# จับภัยคุกคาม Small Network, Real Threats ด้วย Wazuh

**Pongpipat Thunyawiraphap**

https://mikrotiktutorial.com/

**Supadej Suthiphongkanasai**

https://packethunter.net/

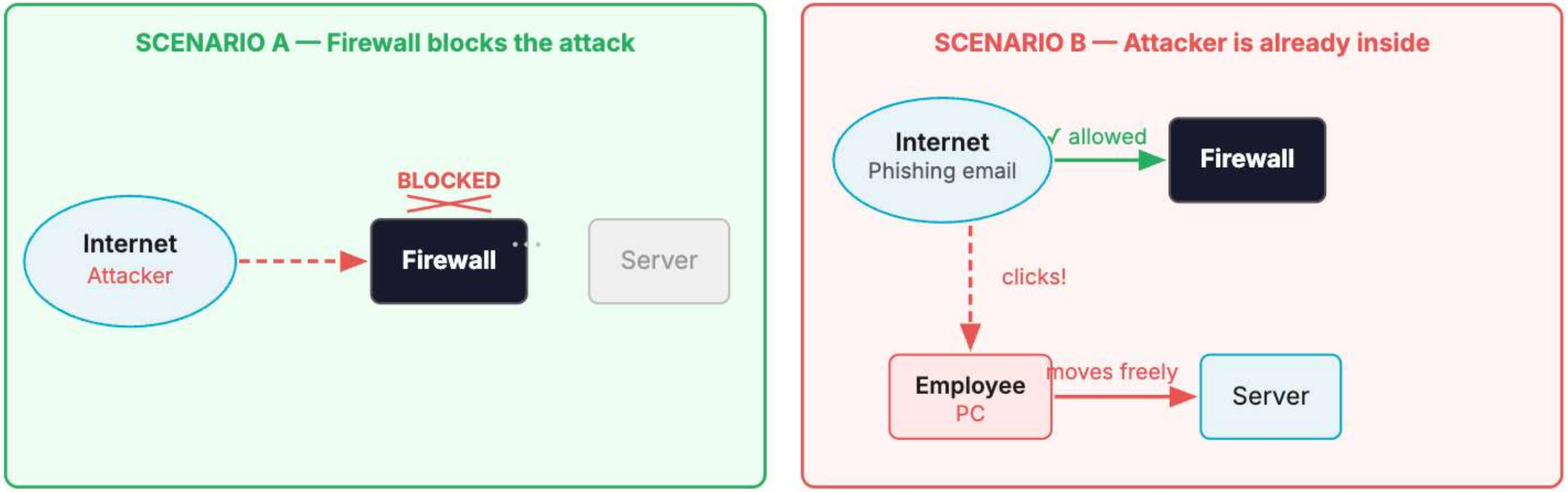
MODULE 0 · WAZUH FOR NETWORK ENGINEERS

# Wazuh for Small Business Networks

Security visibility for teams of 1 to 500 — without the enterprise price tag

Why Wazuh · Where it sits · SMB vs Enterprise · 8 use cases · requirements

# Your firewall can't see inside




**The threat is already in — and the firewall never saw it.**

# SIEM · EDR · XDR — What's the difference?

## SIEM

**Security Information & Event Management**

- 📩 Collects & stores logs from servers, firewalls, switches
- 🔍 Correlates events & triggers alerts
- 📋 Compliance reporting
- 🏛️ Long-term log retention

Watches: network perimeter & servers

**Gap: limited endpoint visibility**

Example: Splunk · IBM QRadar · Wazuh

## EDR

**Endpoint Detection & Response**

- 💻 Runs agent on every endpoint
- 🧬 Detects malware & anomalies
- ⚡ Real-time process monitoring
- 🔬 Deep forensic investigation
- 🚫 Isolate & kill malicious processes

Watches: laptops, servers, workstations

**Gap: no network or cloud log view**

Example: CrowdStrike · Carbon Black

## XDR

**Extended Detection & Response**

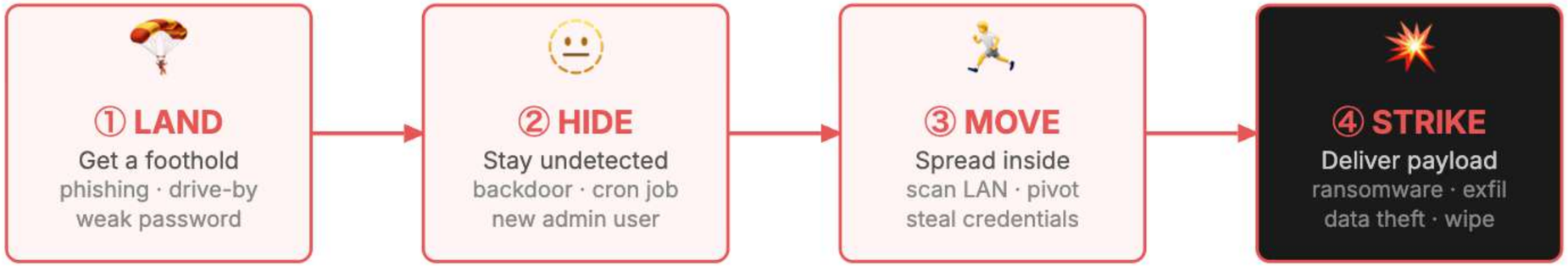
- 🔗 Combines SIEM + EDR + more
- ☁️ Covers endpoint, network & cloud
- 🤖 Automated threat response
- 📡 MITRE ATT&CK mapped alerts
- 🌐 One dashboard for everything

Watches: endpoints + network + cloud

**✓ Wazuh delivers all three**

Example: Wazuh · Palo Alto XDR

# What attackers do after they're in




Average dwell time before discovery: **207 days** (IBM 2024)

🔐 **Ransomware median dwell time: ~10 days** — attackers hide before detonating

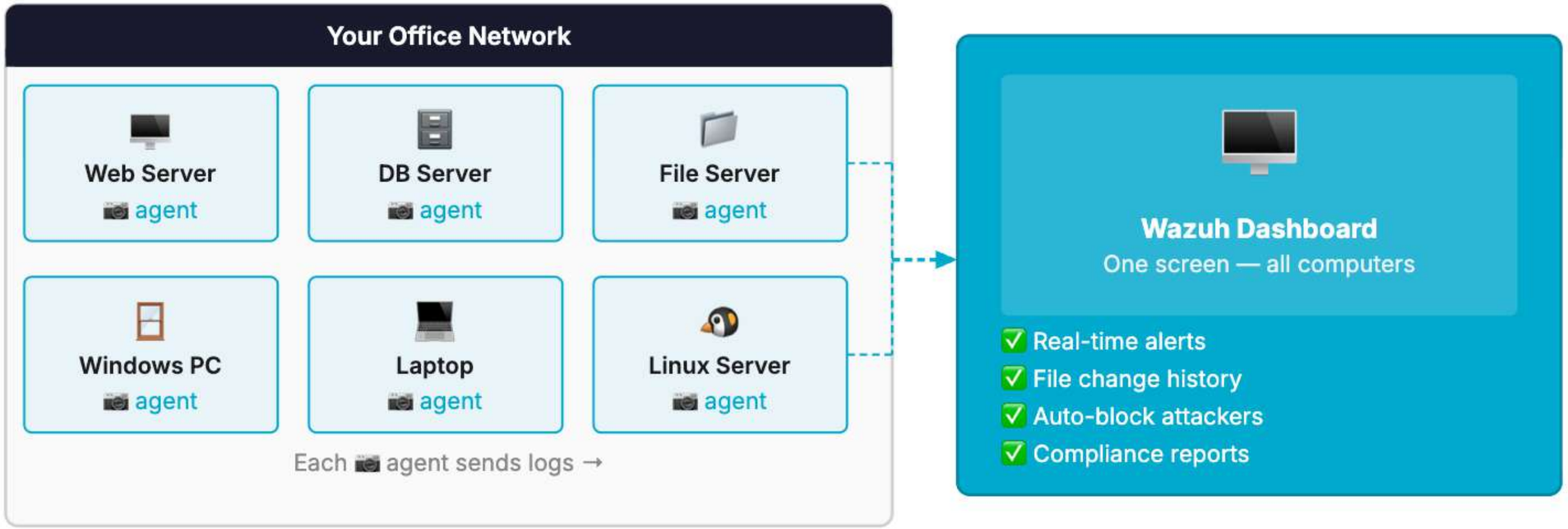
📧 **Phishing → endpoint → lateral movement** — firewall passed the attacker via HTTPS

🩹 **~60% of breaches** exploit a CVE that already had a patch available

⚠️ **Supply chain & zero-day** — SolarWinds, Log4Shell; signature-based AV missed all

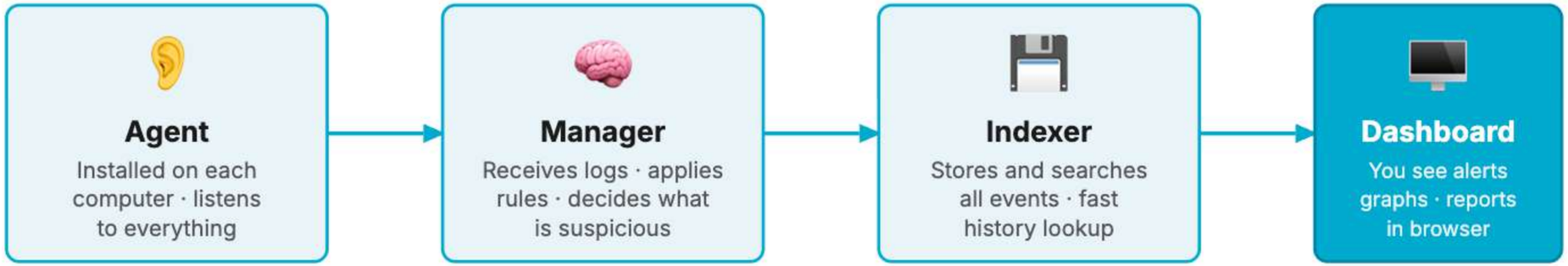
> **The firewall is not enough.** An attacker on a trusted VLAN looks identical to a legitimate admin — at the network layer.

# What is Wazuh?




**Like CCTV cameras — one agent per computer, one screen to watch them all.**

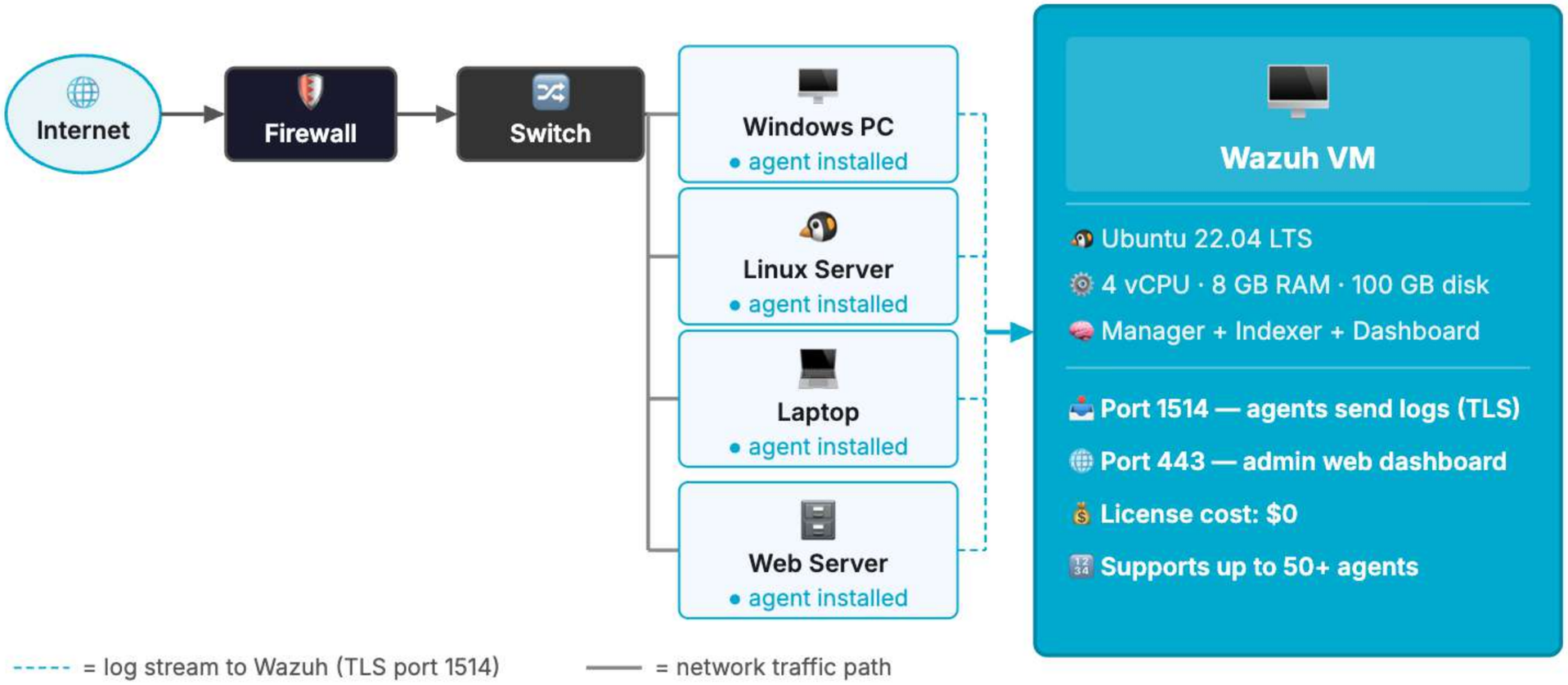
# Wazuh — 4 pieces, one system




All 4 components can run on a single VM for small deployments

**Small business tip:** Run all 4 on one Ubuntu VM — 4 vCPU, 8 GB RAM is enough for up to 50 agents.

# Where Wazuh sits in your network

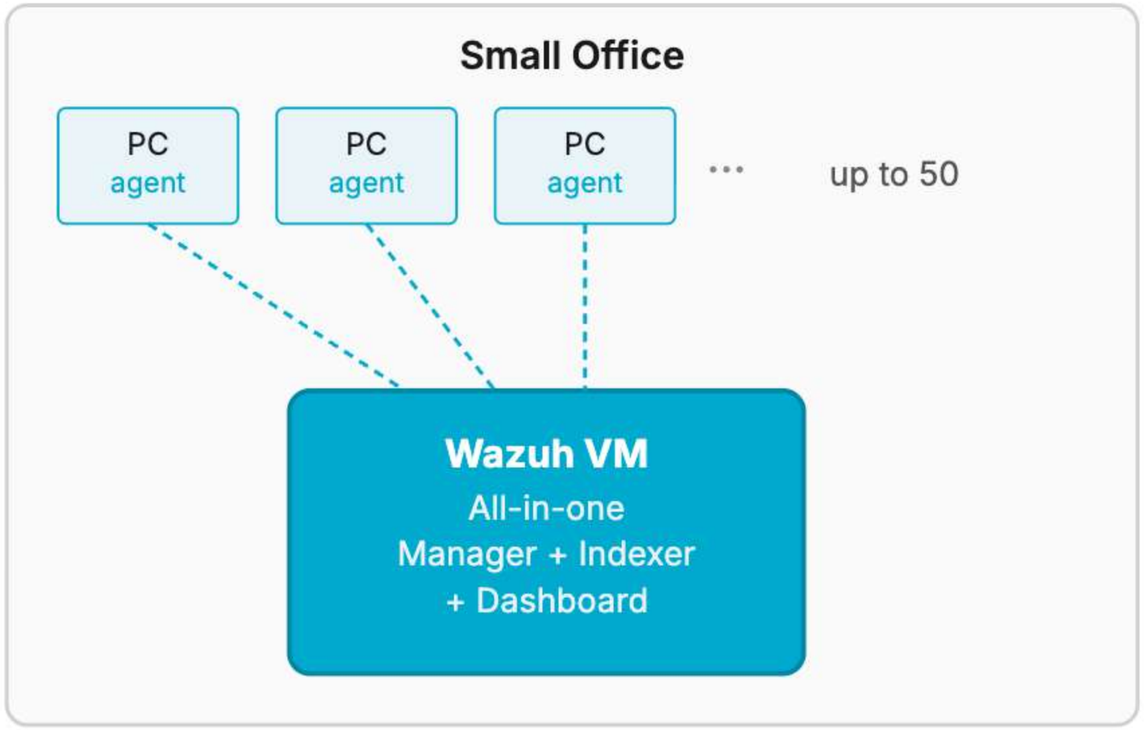


# Setup by business size — Small (10–50 devices)

## SMALL BUSINESS · 10–50 DEVICES

**Wazuh VM:** All-in-one single server
**CPU:** 4 vCPU
**RAM:** 8 GB
**Disk:** 100 GB (≈ 3 months logs)
**OS:** Ubuntu 22.04 LTS
**Install time:** ~30 minutes
**License cost:** $0 (Apache 2.0)

> **Tip:** A spare PC (8 GB RAM) or a cloud VM works perfectly. No dedicated hardware needed.



# Setup by business size — Medium (50–200 devices)

## 🏢 MEDIUM BUSINESS · 50–200 DEVICES

**Wazuh Manager VM:**
8 vCPU · 8 GB RAM · 50 GB

**Wazuh Indexer VM:**
8 vCPU · 16 GB RAM · 500 GB

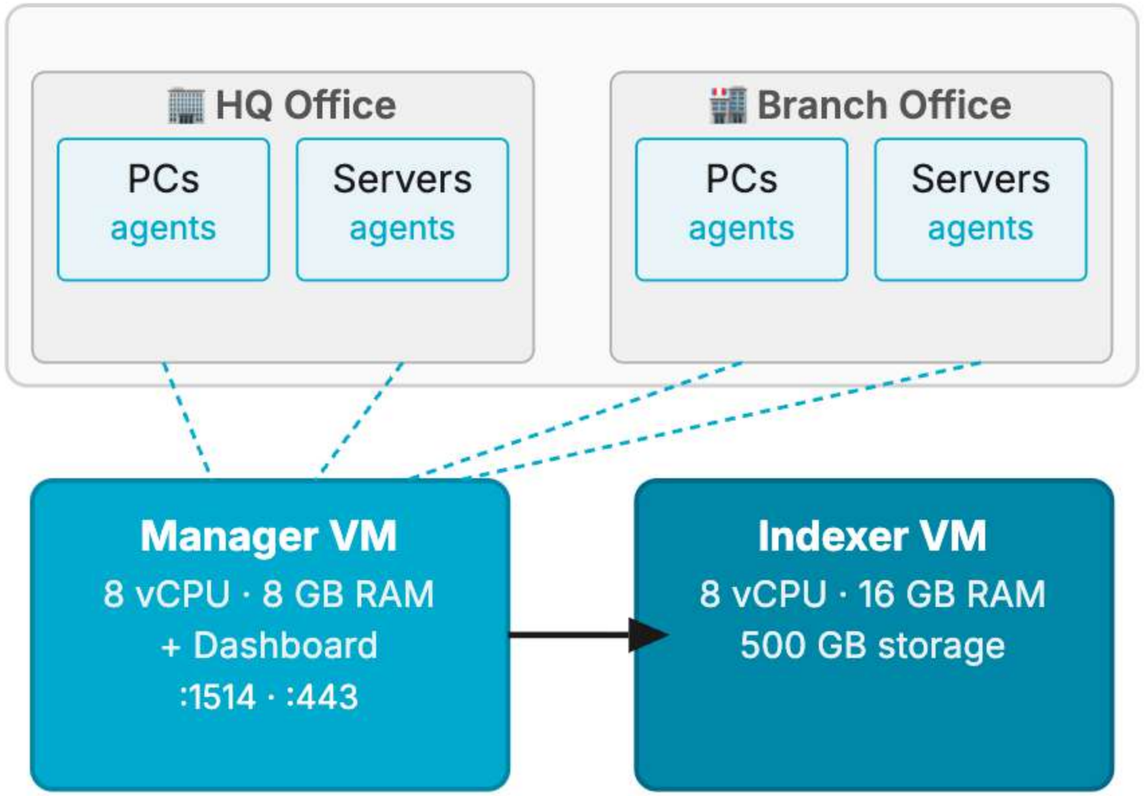
**Dashboard:** on Manager VM

**Total VMs:** 2

**Disk grows:** ~0.5 GB per agent per month

**License cost:** $0

> **Note:** Separate Manager and Indexer when you need more search speed or longer log retention (6–12 months).

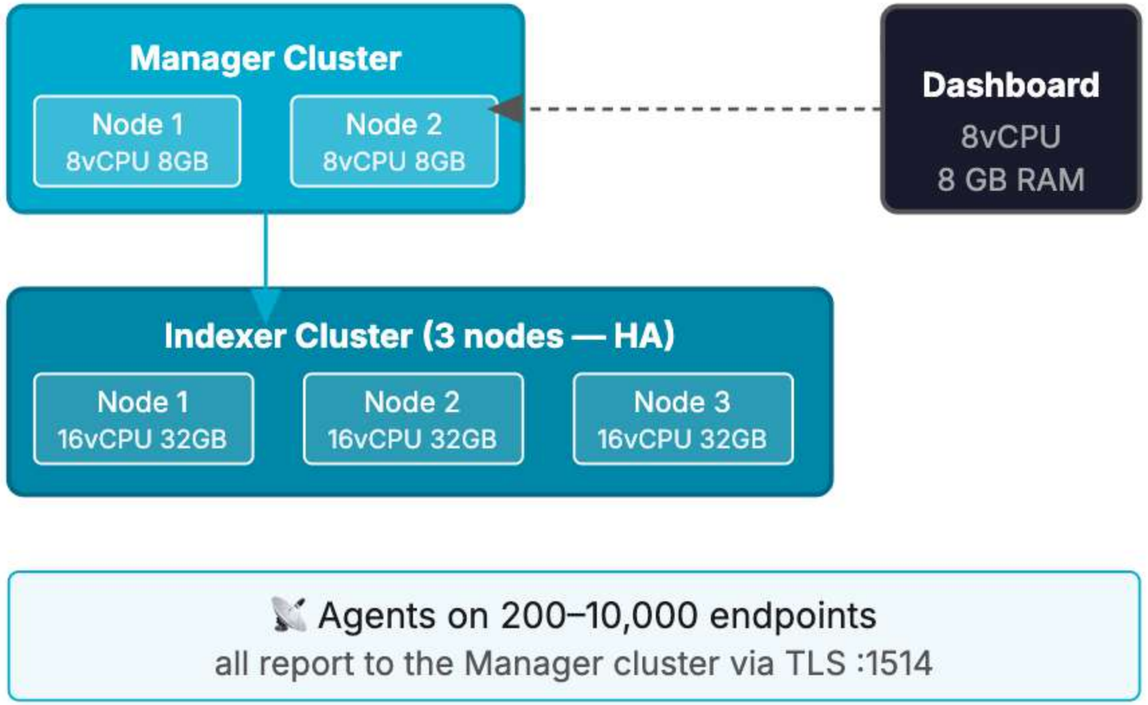


# Setup by business size — Enterprise (200+ devices)

## 🏦 ENTERPRISE · 200+ DEVICES

**Manager cluster:** 2+ nodes
**Indexer cluster:** 3+ nodes (HA)
**Dashboard:** dedicated node
**Each indexer node:** 16 vCPU / 32 GB / 2 TB
**Total VMs:** 6–10+
**Wazuh license:** still $0
**Support contract:** optional ($)

> Enterprise adds high availability and dedicated SOC team — but the software cost is the same: $0.



# Wazuh vs Enterprise SIEM — head to head

| Factor | ✅ Wazuh | Splunk Enterprise | IBM QRadar | Microsoft Sentinel |
|---|---|---|---|---|
| **License cost** | **$0 / year** | $50,000+/yr | $30,000+/yr | $2–10/GB/day |
| **Pricing model** | Free — unlimited agents | Per GB ingested | Per EPS (event/sec) | Per GB ingested |
| **Agent limit** | **Unlimited** | Priced per volume | Priced per EPS | Priced per GB |
| **Built-in FIM** | ✅ Yes | Add-on ($) | Limited | Via Defender add-on |
| **Built-in vuln scan** | ✅ Yes | Add-on ($) | Add-on ($) | Via Defender add-on |
| **Active response** | ✅ Built-in | SOAR required ($) | SOAR required ($) | Logic Apps required |
| **Open source** | **Apache 2.0** | No | No | No |
| **Install time** | 30 minutes | Days–weeks | Days–weeks | Hours (Azure-native) |

**SMB verdict:** Enterprise SIEMs are designed for large SOC teams with large budgets. Wazuh gives the same core capabilities — FIM, vuln scanning, compliance, active response — at any scale, for $0.

# Hardware requirements at a glance

| Size | Agents | vCPU | RAM | Disk | VMs |
|---|---|---|---|---|---|
| 🏪 Small | 1–50 | 4 | 8 GB | 100 GB | 1 (all-in-one) |
| 🏢 Medium | 50–200 | 8 per VM | 16 GB / VM | 500 GB + | 2 (split) |
| 🏦 Enterprise | 200–10,000+ | 16 per node | 32 GB / node | 2 TB + per node | 6–10 (cluster) |

**Disk is the main variable.** CPU and RAM are fixed; disk grows with log volume. Plan ~0.5 GB per agent per month. Add disk first when you're running low.

OS: Ubuntu 22.04 LTS (recommended) or RHEL/CentOS 8+. Wazuh agents run on Linux, Windows, macOS, FreeBSD.

# Getting started — 3 steps


**Total setup time: under 30 minutes · $0 license**

05/2026 : The Latest Wazuh version is 4.14

# Installing agents — per platform

### 🐧 Linux (apt / yum)

```
# Single install
curl -sO packages.wazuh.com/4.10/wazuh-agent.deb
sudo dpkg -i wazuh-agent.deb

# Mass deploy (Ansible)
ansible-playbook wazuh-agent.yml \
-e wazuh_manager=192.168.1.10

Ubuntu · Debian · RHEL · CentOS · Rocky
```

### 🪟 Windows (MSI / GPO)

```
# Single install (PowerShell)
msiexec /i wazuh-agent.msi \
WAZUH_MANAGER=192.168.1.10

# Mass deploy via GPO
Computer Config → Software Settings
→ Add wazuh-agent.msi (All Computers OU)

Windows 10 / 11 / Server 2016+
```

### 🍎 macOS (pkg)

```
# Download & install
curl -sO packages.wazuh.com/4.10/wazuh-agent.pkg
sudo installer -pkg wazuh-agent.pkg -target /

# Start agent
sudo /var/ossec/bin/wazuh-control start

macOS 12 Monterey and later
```

### 🔴 MikroTik — no agent, use syslog

```
# RouterOS — forward logs to Wazuh
/system logging action
add name=wazuh target=remote \
remote=192.168.1.10 remote-port=514
/system logging
add action=wazuh topics=info,error,warning

Wazuh reads syslog on port 514 UDP/TCP
```

# Sample Wazuh Alerts — What gets captured

### 🔴 Brute Force — SSH

Rule 5763 · Level 10

```
** Alert 2026-05-24 08:15:43 web-server→sshd
Rule: SSHD brute force trying to get access
srcip: 45.33.32.156 attempts: 10 in 60s

sshd: Failed password for root from
45.33.32.156 port 42156 ssh2
sshd: Failed password for root from
45.33.32.156 port 42157 ssh2 [+8 more]
```

### 🟡 File Integrity — /etc/passwd modified

Rule 550 · Level 7

```
** Alert 2026-05-24 09:22:11 server1→syscheck
Rule: Integrity checksum changed
File: /etc/passwd Changed: md5,mtime

Old md5: a1b2c3d4e5f67890abcdef1234567890
New md5: f09e8d7c6b5a4321fedcba9876543210
Changed by: root (uid=0) via: echo >>
Action: ALERT — possible backdoor account
```

### 🟣 Vulnerability Detected — CVE

Rule 23504 · Level 7

```
** Alert 2026-05-24 10:00:00 db-server
Rule: CVE-2023-4911 affects package
CVE: CVE-2023-4911 Severity: HIGH Score: 7.8

Package: openssl Version: 1.1.1f
Fixed in: 1.1.1f-1ubuntu2.21
Agent: db-server (192.168.1.20)
Action: Run apt upgrade openssl
```

### 🔵 MikroTik — Firewall DROP event

Rule 4100 · Level 5

```
** Alert 2026-05-24 10:05:33 mikrotik-gw
Rule: Firewall packet dropped (forward)
src: 192.168.1.105 dst: 10.0.0.1:22

mikrotik: firewall,forward,drop
in-interface=ether1 proto=tcp
src-mac=AA:BB:CC:DD:EE:FF
Via: syslog UDP port 514 → Wazuh
```

# How Wazuh notifies the admin

### 📧 Email (SMTP)

Built-in — no plugin needed.
Set SMTP server in ossec.conf.

```
<email_notification>yes
<smtp_server>smtp.gmail.com
```

Alert on Level ≥ 7 by default

### 💬 Slack (Webhook)

Wazuh integration → Slack app.
Sends JSON alert to channel.

```
integration name="slack"
hook_url: hooks.slack.com/...
```

Posts to #security-alerts channel

### ✈️ Telegram Bot

Custom script via active response.
Sends message to group/channel.

```
curl -s https://api.telegram.org/
bot<TOKEN>/sendMessage -d ...
```

Popular for Thai teams · free

### 🟢 LINE Notify

LINE Notify API — free token.
Push alert to LINE group chat.

```
curl -X POST notify-api.line.me/
api/notify -H "token: <TOKEN>"
```

Most popular in Thai SMBs

### 🚨 PagerDuty / OpsGenie

On-call escalation platform.
Wakes the right person on-call.

```
integration name="pagerduty"
api_key: <PAGERDUTY_KEY>
```

Best for 24×7 SOC teams

### 🖥️ Wazuh Dashboard

Real-time alert feed in browser.
Filter · drill-down · export.

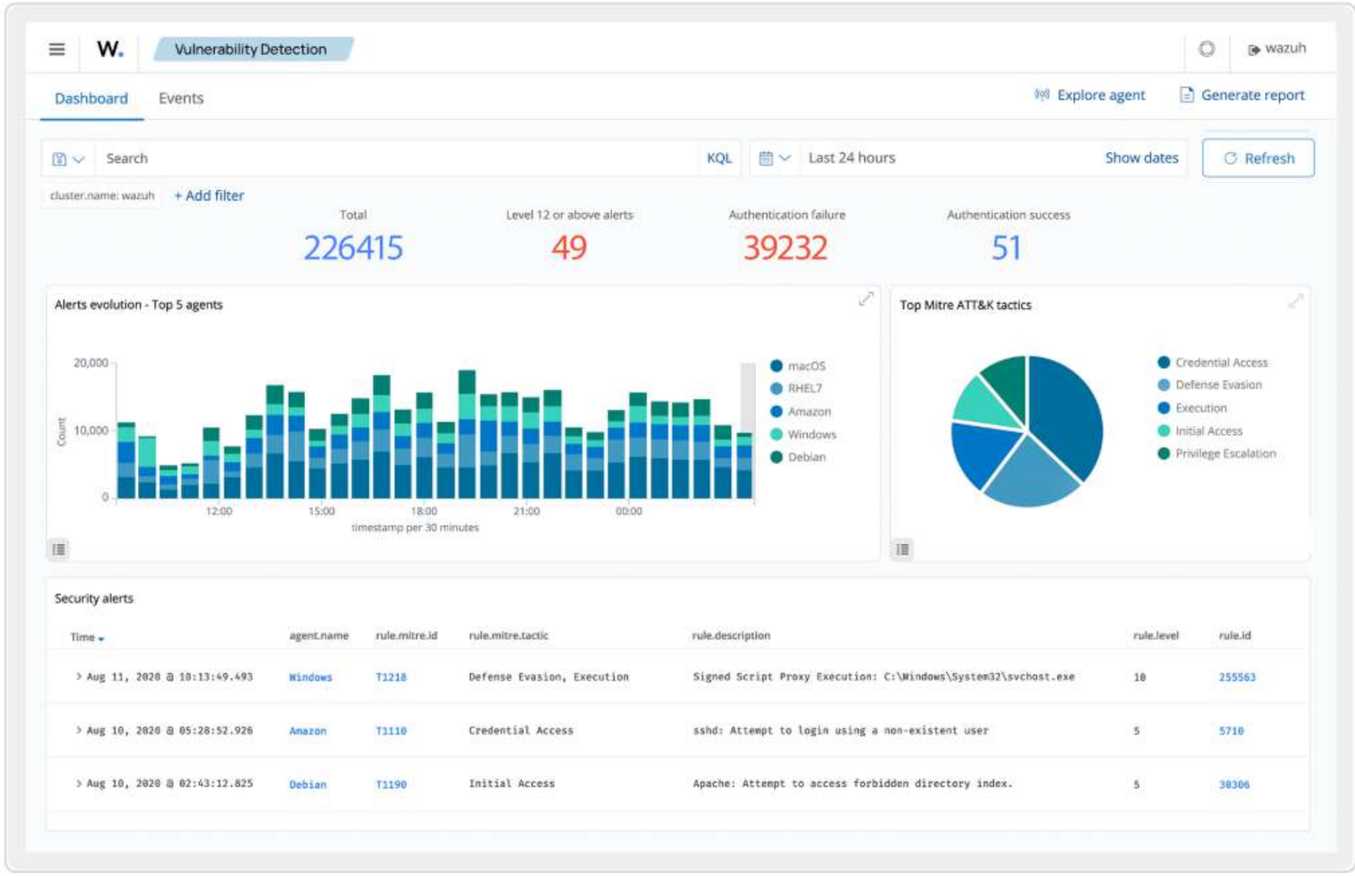
```
https://<wazuh-server>
Threat Hunting → Events
```

No config needed — works out of box

# XDR Capability: Threat Hunting

Focus analyst attention and cut time spent analyzing telemetry from multiple security platforms.

- Query across all endpoint telemetry in one place
- Filter by agent, time range, rule group, or MITRE technique
- Pivot from a single alert to full host timeline
- Save and share custom searches across the team



# XDR Capability: Behavioral Analysis

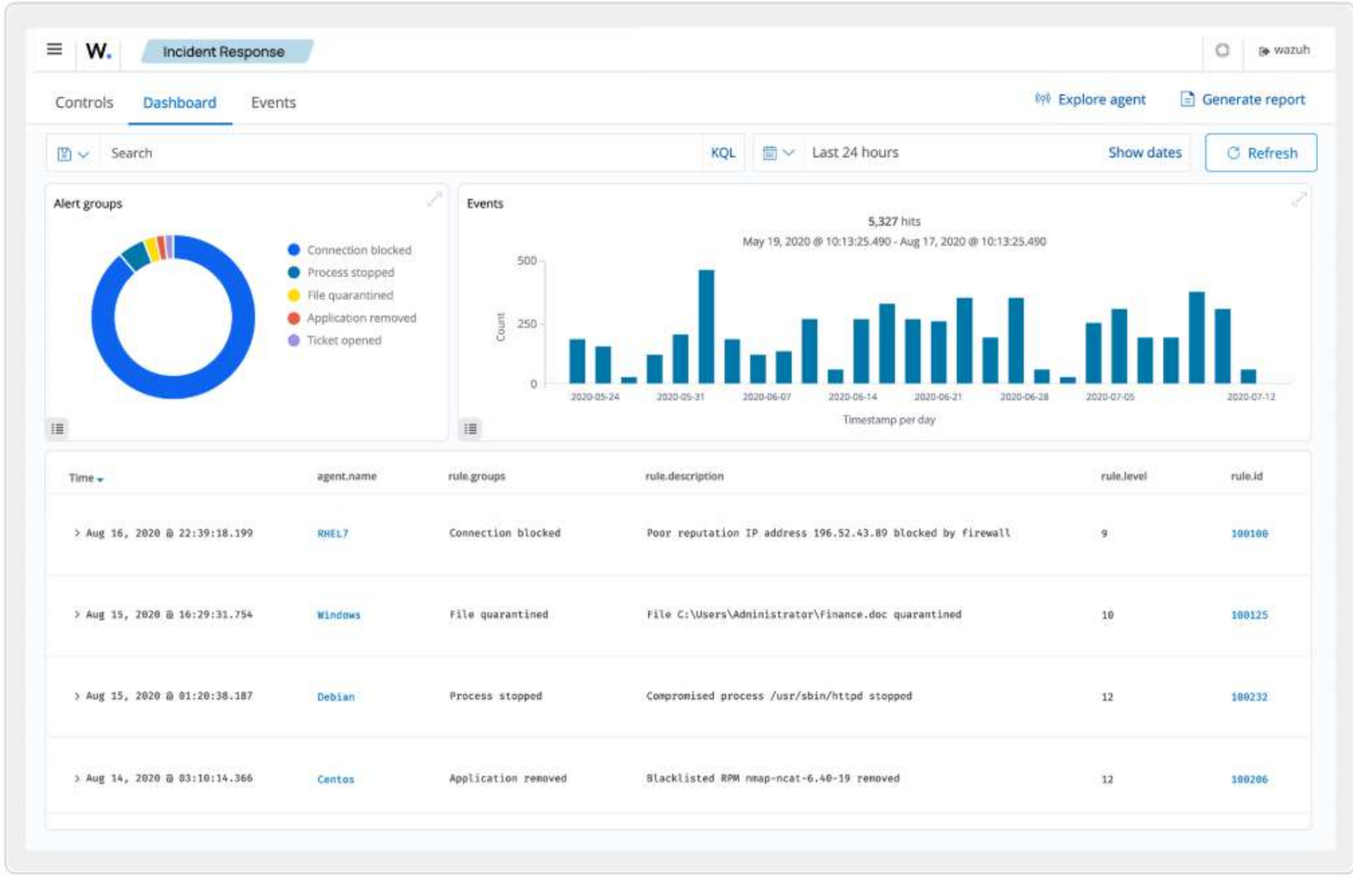
Identify deviations from normal behavior using advanced analytics to spot threats before signatures exist.

- **File Integrity Monitoring** — alerts on unexpected file changes
- **Network traffic** — unusual connection patterns or new listening ports
- **User behavior** — off-hours logins, new admin accounts, privilege escalation
- **Process behavior** — shell spawned from a web server, encoded PowerShell

# XDR Capability: Automated Response

Reduce average incident response time with the Wazuh active response module — automatic threat mitigation without waiting for a human.

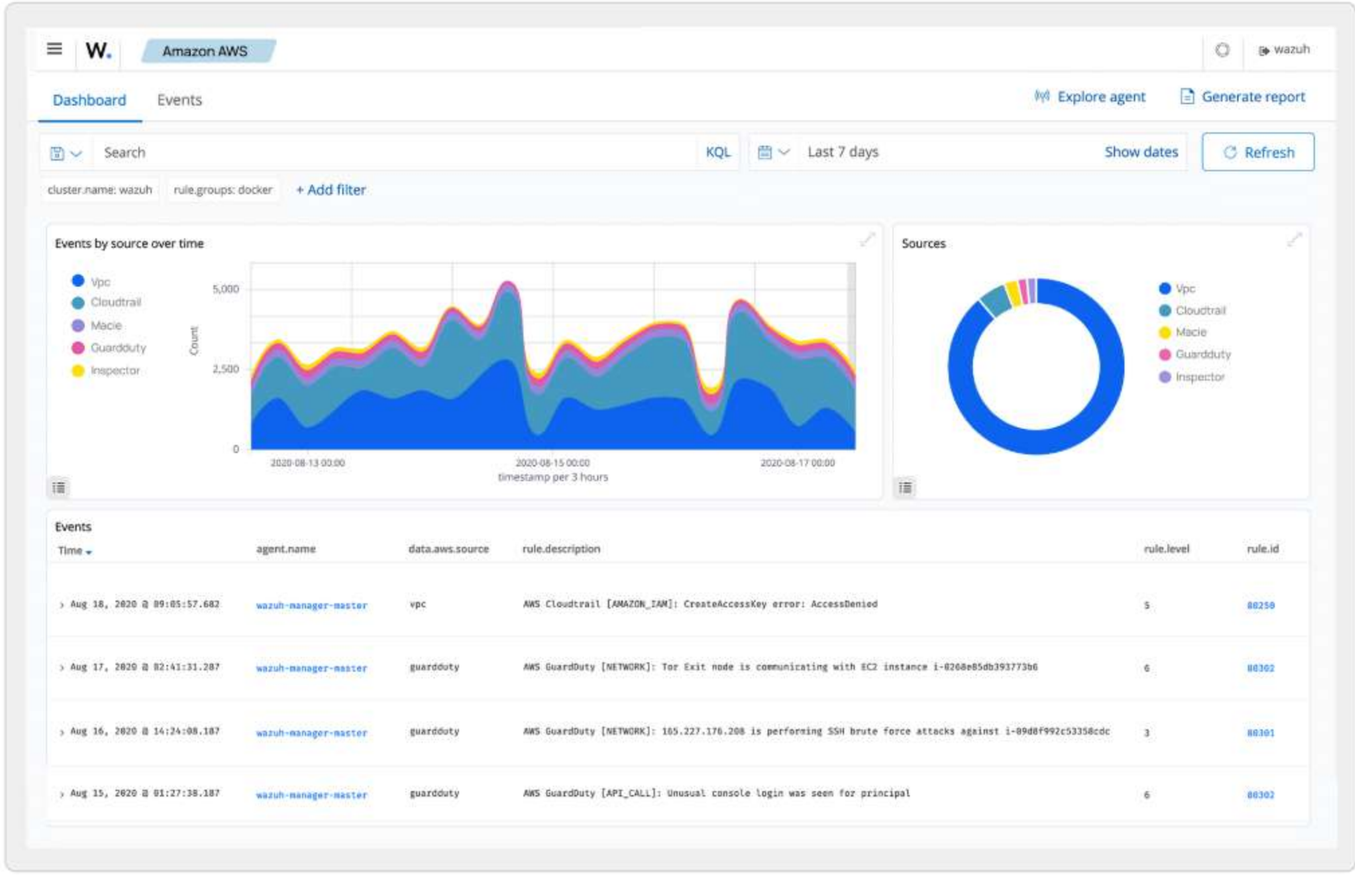
- **Block IP** — firewall-drop script runs on agent in milliseconds
- **Kill process** — terminate malicious process immediately
- **Disable user** — lock compromised account automatically
- **Custom scripts** — any action triggered by any rule match
- Stateful — auto-unblock after configurable timeout



# XDR Capability: Cloud Workload Protection

Security for cloud workloads and containers through built-in integrations and telemetry analysis — covering hybrid and cloud-native environments.

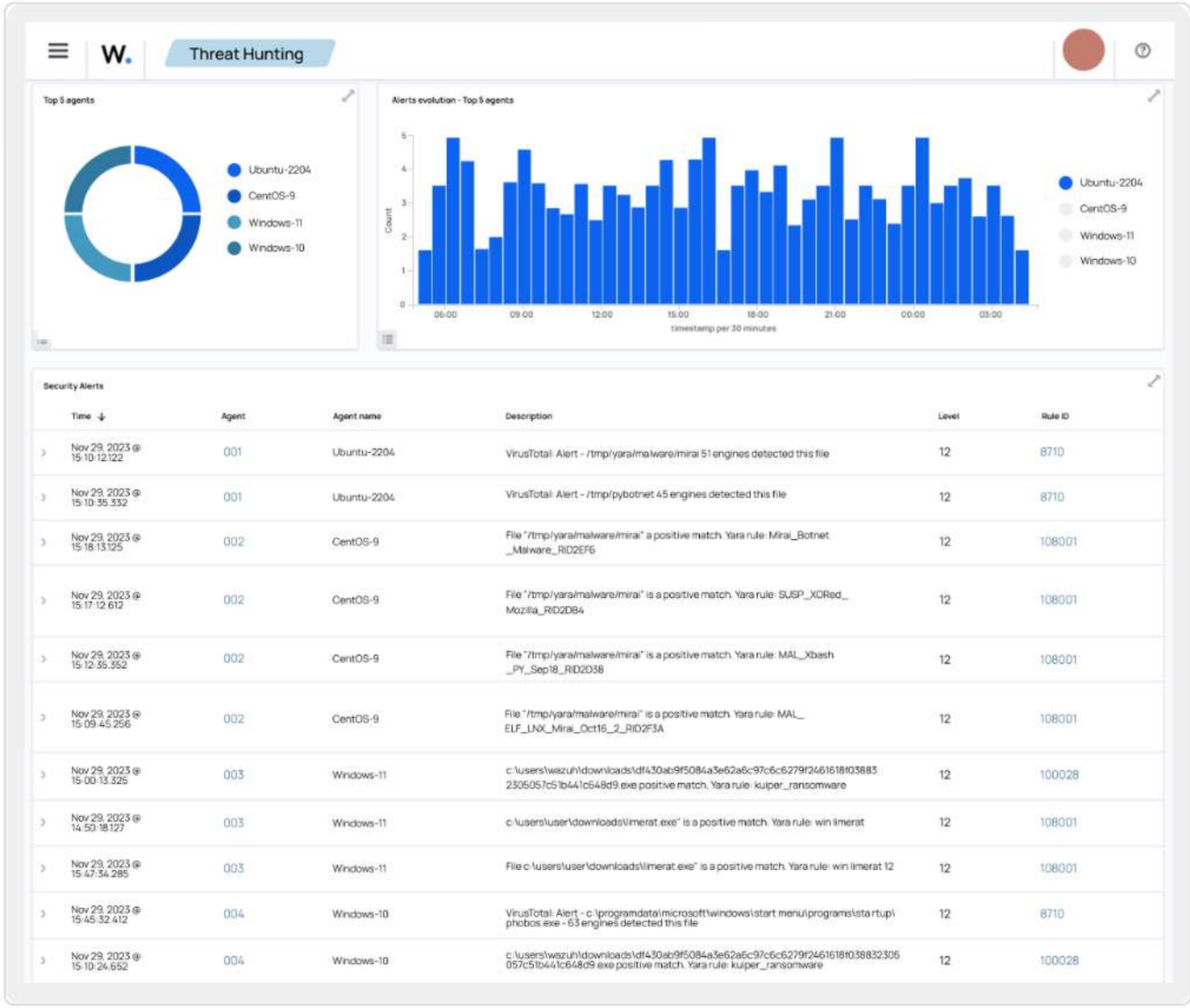
- **AWS** — CloudTrail, GuardDuty, S3, VPC Flow, Inspector
- **Azure** — Activity Log, Microsoft Defender, Entra ID
- **GCP** — Cloud Audit Logs via Pub/Sub
- **Docker / Kubernetes** — container events, image integrity
- Agentless — pulls via API, no agent inside cloud resources



# XDR Capability: Threat Intelligence

Incorporate threat intelligence feeds from OSINT, commercial sources, and community data to detect and respond to known threats.

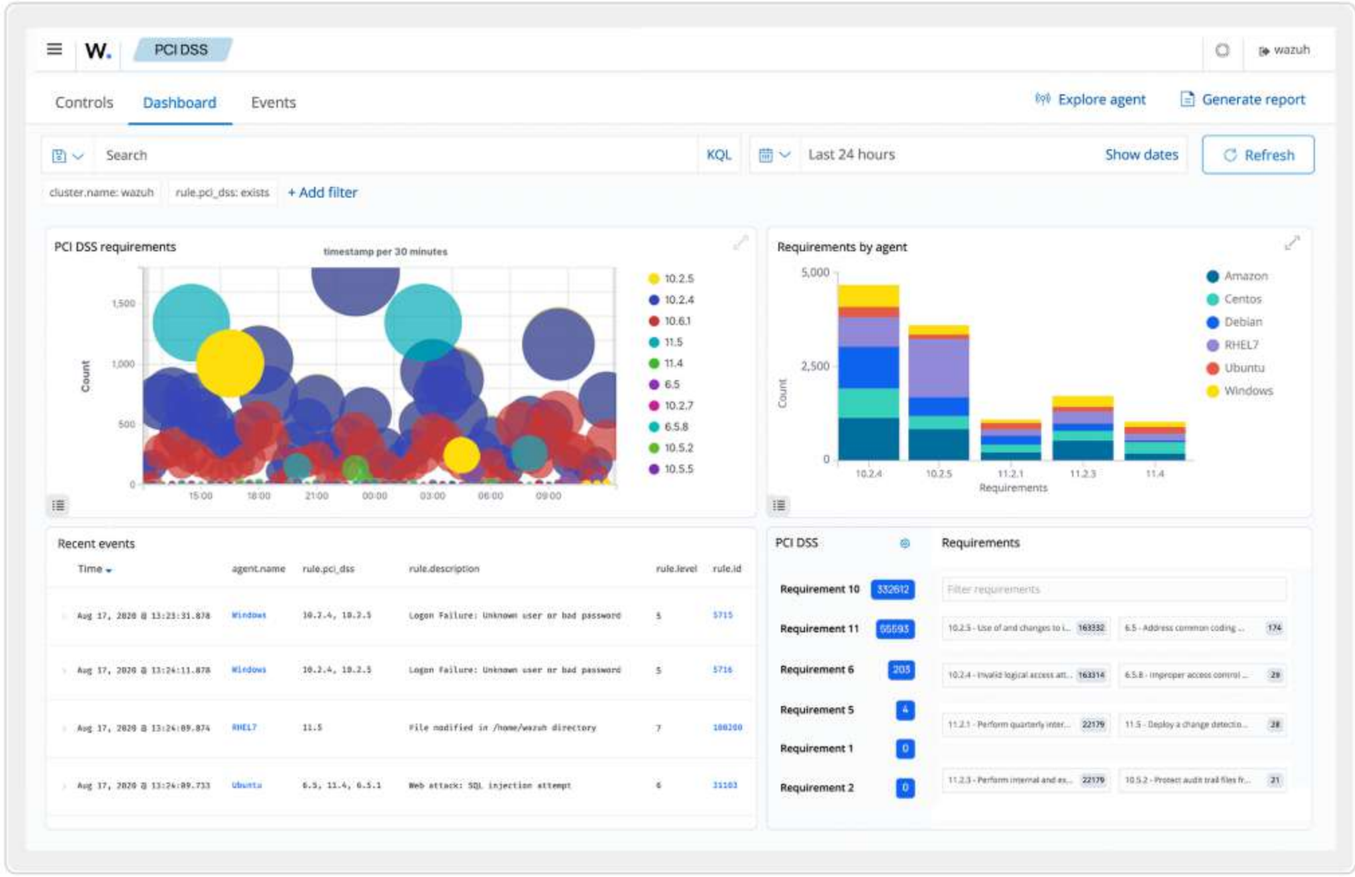
- **MISP integration** — ingest IoCs (IPs, domains, hashes) from threat sharing platforms
- **VirusTotal** — auto-lookup file hashes on FIM alerts
- **MITRE ATT&CK mapping** — every alert tagged to a technique ID
- **Custom feeds** — load any STIX/TAXII or CSV IoC list
- Correlates observed behavior against known attacker TTPs



# XDR Capability: Compliance & Reporting

Meet regulatory requirements, generate audit-ready reports, and demonstrate the effectiveness of your security program.

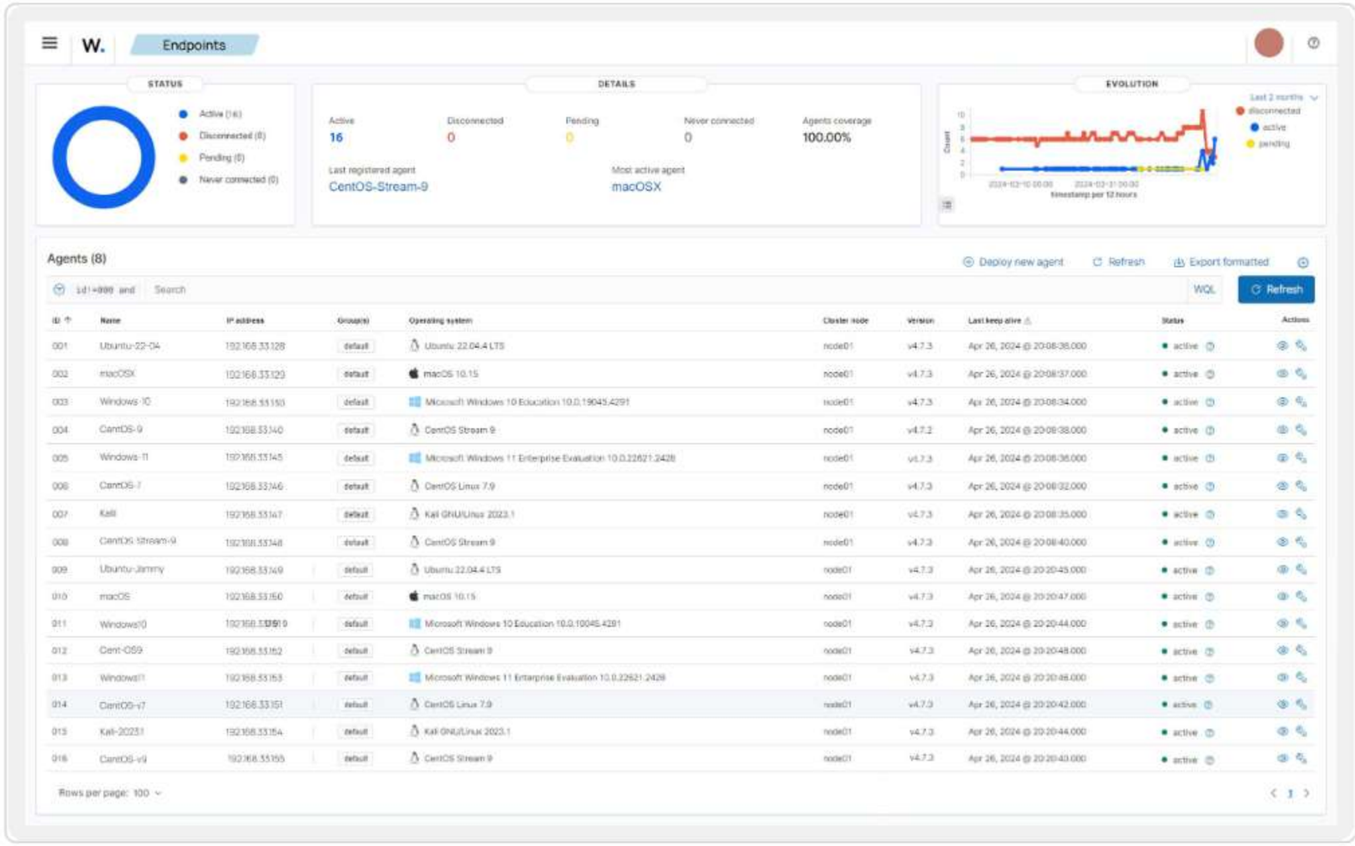
- **PCI-DSS** — cardholder data environment log retention, FIM on in-scope systems
- **HIPAA** — access logging, integrity monitoring for ePHI systems
- **GDPR** — breach detection, data access auditing
- **CIS Benchmarks** — automated SCA scoring against hardening guides
- **NIST CSF / ISO 27001** — control mapping pre-built in dashboard



# XDR Capability: Universal Agent

A single lightweight agent deployable across all major operating systems — provides full endpoint protection without multiple tools.

- **Linux** — RPM/DEB, all major distros
- **Windows** — MSI, supports Server 2012R2+
- **macOS** — PKG installer
- **Capabilities per agent:** FIM · SCA · vuln scan · log collection · active response · syscall monitoring
- ~15 MB memory footprint; no noticeable CPU overhead at rest



# XDR Capability: Third-Party Integrations

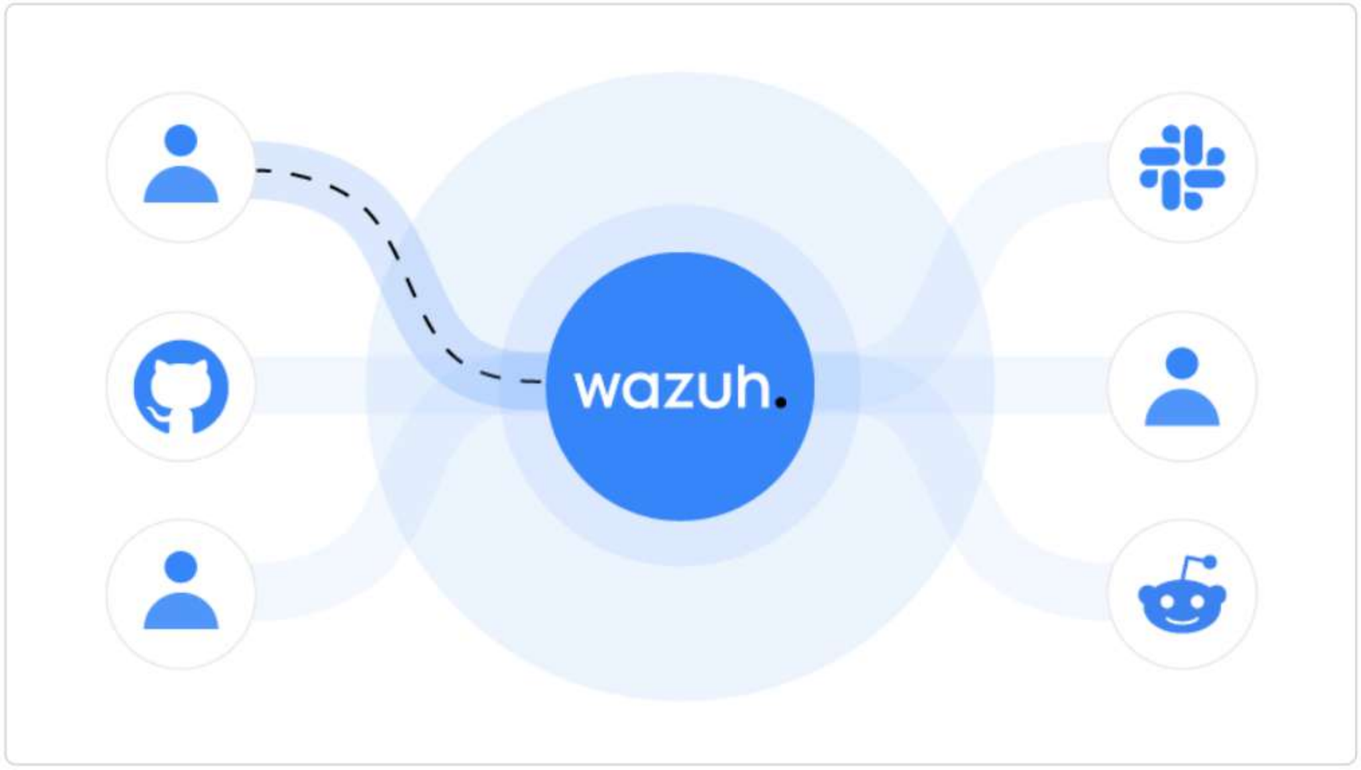
Extend detection by unifying telemetry from any source via syslog, REST APIs, or native modules.

- **Network devices** — MikroTik, Cisco, Fortinet via syslog (UDP 514)
- **Cloud platforms** — AWS, Azure, GCP via API polling
- **SaaS apps** — Microsoft 365, Google Workspace, GitHub
- **Ticketing & alerting** — Slack, PagerDuty, Jira, ServiceNow
- **Threat sharing** — MISP, OpenCTI, VirusTotal

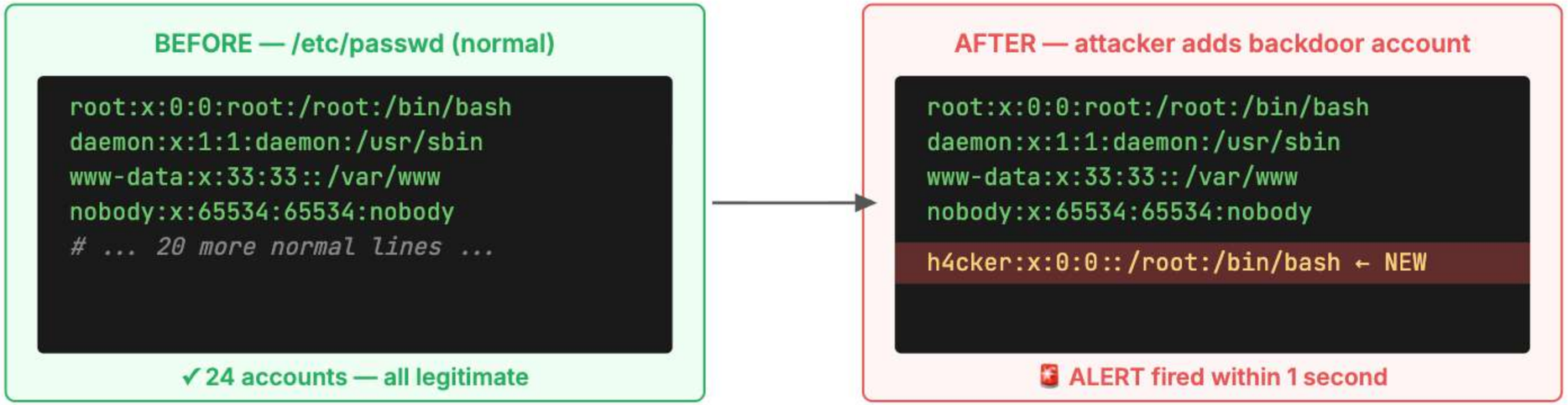
# XDR Capability: Open Source

A fully open, customizable platform — flexibility, community support, and broad integration capabilities.

- **Apache 2.0 license** — use commercially, modify, redistribute freely
- **GitHub** — 10,000+ stars, active issue tracker, public roadmap
- **Custom decoders** — write regex parsers for any log format
- **Custom rules** — XML rule engine; thousands of community rules on GitHub
- **No vendor lock-in** — your data, your infrastructure, your rules

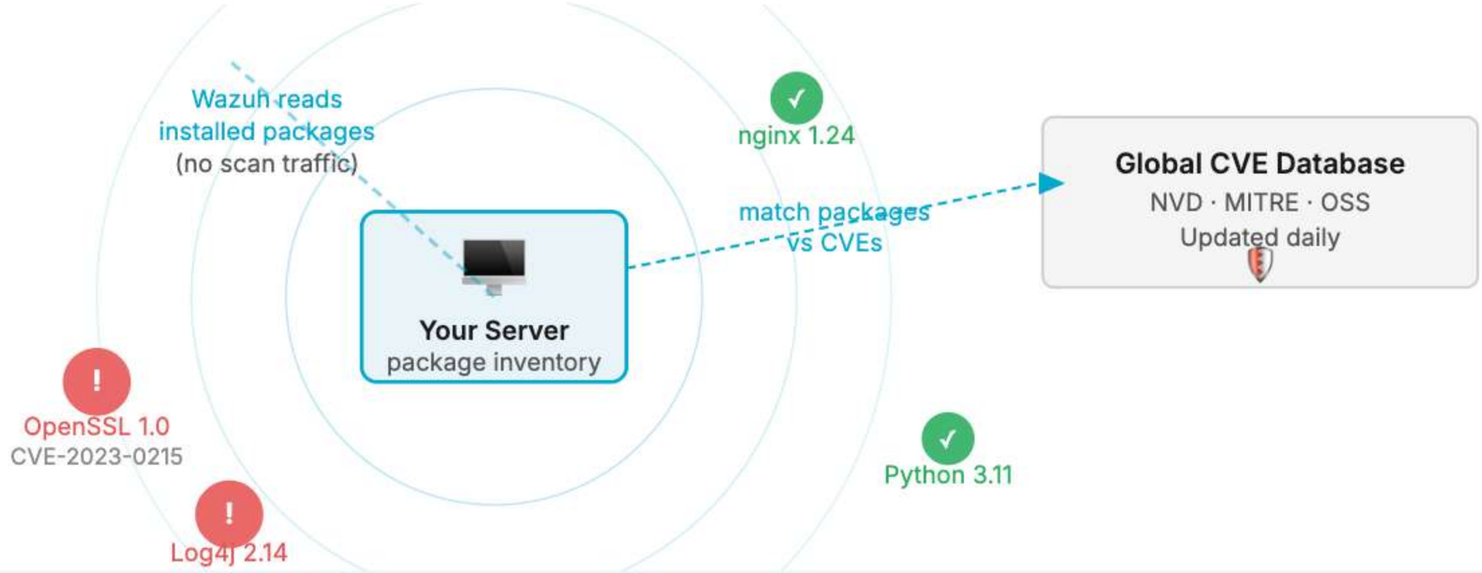


# Use Case 1 — File Integrity Monitoring



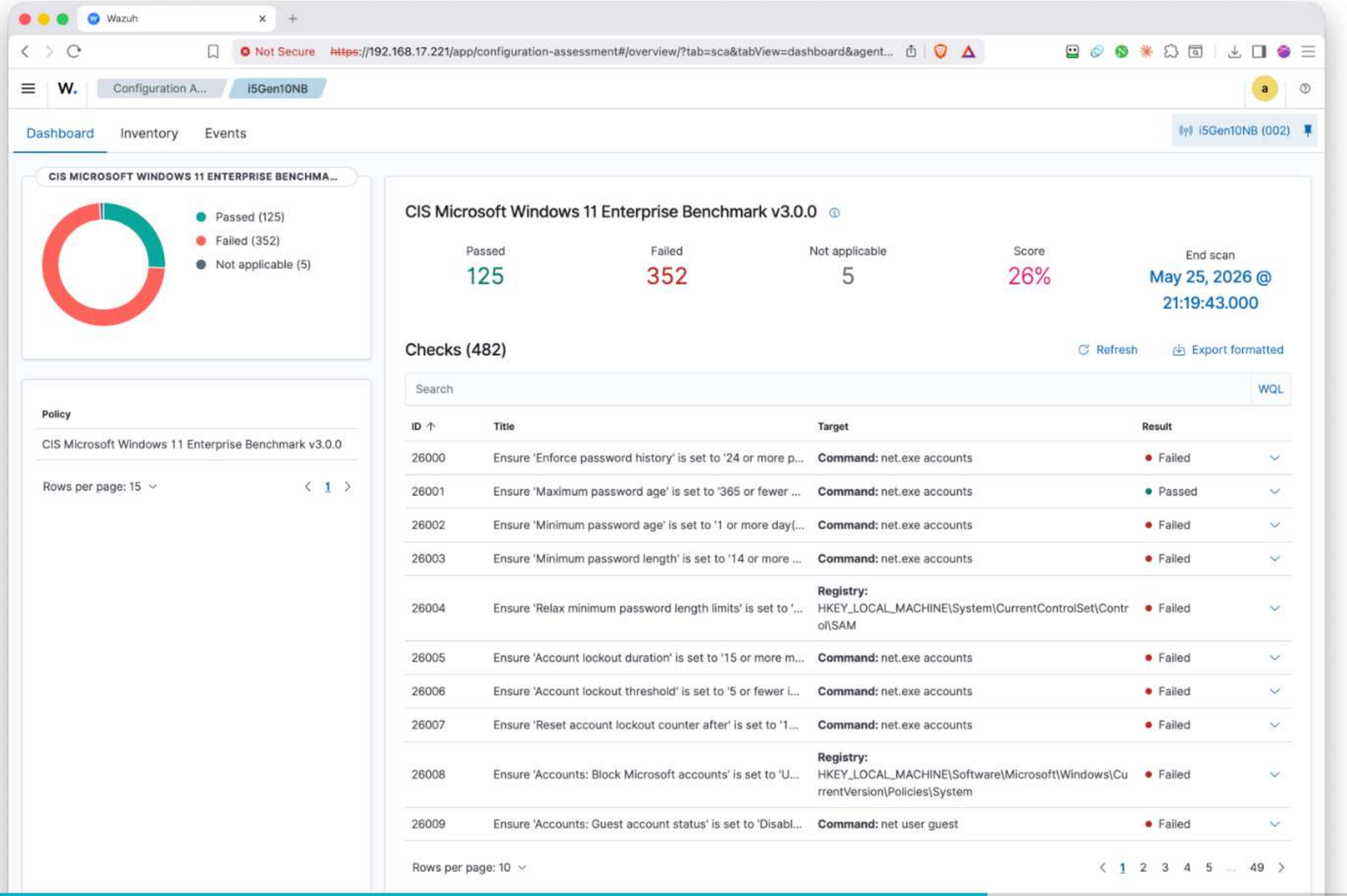

**What Wazuh catches:** Any add, modify, or delete on watched files — /etc/passwd, SSH keys, web files, Windows registry, scheduled tasks.

# Use Case 2 — Vulnerability Scanning

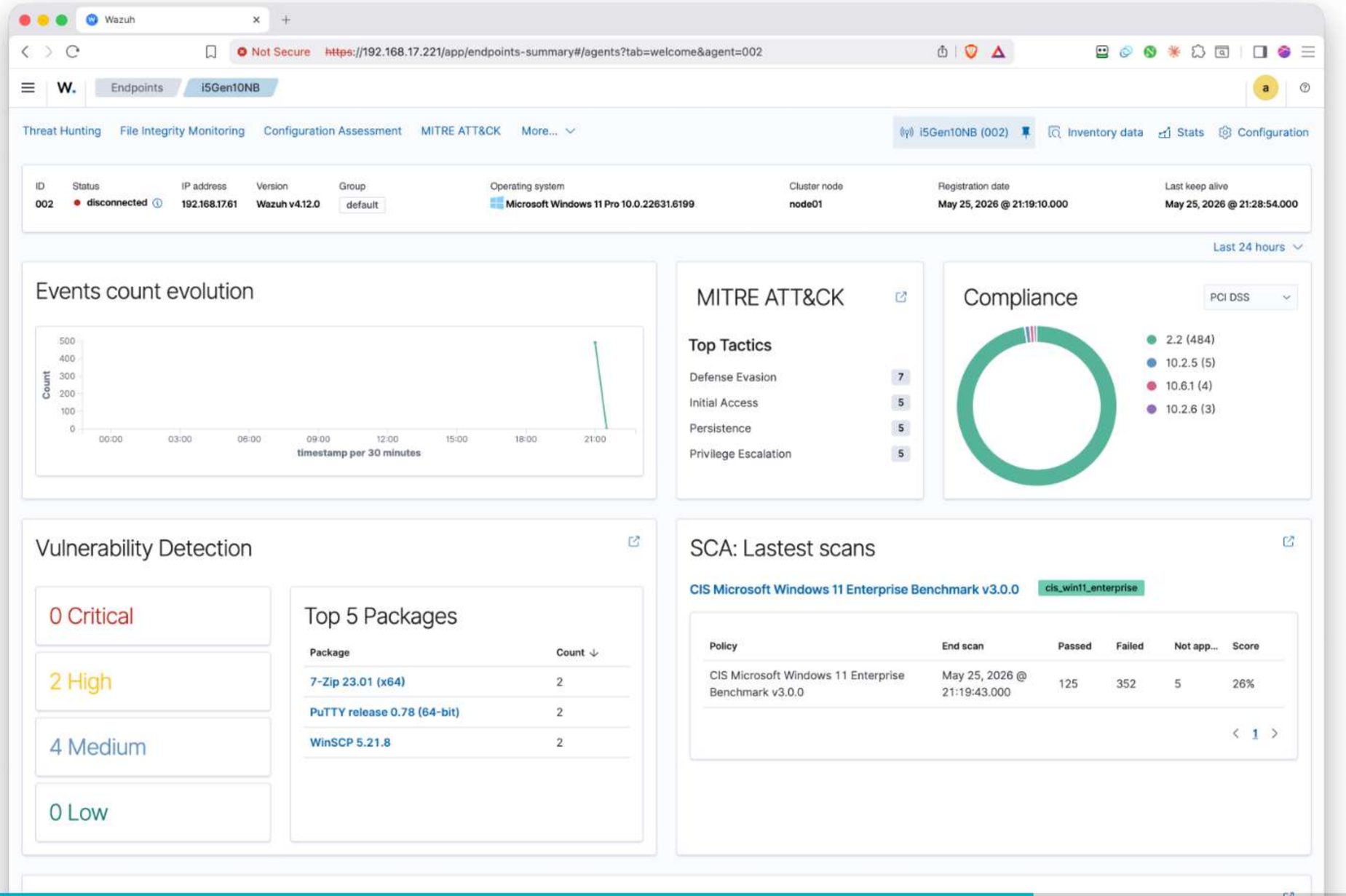



**No scan traffic.** Wazuh reads the installed package list locally — no port scanning, no network noise. Results appear in the dashboard within minutes of a new CVE being published.

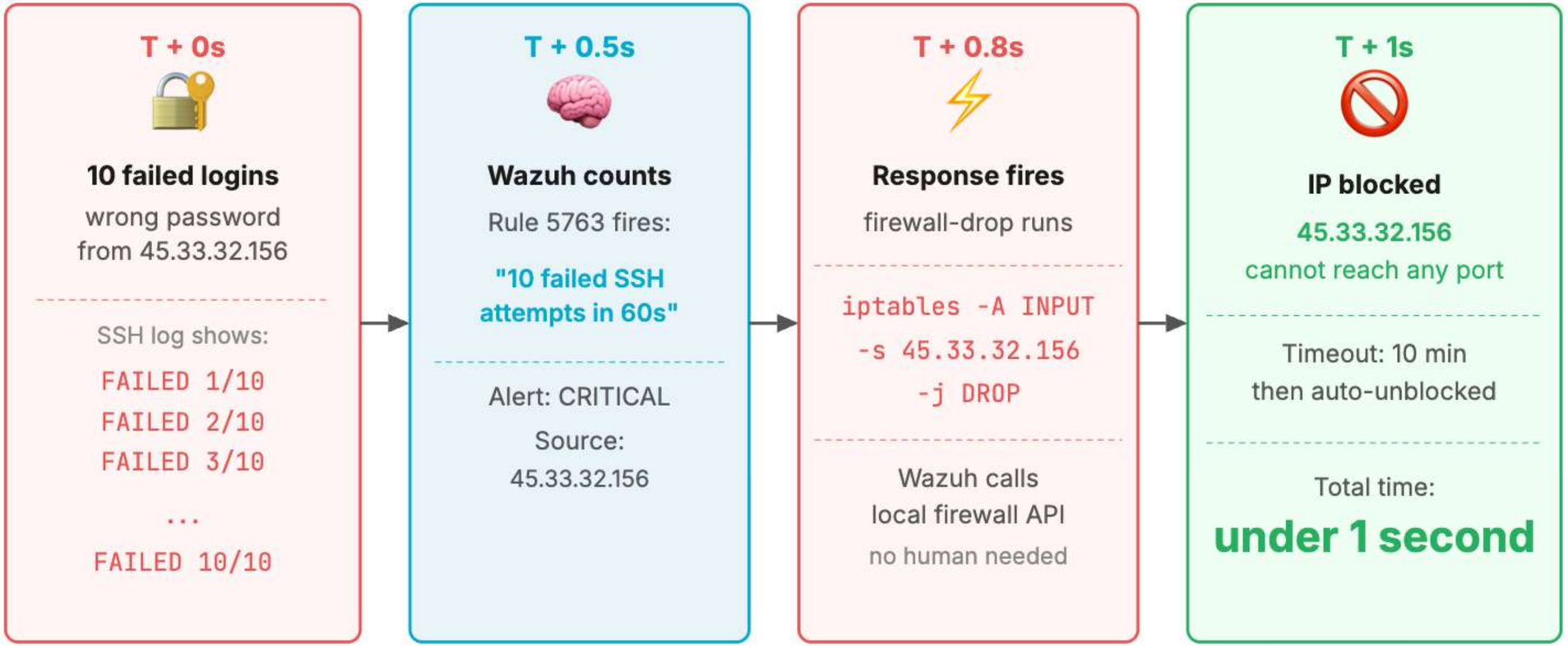
# Vulnerability Dashboard



# Endpoint Summary



# Use Case 3 — Brute Force Auto-Block



# Use Case 4 — Compliance Reporting

| PCI-DSS | CIS Benchmarks | NIST CSF | HIPAA | GDPR | ISO 27001 |
|---|---|---|---|---|---|
| Payment card | Hardening | Gov / critical infra | Healthcare | EU data privacy | ISMS standard |

Wazuh auto-tags every alert with the matching requirement — export PDF for auditors

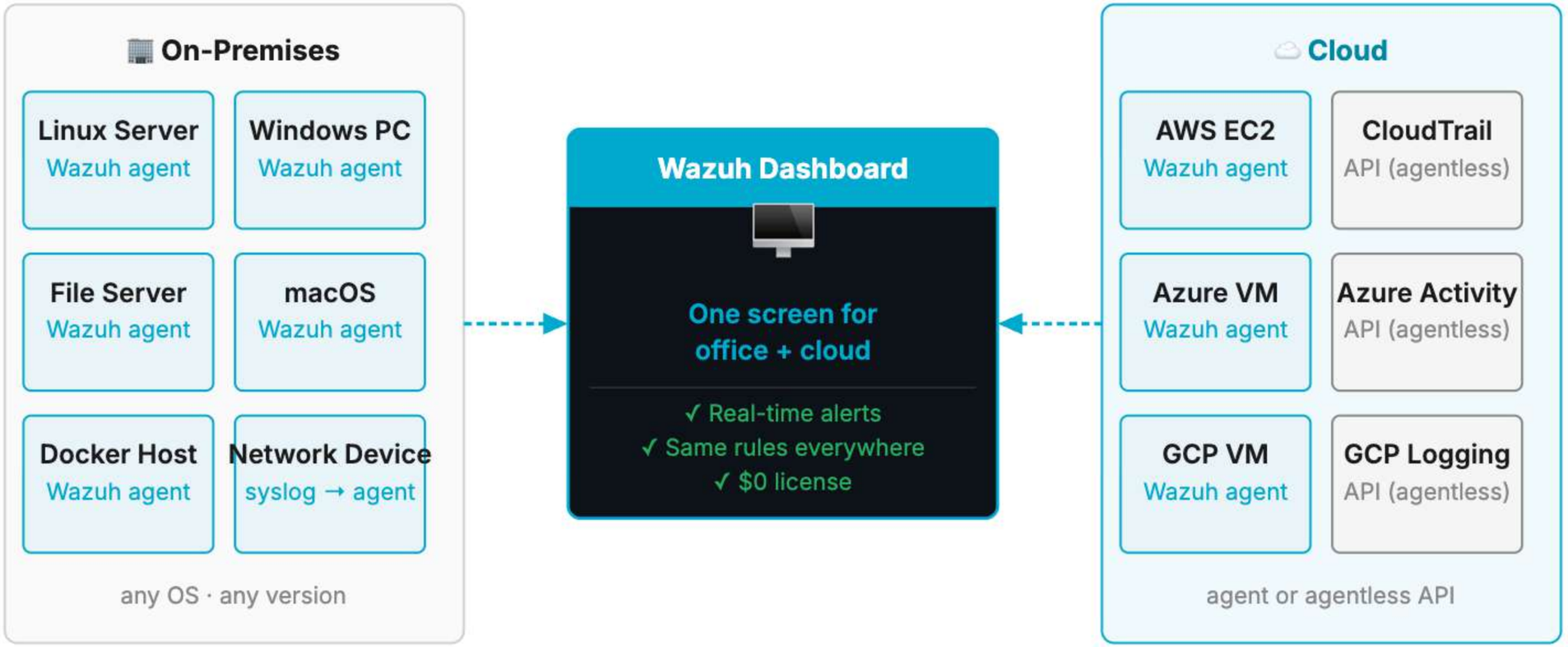
### 📋 PCI-DSS — Req 10.2.4 — Sample Alert

```
ALERT Rule 5710 · Level HIGH (10)
Req: PCI DSS 10.2.4 - Invalid access

Agent pos-terminal-01 (192.168.1.45)
User root
Src IP 45.33.32.156 → port :22
Time 2026-05-24T08:31:05Z
Event 10 failed SSH logins in 60s

Action IP auto-blocked ✓
Ticket WZ-4411 (auditor evidence)

Report Dashboard → PCI-DSS → Export PDF
Period Last 90 days — auto-generated
```

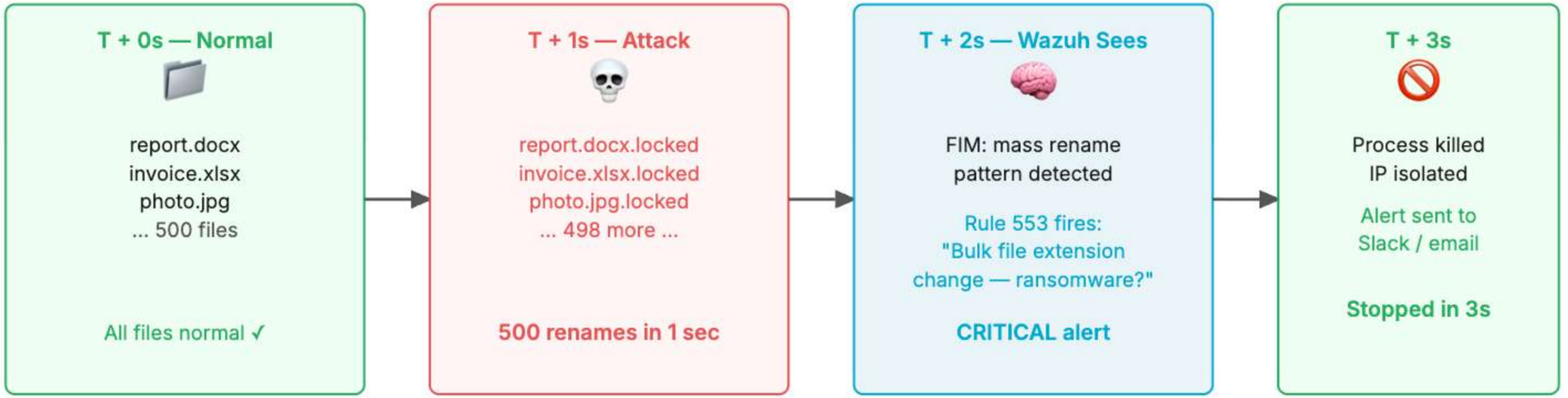
### 📋 ISO 27001 — Control A.12.4.3 — Sample Alert

```
ALERT Rule 550 · Level MEDIUM (7)
Ctrl: ISO 27001 A.12.4.3 - Admin logs

Agent web-server-01 (192.168.1.10)
File /etc/passwd
User root (after-hours: 02:14 AM)
Time 2026-05-24T02:14:22Z
Change line appended to end of file

Action SOC team notified ✓
Ticket WZ-4412 (auditor evidence)

Report Dashboard → ISO 27001 → Export PDF
Period Last 90 days — auto-generated
```

# Use Case 5 — Cloud Security Monitoring



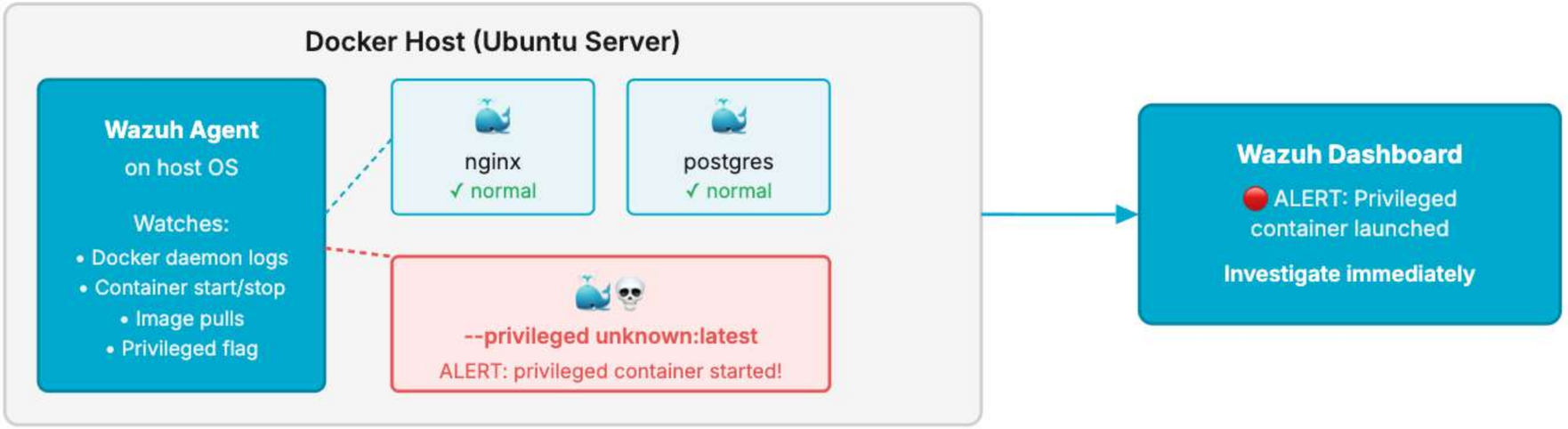
# Use Case 6 — Ransomware Detection



# Use Case 7 — Insider Threat Detection


**Note:** Wazuh detects the behaviour — investigation and response remain with your security team. Automated blocking for insider threats requires careful tuning to avoid false positives.

# Use Case 8 — Container & Docker Security




**No agent inside containers.** One Wazuh agent on the Docker host monitors all containers — container start/stop, image source, privileged mode, volume mounts.

# What about support?

### 🌐 Community

Free

- GitHub issues & Discussions
- Wazuh Slack channel
- Official documentation
- 40,000+ member forum
- Community-built rules

**Best for:**
self-managed SMB
with IT admin

### 🏢 Wazuh Commercial

Paid — contact for pricing

- SLA-backed support
- Dedicated engineers
- Training programs
- Custom integrations
- Priority bug fixes

**Best for:**
regulated industries
HIPAA / PCI-DSS / ISO 27001

### 🤝 MSP / Partner

Bundled with managed service

- Managed deployment
- 24/7 monitoring
- Incident response
- Monthly per-device fee
- No IT staff needed

**Best for:**
no in-house IT team
outsourced security

All options use the same free Wazuh software — only the service wrapper differs.

# What you now know about Wazuh

- 👁️ Watches every file change on every computer — catches backdoors within 1 second
- 🐛 Scans for vulnerabilities daily against the global CVE database — no scan traffic
- 🚫 Auto-blocks brute force attackers at the firewall in under 1 second
- ☁️ Covers on-premises, cloud (AWS/Azure/GCP), and containers — one dashboard
- 📋 Maps every event to PCI-DSS, CIS, NIST, HIPAA, GDPR, ISO 27001 automatically
- 🏢 Scales from 10 devices (1 VM, 30 min install) to 10,000+ devices (cluster)
- 💰 Apache 2.0 license — $0/year regardless of how many agents you deploy
- 🕐 Full working system in under 30 minutes — you'll do it in today's lab

# Tips & Tricks — Reduce False Alarms in Wazuh

## ① Tune minimum alert level

Set `log_alert_level` to 6+ in `ossec.conf` — levels 1–5 are mostly noise.

```
<alerts>
  <log_alert_level>6</log_alert_level>
</alerts>
```

## ② Whitelist admin & monitoring IPs

Prevent active-response from blocking your own tools.

```
<active-response>
  <white_list>192.168.1.10</white_list>
  <white_list>10.0.0.0/8</white_list>
</active-response>
```

## ③ Suppress noisy rule per agent

`level="0"` silences a rule for a specific host only.

```
<rule id="5503" level="0">
  <if_sid>5500</if_sid>
  <hostname>backup-server</hostname>
</rule>
```

## ④ FIM — exclude volatile directories

Stop alerts from log files, tmp, and cache folders.

```
<syscheck>
  <ignore>/var/log</ignore>
  <ignore>/tmp</ignore>
  <ignore type="sregex">.log$|.tmp$</ignore>
</syscheck>
```

## ⑤ Raise brute-force threshold

Default 8 attempts is too sensitive — tune frequency + timeframe.

```
<rule id="100200" level="10"
  frequency="15" timeframe="60">
  <if_matched_sid>5710</if_matched_sid>
</rule>
```

## ⑥ Monitor first — Active Response last

Run *monitor-only* for 1–2 weeks before enabling auto-block.
Review what *would have* been blocked — then enable.

🚫 Never enable active-response on Day 1

# Wazuh + Claude Code — AI-Assisted Analysis

## Claude Code

by Anthropic — AI in your terminal

### When Claude adds value to Wazuh

- 🔍 **Bulk alert triage** — "which of these are true positives?"
- ✍️ **Custom rule authoring** — describe behavior, get XML
- 📖 **Incident narrative** — sequence of alerts → attack story
- 📋 **Compliance gap analysis** — dump SCA results, ask Claude
- 📊 **Executive summary** — weekly alert trends in plain Thai/English

Pull alerts via REST API and pipe to Claude:

```
# Query critical alerts from Wazuh API
curl -u admin:password -k \
  "https://wazuh:55000/alerts?level=12&limit=20" \
  | claude -p "Summarize these alerts and flag
    any that look like active intrusion"
```

Or connect Wazuh as an MCP tool in Claude Code:

```
// .mcp.json
{
  "mcpServers": {
    "wazuh": {
      "command": "npx",
      "args": ["wazuh-mcp-server"],
      "env": {
        "WAZUH_URL": "https://10.0.0.10:55000",
        "WAZUH_USER": "admin"
      }
    }
  }
}
```

MODULE 0 · END

# Questions?

Wazuh for Small Business — Why & Where

Docs: `wazuh.com/documentation` · Community: `wazuh.com/community` · Lab: `labs/01-intro.md`