initMAX

Discover the power of the open source security platform Wazuh 4.5

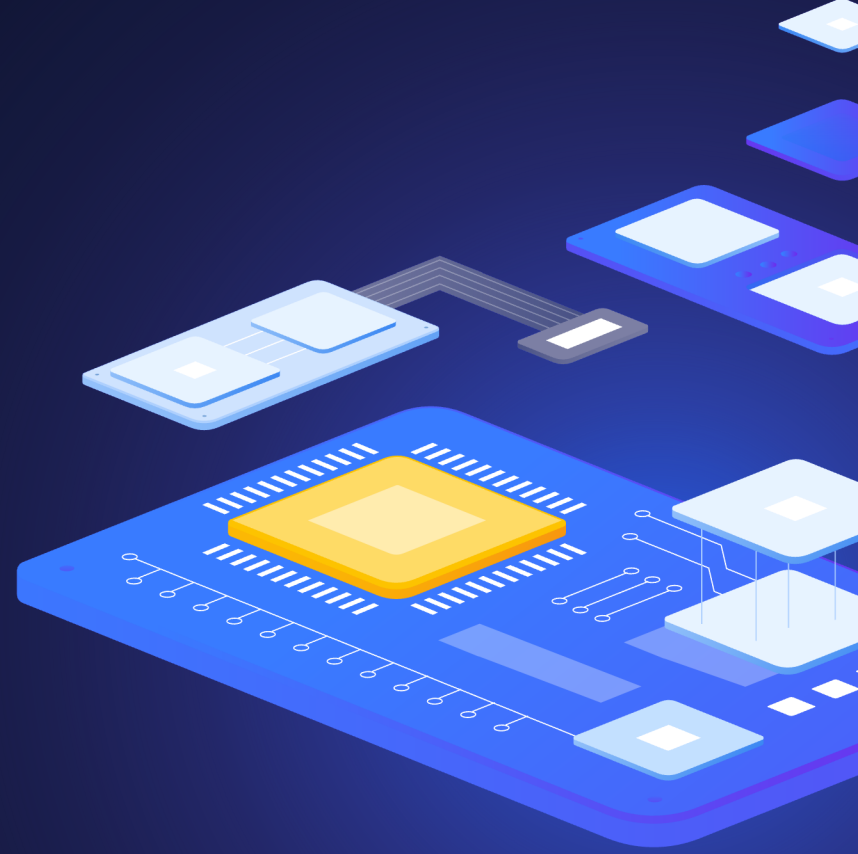
all our microphones are muted

ask your questions in Q&A, not in the Chat

use Chat for discussion, networking or applause

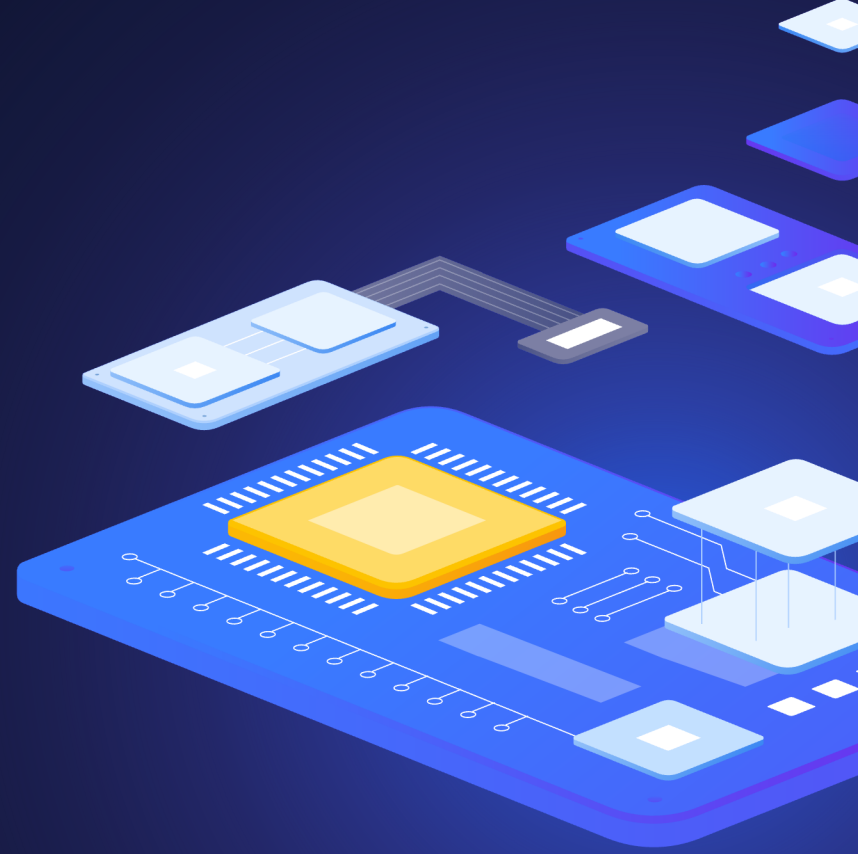
Agenda

1. Basics
2. Components & Architecture
3. Capabilities
4. Demo



1

Basics



Discover the power of the open source security platform Wazuh

initMAX

Why security monitoring

- Regulatory requirements like
  - NIS2
    - Network & Information Systems Regulations
  - GDPR
    - General Data Protection Regulation
  - DORA
    - Digital Operational Resilience Act

- Standards compliance like
  - PCI DSS
  - HIPAA
  - ISO/IEC 27001

initMAX

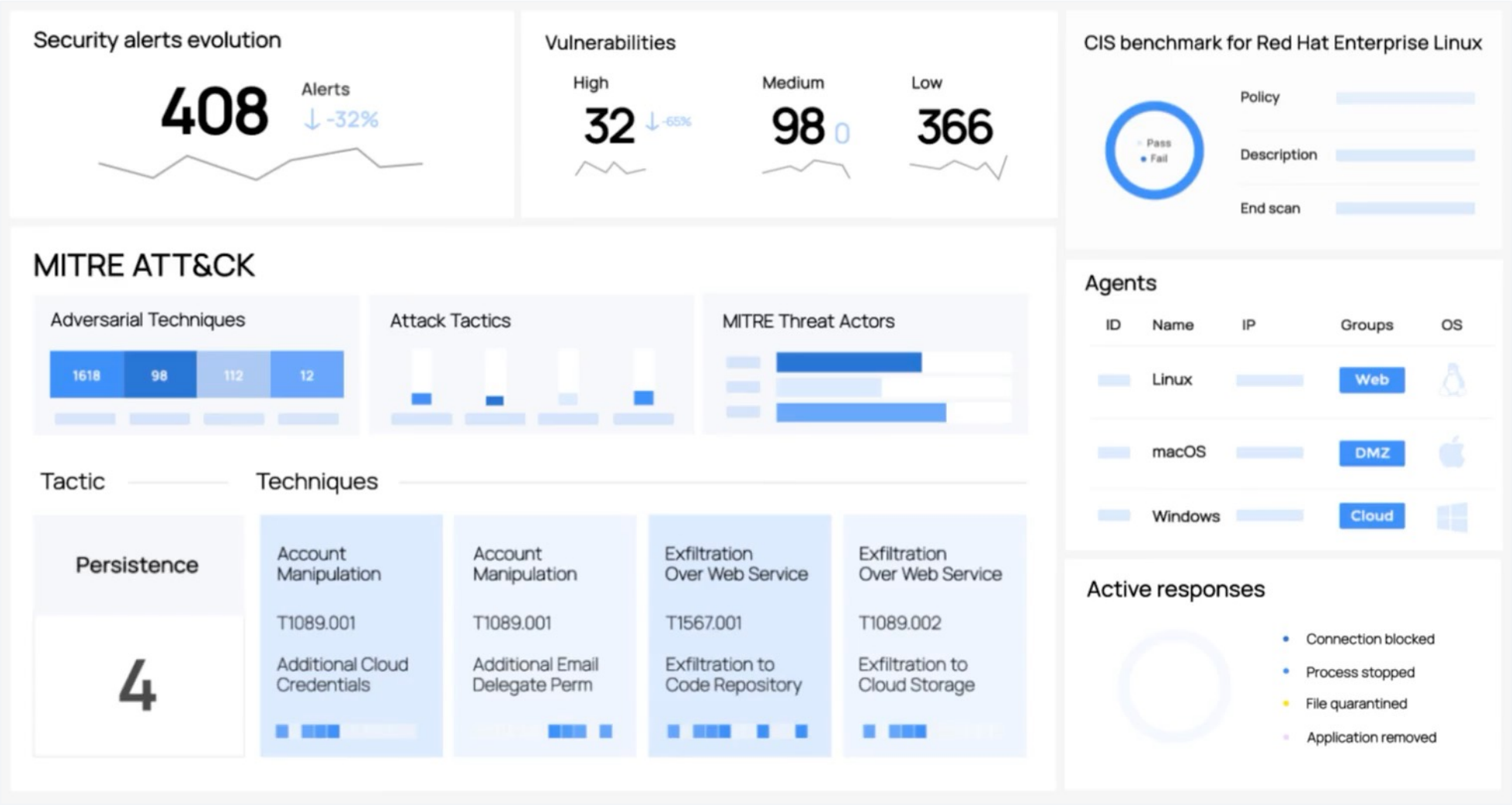
Why security monitoring

- OWASP Top 10
  - Security Misconfiguration
  - Vulnerable and Outdated Components
  - Security Logging and Monitoring Failures
- Local regulations
- Improved monitoring - better visibility and observability
  - Faster and better response = better reliability
  - Better reliability = happy customers and managers
- Peaceful sleep

Discover the power of the open source security platform Wazuh

initMAX

About Wazuh

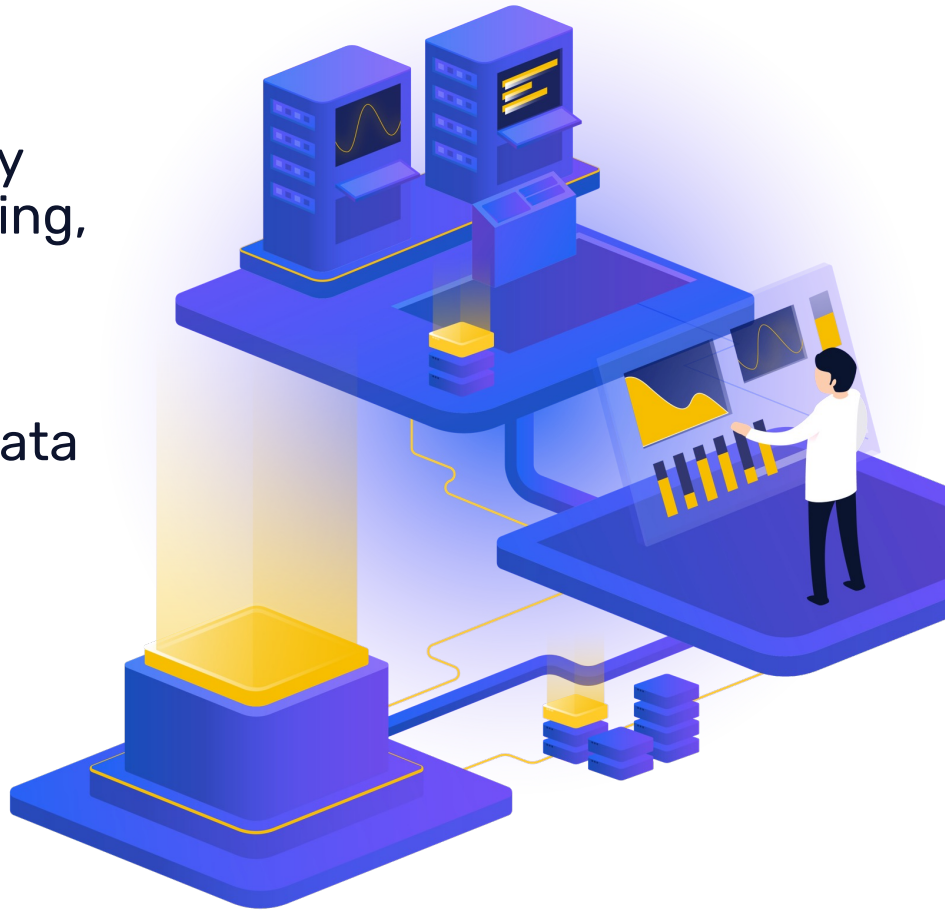


Discover the power of the open source security platform Wazuh

initMAX

About Wazuh

- Wazuh is a free, open source and enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response and compliance
- Flexible, scalable, no vendor lock-in, and no license cost
- Usable for public clouds, private clouds, and on-premise data centers
- On-premise or cloud installation
- Provides real-time analytics, correlation and context
- Provides monitoring, detection and alerting of security events and incidents
- Enhance your visibility and standard monitoring



Discover the power of the open source security platform Wazuh

initMAX

About Wazuh

- Founded in 2015 by Santiago Bassett and rapidly grown
- Based in San Jose California
- Wazuh has nearing 200 employees across the globe
- Has some 100,000 users in companies of all sizes
- Has more than 700 paying customers of its subscription-based professional services
- Customers include enterprises like Salesforce, Walgreens, Verifone, NASA and PWC
- “Wazuh” doesn’t have any other meaning, is simply distinctive enough

- **We are proved Wazuh partner and certified Enginers**

initMAX

Discover the power of the open source security platform Wazuh

What's new in latest version (4.5)

- Vulnerability detection support for SUSE agents
- Support for Azure Integration in Linux agents
- Added a new module to integrate with Amazon Security Lake
- Updated all current rule descriptions from "Ossec" to "Wazuh„
- Vulnerability Detector now fetches the NVD feed from https://feed.wazuh.com, based on the NVD API 2.0
- Vulnerability Detector now fetches the RHEL 5 feed URL from https://feed.wazuh.com by default.
- The Wazuh dashboard is now based on OpenSearch dashboards 2.6.0
- The Wazuh indexer is now based on OpenSearch 2.6.0

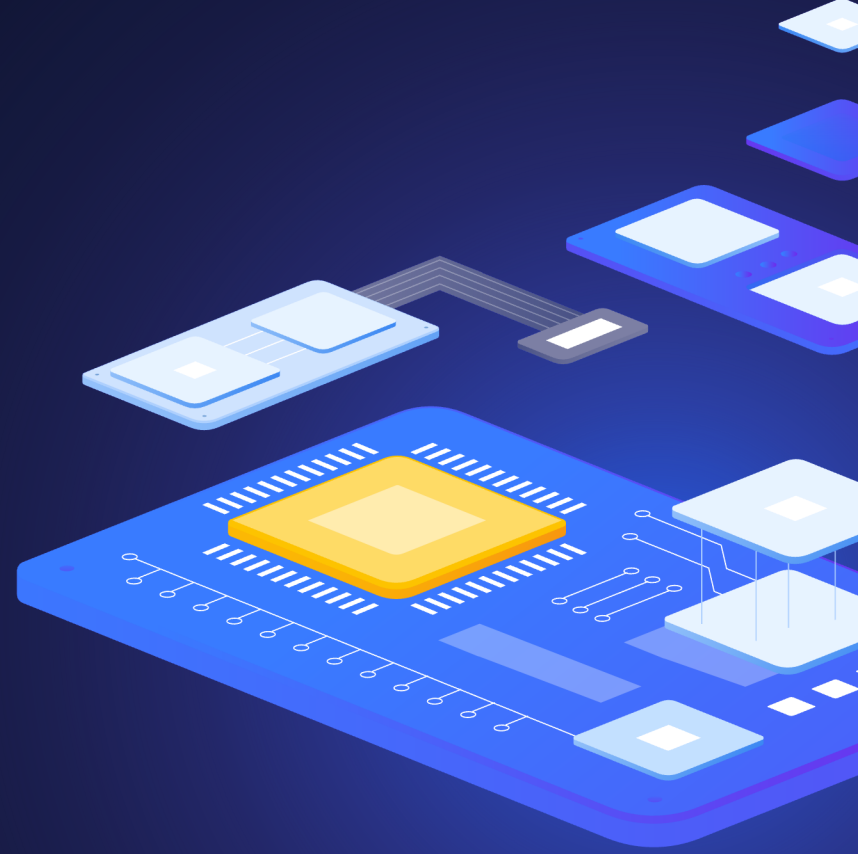
- More informations and details at: https://documentation.wazuh.com/current/release-notes/index.html

initMAX

Customers

2

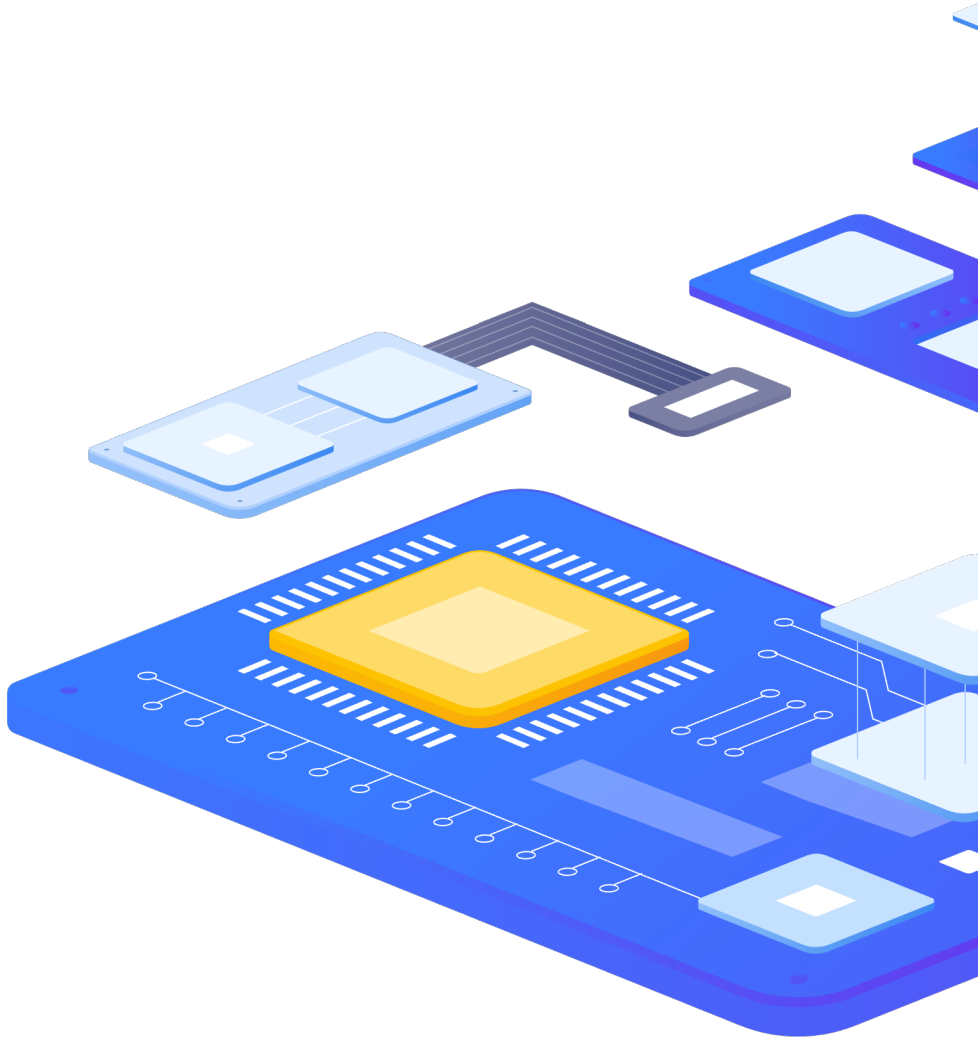
Components & Architecture



initMAX

Components

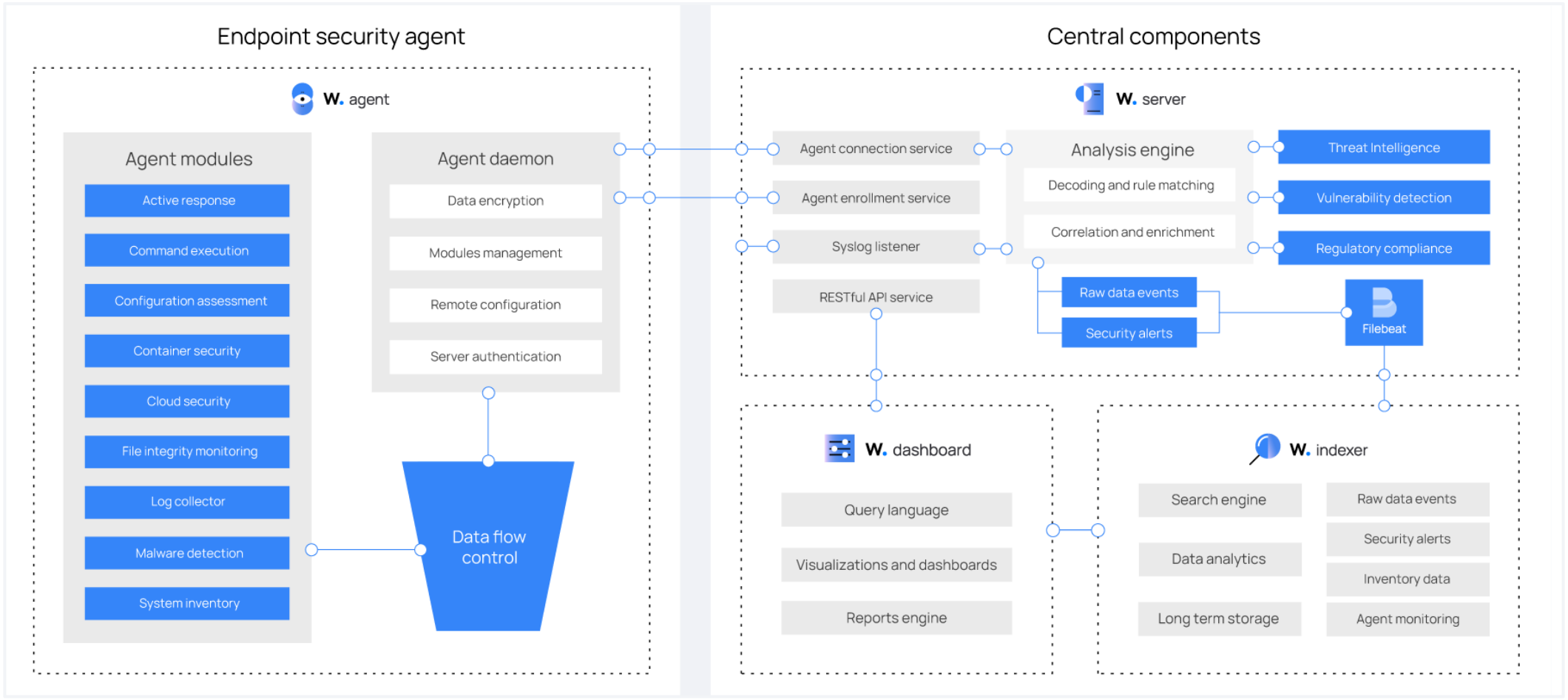
- Wazuh solution is based on four components
  - Wazuh agents
    - Installed on endpoints
  - Wazuh server
    - Analyzes received data
  - Wazuh indexer
    - Component for indexing and storing alerts generated by the Wazuh server
  - Wazuh dashboard
    - Web user interface for data visualization and analysis



Discover the power of the open source security platform Wazuh

initMAX

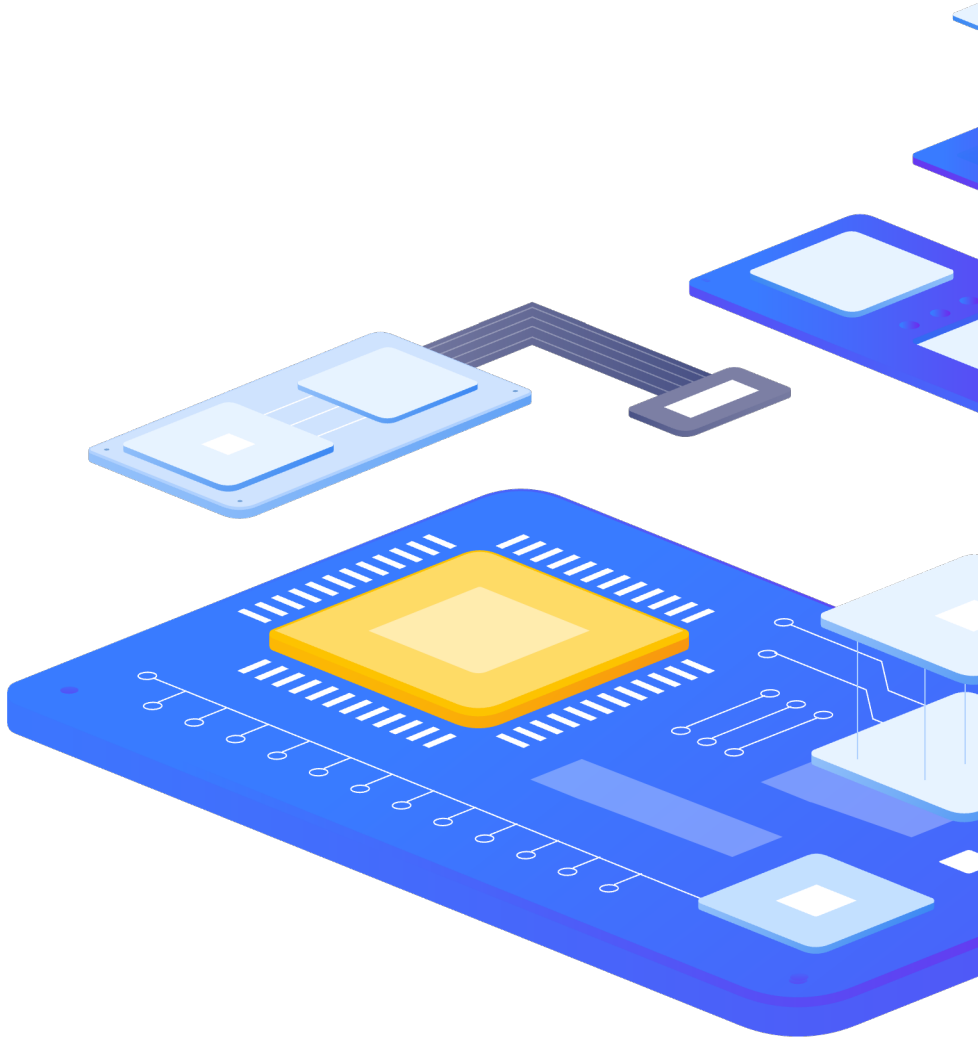
Components



initMAX

Wazuh agent

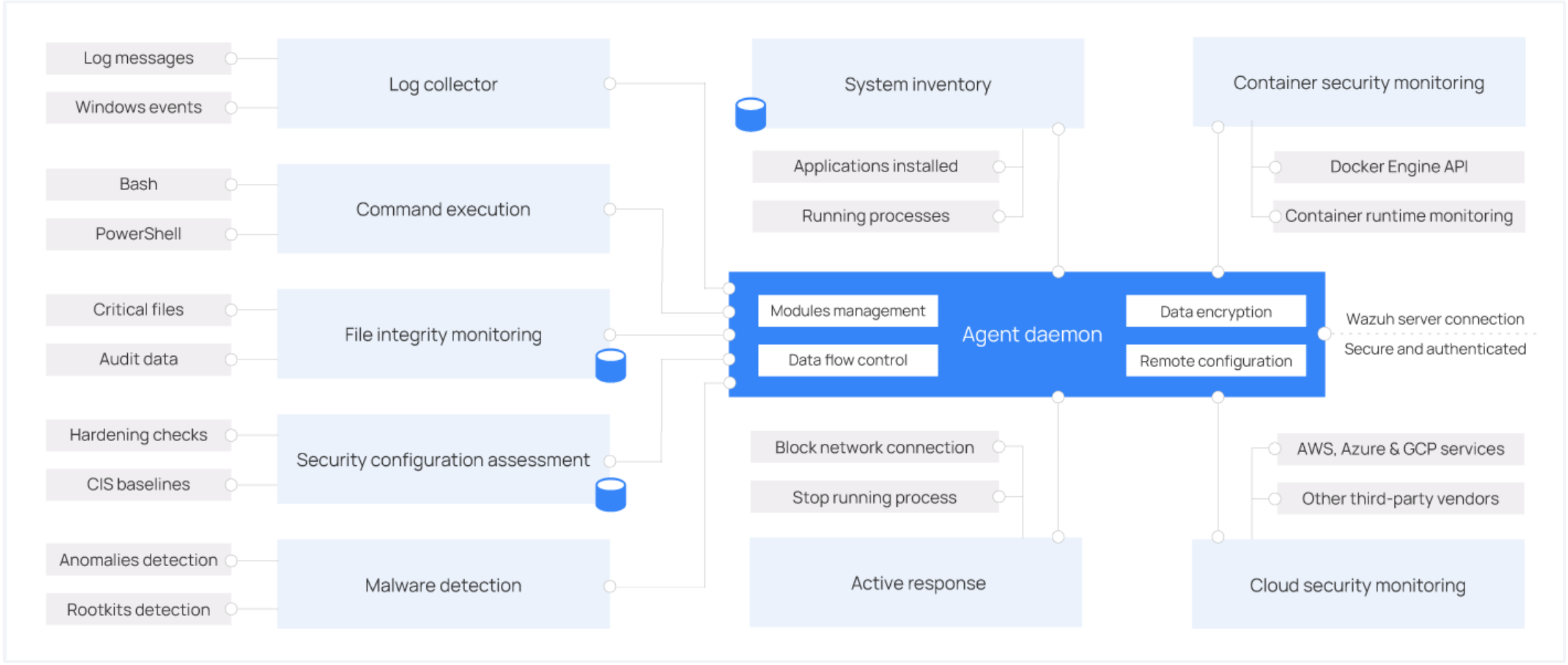
- Agent can be installed on:
  - Linux
  - Windows
  - macOS
  - etc.
- Is used to collect system and application data and forwards it to the Wazuh server
- Communication channel is encrypted and authenticated
- Can be upgraded, monitored and configured remotely from the Wazuh server
- Includes flow control mechanisms to avoid flooding



Discover the power of the open source security platform Wazuh

initMAX

Wazuh agent

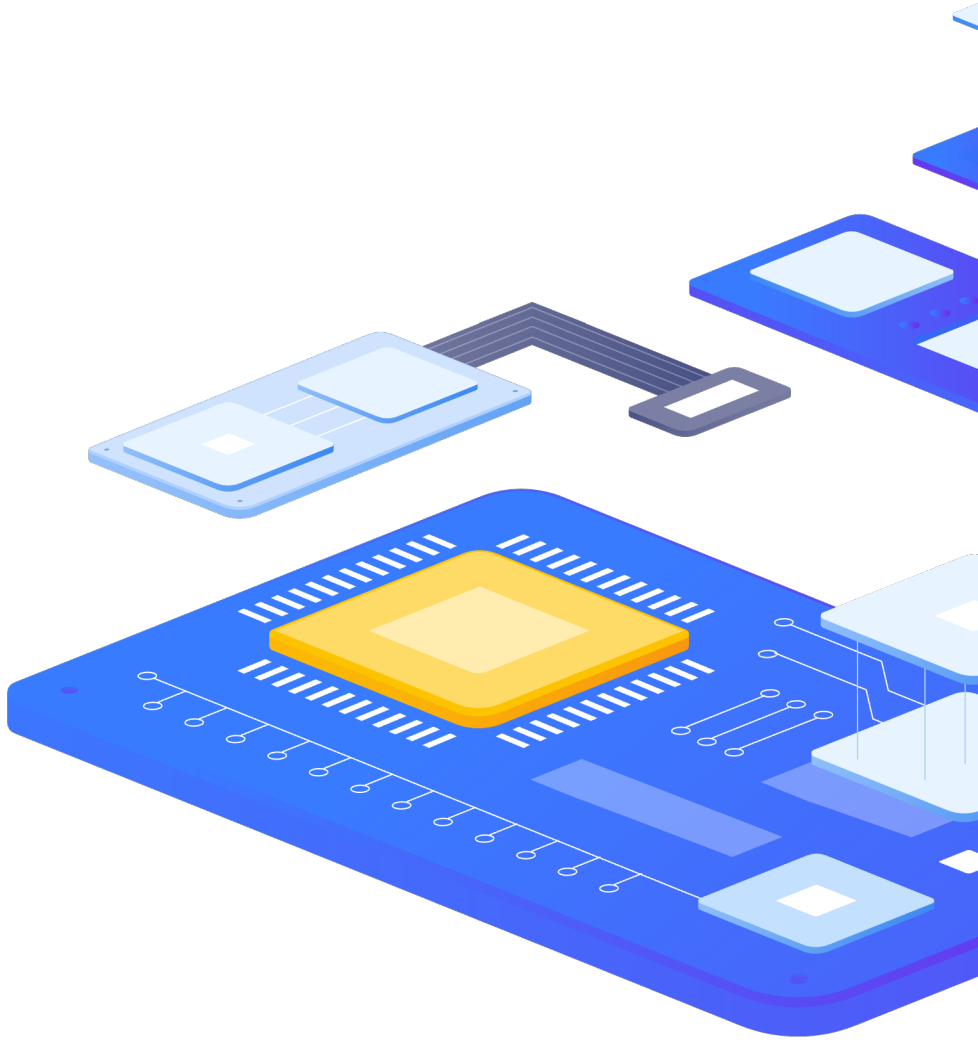


Discover the power of the open source security platform Wazuh

initMAX

Wazuh server

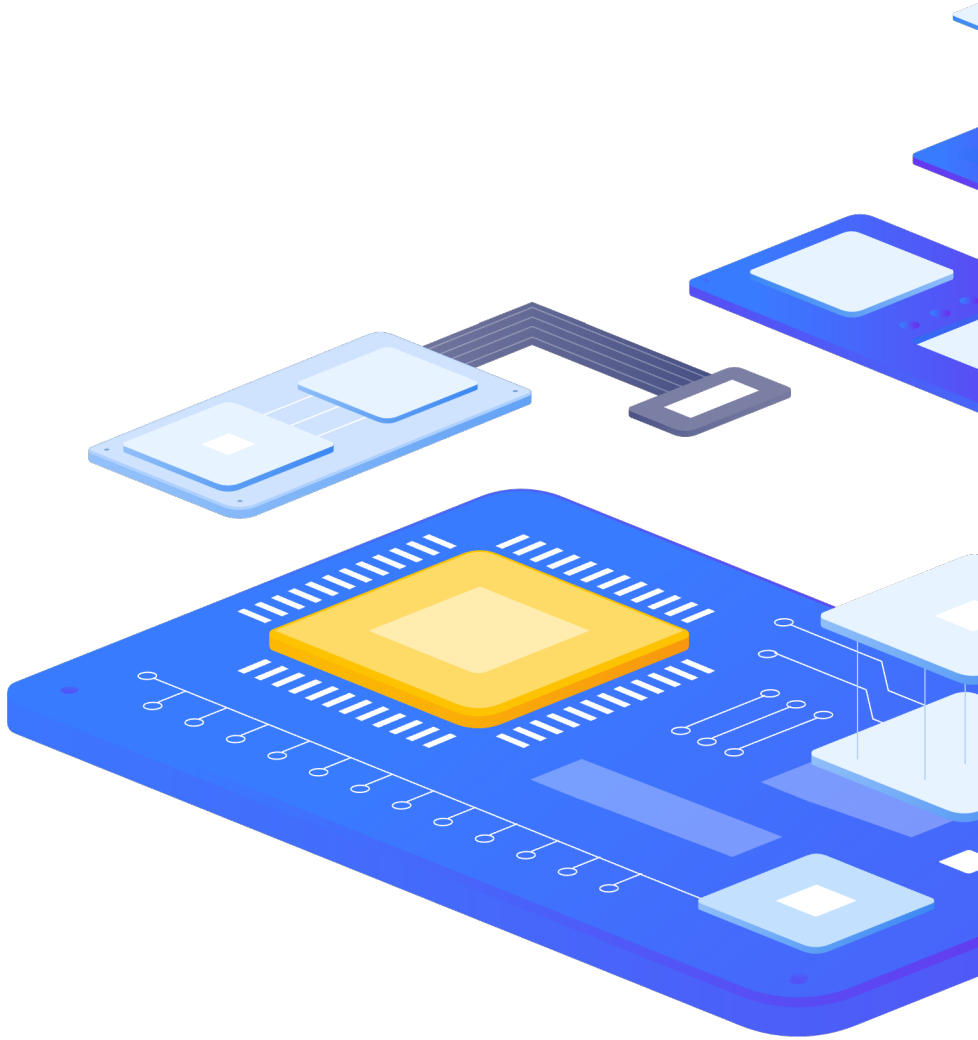
- Analyzes the data received from the agents
- Triggering alerts when threats or anomalies are detected
- Manage the Wazuh agents configuration remotely and monitor their status
- Uses threat intelligence sources for data enrichment
- Enriches alert data by using the MITRE ATT&CK and regulatory compliance requirements etc.
- Providing context for security analytics
- Can be integrated with external software like
  - Jira, Slack, PagerDuty, Zabbix etc.
  - Security Incident Response Platforms



initMAX

Wazuh indexer

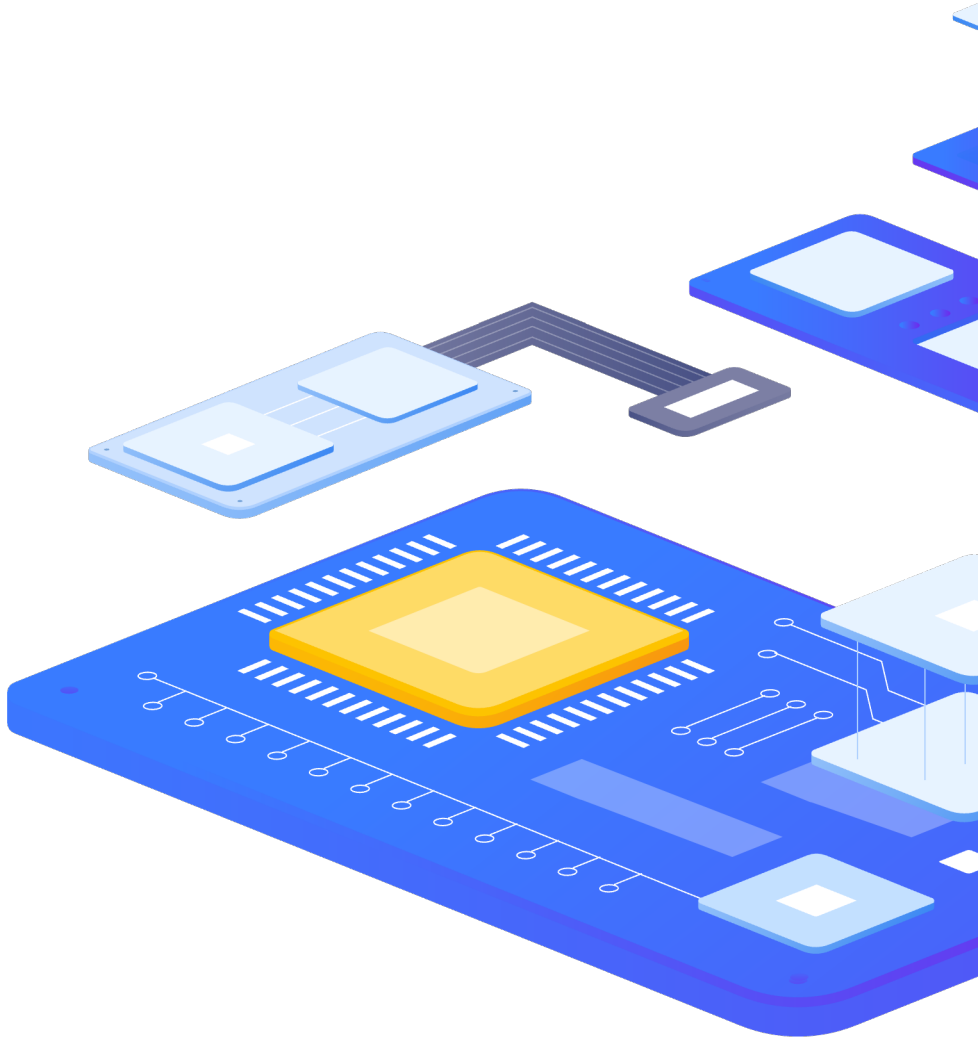
- Central component
- Highly scalable, full-text search and analytics engine
- Indexes and stores alerts generated by the Wazuh server
- Provides near real-time data search and analytics capabilities
- Can be configured as a single-node or multi-node cluster



initMAX

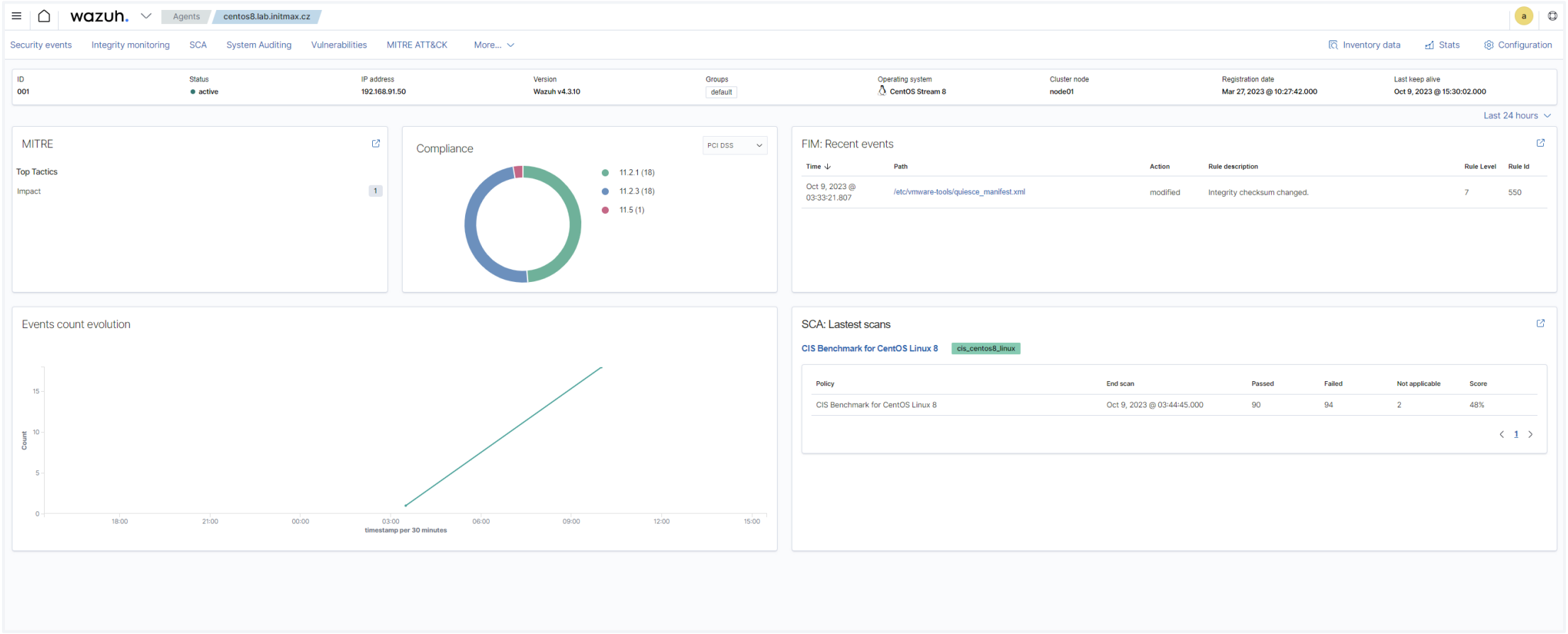
Wazuh dashboard

- Flexible web user interface for:
  - Mining
  - Analyzing
  - Visualizing security events and alerts data
- GUI for the management, monitoring and configuration of the Wazuh platform
- Provides features for role-based access control (RBAC) and single sign-on (SSO)



Discover the power of the open source security platform Wazuh

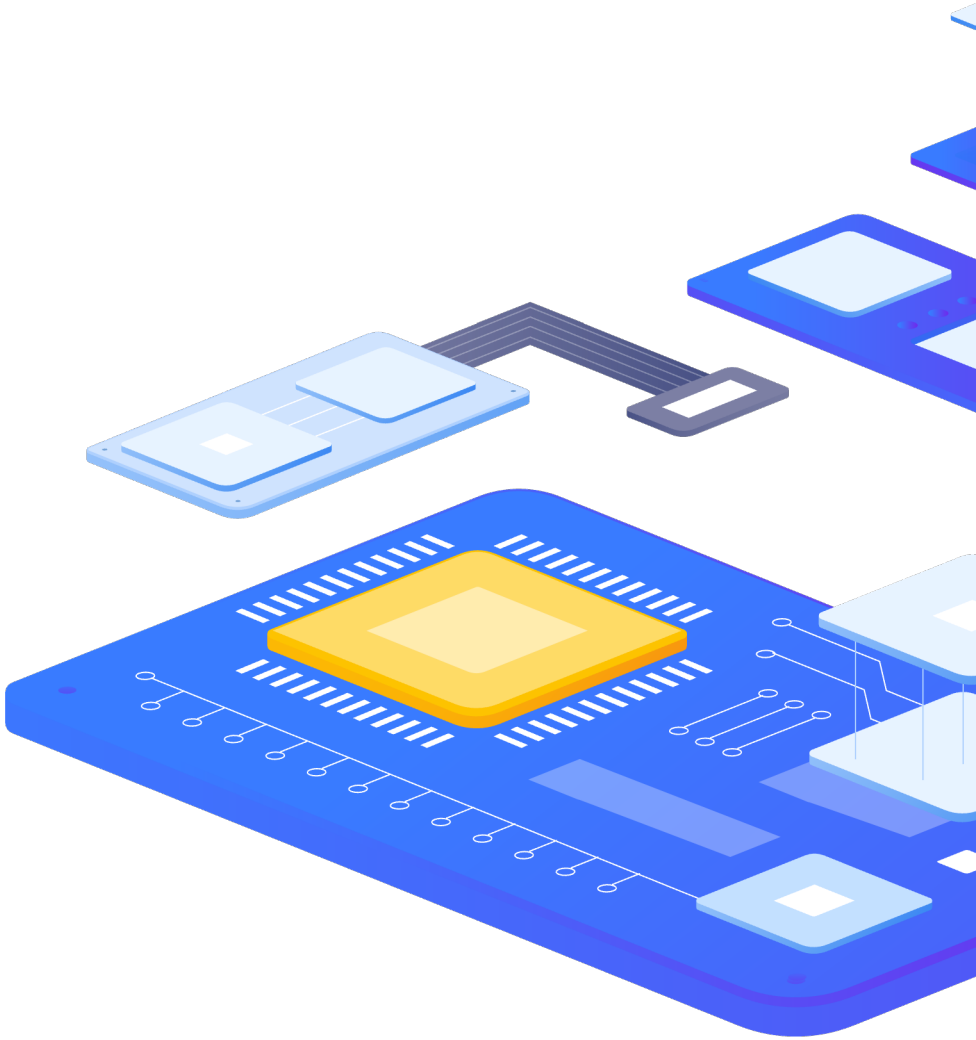
Wazuh dashboard



initMAX

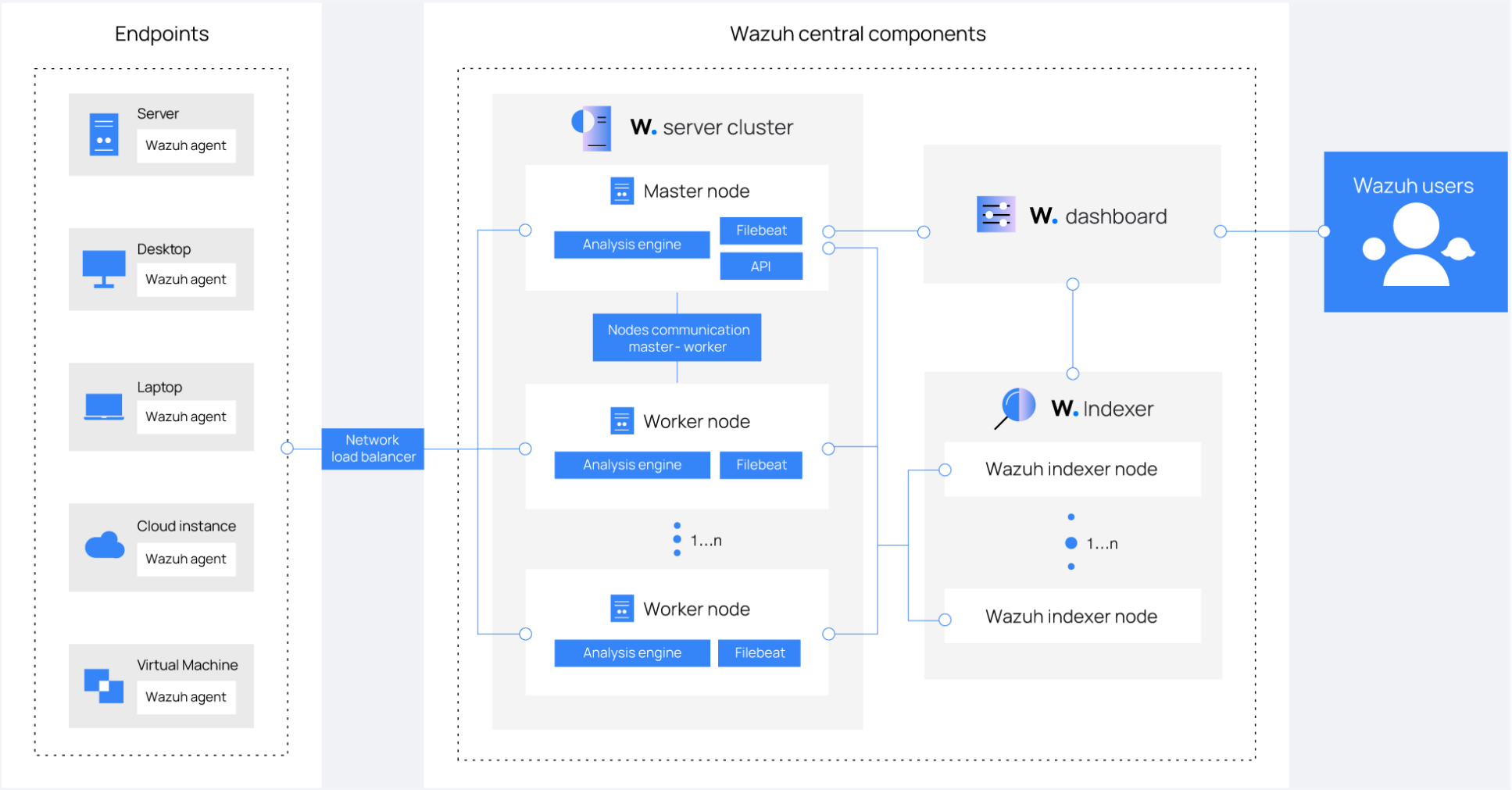
Architecture

- Based on agents, running on the monitored endpoints
  - Agents forward security data to a central server
- Agentless devices can actively submit log data via:
  - Syslog
  - SSH
  - Filebeat
  - Fluentd
  - API
  - etc.
- The central server decodes and analyzes the incoming information
- Results are passed to the Wazuh indexer for indexing and storage



Discover the power of the open source security platform Wazuh

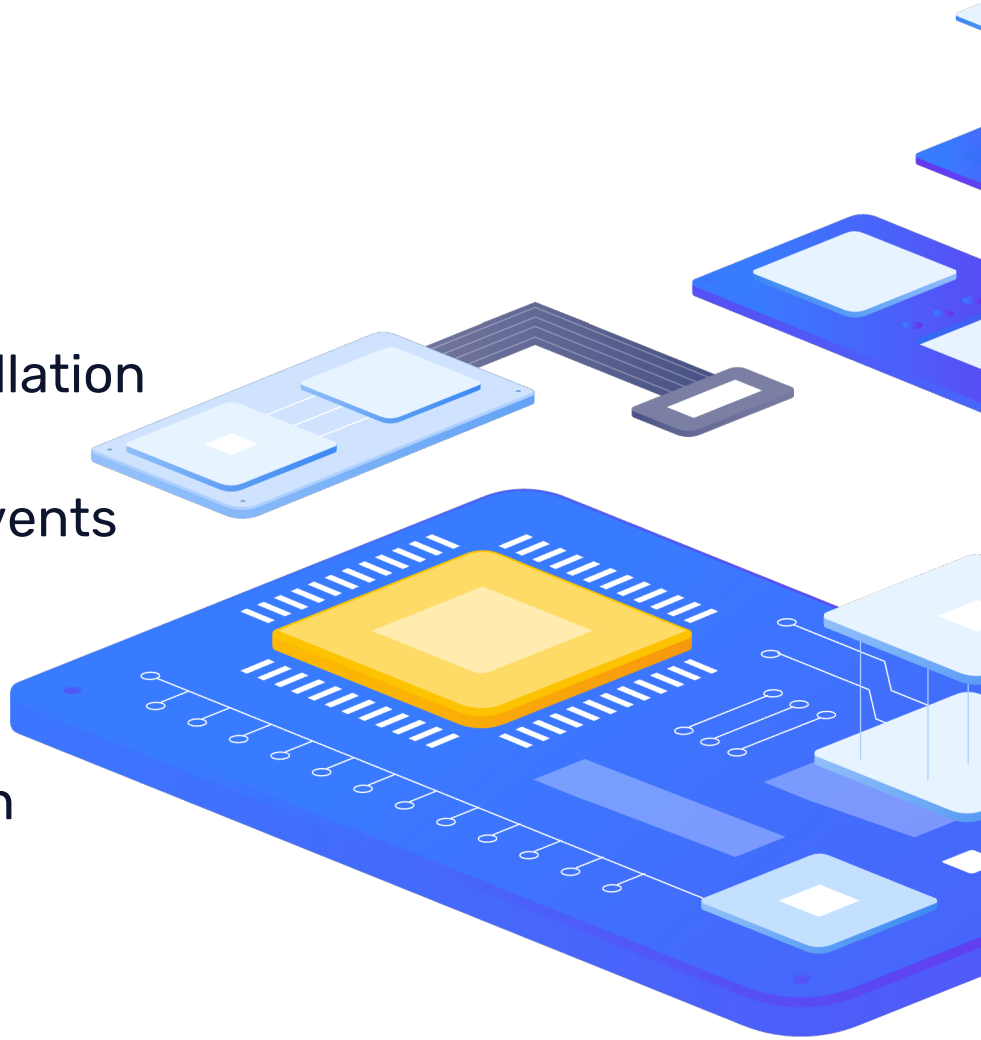
Architecture



initMAX

Architecture

- In small deployments is possible all-in-one installation
  - Wazuh server, indexer and dashboard on same host
- In large environments is recommended multi-node installation
  - Wazuh server and Wazuh indexer to different hosts
  - Filebeat is used to forwarding alerts and archiving events to indexer cluster (single-node or multi-node)
- Wazuh server and the Wazuh indexer nodes can be configured as clusters, providing load balancing and high availability

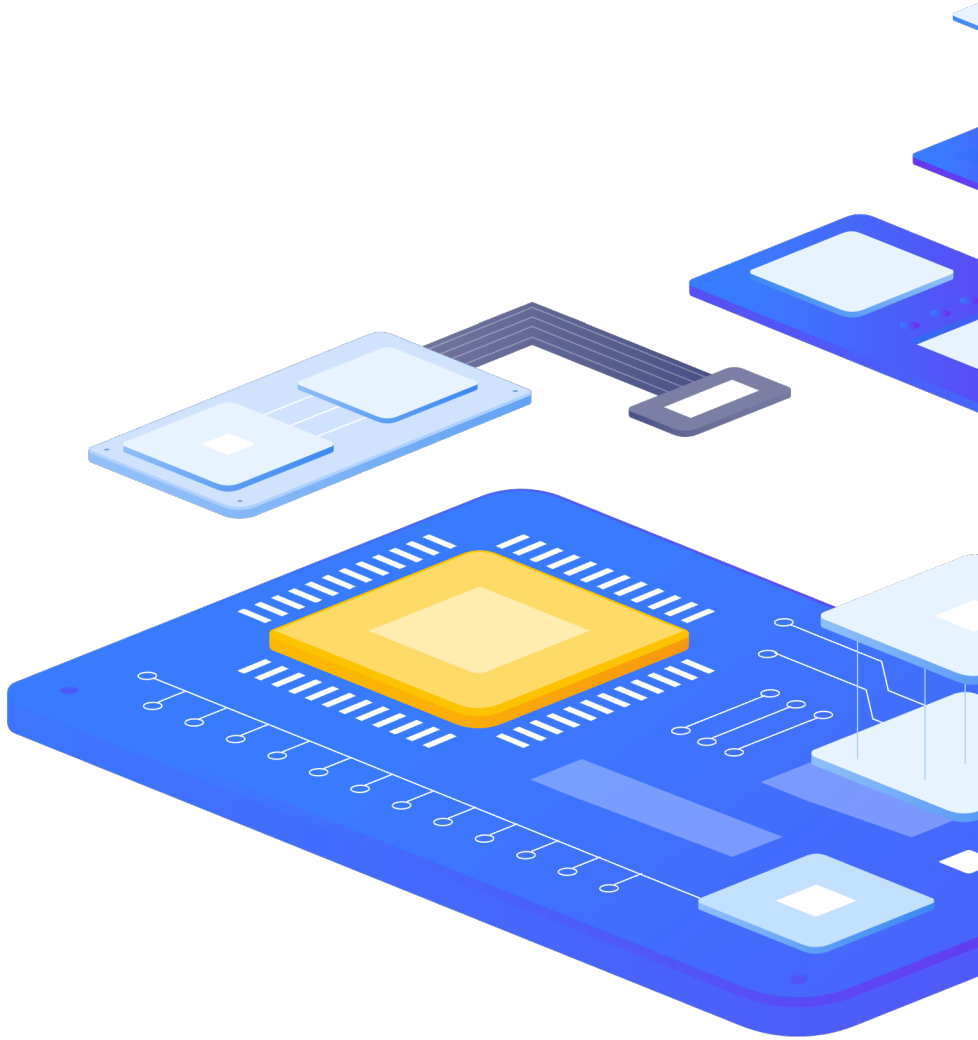


initMAX

Architecture

Wazuh agent - Wazuh server communication

- The Wazuh agent sends events to the Wazuh server for analysis and threat detection
- Agent establishes a connection with the server for agent connection
- Message protocol uses AES encryption by default, with 128-bits per block and 256-bit keys
- Wazuh server performs decoding and rule checking of received events, utilizing the analytics engine

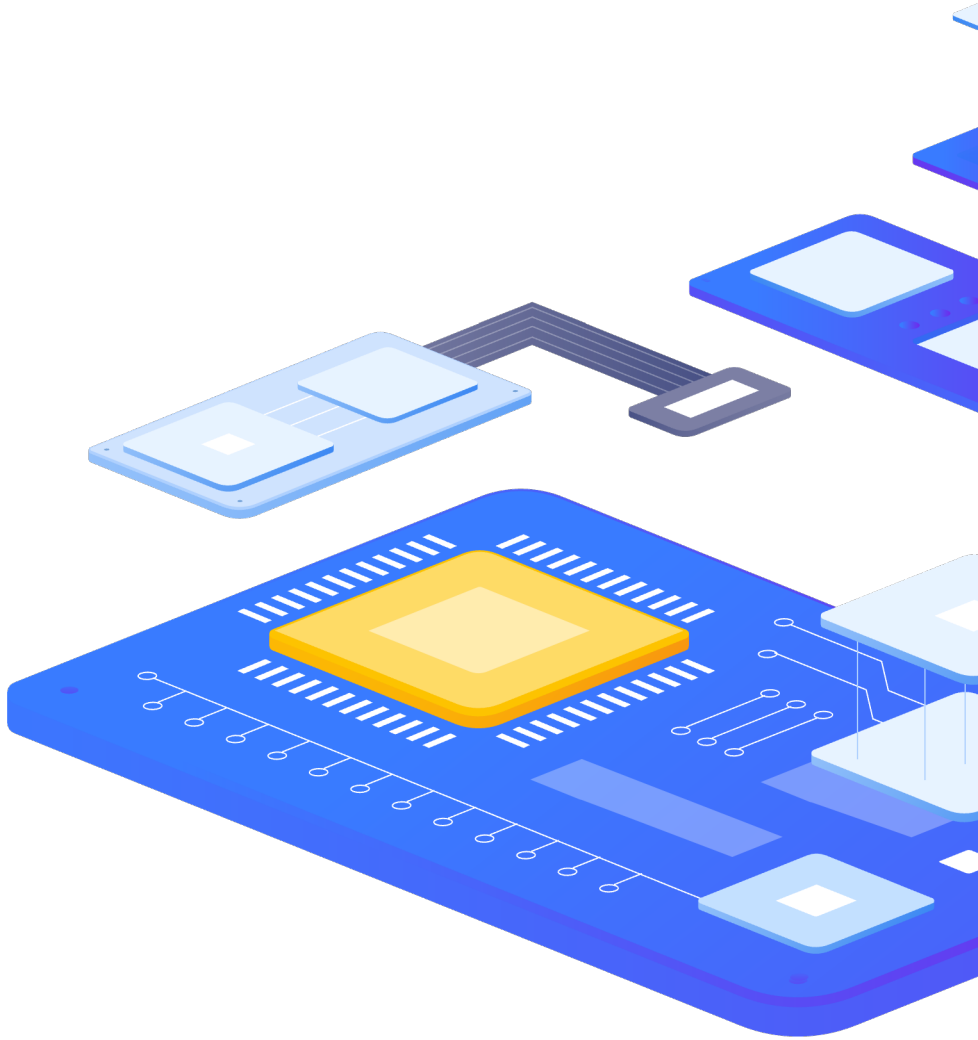


initMAX

Architecture

Wazuh server - Wazuh indexer communication

- Wazuh server uses Filebeat to send alert and event data to the Wazuh indexer, using TLS encryption
- Data are indexed by the Wazuh indexer
- Wazuh dashboard is used to mine and visualize information
- Wazuh dashboard is using the Wazuh RESTful API
- Communication is encrypted with TLS and authenticated with a username and password



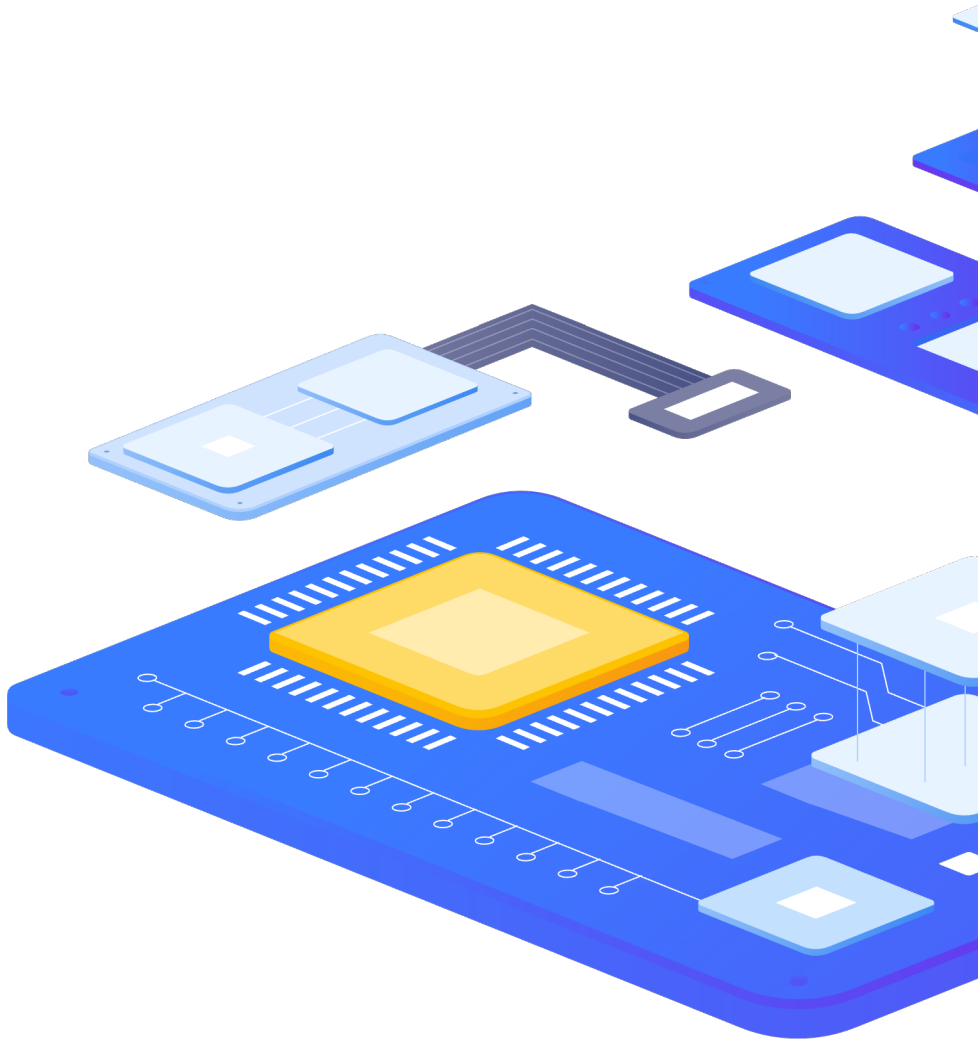
initMAX

Architecture

PCI DSS 10.5.1 requires that you retain audit log history for at least 12 months, with at least the most recent 3 months immediately available for analysis.

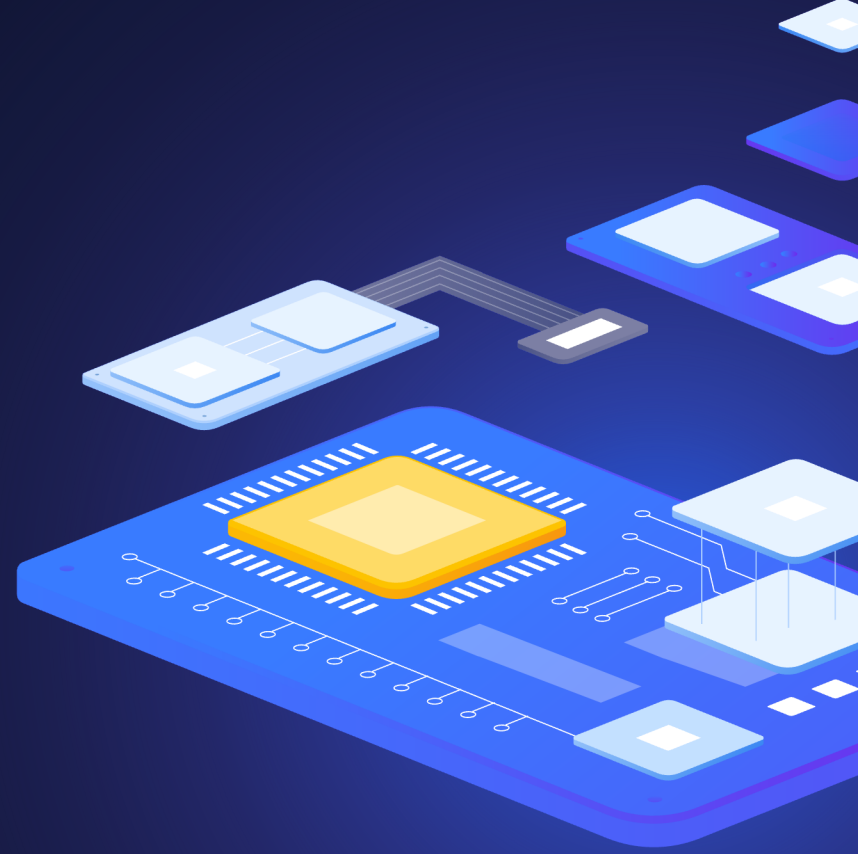
Archival data storage

- Alerts and non-alert events are stored in files on the Wazuh server too
- Files can be written in JSON format or plain text format
- Files are daily compressed and signed using MD5, SHA1 or SHA256 checksums
- Index management policies can be configured for indexed events



3

Wazuh Capabilities



Discover the power of the open source security platform Wazuh

initMAX

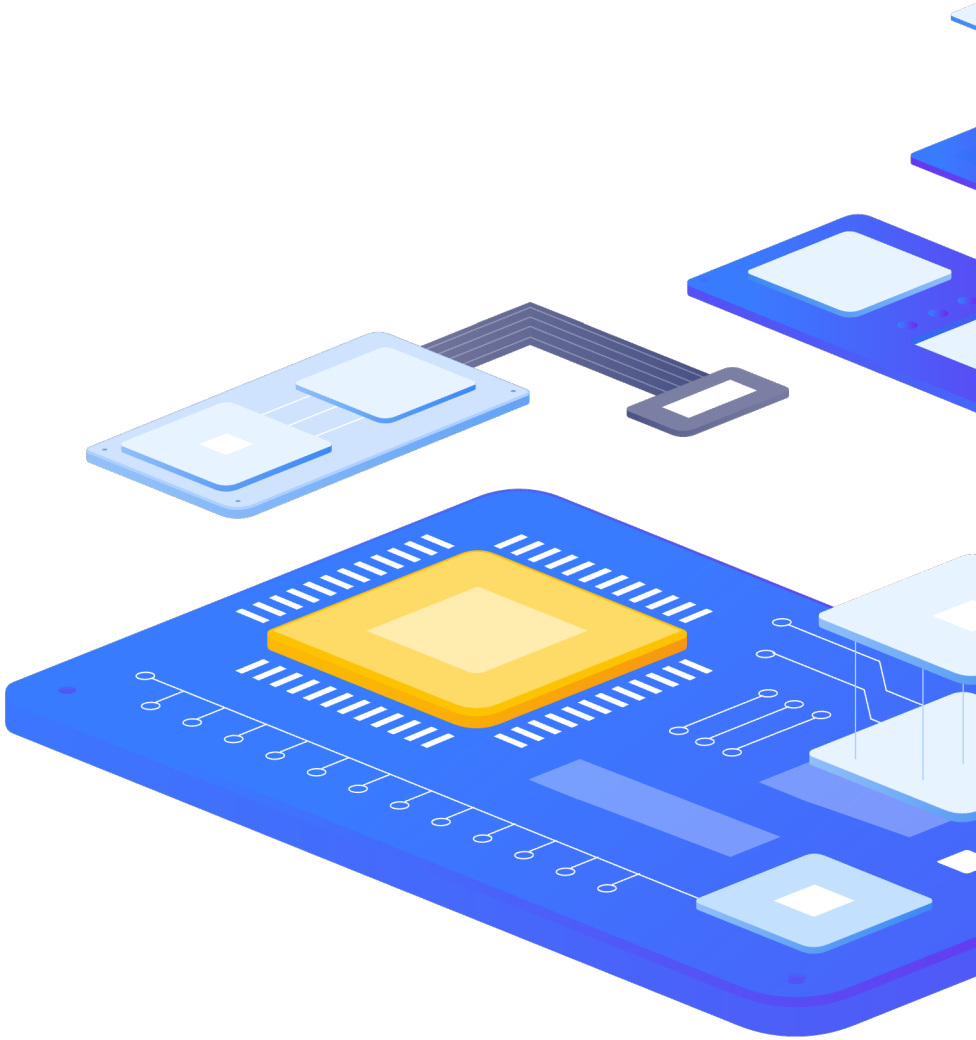
Popular capabilities from a customers perspective

- Log data analytics
- Security configuration assessment (SCA)
- Regulatory compliance
- Vulnerability detection
- File integrity monitoring (FIM)

initMAX

Log data analysis

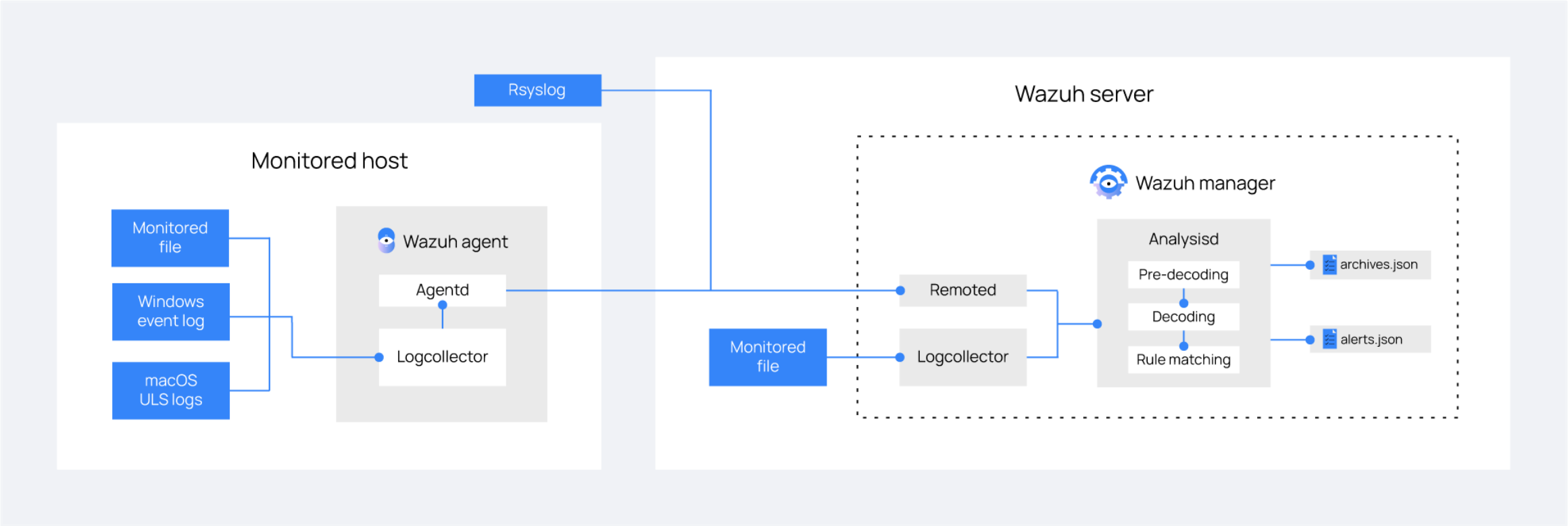
- Main purpose of this component is the identification of:
  - Application or system errors
  - Misconfigurations
  - Intrusion attempts
  - Policy violations and security issues
- Receives logs through text files or Windows event logs
- Can receive logs via remote syslog
- Analyzes received log data
- Decoding and rule matching on the received data
- Rules and decoders can be fully customized or added as needed
- Currently more than 3.000 maintained built-in rules



Discover the power of the open source security platform Wazuh

initMAX

Log data analysis



Discover the power of the open source security platform Wazuh

initMAX

Security configuration assessment (SCA)

- Helps maintain a standard configuration through the monitored endpoints
- Use predefined checks based on the Center of Internet Security (CIS)
- Provides periodic scanning and reporting of misconfigurations in the monitored system
- Policies for the SCA scans are written in YAML format
- Policies can be extended or write completely new to fit organization needs
- For example, a rule can be used to look for the existence of a file, a directory, a Windows registry key, or a running process and many others. It is also possible to execute a command and check its output against a regular expression

initMAX

Configuration assessment (SCA)

Linux SCA rule example

```
- id: 5546
  title: "Ensure IP address forwarding is disabled"
  description: "The net.ipv4.ip_forward flag is used to tell the system whether it can forward packets or not."
  rationale: "Setting the flag to 0 ensures that a system with multiple interfaces (for example, a hard proxy)…"
  remediation: "Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.ip_forward = 0 and…"
  compliance:
    - cis: ["3.1.1"]
    - cis_csc: ["3", "11"]
    - pci_dss: ["2.2.4"]
    - nist_800_53: ["CM.1"]
  condition: all
  rules:
    - 'c:sysctl net.ipv4.ip_forward -> r:^net.ipv4.ip_forward\s*=\s*0$'
    - 'c:grep -Rh net\.ipv4\.ip_forward /etc/sysctl.conf /etc/sysctl.d -> r:^net.ipv4.ip_forward\s*=\s*0$'
```

initMAX

Configuration assessment (SCA)

Windows SCA rule example

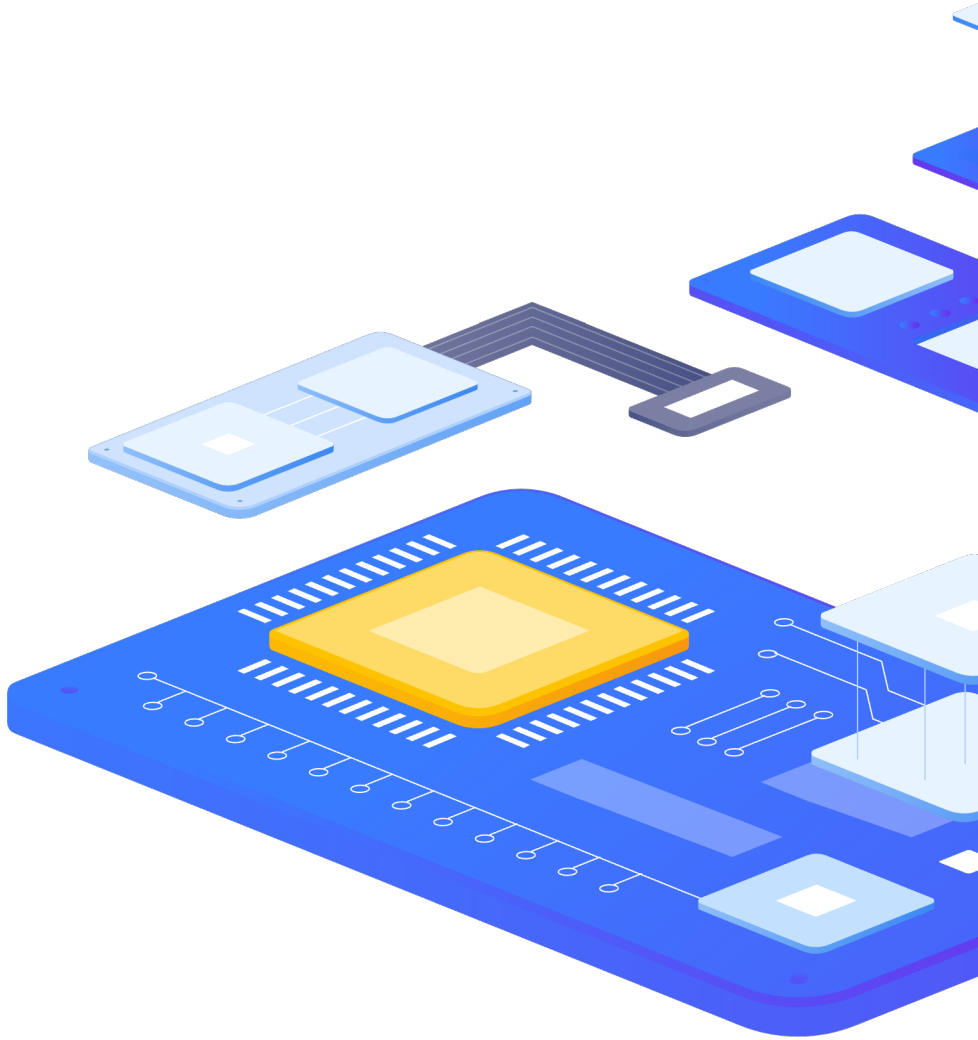
```
- id: 14038
  title: "Ensure Microsoft Firewall is enabled"
  compliance:
    - pci_dss: ["10.6.1", "1.4"]
    - hipaa: ["164.312.b", "164.312.a.1"]
    - nist_800_53: ["AU.6", "SC.7"]
    - tsc: ["CC6.1", "CC6.8", "CC7.2", "CC7.3", "CC6.7"]
  condition: all
  rules:
    - 'r:HKEY_LOCAL_MACHINE\software\policies\microsoft\windowsfirewall\domainprofile -> enablefirewall -> 1'
```

Discover the power of the open source security platform Wazuh

initMAX

File integrity monitoring (FIM)

- Watches selected files or Windows registry and triggers alerts when these files are modified, including changes, additions and deletions
- Stores the checksum and other attributes of files
- Regularly compares received information against the historical for those files
- Supports near real-time file integrity monitoring
- Provides information on who made the changes to the monitored files and the name of the program or process used to make the changes



initMAX

File integrity monitoring (FIM)

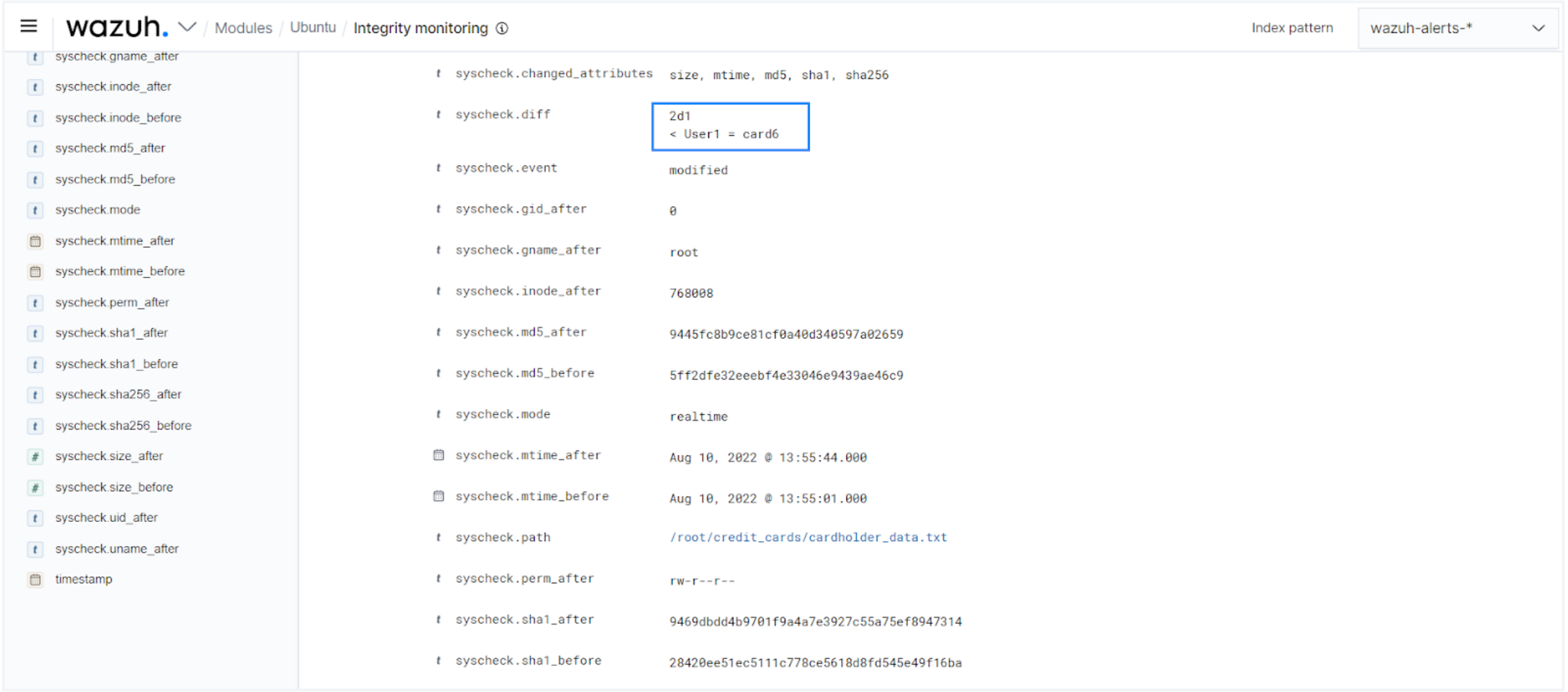
An example alert generated by FIM

```
** Alert 1540815355.847397: - ossec,syscheck,pci_dss_11.5,gpg13_4.11,gdpr_II_5.1.f,
2018 Oct 29 13:15:55 (ubuntu) 10.0.0.144->syscheck
Rule: 550 (level 7) -> 'Integrity checksum changed.'
File '/test/hello' checksum changed.
Old md5sum was: '2a4732b1de5db823e94d662d207b8fb2'
New md5sum is : '146c07ef2479cedcd54c7c2af5cf3a80'
Old sha1sum was: 'b89f4786dcf00fb1c4ddc6ad282ca0feb3e18e1b'
New sha1sum is : 'e1efc99729beb17560e02d1f5c15a42a985fe42c'
Old sha256sum was: 'a8a3ea3ddbea6b521e4c0e8f2cca8405e75c042b2a7ed848baaa03e867355bc2'
New sha256sum is : 'a7998f247bd965694ff227fa325c81169a07471a8b6808d3e002a486c4e65975'
Old modification time was: 'Mon Oct 29 13:15:19 2018', now it is 'Mon Oct 29 13:15:54 2018'
(Audit) User: 'root (0)'
(Audit) Login user: 'test (1000)'
(Audit) Effective user: 'root (0)'
(Audit) Group: 'root (0)'
(Audit) Process id: '26089'
(Audit) Process name: '/bin/nano'
```

Discover the power of the open source security platform Wazuh

initMAX

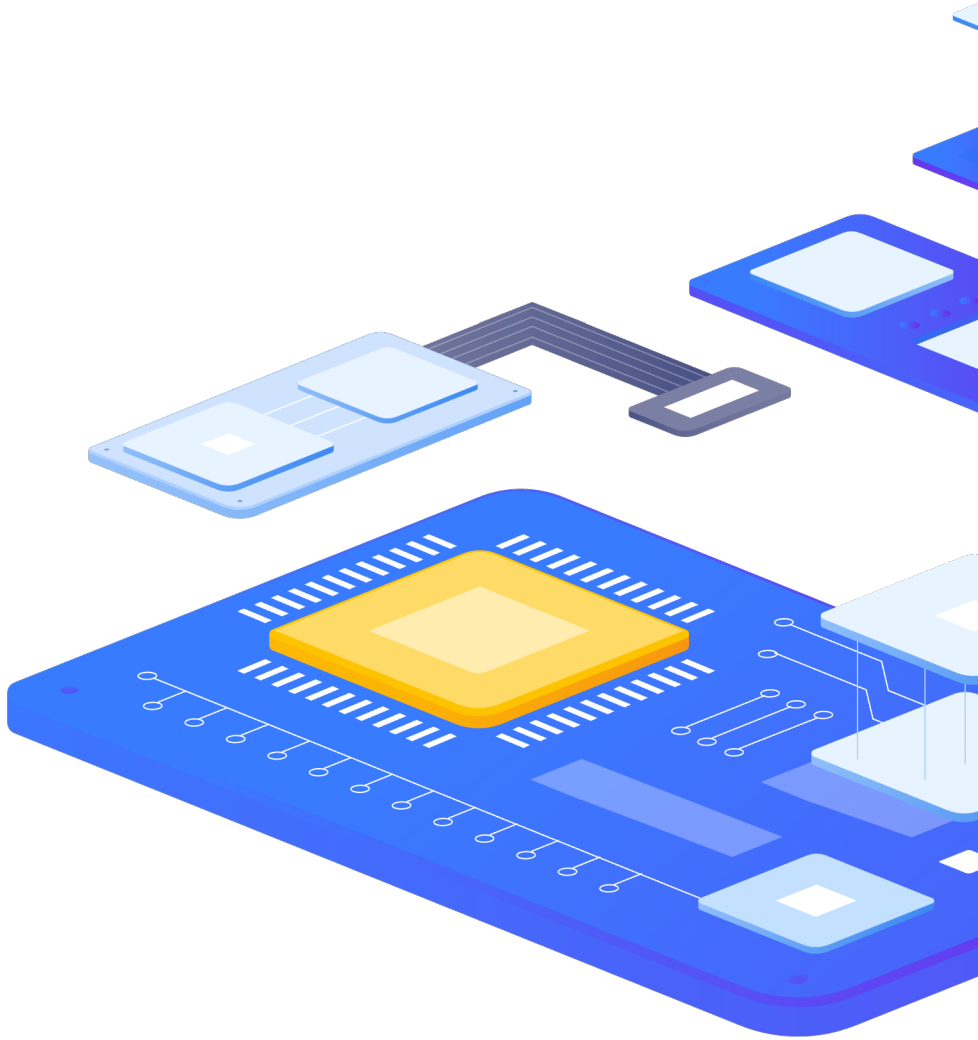
File integrity monitoring (FIM)



initMAX

Vulnerability detection

- Helps discover vulnerabilities in the operating system and applications
- Using integration with external vulnerability feeds
  - Canonical
  - Debian
  - Red Hat
  - Amazon Linux Advisories Security (ALAS)
  - Microsoft
  - National Vulnerability Database (NVD)

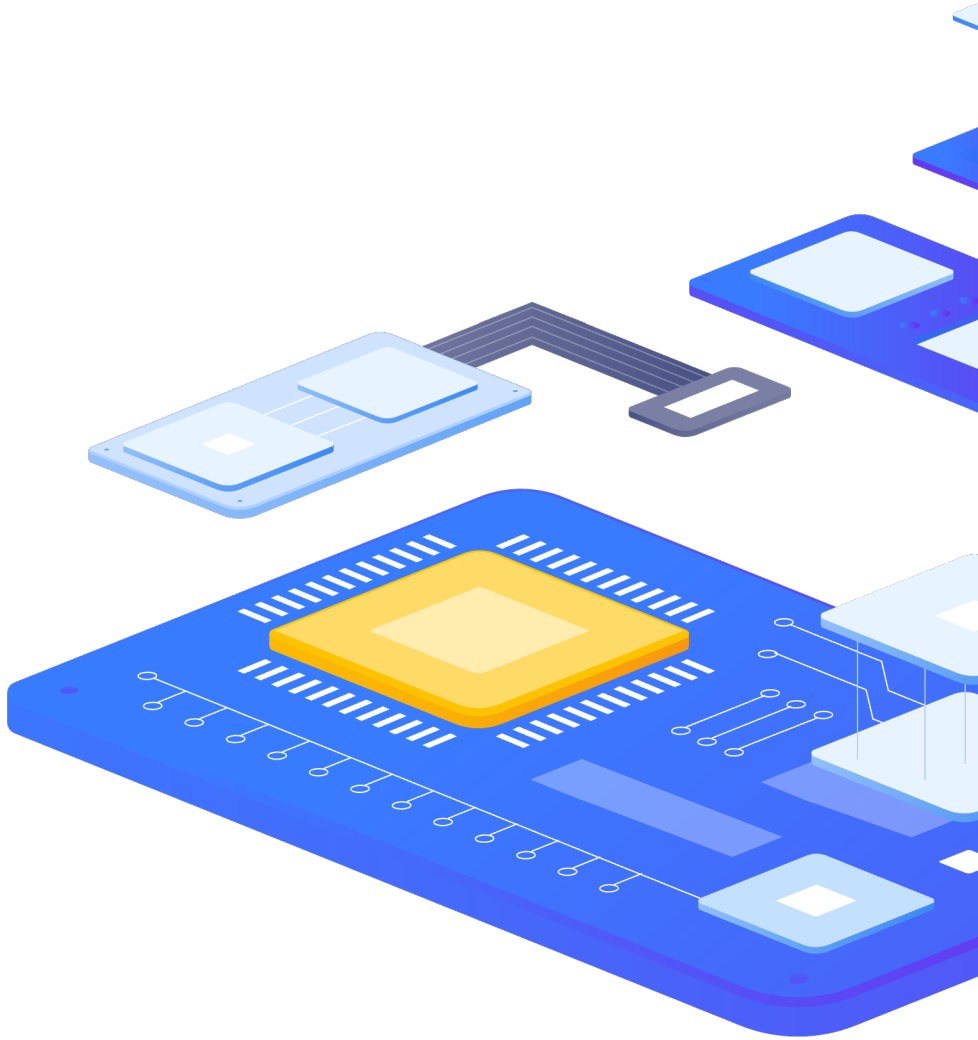


Discover the power of the open source security platform Wazuh

initMAX

Vulnerability detection

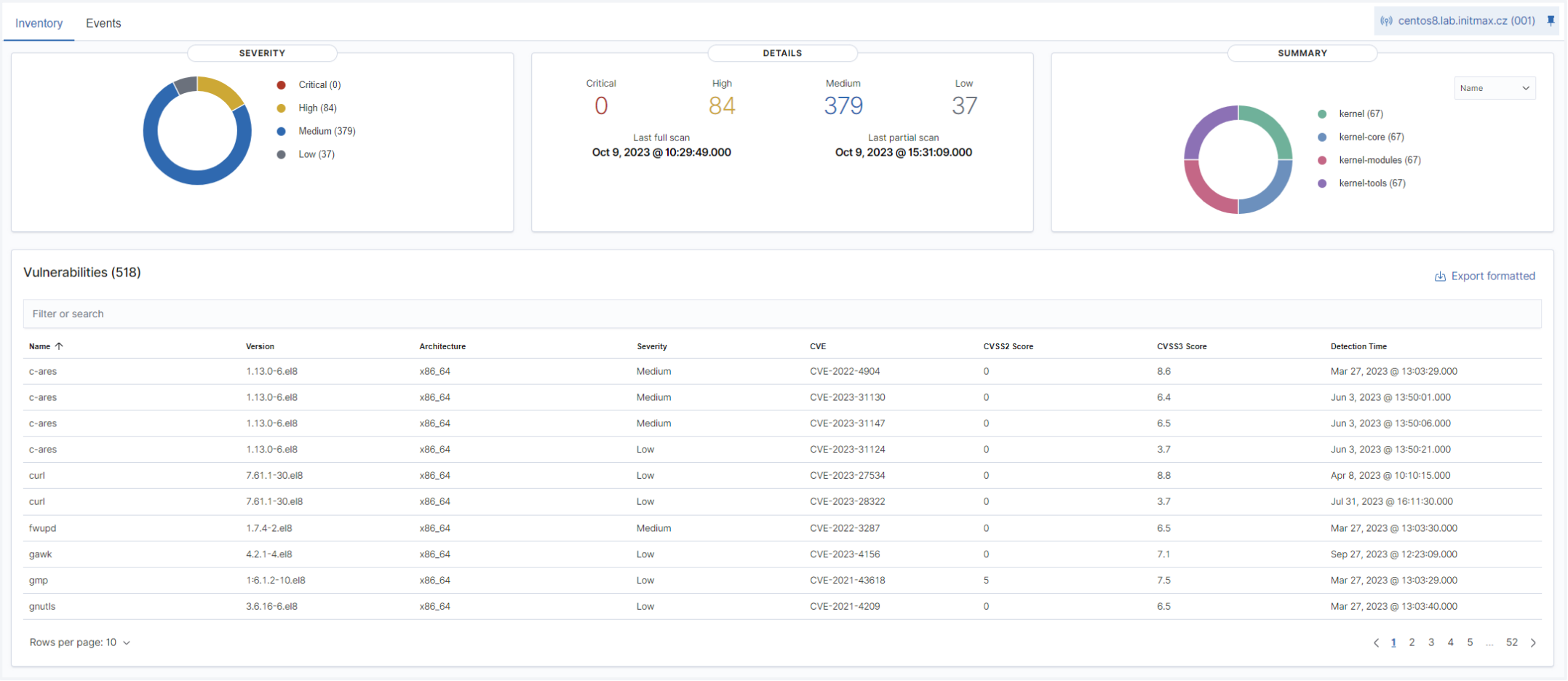
- Agents collect a list of installed applications from monitored endpoints
- Wazuh server builds a global vulnerability database from publicly available CVE repositories
- Uses this database to cross-correlate this information with the application inventory data of the agent
- Wazuh updates this database on a regular basis
- Vulnerability inventory contains the current state of every agent and includes vulnerabilities that have been detected and not resolved



Discover the power of the open source security platform Wazuh

initMAX

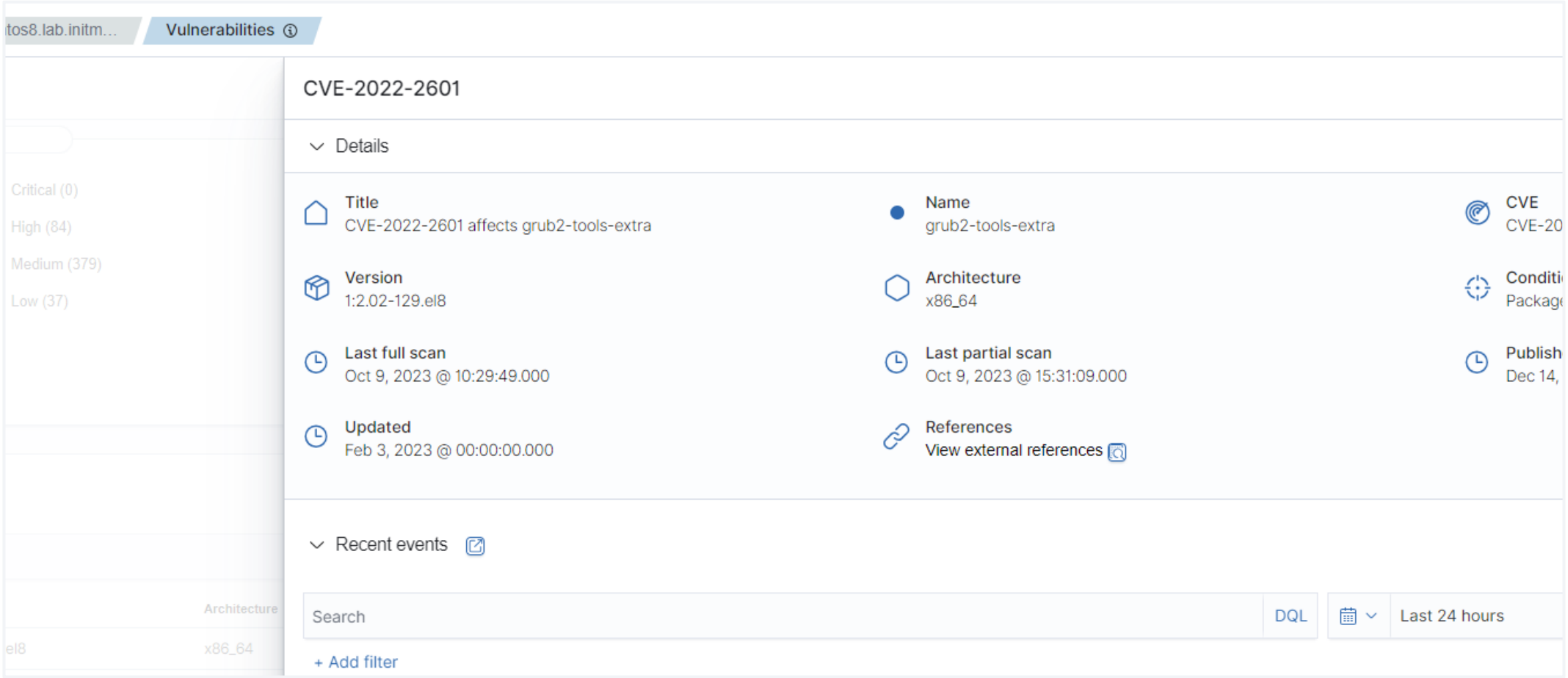
Vulnerability detection



Discover the power of the open source security platform Wazuh

initMAX

Vulnerability detection



Discover the power of the open source security platform Wazuh

initMAX

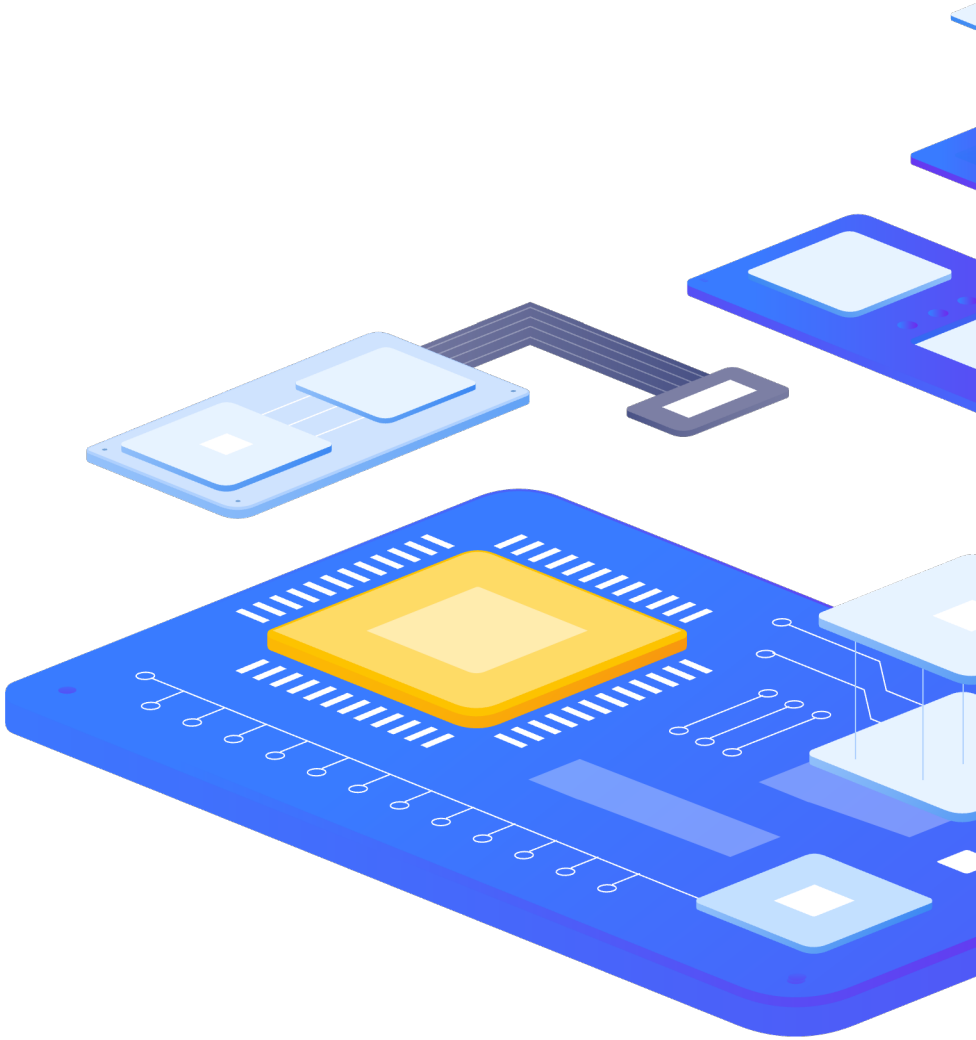
Vulnerability detection

t data.vulnerability.package.condition	Package less than 1.19.7ubuntu3.2
t data.vulnerability.package.name	dpkg
t data.vulnerability.package.version	1.19.7ubuntu3
data.vulnerability.published	May 26, 2022 @ 03:00:00.000
t data.vulnerability.rationale	Dpkg::Source::Archive in dpkg, the Debian package management system, before version 1.21.8, 1.20.10, 1.19.8, 1.18.26 is prone to a directory traversal vulnerability. When extracting untrusted source packages in v2 and v3 source package formats that include a debian.tar, the in-place extraction can lead to directory traversal situations on specially crafted orig.tar and debian.tar tarballs.
t data.vulnerability.references	https://lists.debian.org/debian-security-announce/2022/msg00115.html, https://git.dpkg.org/cgit/dpkg/dpkg.git/commit/?id=faa4c92debe45412bfcf8a44f26e827800bb24be, https://git.dpkg.org/cgit/dpkg/dpkg.git/commit/?id=7a6c03cb34d4a09f35df2f10779cbf1b70a5200b, https://lists.debian.org/debian-lts-announce/2022/05/msg00033.html, https://git.dpkg.org/cgit/dpkg/dpkg.git/commit/?id=58814cacee39c4ce9e2cd0e3a3b9b57ad437eff5, https://git.dpkg.org/cgit/dpkg/dpkg.git/commit/?id=1f23dddc17f69c9598477098c7fb9936e15fa495, https://nvd.nist.gov/vuln/detail/CVE-2022-1664, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CV
t data.vulnerability.severity	Critical
t data.vulnerability.status	Active
t data.vulnerability.title	CVE-2022-1664 affects dpkg
t data.vulnerability.type	PACKAGE

initMAX

System inventory

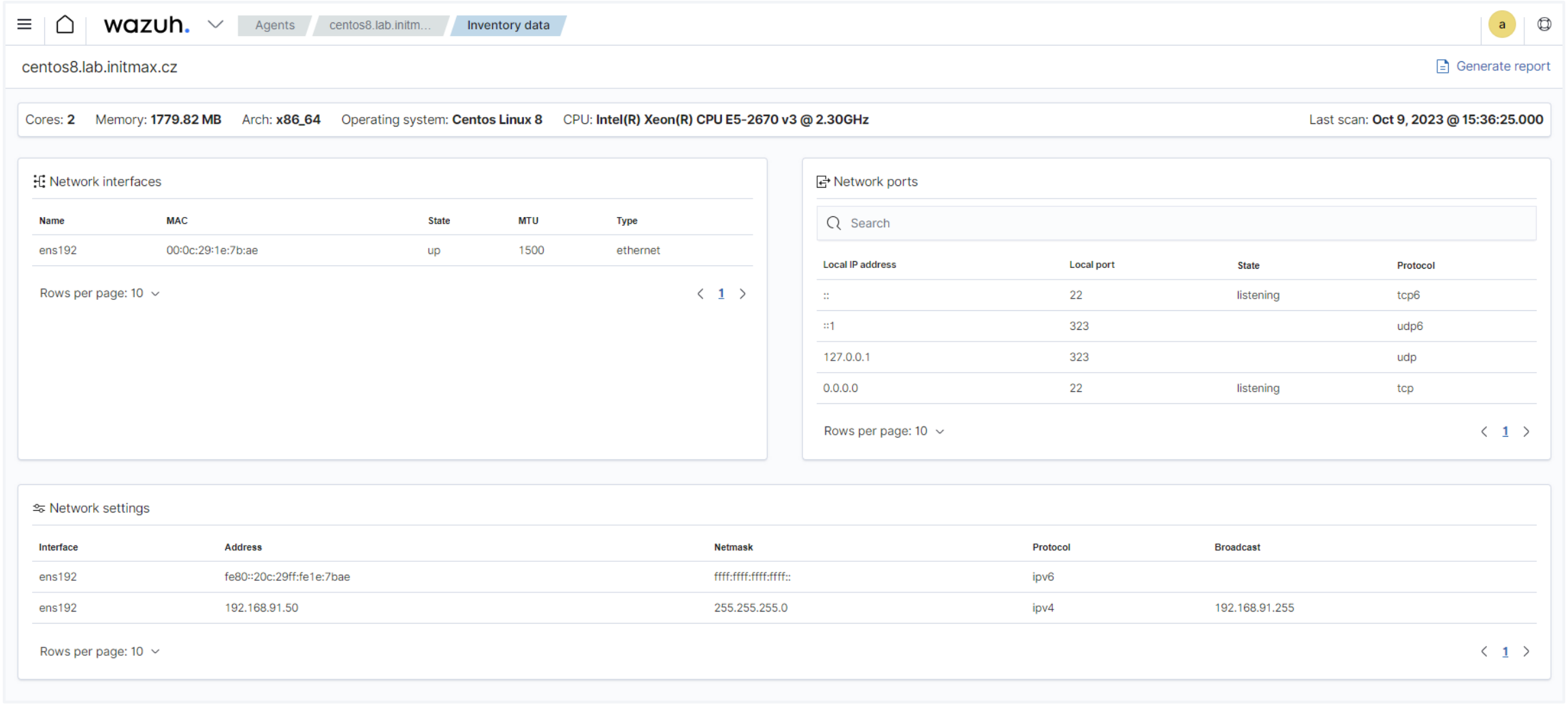
- Agents can collect interesting information for each systemOnce the agent starts, runs periodically scans of defined targets and forwarding the newly collected data to the manager, which updates the appropriate tables of the database
- The entire inventory can be found
  - At the inventory tab of the Wazuh dashboard for each agent
  - By querying the Wazuh API
  - By querying the database directly on the manager side



Discover the power of the open source security platform Wazuh

initMAX

System inventory



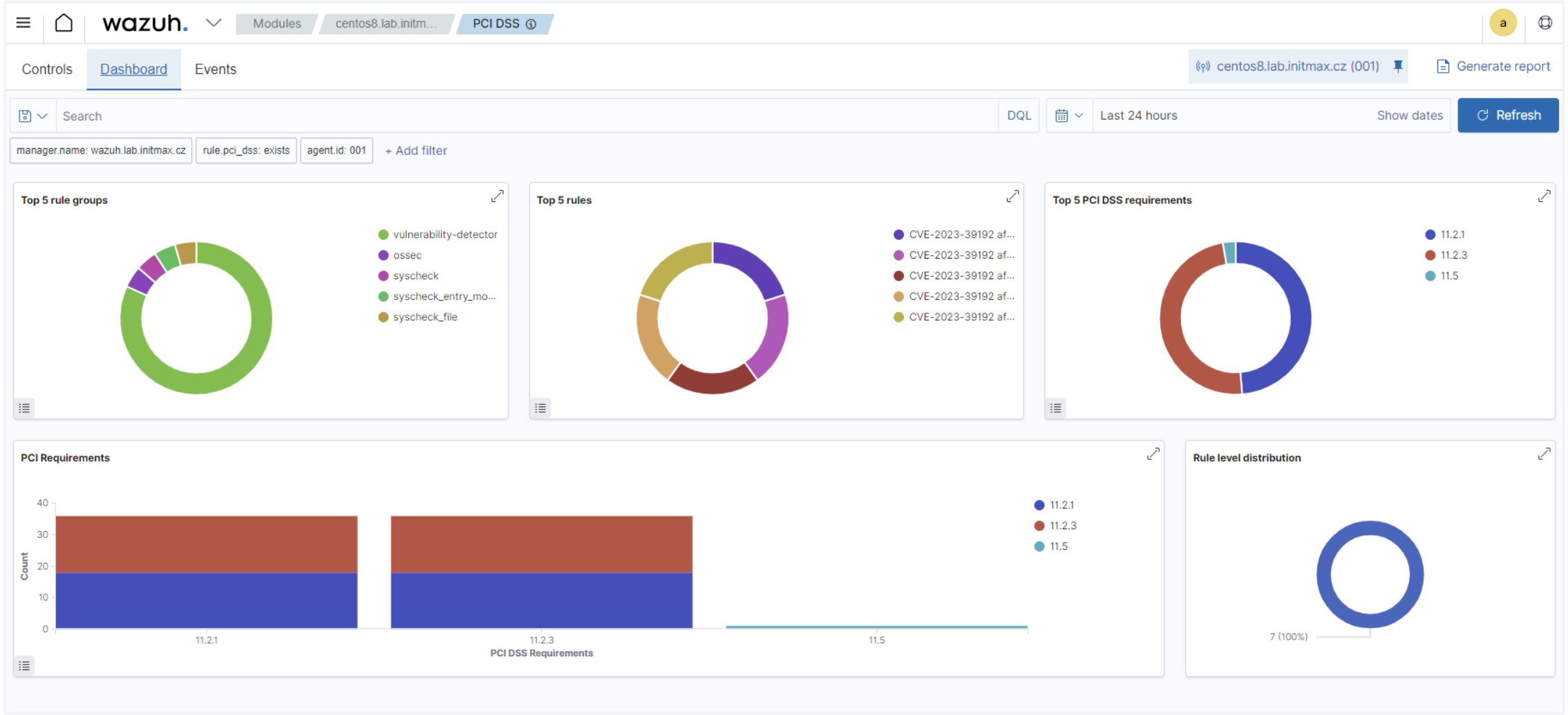
initMAX

Regulatory compliance

- Helps implement compliance requirements for regulatory compliance support and visibility
- Support for frameworks and standards
  - **PCI DSS** - Payment Card Industry Data Security Standard
  - **GDPR** - General Data Protection Regulation
  - **HIPAA** - Health Insurance Portability and Accountability Act
  - **NIST 800-53** - NIST Special Publication 800-53
  - **TSC** - Trust Services Criteria
- **Ability to monitor** for custom compliance standards, such as **local regulatory** or **company-specific compliance support.**
- Wazuh rules also include mapping with the MITRE ATT&CK framework

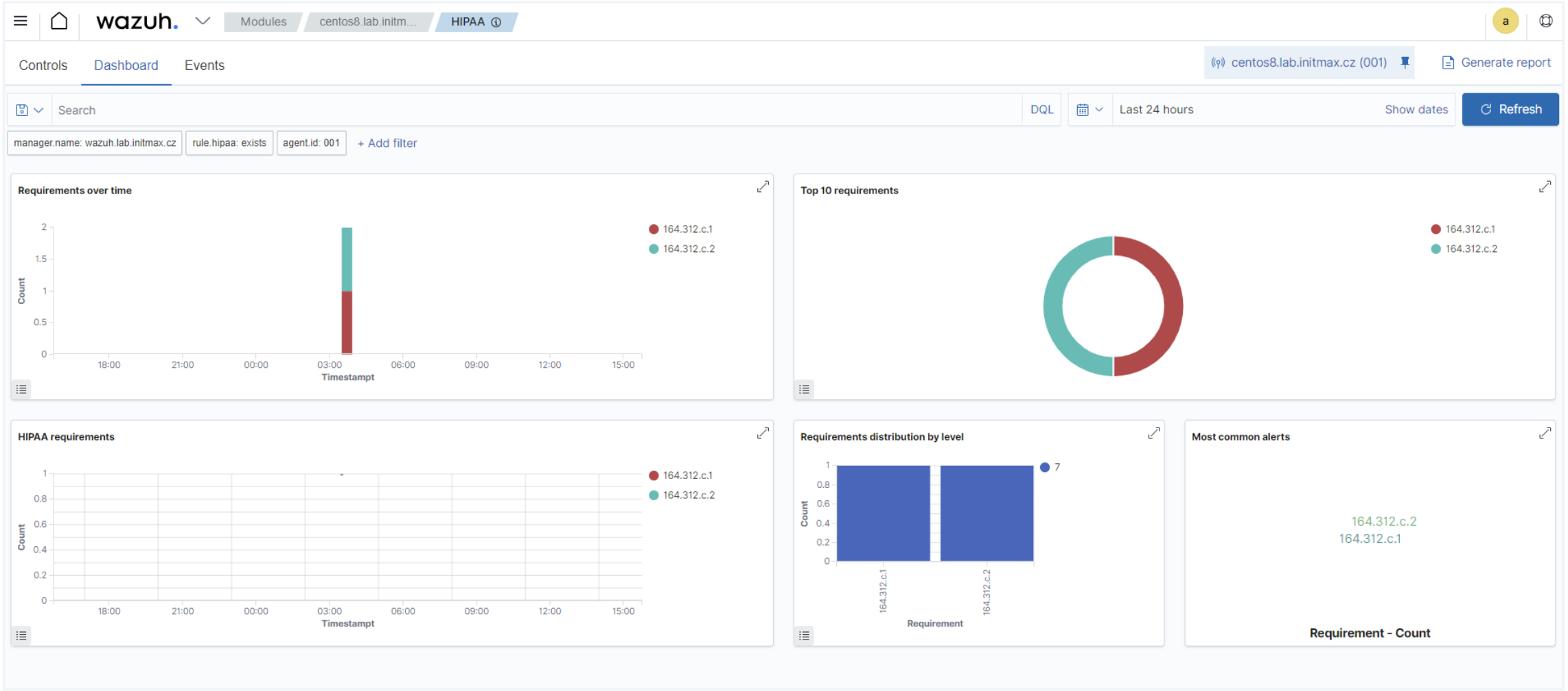
Discover the power of the open source security platform Wazuh

Regulatory compliance



Discover the power of the open source security platform Wazuh

Regulatory compliance

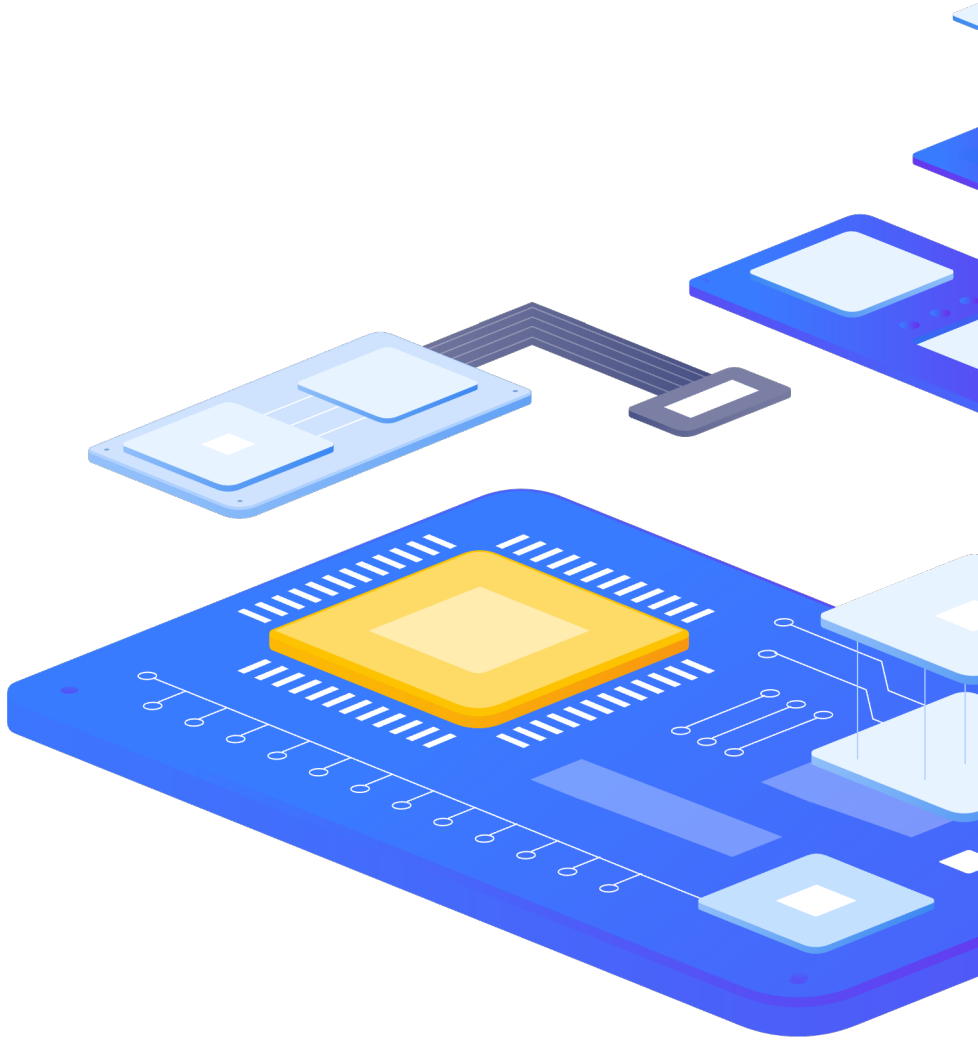


Discover the power of the open source security platform Wazuh

initMAX

Cloud security

- Support of the most widespread cloud platforms
  - Microsoft Azure
  - Microsoft 365
  - AWS - Amazon Web Services
  - GCP - Google Cloud Platform
- Support also GitHub audit log
- Two level protection
  - Endpoint level
    - Monitoring cloud instances or virtual machines
  - Cloud infrastructure level
    - Monitoring cloud services and activity by collecting and analyzing data from the API



initMAX

Container security

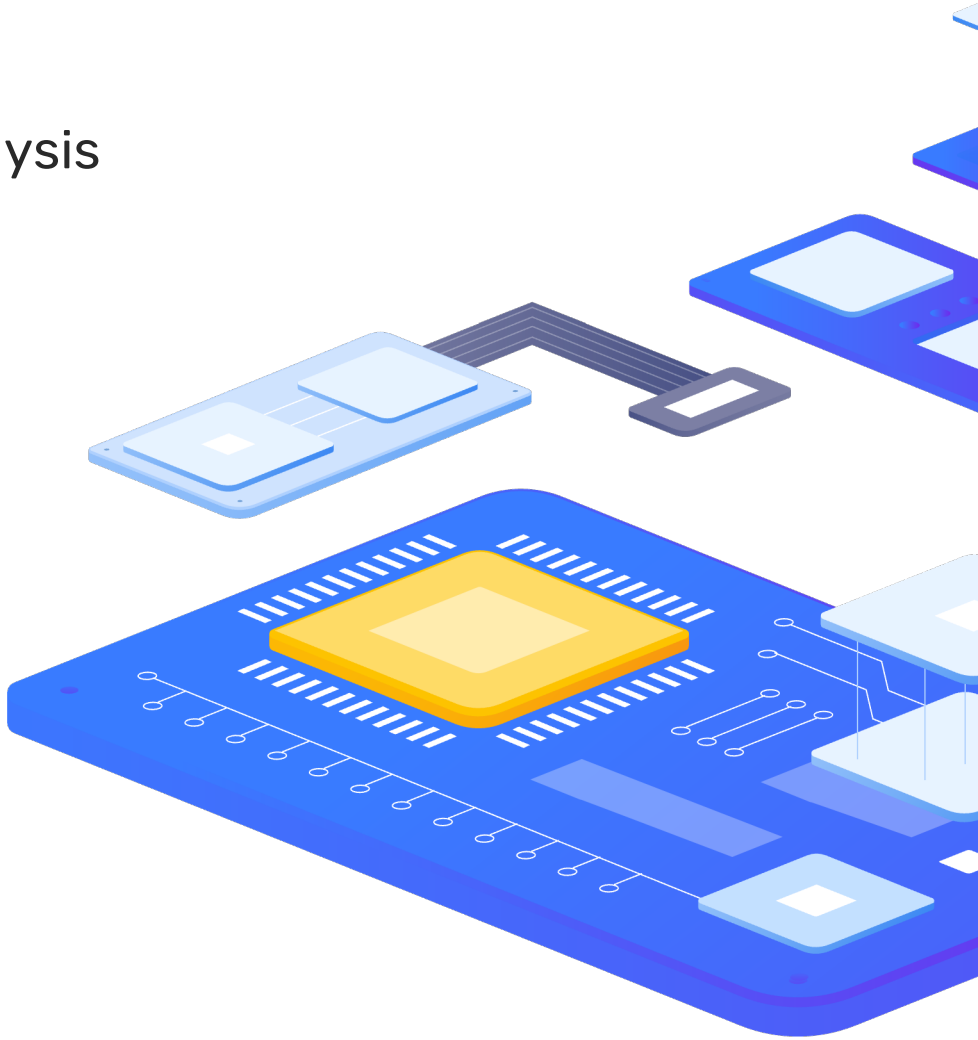
- Monitor for signs of security incidents across containers
- Alerting in real time
- Two level protection
  - Infrastructure level
    - Integration with Docker engine and Kubernetes APIs
    - Wazuh agent deployment to Docker hosts and Kubernetes nodes
    - Integration with hosted infrastructure providers
  - Container level
    - Visibility on a container level
    - Ability to send data, like application log messages and forward it to the Wazuh server for security analysis

Discover the power of the open source security platform Wazuh

initMAX

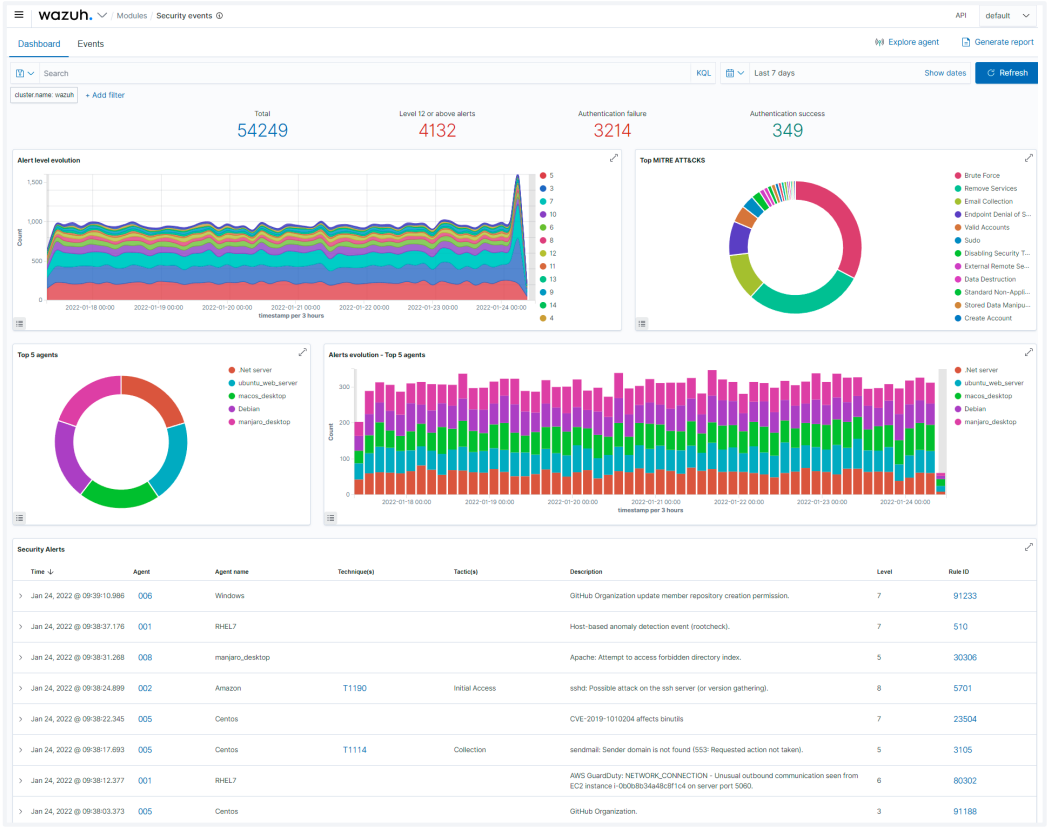
Visualization and dashboards

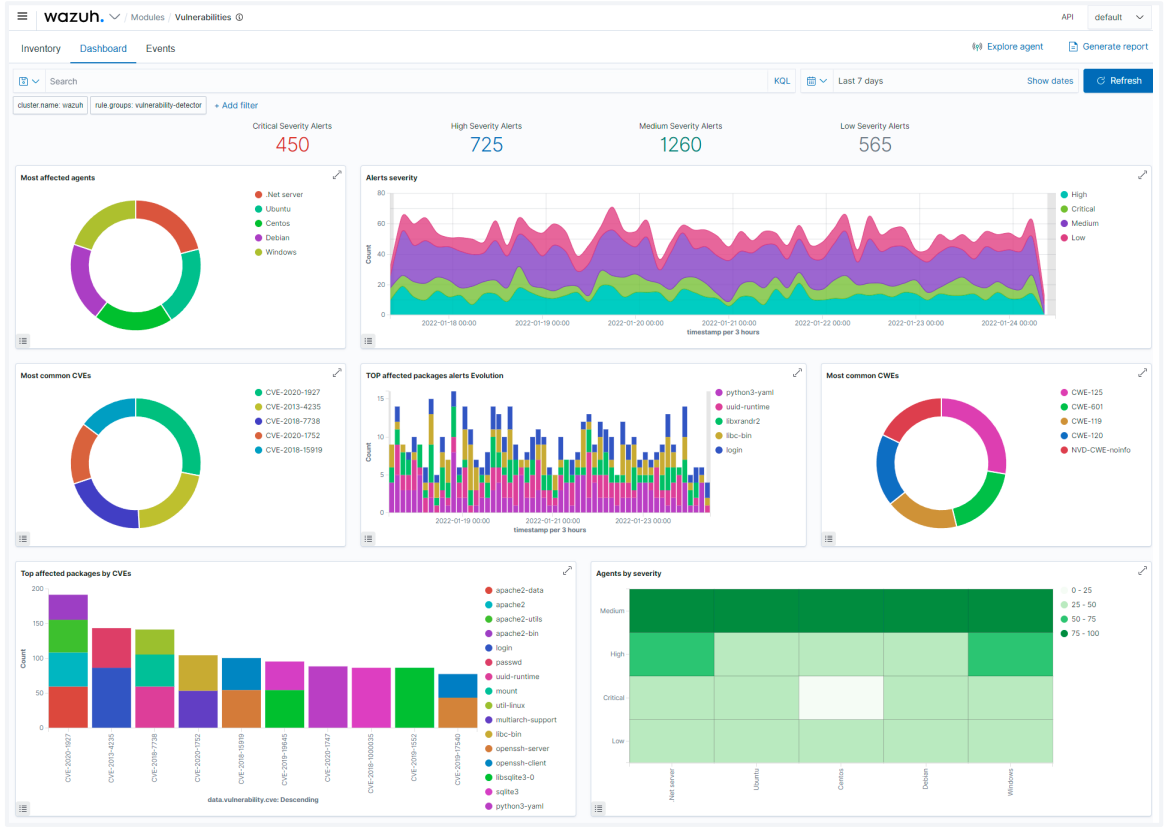
- Provides a web dashboard for data visualization and analysis
- Out-of-the-box modules for
  - Security events
  - PCI DSS compliance
  - Vulnerabilities detection
  - File integrity monitoring
  - Configuration assessment results
  - Cloud infrastructure monitoring events
  - etc.
- Perform forensic and historical analysis of your alerts



Discover the power of the open source security platform Wazuh

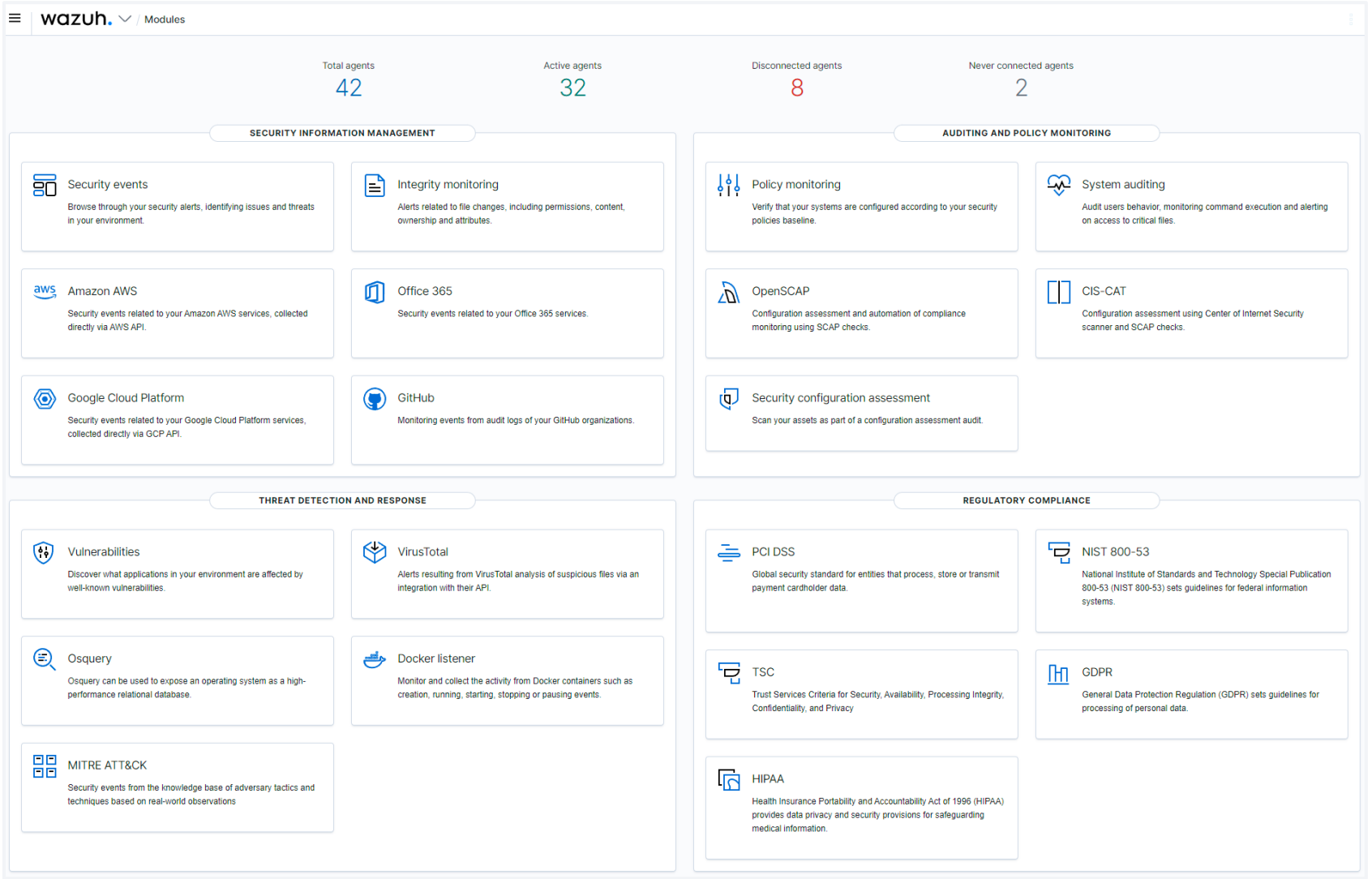
Visualization and dashboards





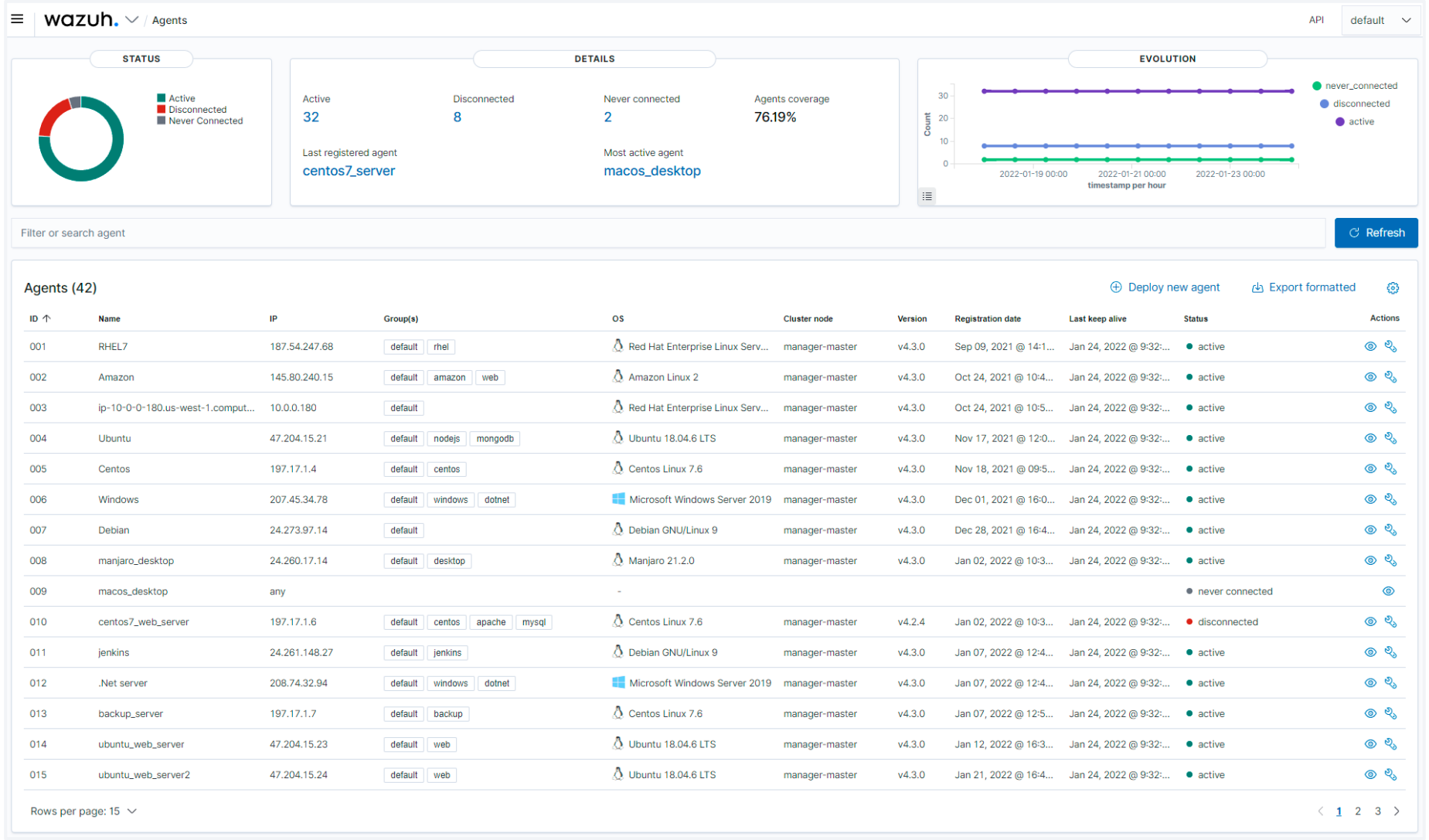
Discover the power of the open source security platform Wazuh

Visualization and dashboards



Discover the power of the open source security platform Wazuh

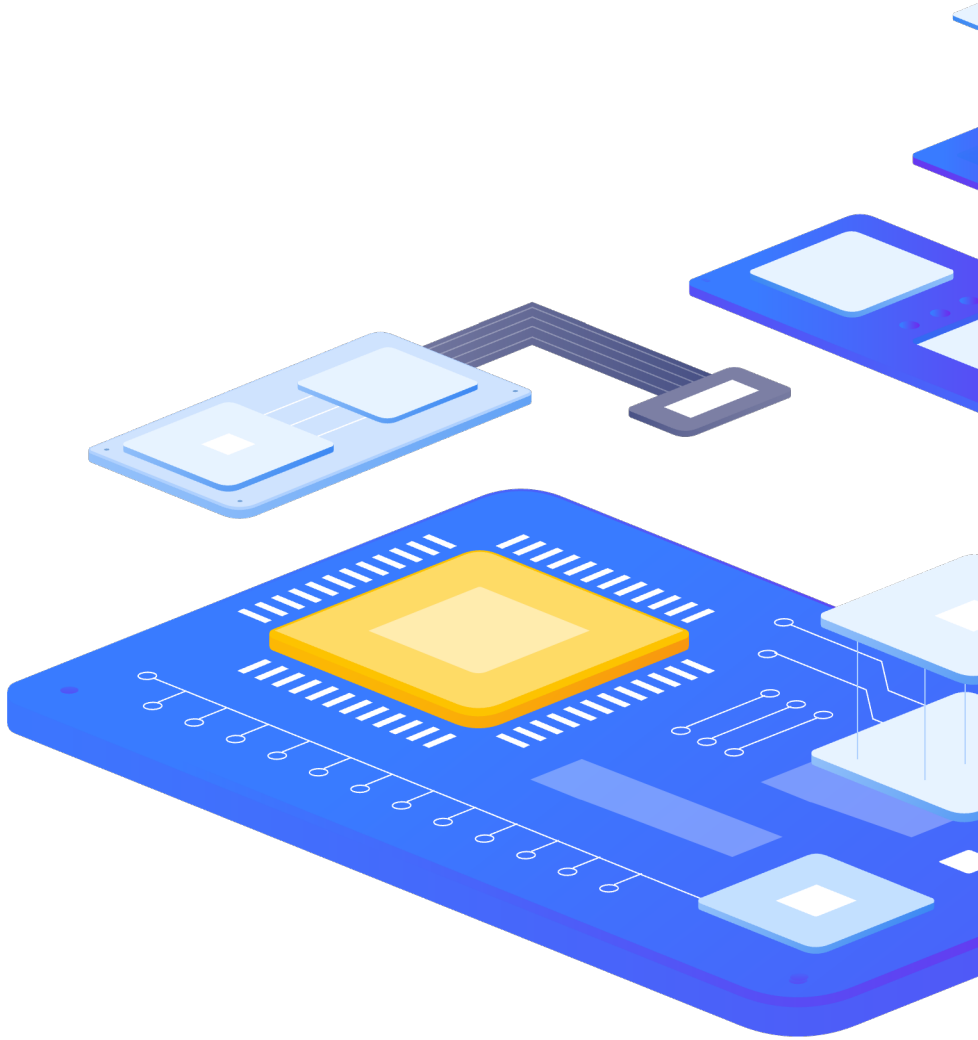
Visualization and dashboards



initMAX

Active response

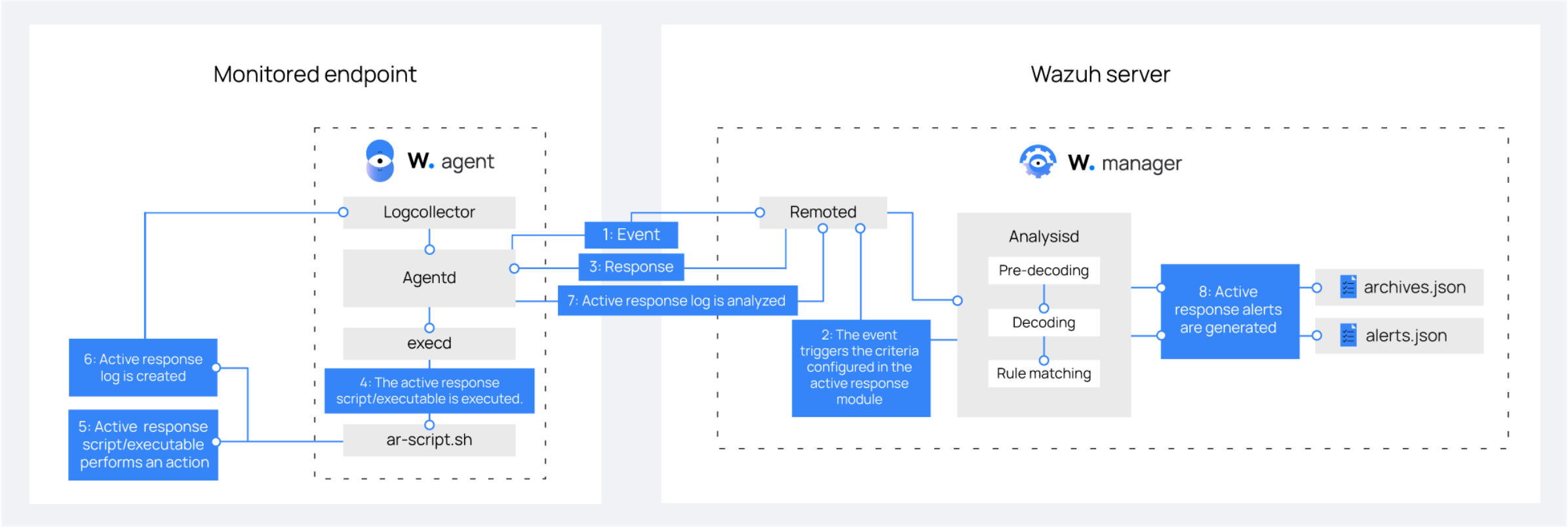
- Allows the execution of scripts whenever an event matches certain rules in your Wazuh ruleset
- Actions executed could be a firewall block or drop, traffic shaping or throttling, or account lockout, among others
- Providing out-of-the-box response scripts
- It can also run customized scripts developed by the user (Python, Bash, PowerShell, etc.)
- **Poor implementation of rules and responses might increase the vulnerability of an endpoint**



Discover the power of the open source security platform Wazuh

initMAX

Active response

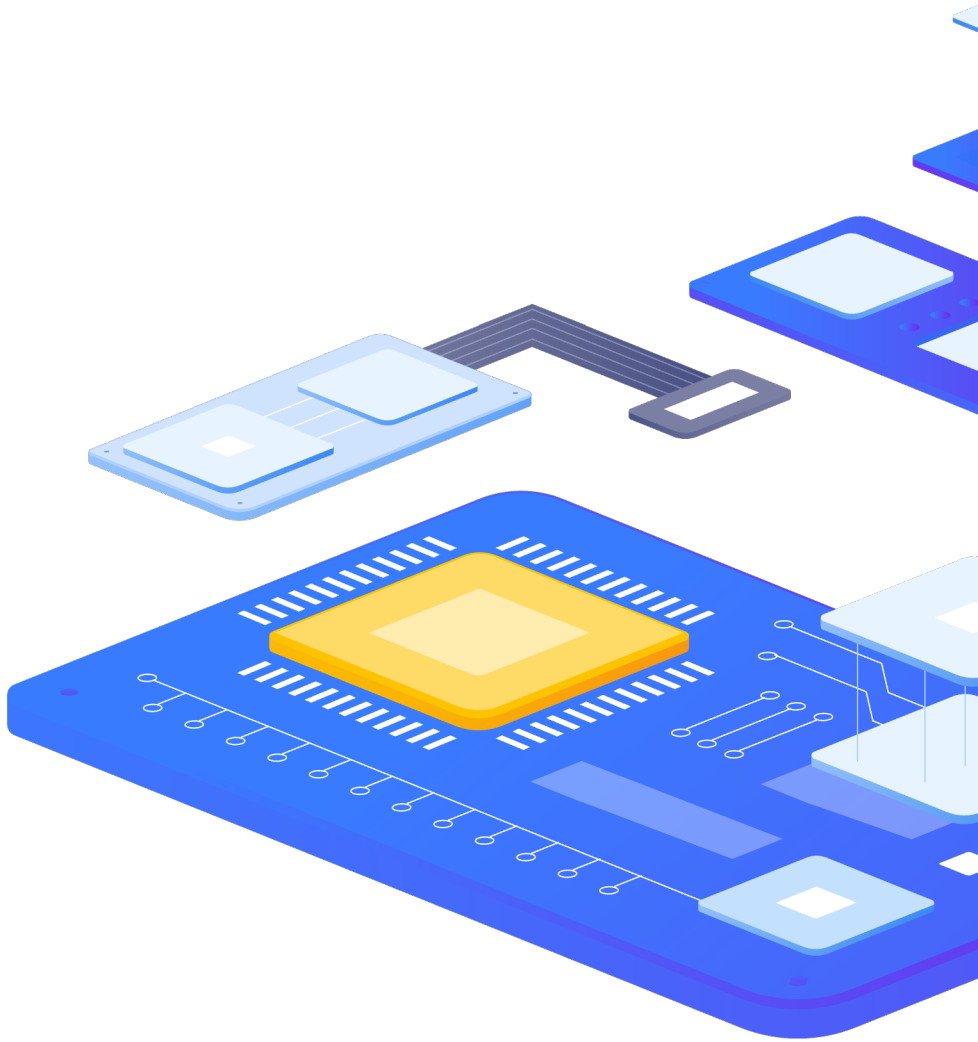


Discover the power of the open source security platform Wazuh

initMAX

Malware detection

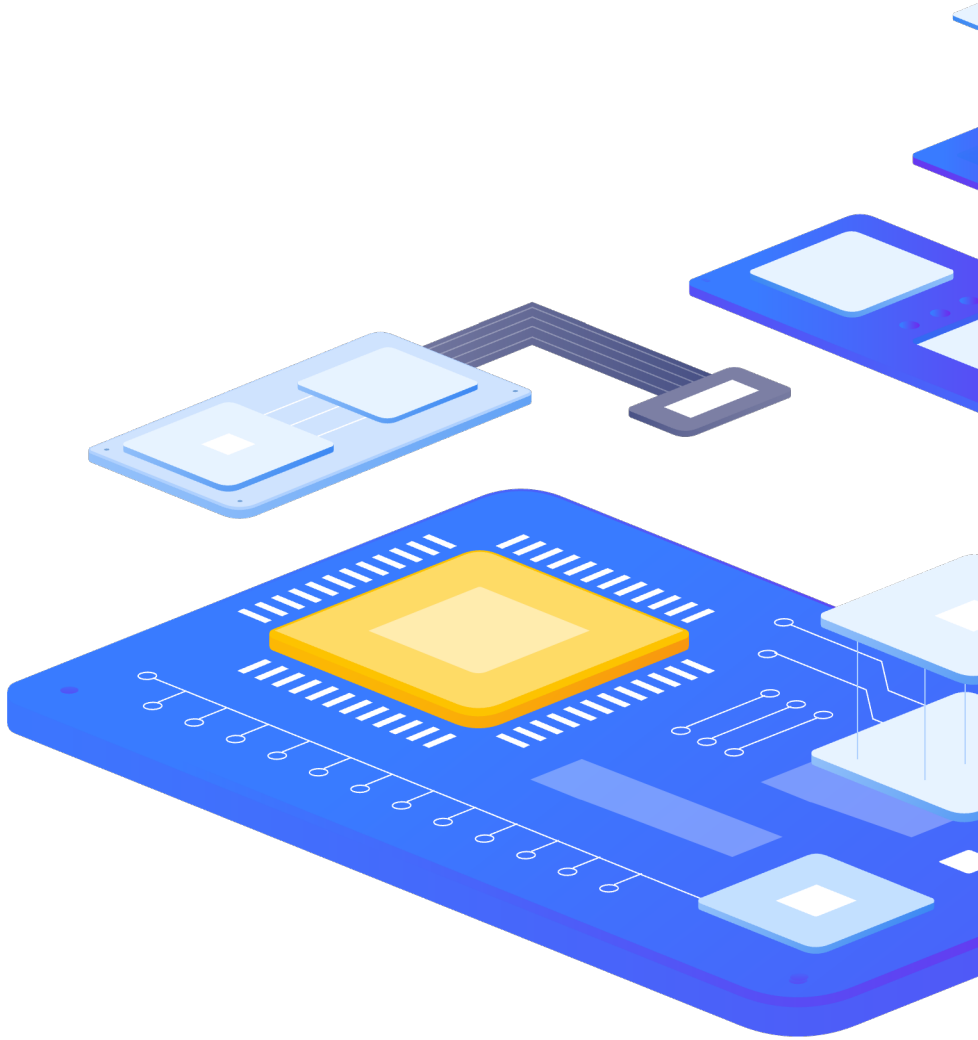
- Analyzing a computer system or network for the existence of malicious software and files
- Combines VirusTotal and CDB lists containing file hashes, and YARA scans to detect malware
- Wazuh can detects rootkit behavior on monitored endpoints
- Rootcheck continuously monitors endpoints and generates alerts when it detects any anomaly
- **Log data collection allows you to collect and analyze logs from third-party malware detection software like Windows Defender and ClamAV etc.**



initMAX

Integration with external tools

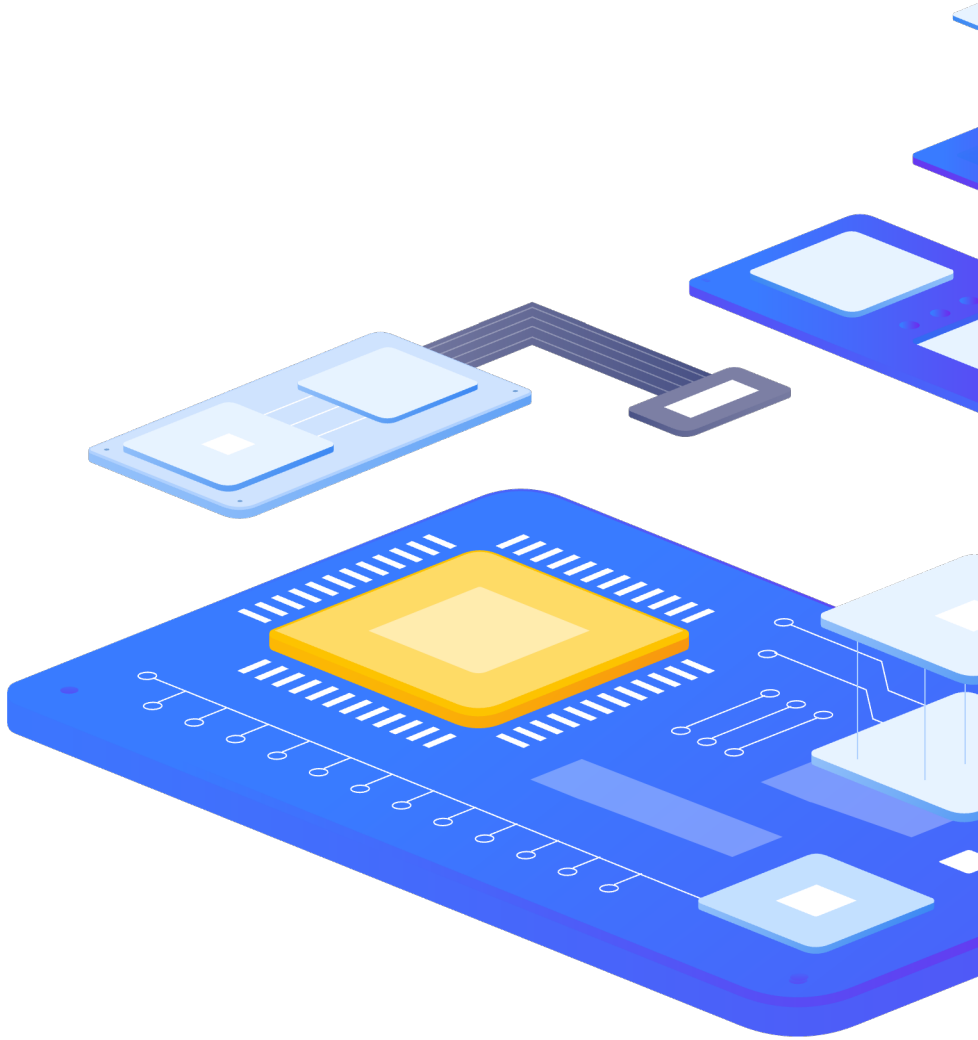
- Integrator daemon allows Wazuh to connect to external APIs and alerting tools such as
  - Slack
  - PagerDuty
  - Jira
  - TheHive
  - IRIS
  - VirusTotal
  - and whatever you need



initMAX

REST API

- API that allows interaction with the Wazuh manager
- Wazuh UI relies on the Wazuh API
- API to performs actions such as adding an agent, restarting the managers or agents, or looking up syscheck details etc.
- Some Wazuh API capabilities
  - Agent management
  - Cluster control and overview
  - Testing and verifying rules and decoders
  - Access restriction and security
  - User management
  - Statistical information
  - Error handling



initMAX

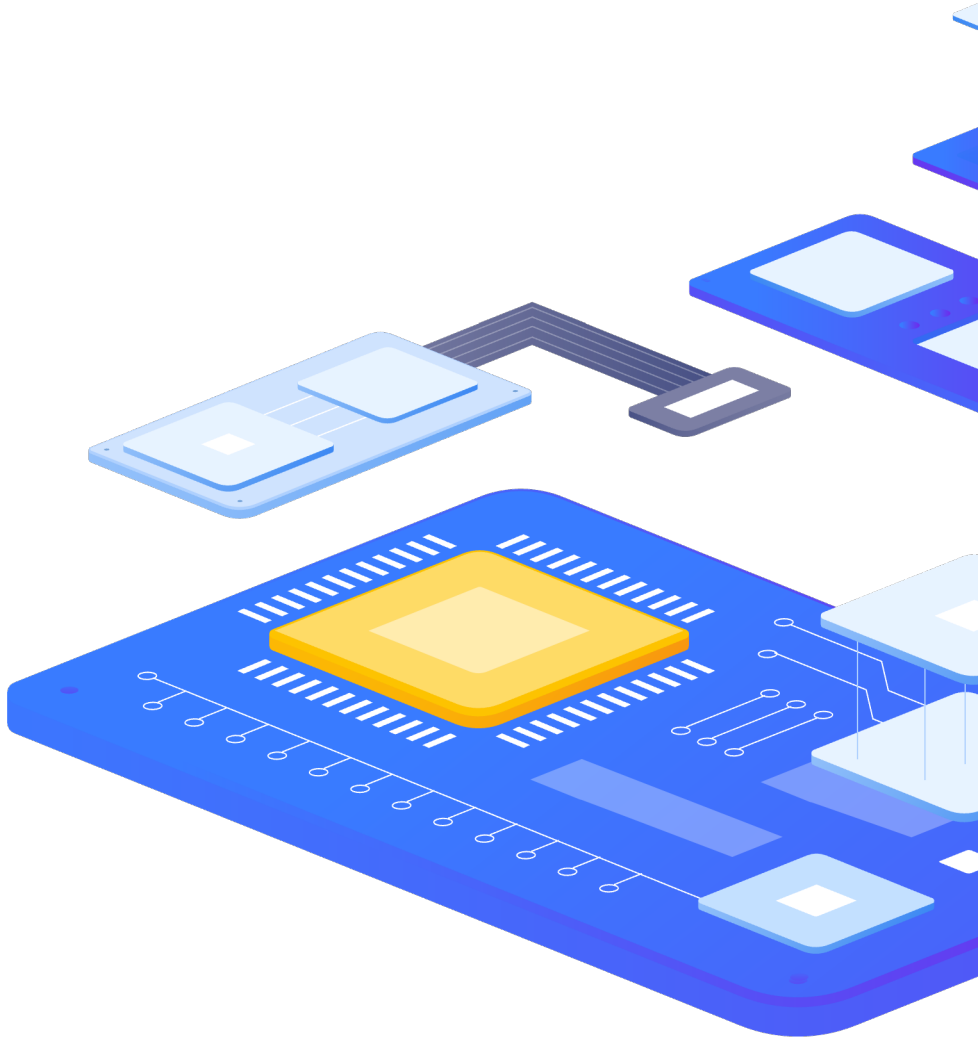
Last but not least

- Command monitoring
  - Monitor things that are not in the logs
  - Ability to monitor the output of specific commands and treat the output as though it were log file content
- Agentless monitoring
  - Allows you to monitor devices or systems with no agent via SSH, such as routers, firewalls, switches etc.
- Osquery
  - Allows managing the Osquery tool from the Wazuh agents
  - Allows you to write SQL-based queries to explore operating system data
- Fluentd forwarder
  - Allows Wazuh to forward messages to a Fluentd server
- Network IDS integration
  - integrates with a network-based intrusion detection system (NIDS) to enhance threat detection by monitoring network traffic

initMAX

Agents remote management

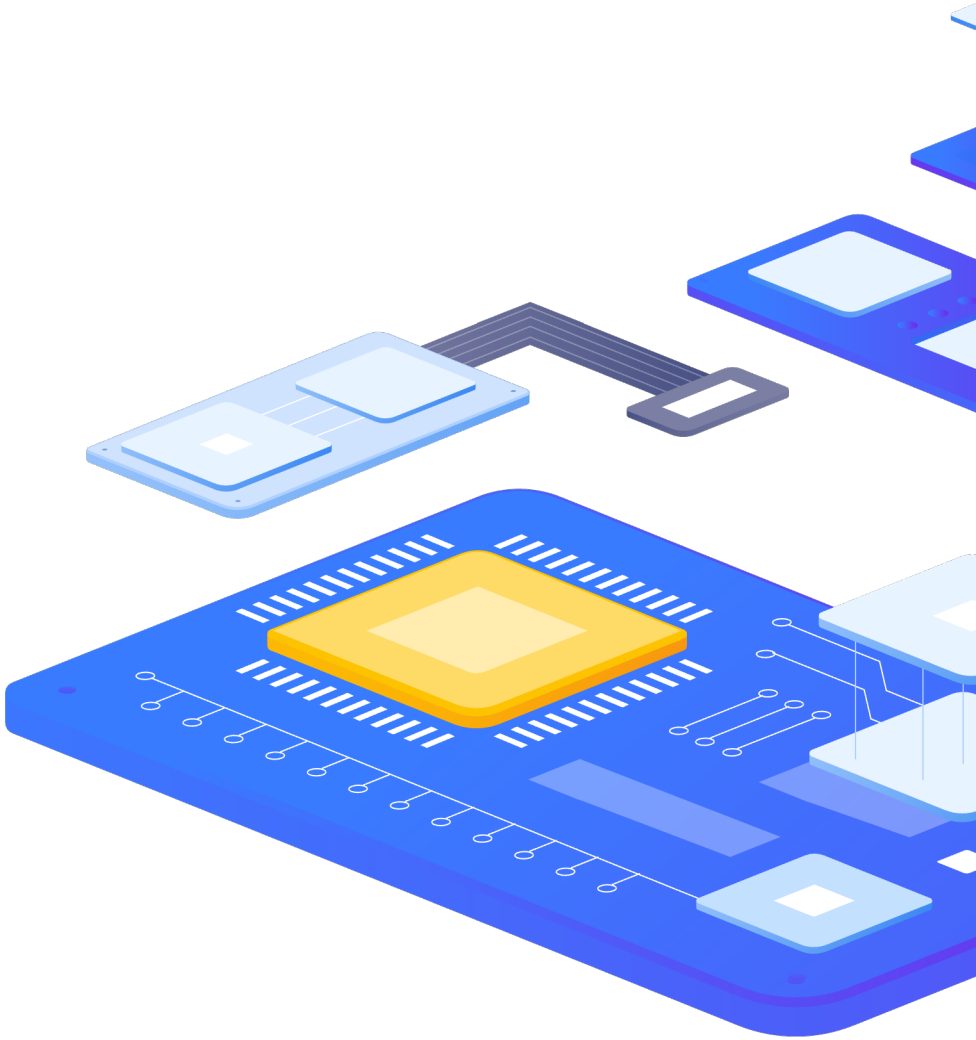
- From version 3.0.0, agents can be upgraded remotely
- Agents can be remotely configured and their status monitored
- Can be grouped together in order to send them a unique centralized configuration that is group specific
- Each agent can belong to more than one group
- Manager pushes all files included in the group folder to the agents belonging to this group
- In case an agent is assigned to multiple groups, all the files contained in each group folder will be merged into one



initMAX

Security

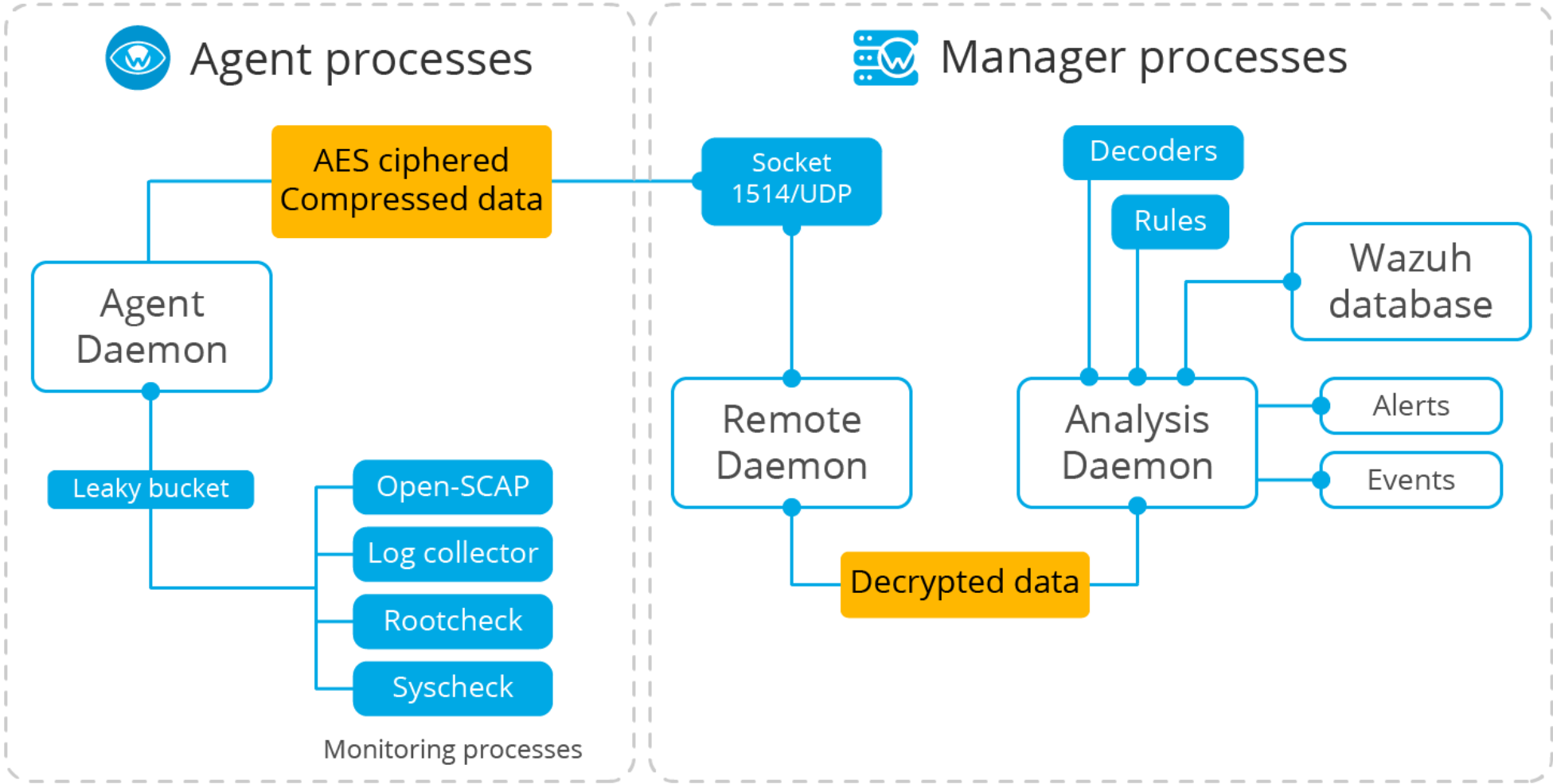
- Wazuh messages protocol uses AES encryption by default, with 128-bits per block and 256-bit keys
- All communications among nodes in the cluster are encrypted using AES algorithm
- AES encryption is used for agent-manager communications
- Communication between Wazuh server and Wazuh indexer using TLS encryption
- Dashboard communication with Wazuh RESTful API is encrypted with TLS and authenticated with a username and password
- Wazuh API is encrypted with HTTPS by default



Discover the power of the open source security platform Wazuh

initMAX

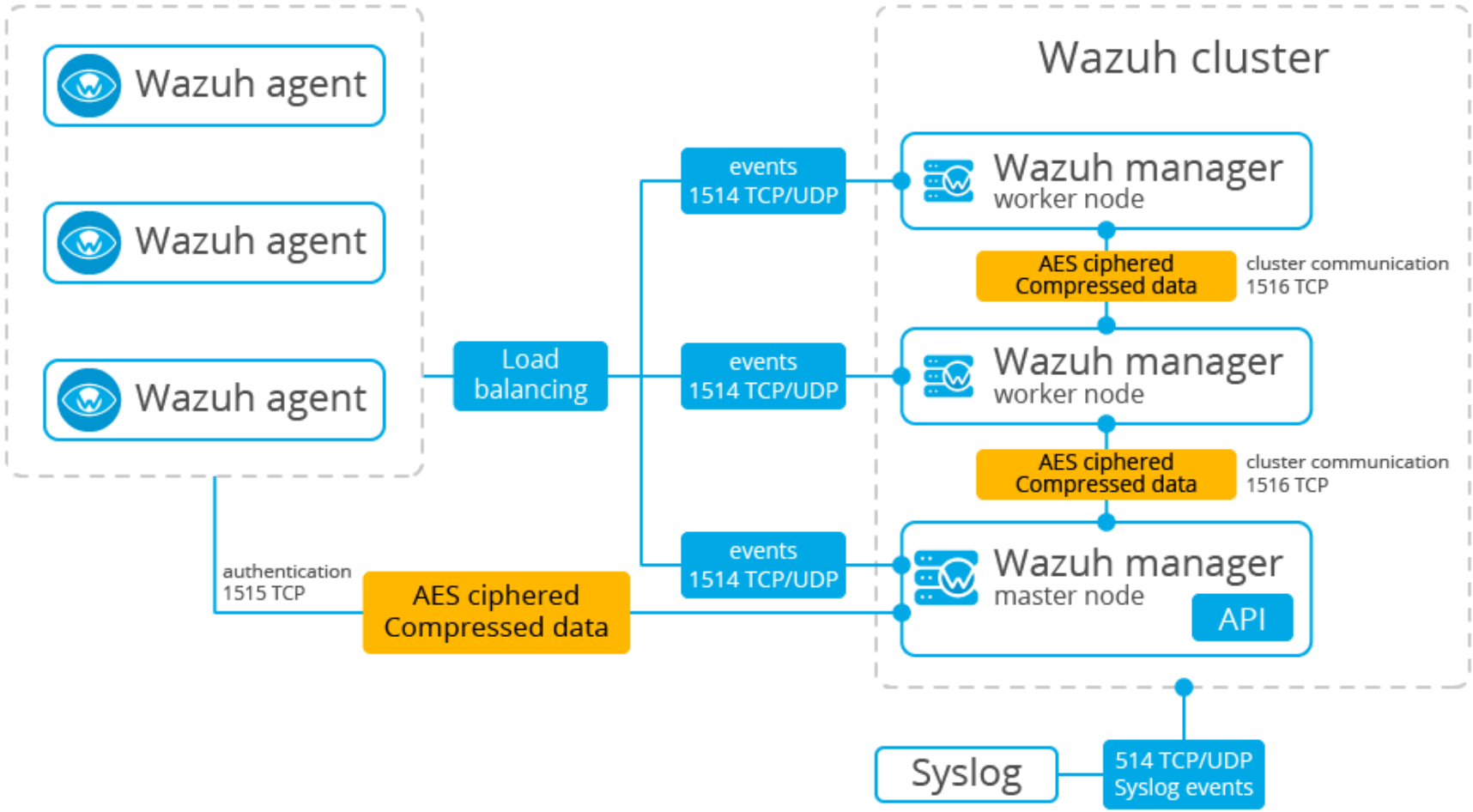
Security



Discover the power of the open source security platform Wazuh

initMAX

Security

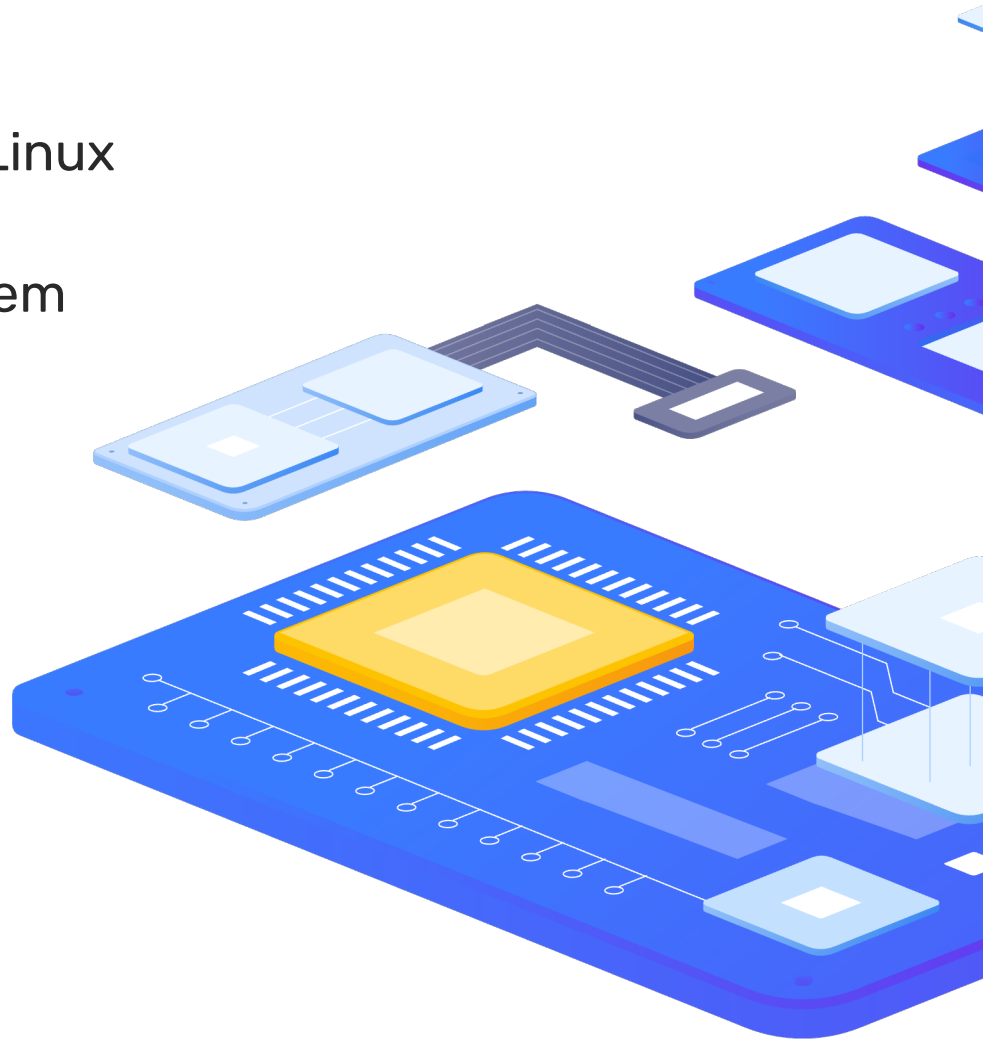


Discover the power of the open source security platform Wazuh

initMAX

Deployment Options

- Wazuh central components can be installed on a 64-bit Linux operating system
- Wazuh **recommends** any of the following operating system versions:
  - CentOS 7, 8
  - Ubuntu 16.04, 18.04, 20.04, 22.04
  - Red Hat Enterprise Linux 7, 8, 9
  - Amazon Linux 2
- Wazuh Agent supported platforms



initMAX

Deployment Options

Quickstart deployment

- Deploying the Wazuh server, the Wazuh indexer, and the Wazuh dashboard on the same host
- This is usually enough for monitoring up to 100 endpoints and for 90 days of queryable/indexed alert data

Agents	CPU	RAM	Storage (90 days)
1-25	4 vCPU	8 GiB	50 GB
25-50	8 vCPU	8 GiB	100 GB
50-100	8 vCPU	8 GiB	200 GB

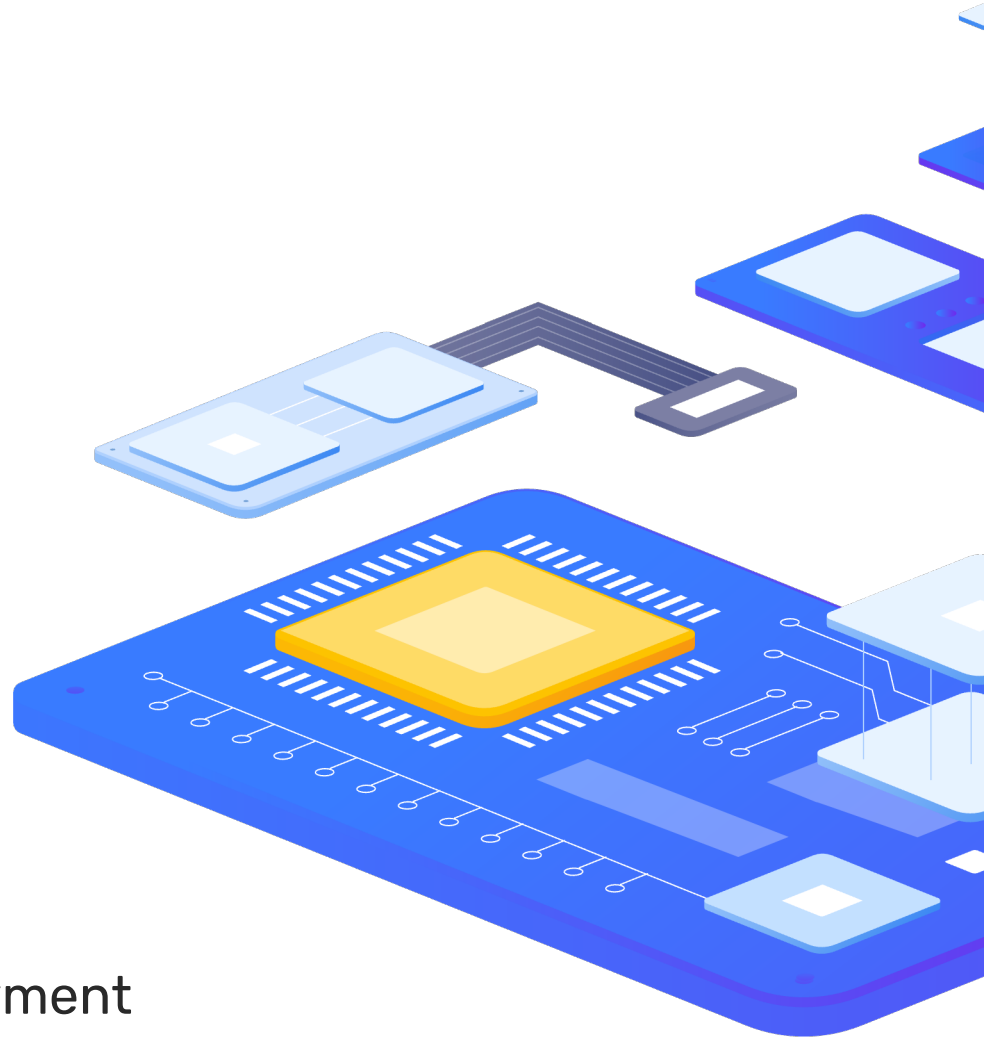
Larger environments

- Is recommended a distributed deployment
- Multi-node cluster configuration is available for the Wazuh server and for the Wazuh indexer, providing high availability and load balancing

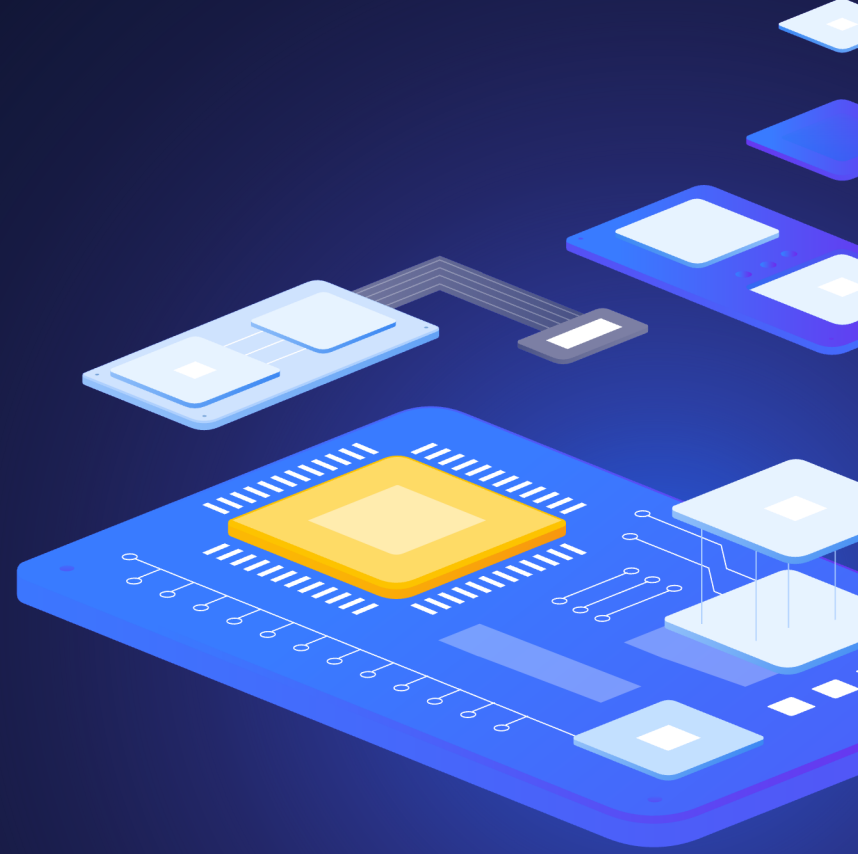
initMAX

Deployment Options

- Ready-to-use machines
  - Virtual Machine (OVA)
  - Amazon Machine Images (AMI)
- Containers
  - Deployment on Docker
  - Deployment on Kubernetes
- Offline
- From sources
- Commercial options
  - Installation with Elastic Stack basic license
  - Installation with Splunk
- It is also possible to use Ansible or Puppet for the deployment

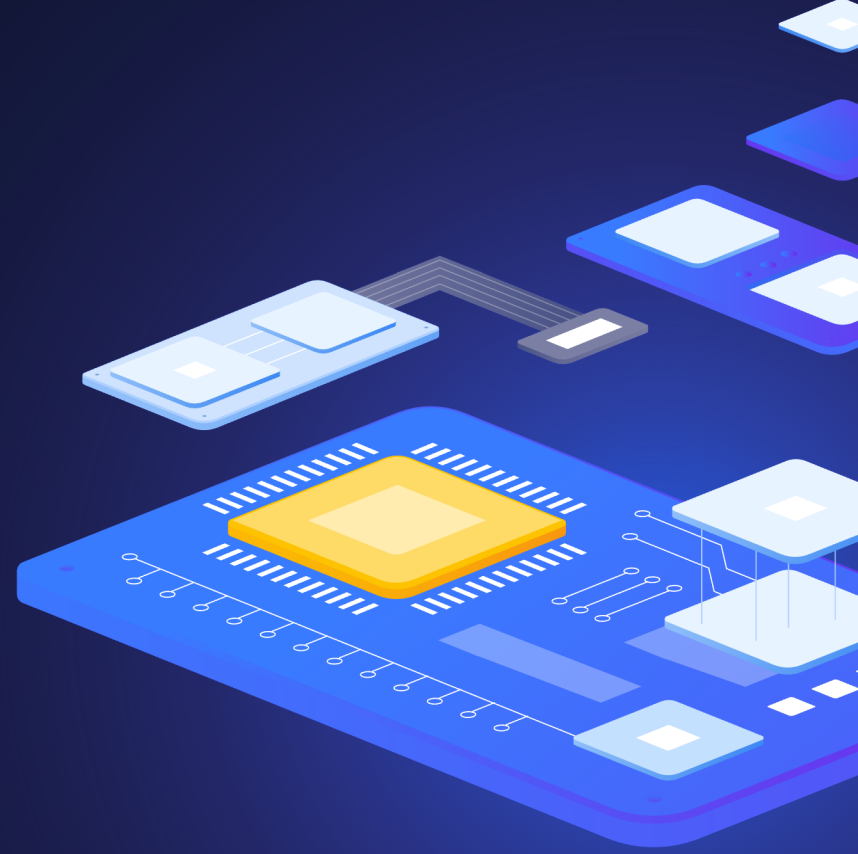


Demo time



initMAX

Questions?



Discover the power of the open source security platform Wazuh

initMAX

Contact us:

Phone:	+420 800 244 442
Web:	https://www.initmax.cz
Email:	tomas.hermanek@initmax.cz
LinkedIn:	https://www.linkedin.com/company/initmax
Twitter:	https://twitter.com/initmax
Tomáš Heřmánek:	+420 732 447 184