



## **MidPoint Integrations: Partner Series**

**Improving MidPoint Security  
using Wazuh**

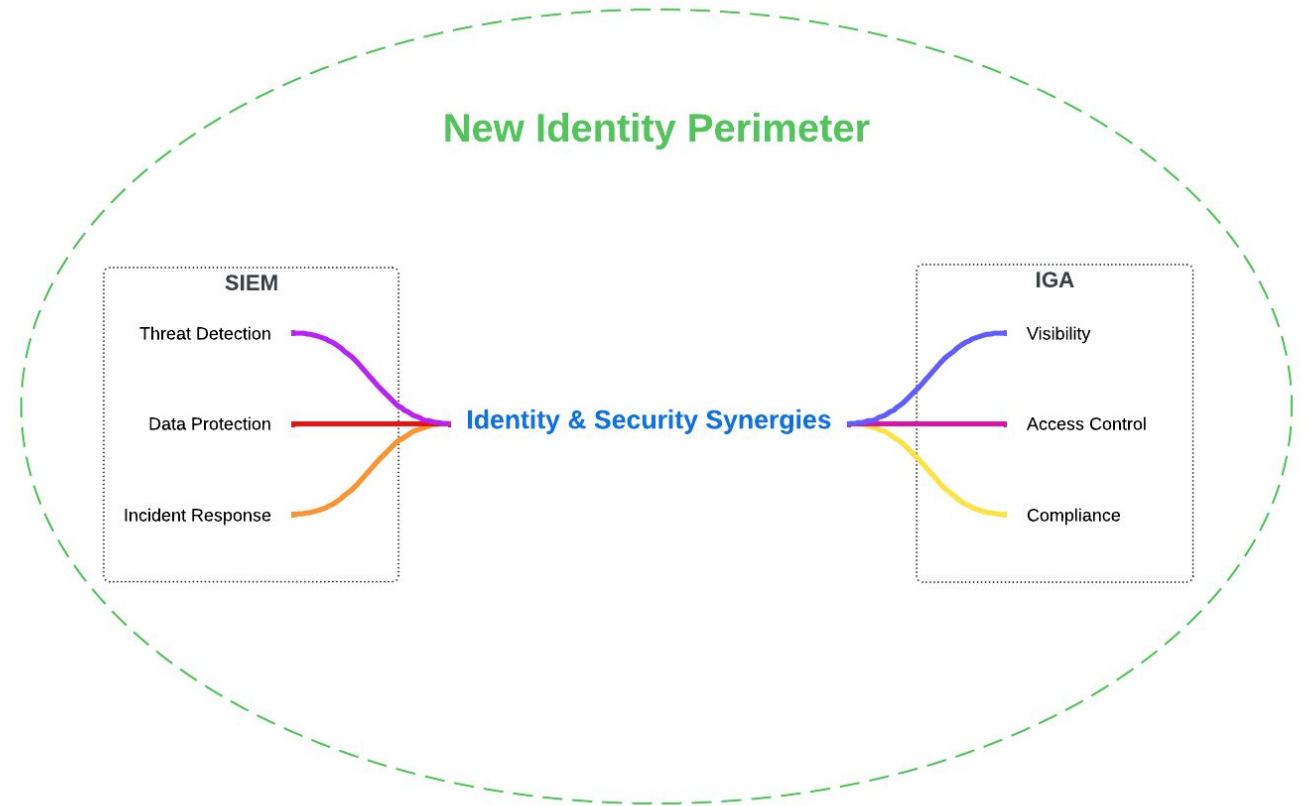
# Agenda

- Identity is the new perimeter: Challenges
- Benefits of Integrating MidPoint with Wazuh
- Integration and Installation
- Configuration Assessment
- File Integrity Monitoring
- Threat Hunting
- Active Response
- Q&A

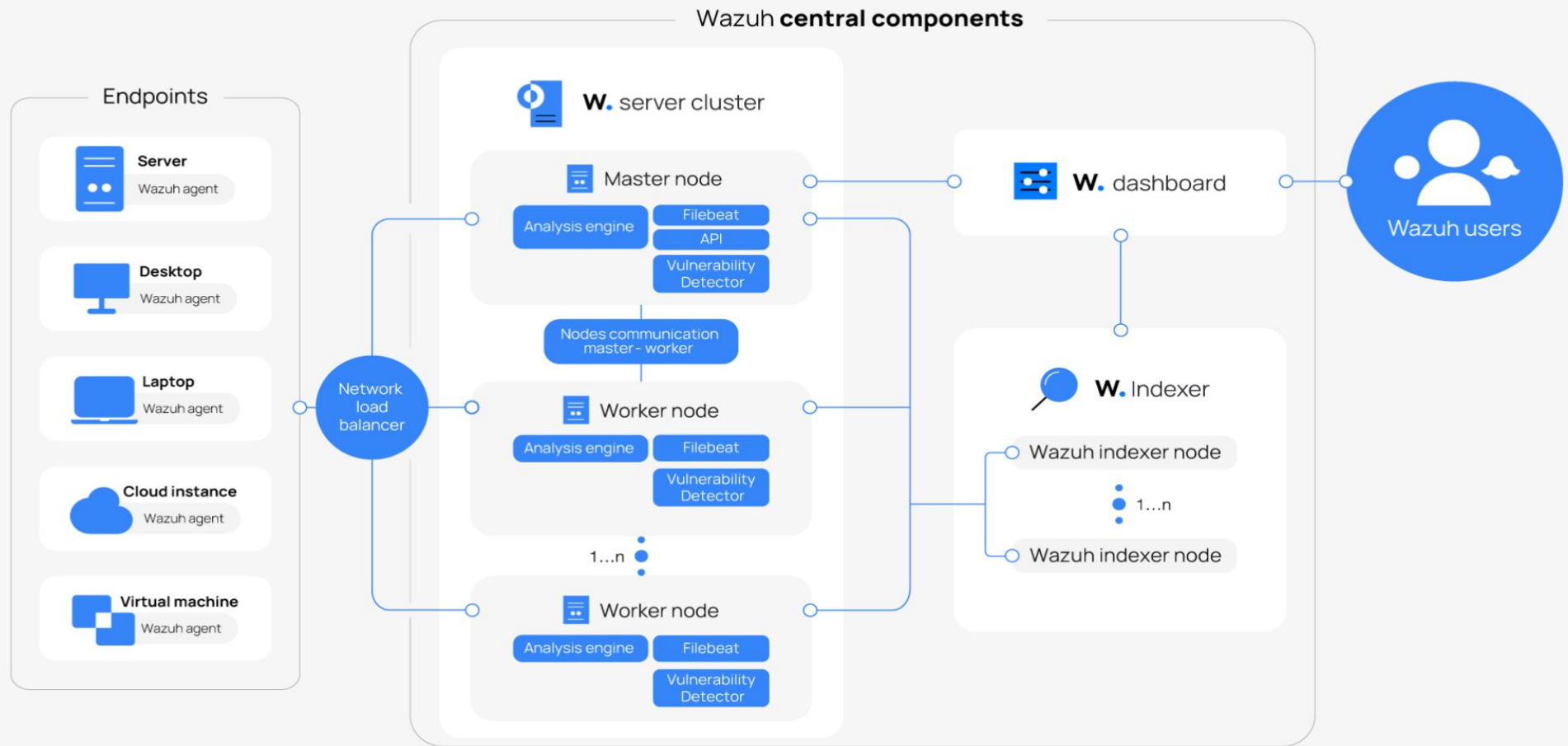


# Identity is the new perimeter: Challenges

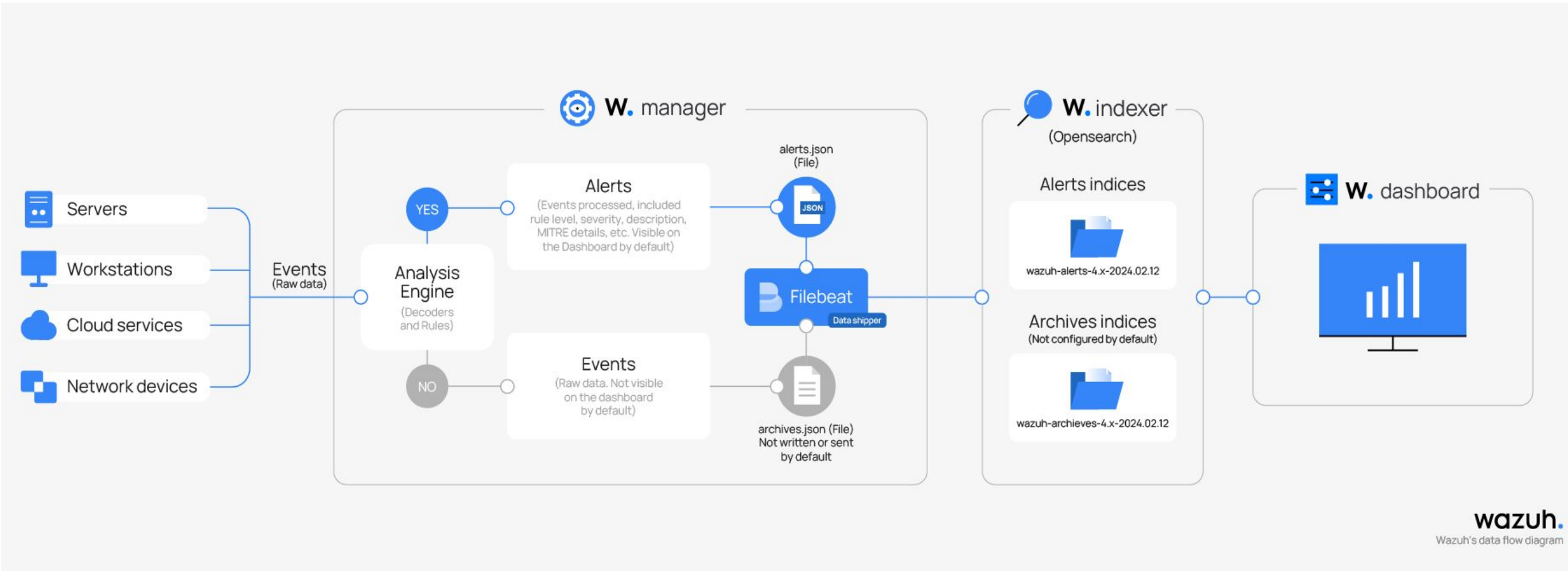
- Protect against identity-based attacks
- Cohesive security governance
- IGA as the “keys to the kingdom”
- Fragmented visibility and slow detection of identity-based threats



# Wazuh's Central Components



# Wazuh's Data Flow



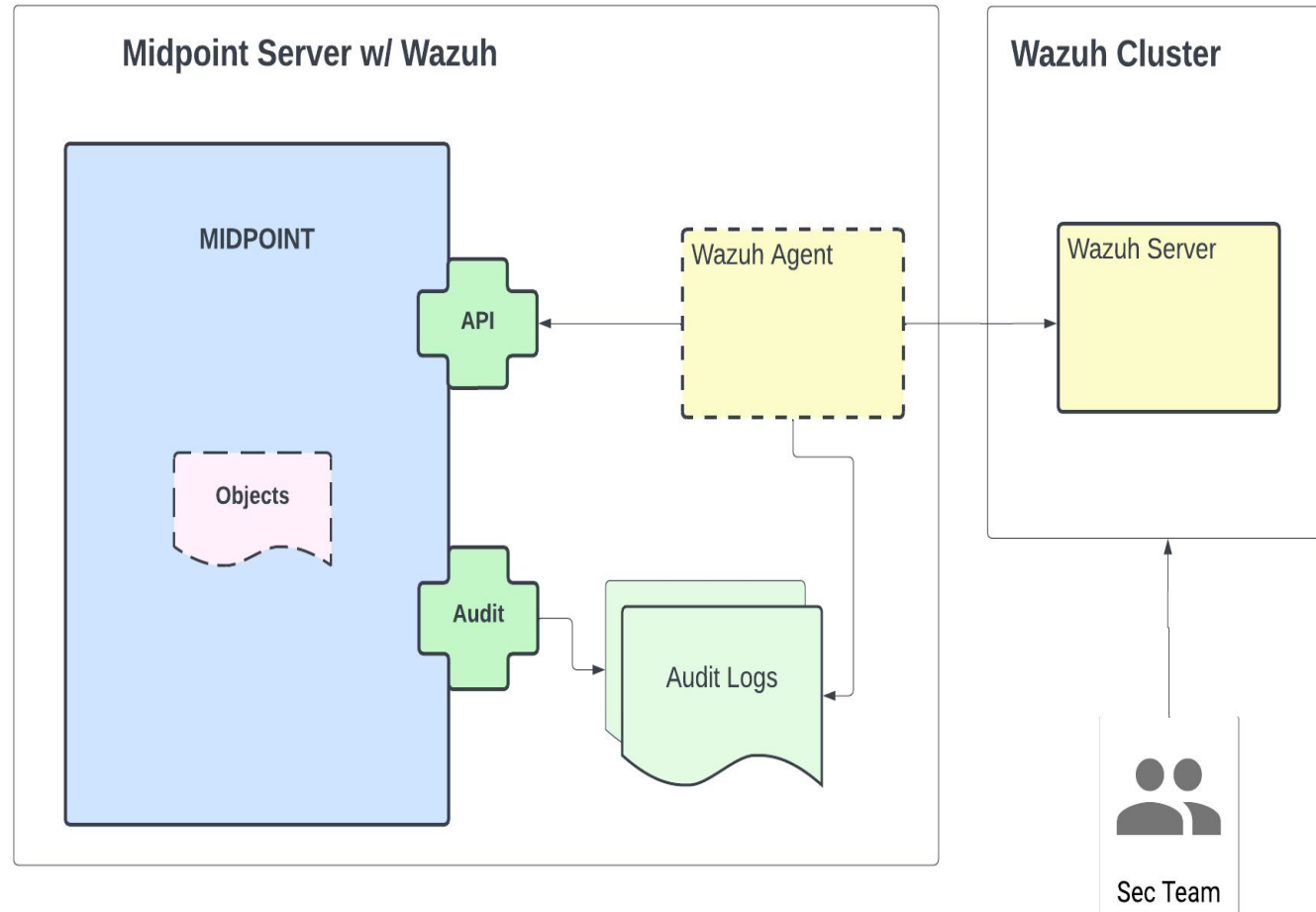
# Benefits of Integrating MidPoint with Wazuh

- Monitor System Integrity
- Security Configuration Assessment
- Identify Suspicious Activity
- Threat Mitigation



# Integration

- MidPoint Auditing
- MidPoint API
- Wazuh Agent



# MidPoint Configuration

- Auditing
- API
- Integrations

**Logging** (SystemConfiguration)

Operations

[← Back](#) [Save](#) [Edit raw](#)

- Logging
- Class loggers **9**
- Appenders **3**

**Logging** ⓘ ⬇️ ⬆️

Root appender \*

Root logger \*

[Show empty fields](#)

**Audit** ⓘ ⬇️ ⬆️

Enabled

Details

Appender  + -

[Show empty fields](#)

**Advanced**



# Wazuh Configuration

- Policies
- Decoders and Rules
- Integrations
- Groups

## Rules (9)

From here you can manage your rules.

relative\_dirname=etc/rules

ID ↑	Description	Groups
100001	sshd: authentication failed from IP 1.1.1.1.	authentication_failed, local, syslog, sshd
100900	Midpoint Audit messages grouped.	midpoint
100901	Midpoint Authentication	midpoint
100902	Midpoint Authentication failed for <b>principal</b>	midpoint
100910	Midpoint Configuration action	midpoint
100920	Midpoint Archetype action: <b>event_type</b>	midpoint
100920	Midpoint Archetype action: <b>event_type</b>	midpoint
100920	Midpoint Archetype action: <b>event_type</b>	midpoint
100921	Midpoint Employee Archetype action <b>event_type</b> !	midpoint

# Threat Hunting

- Real-time Alerts and Activity Logs
- Analyzing Security Events: Decoders and Rules
- Investigating Suspicious Activities

rule.description	rule.level
Midpoint UserType action: ADD_OBJECT	7
Midpoint Audit messages grouped.	4
Midpoint UserType action: ADD_OBJECT	7
Midpoint Audit messages grouped.	4
Midpoint UserType action: ADD_OBJECT	7
Midpoint Audit messages grouped.	4
Midpoint UserType action: ADD_OBJECT	7
Midpoint Audit messages grouped.	4
Midpoint Audit messages grouped.	4
Midpoint Audit messages grouped.	4
Midpoint Audit messages grouped.	4

# Configuration Assessment

- Security Configuration Assessments
- Creating Custom Policies

System audit for Midpoint running systems ⓘ

Passed	Failed
1	0

Checks (1)

Search

ID ↑	Title
2000	Ensure MidPoint configuration file is read-only by the owner

Rows per page: 10 ▾

# File Integrity Monitoring

- Setting Up File Integrity Monitoring
- Monitoring Critical Files
- Responding to Unauthorized Changes

Groups:  
default Linux Midpoint

< Integrity monitoring **ENABLED**  
Identify changes in content, permissions, ownership, and attr

General **Monitored** Ignored No diff Who-data

**Monitored directories**  
These directories are included on the integrity scan

- /bin
- /boot
- /etc
- /opt/midpoint/bin
- /opt/midpoint/lib
- /opt/midpoint/var/config...
- /opt/midpoint/var/conni...
- /opt/midpoint/var/keyst...
- /opt/midpoint/var/schema

# Active Response

- Automated Threat Mitigation
- Configuring Active Response Action
- React to conditions outside MidPoint

# Resources

- Midpoint Config
- Rules and Decoders
- SCA Policies
- API Client



**Thank you for your attention**

Q & A