



De cero a seguro

Instalá Wazuh y detectá amenazas en
minutos

wazuh.

```
$ whoami
```

@sultanovich (Pablo)

- Sysadmin veterano y SecOps por adopción
- Arranqué en GNU/Linux con Mandrake 7 y Debian 3
- Entré en seguridad por casualidad y terminé quedándome a vivir
- Uso software libre y una consola para resolver casi todo (a veces con una Raspberry Pi)
- Colaboro con las comunidades BairesNorteLug y OpenSSF
- Ayudo a proteger infra cloud (hoy, desde Wazuh)
- A veces doy charlas... como esta 😊

El problema en muchas empresas

- Tenés servidores, pero no sabés qué está pasando
- Querés ver vulnerabilidades, sin licencias ni dolores de cabeza
- No todos los equipos tienen un especialista en seguridad
- Lo ideal: algo fácil, abierto y que te avise cuando algo anda mal

¿Qué es Wazuh?

“ *Wazuh es una plataforma de seguridad (XDR / SIEM) open source, que permite **monitorear, detectar y responder ante amenazas** en entornos locales, virtualizados, contenedores y basados en la nube.* ”

- Centraliza logs, alertas y vulnerabilidades
- Dashboard web unificado
- Agente multiplataforma
- Sin costos de licencia
- Comunidad muy activa

¿Qué ofrece?

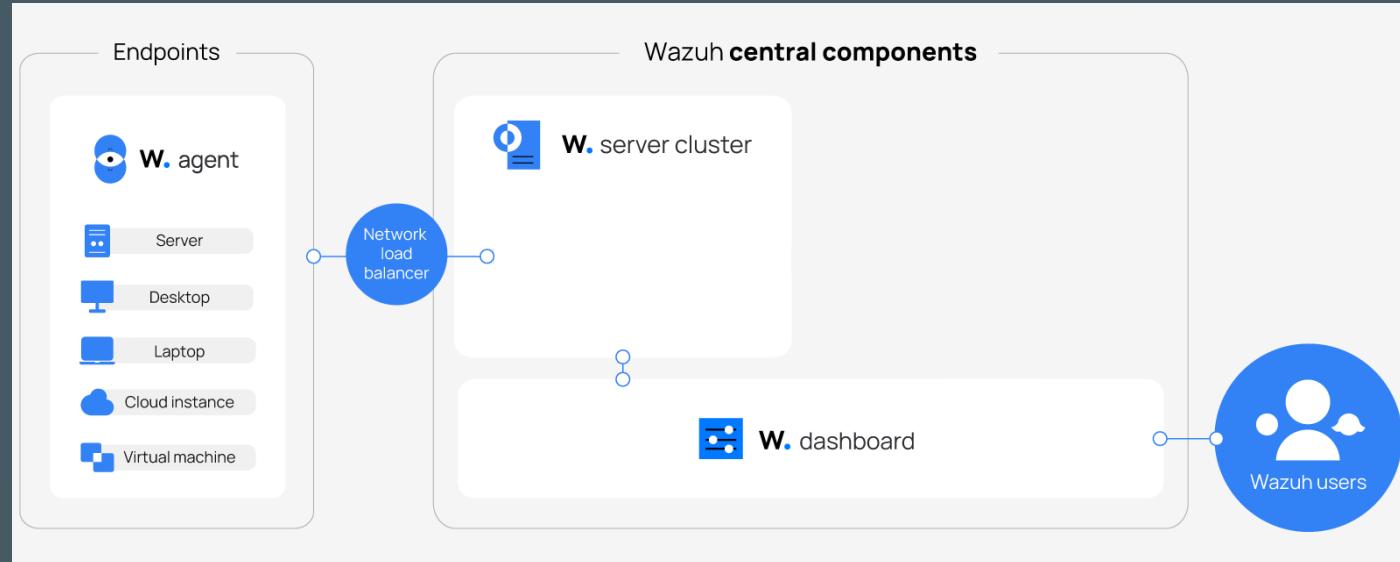
→ Desde el inicio:

- Detecta accesos y escaladas de privilegio
- Comprueba integridad de archivos (FIM)
- Identifica CVEs del software instalado
- Mide qué tan alineado estás a estándares (PCI, NIST, etc)

→ Si lo configurás a fondo:

- Se integra con Slack, AWS, VirusTotal y más
- Puede reaccionar automáticamente ante ciertos eventos

Arquitectura simplificada de Wazuh



- Modelo Cliente / Servidor
- Eventos Centralizados
- Se gestiona desde una Web (Dashboard)

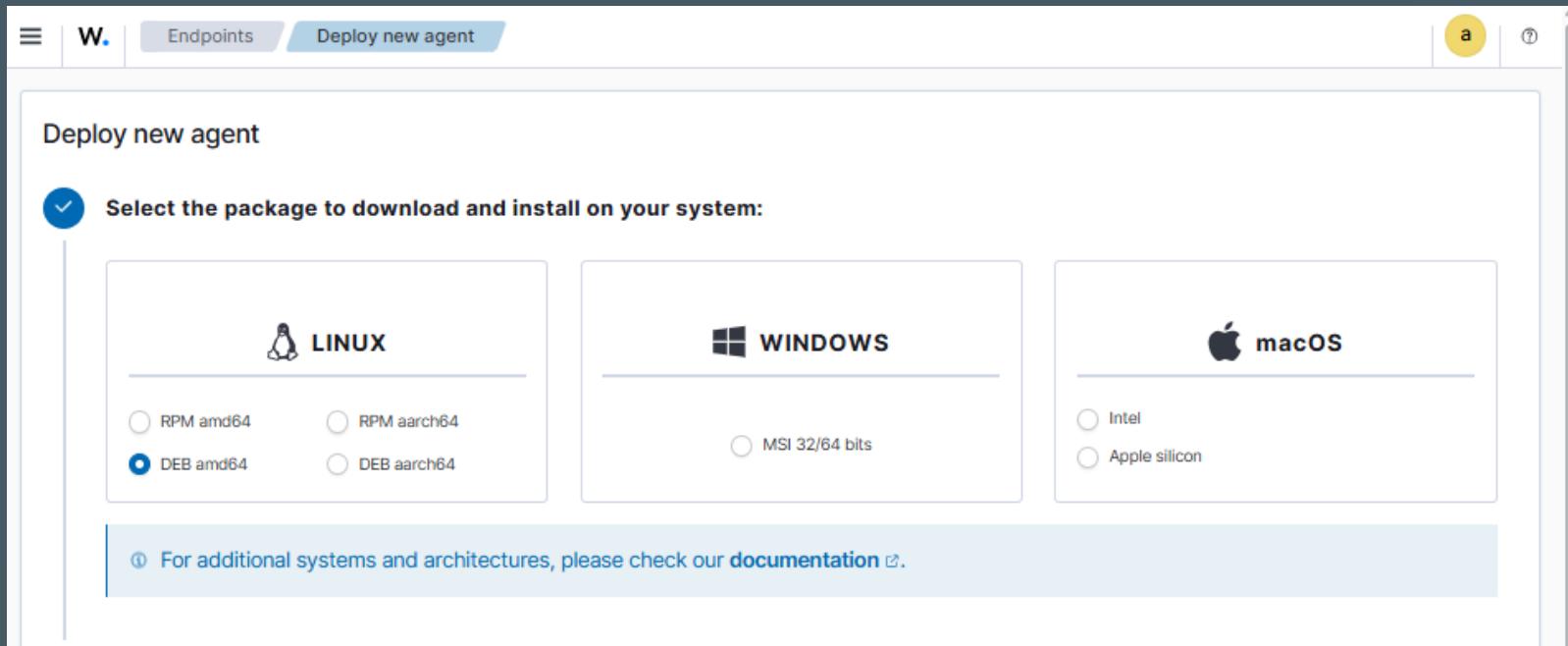
Wazuh Dashboard

The screenshot displays the Wazuh Dashboard interface. At the top, there is a navigation bar with a back arrow, forward arrow, refresh icon, and a URL field showing [https://192.168.0.5/app/wz-home#/overview/?_g=\(filters:!\(\),refreshInterval\(pause:!t,value:0\),time:\(from:now-24h,to:now\)\)&_a=\(filters:!\(\).query;\(language:kquery,query:''\)\)](https://192.168.0.5/app/wz-home#/overview/?_g=(filters:!(),refreshInterval(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(filters:!().query;(language:kquery,query:''))). On the right side of the header, there are icons for a star, a user profile, a download, and a help.

The main dashboard area is divided into several sections:

- AGENTS SUMMARY**: A box stating "This instance has no agents registered. Please deploy agents to begin monitoring your endpoints." with a blue "Deploy new agent" button.
- LAST 24 HOURS ALERTS**: A summary of alerts by severity:
 - Critical severity: 0 (Rule level 15 or higher)
 - High severity: 0 (Rule level 12 to 14)
 - Medium severity: 2 (Rule level 7 to 11)
 - Low severity: 6 (Rule level 0 to 6)
- ENDPOINT SECURITY**: A row of four boxes:
 - Configuration Assessment: Scan your assets as part of a configuration assessment audit.
 - Malware Detection: Check indicators of compromise triggered by malware infections or cyberattacks.
 - File Integrity Monitoring: Alerts related to file changes, including permissions, content, ownership, and attributes.
 - Threat Hunting: Browse through your security alerts, identifying issues and threats in your environment.
- THREAT INTELLIGENCE**: A row of two boxes:
 - MITRE ATT&CK: Explore security alerts mapped to adversary tactics and techniques for better threat understanding.
 - Vulnerability Detection: Discover what applications in your environment are affected by well-known vulnerabilities.
- SECURITY OPERATIONS**: A row of two boxes:
 - PCI DSS: Global security standard for entities that process, store, or transmit payment cardholder data.
 - GDPR: General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.
- CLOUD SECURITY**: A row of two boxes:
 - Docker: Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.
 - Amazon Web Services: Security events related to your Amazon AWS services, collected directly via AWS API.

Instalar un agente en GNU/Linux



```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.2-1_amd64.deb \
&& sudo WAZUH_MANAGER='192.168.0.5' dpkg -i ./wazuh-agent_4.11.2-1_amd64.deb
```

¿Qué veo cuando instalo un agente?

W. Endpoints Terminus

Threat Hunting File Integrity Monitoring Configuration Assessment MITRE ATT&CK Vulnerability Detection More... Terminus (001) Inventory data Stats Configuration

ID: 001 Status: active IP address: 192.168.0.6 Version: Wazuh v4.11.2 Group: default	Operating system: Debian GNU/Linux 12	Cluster node: node01	Registration date: Apr 23, 2025 @ 15:39:50.000	Last keep alive: Apr 23, 2025 @ 15:42:16.000
--	---------------------------------------	----------------------	--	--

Last 24 hours

Events count evolution

Count

timestamp per 30 minutes

MITRE ATT&CK

Top Tactics: Defense Evasion (2)

Compliance

PCI DSS

- 2.2 (181)
- 10.6.1 (4)
- 10.2.6 (3)

Vulnerability Detection

13 Critical
93 High

Top 5 Packages

Package	Count
grub-common	21
grub-pc	21

SCA: Lastest scans

Center for Internet Security Debian Family Linux Benchmark v1.0.0 cis_debian12

Policy	End scan	Passed	Failed	Not appl...	Score
Center for Internet Security Debian Family Linux Benchmark v1.0.0	Apr 23, 2025 @ 15:40:23.000	79	77	24	50%

Cumplimiento Normativo

PCI DSS

GDPR

HIPAA

NIST 800-53

TSC

- Vista simple que muestra qué controles se cumplen
- Ideal para auditar servidores sin herramientas pagas

Detección de vulnerabilidades

The screenshot shows the Wazuh Vulnerability Detection interface. At the top, there are tabs for 'Dashboard' (selected), 'Inventory', and 'Events'. A search bar contains the query 'wazuh.cluster.name: wazuh-server agent.id: 001'. Below the search bar are five summary cards with counts: Critical - Severity (13), High - Severity (93), Medium - Severity (135), Low - Severity (12), and Pending - Evaluation (10). Under each card is a table of top findings.

Top 5 vulnerabilities	Count	Top 5 OS	Count	Top 5 agents	Count	Top 5 packages	Count
CVE-2025-0395	7	Debian GNU/Linux 12 (bookworm)	263	Terminus	263	grub-common	21
CVE-2025-3576	5					grub-pc	21
CVE-2023-27043	4					grub-pc-bin	21
CVE-2023-46809	4					grub2-common	21
CVE-2024-11168	4					intel-microcode	15

¿Cómo instalar Wazuh?

“ Wazuh ofrece múltiples métodos de instalación, según tu entorno y experiencia. ”



Install.sh



OVA



AMI



Docker



Kubernetes



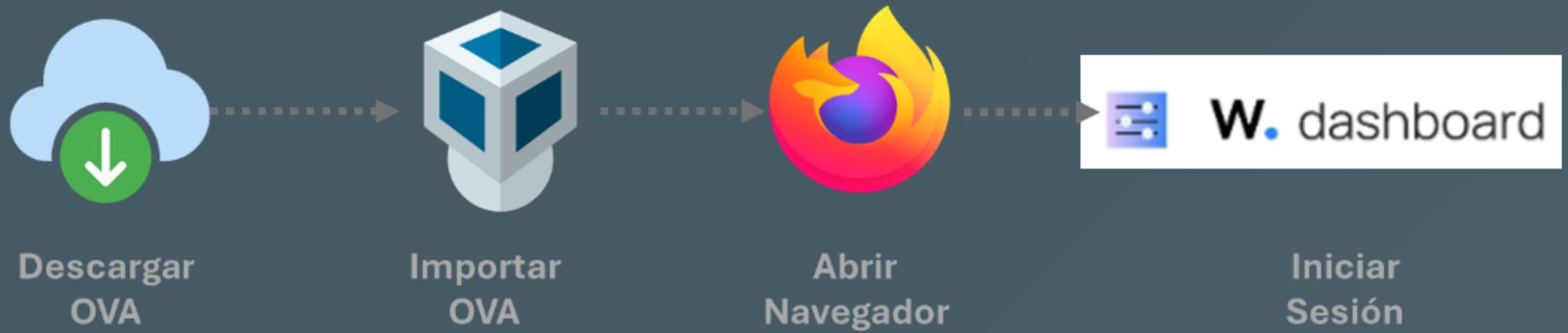
Paquetes
(RPM / DEB)



Wazuh
SaaS

Te permite iniciar con un entorno simple y escalarlo a despliegues complejos en producción

Instalación rápida (OVA)



Instalación rápida (OVA)



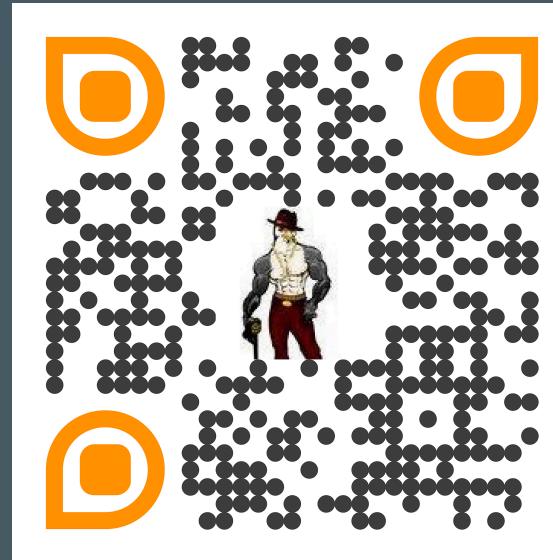
¿Qué vimos hoy?

- ➔ Qué es y qué hace Wazuh
- ➔ Qué información tenemos cuando lo instalamos
- ➔ Cómo ayuda a cumplir normas de seguridad
- ➔ Cómo instalarlo rápidamente
- ➔ Cómo agregar un agente (Desktop/Server)

¿Preguntas?



¿Preguntas, ideas o ganas de seguir charlando?



🌐 linktr.ee/sultanovich.sh | 🐦 github.com/sultanovich

```
$ echo "despedida.txt"
```

Gracias por quedarte hasta el final 🙏