Security infrastructures and intrusion systems

Matthias Mildenberger

Intrusion Detection

- Detection of attacks
- NOT intrusion prevention or forensic tools

Intrusion detection

- Host based intrusion Detection (HIDS)
  - File integrity monitoring, rootcheck analysis, suspicious accesses
- Network based intrusion detection (NIDS)
  - Suspicious Signatures of packes, DoS...

Software on the market

OSSEC

HIDS

splunk>

NIDS

SNORT®

NIDS

SURICATA

NIDS

tripwire

HIDS

wazuh.

NIDS+

Software on the market

splunk>

NIDS **Not opensource ??**

OSSEC

HIDS ☆ Star 3.9k

SNORT®

NIDS ☆ Star 1.7k

SURICATA

NIDS ☆ Star 3k

tripwire®

HIDS **Not really opensource ??**

wazuh.

NIDS+ ☆ Star 5.6k

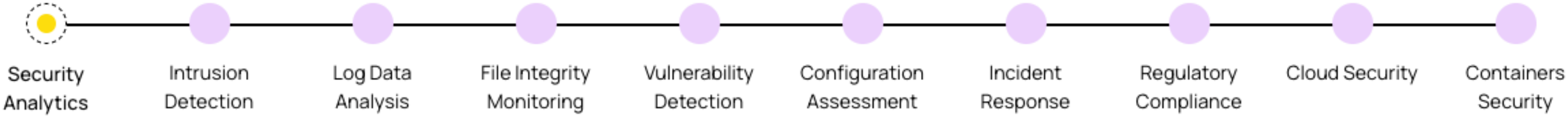
wazuh.

+ SURICATA

wazuh.

The Open Source Security Platform

Unified XDR and SIEM protection for endpoints and cloud workloads.



Security Analytics

Intrusion Detection

Log Data Analysis

File Integrity Monitoring

Vulnerability Detection

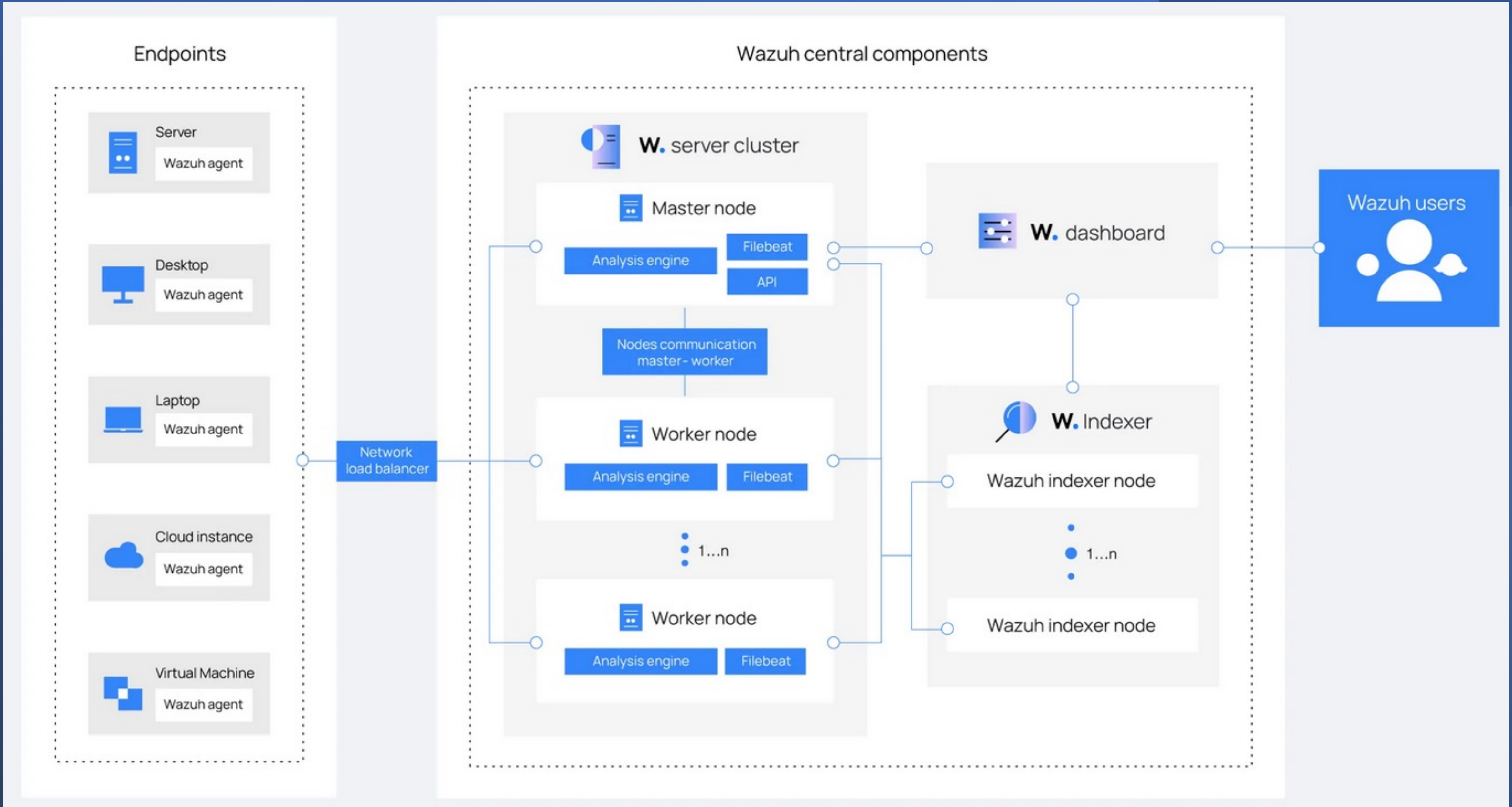
Configuration Assessment

Incident Response

Regulatory Compliance

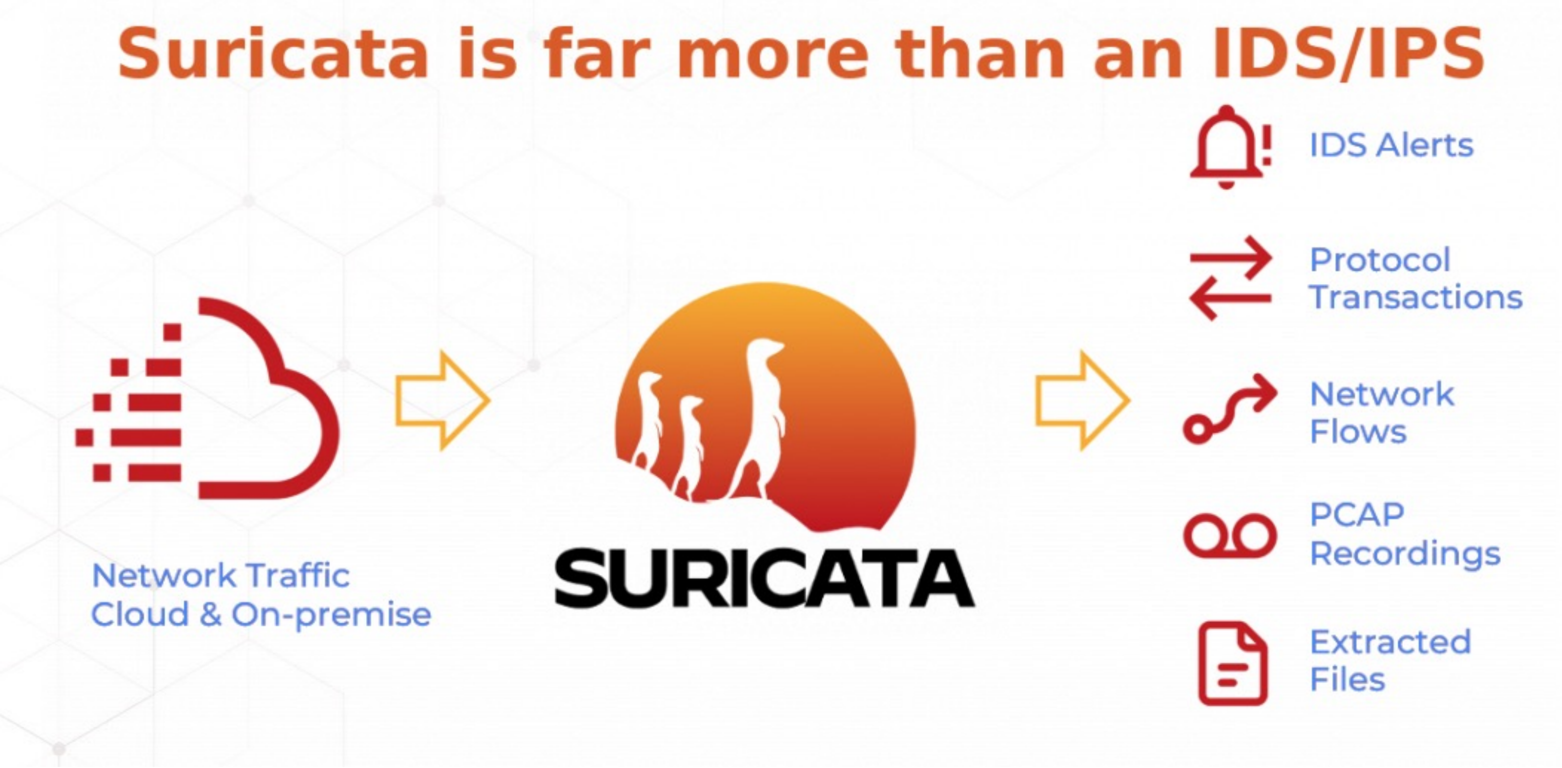
Cloud Security

Containers Security


Endpoints
Server
Wazuh agent
Desktop
Wazuh agent
Laptop
Wazuh agent
Cloud instance
Wazuh agent
Virtual Machine
Wazuh agent
Network load balancer
Wazuh central components
W. server cluster
Master node
Analysis engine
Filebeat
API
Nodes communication master - worker
Worker node
Analysis engine
Filebeat
1...n
Worker node
Analysis engine
Filebeat
W. dashboard
W. Indexer
Wazuh indexer node
1...n
Wazuh indexer node
Wazuh users

SURICATA

Observe. Protect. Adapt.



Suricata is far more than an IDS/IPS

Network Traffic
Cloud & On-premise

SURICATA

IDS Alerts

Protocol Transactions

Network Flows

PCAP Recordings

Extracted Files

Let’s get physical (tech-demo)