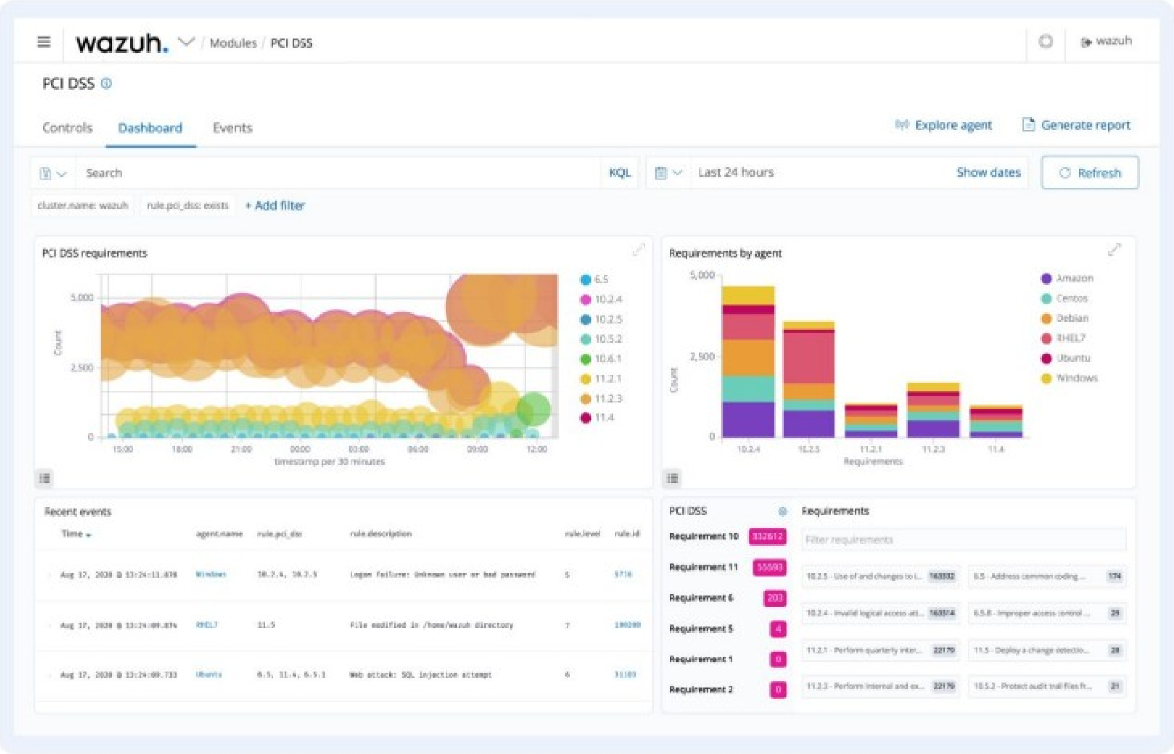


Time	agent.name	rule.groups	rule.description	rule.level	rule.id
Aug 16, 2020 @ 22:39:18.199	RHEL7	Connection blocked	Poor reputation IP address 196.52.43.89 blocked by firewall	9	100100
Aug 15, 2020 @ 16:29:31.754	Windows	File quarantined	File C:\Users\Administrator\Finance.doc quarantined	10	100125
Aug 15, 2020 @ 01:20:38.187	Debian	Process stopped	Compromised process /usr/sbin/httpd stopped	12	100112
Aug 14, 2020 @ 03:10:14.366	Centos	Application removed	Blacklisted RPM nmap-ncat-6.40-19 removed	12	100205

Wazuh provides out-of-the-box active responses to perform various countermeasures to address active threats, such as blocking access to a system from the threat source when certain criteria are met.

In addition, Wazuh remotely runs commands or system queries, identifying indicators of compromise (IOCs) and helping perform other live forensics or incident response tasks.

Regulatory Compliance



Recent events

Time	agent.name	rule.pci_dss	rule.description	rule.level	rule.id
Aug 17, 2020 @ 13:24:11.478	Windows	10.2.4, 10.2.5	Logon failure: Unknown user or bad password	5	5716
Aug 17, 2020 @ 13:24:09.874	RHEL7	11.5	File modified in /home/wazuh directory	7	100200
Aug 17, 2020 @ 13:24:09.733	Ubuntu	6.5, 11.4, 6.5.1	Web attack: SQL injection attempt	6	31103

PCI DSS	
Requirement 10	332612
Requirement 11	55593
Requirement 6	203
Requirement 5	4
Requirement 1	0
Requirement 2	0

Requirements

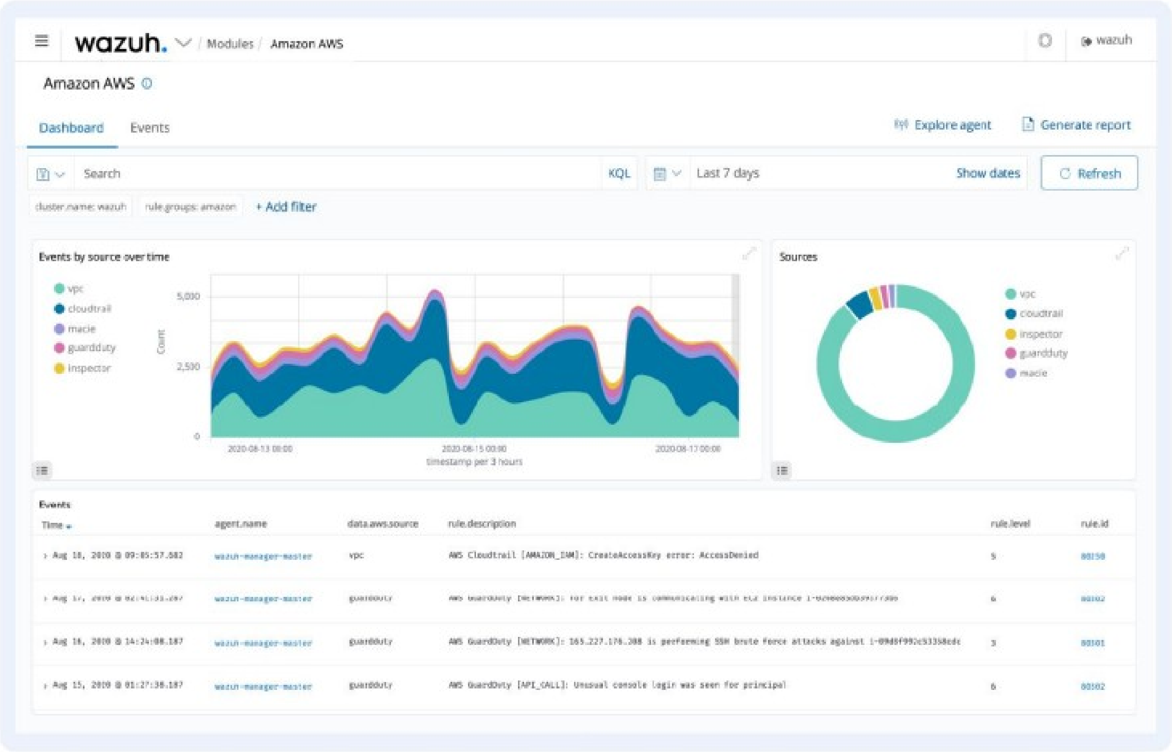
Filter requirements

10.2.5 - Use of and changes to i...	163332	6.5 - Address common coding ...	174
10.2.4 - Invalid logical access att...	163314	6.5.8 - Improper access control ...	29
11.2.1 - Perform quarterly inter...	22179	11.5 - Deploy a change detectio...	28
11.2.3 - Perform internal and ex...	22179	10.5.2 - Protect audit trail files fr...	21

Wazuh provides some of the necessary security controls to become compliant with industry standards and regulations. These features combined with its scalability and multi-platform support help organizations meet technical compliance requirements.

Wazuh is widely used by payment processing companies and financial institutions to meet PCI DSS (Payment Card Industry Data Security Standard) requirements. Its web user interface provides reports and dashboards that help with this and other regulations such as SOC2, GDPR, NIST or HIPAA.

Cloud Security Monitoring



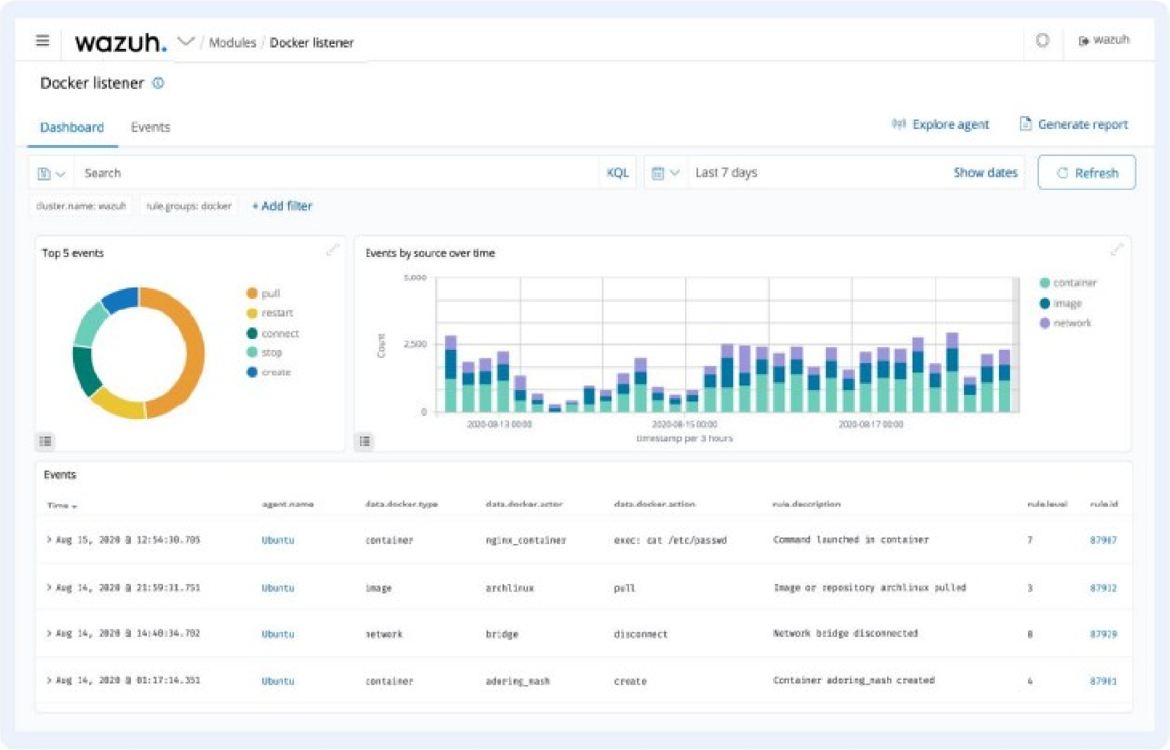
Events

Time	agent.name	data.aws.source	rule.description	rule.level	rule.id
Aug 18, 2020 @ 09:05:57.682	wazuh-manager-master	vpc	AWS Cloudtrail [AMAZON_IAM]: CreateAccessKey error: AccessDenied	5	80258
Aug 17, 2020 @ 02:41:33.287	wazuh-manager-master	guardduty	AWS GuardDuty [NETWORK]: Tor exit node is communicating with EC2 instance [illegible]	6	80302
Aug 16, 2020 @ 14:24:08.187	wazuh-manager-master	guardduty	AWS GuardDuty [NETWORK]: 165.227.176.208 is performing SSH brute force attacks against i-09d8f992c53358cdc	3	80301
Aug 15, 2020 @ 01:27:38.187	wazuh-manager-master	guardduty	AWS GuardDuty [API_CALL]: Unusual console login was seen for principal	6	80302

Wazuh helps monitoring cloud infrastructure at an API level, using integration modules that are able to pull security data from well-known cloud providers, such as Amazon AWS, Azure or Google Cloud. It provides rules to assess the configuration of your cloud environment, easily spotting weaknesses.

In addition, Wazuh lightweight and multi-platform agents are commonly used to monitor cloud environments at the instance level.

Containers Security



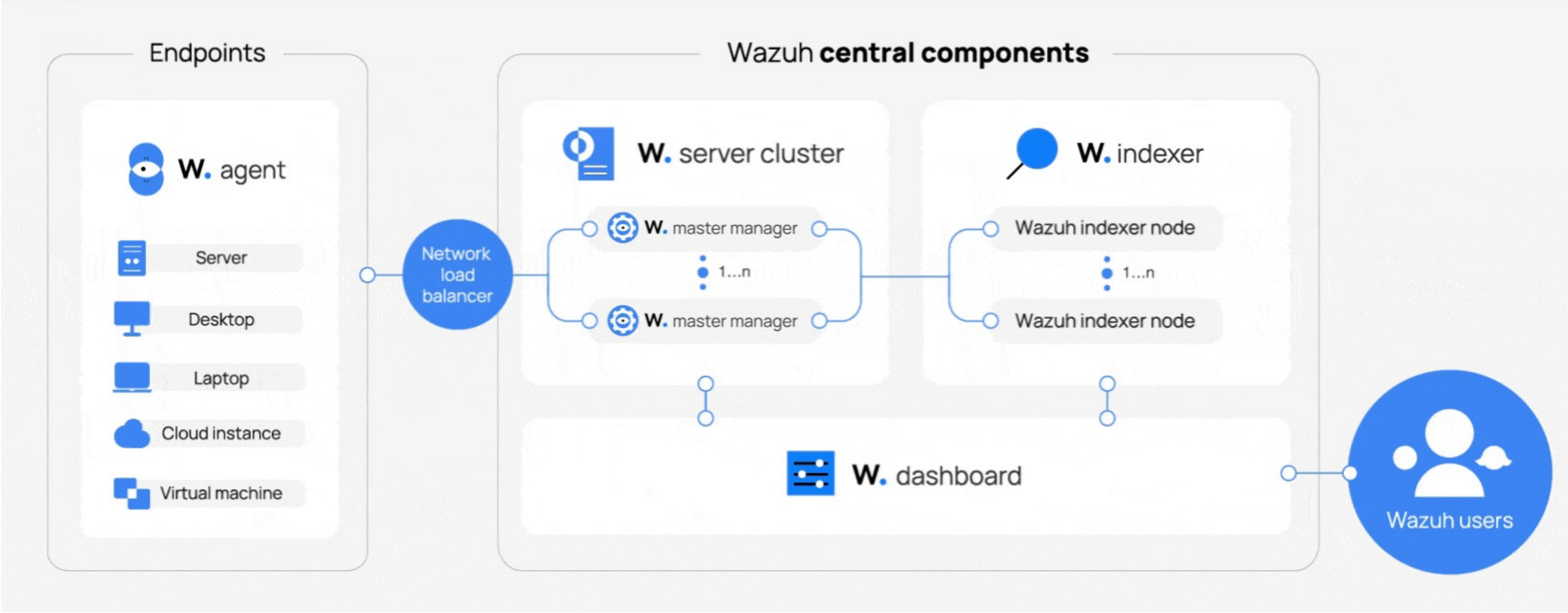
Events

Time	agent.name	data.docker.type	data.docker.actor	data.docker.action	rule.description	rule.level	rule.id
> Aug 15, 2020 @ 12:54:30.705	Ubuntu	container	nginx_container	exec: cat /etc/passwd	Command launched in container	7	87907
> Aug 14, 2020 @ 21:59:31.751	Ubuntu	image	archlinux	pull	Image or repository archlinux pulled	3	87932
> Aug 14, 2020 @ 14:40:34.702	Ubuntu	network	bridge	disconnect	Network bridge disconnected	8	87929
> Aug 14, 2020 @ 01:17:14.351	Ubuntu	container	adoring_nash	create	Container adoring_nash created	4	87901

Wazuh provides security visibility into your Docker hosts and containers, monitoring their behavior and detecting threats, vulnerabilities and anomalies. The Wazuh agent has native integration with the Docker engine allowing users to monitor images, volumes, network settings, and running containers.

Wazuh continuously collects and analyzes detailed runtime information. For example, alerting for containers running in privileged mode, vulnerable applications, a shell running in a container, changes to persistent volumes or images, and other possible threats.

Wazuh Architecture



Why Wazuh is preferred

- Average of 20 million downloads per year
- Auditors want evidence, not claims. Wazuh produces exportable, timestamped, immutable audit logs.
- Each regulation is mapped to features — making it easy to show clients "this control → this Wazuh function → this compliance evidence."
- Cost-effective SOC baseline: Instead of buying multiple tools for FIM, vulnerability scanning, log management, and compliance dashboards, Wazuh covers all in one open-source framework.

Wazuh from NETCB

- NETCB is a Platinum Partner
- NETCB's Wazuh version is ONLY available from NETCB which makes us sole provider and distributor:
  - Custom Decoders (eDirectory, GroupWise, pfSense, and SecureAnyBox)
  - Localised branding (SEC-COM)
  - Custom Integrations
- Available as On-Premise solution or as a Cloud-hosted solution
- Three Costing Tiers
  - Essential
  - Standard
  - Premium

Demo