FORTINET

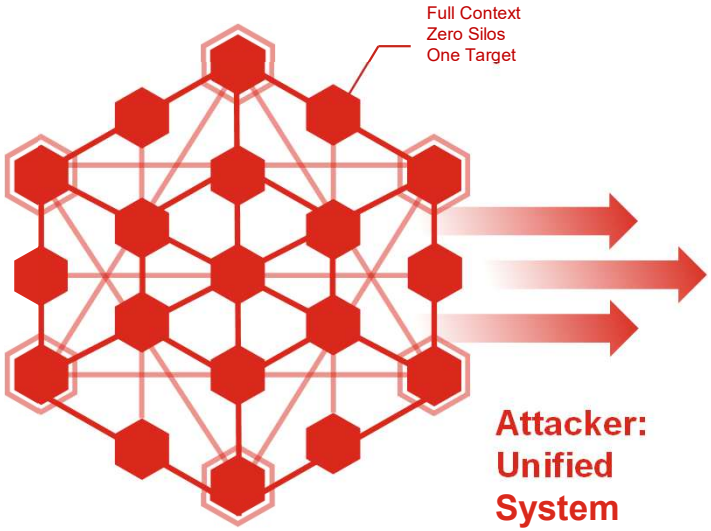
The AI Shift:
Driving Autonomous Security While Containing Risk

Malcolm Orekoya (CISSP, CISM)
Channel SE – GSI Partners
Advanced Threat Protection SME

AI vs AI
The Killer App Only a Platform Can Deliver

Attackers Have Already Figured Out AI: Who has the Advantage?

The question is structural



The Asymmetry

Threat actors operate as a unified system
Defenders are fragmented

VS

The Reality

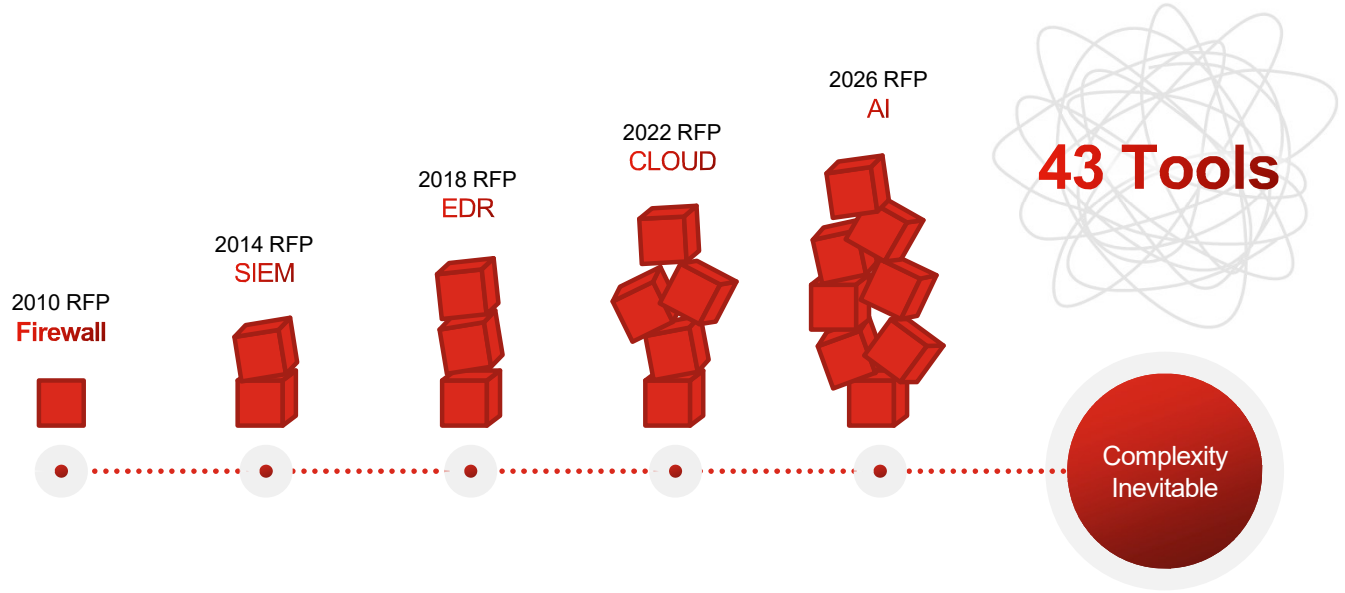
This structural gap—Does your security architecture give your AI a fighting chance?

Security Was Never Bought as Security

We bought projects…

The Procurement Trap

- Every purchase was rational
- The firewall had an RFP
- The SIEM had an evaluation, but nobody was accountable for the portfolio
- The result is fragmentation that blocks AI efficacy



Best of Breed Assumes Tools Work Alone

In the AI era, they can't

Then

Assumption:
Tools work in isolation

Now

Reality: The signal is in correlations between the tools

The SecOps Reality: Faster Attacks, More Surfaces, More Work

We're moving from reactive, human-driven security to proactive, machine-led security

Evolving Threat Landscape

Attackers now move faster than human analysts can investigate or traditional SOC capabilities can defend .

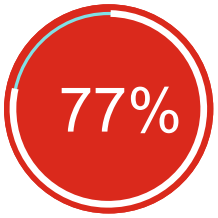
Expanding Attack and Risk Surfaces

External Threats

25+

New exploitable paths per week across cloud, OT, identities…
And now AI

Insider Risks



Percent of organizations that experienced one or more data loss incidents involving an insider in the past 18 months.

SecOps Complexity

Teams can't correlate alerts, scale investigations, and lack analysts.

Security Operations Is Entering a Machine-Speed Era

The market reality - every major vendor is now pitching:

AI-Powered
AI-Augmented
AI-Led

Autonomous

Platform

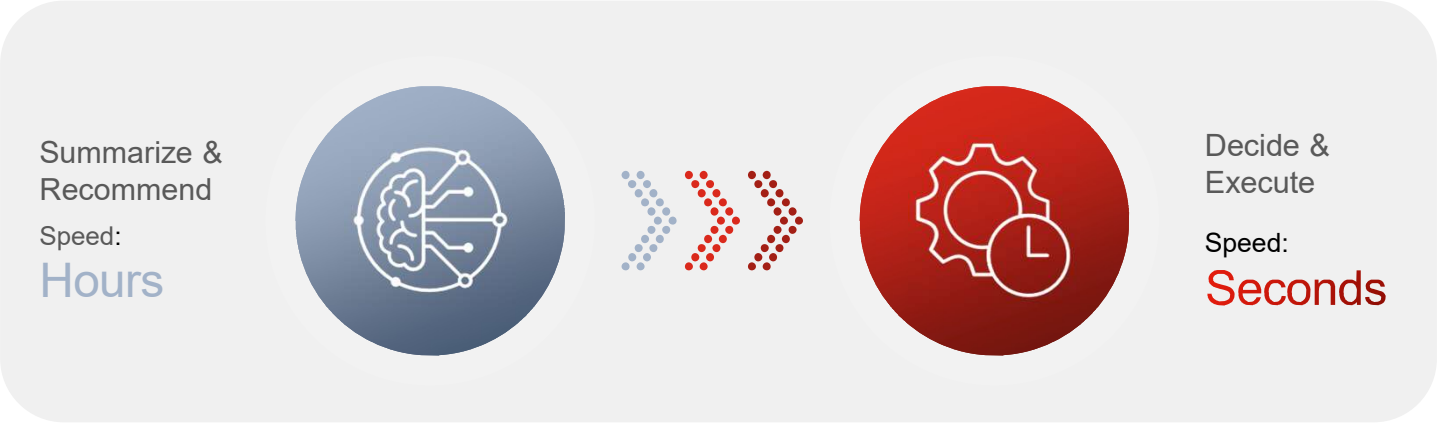
What you need to understand

GenAI Assists. Agentic AI Acts.

The speed of response must match the speed of the attack

The Evolution

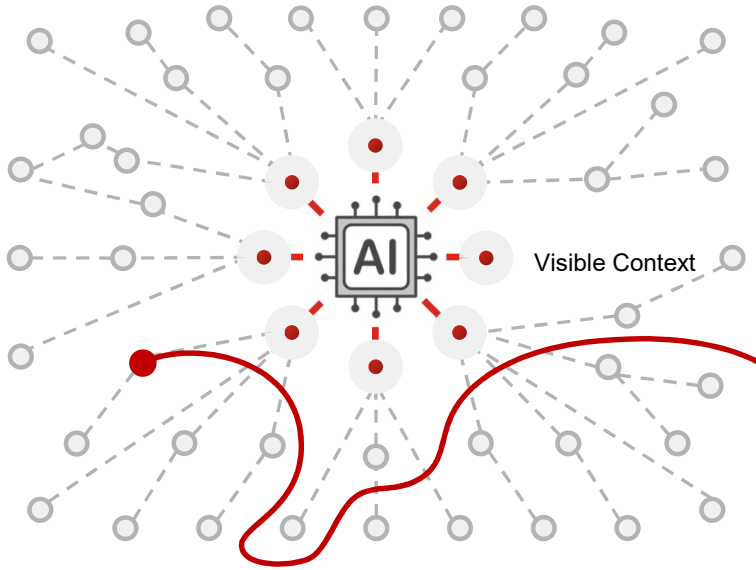
We're moving from summarization and Q&A to autonomous action. Modern attacks move at machine speed. Humans cannot keep up. But speed without visibility and intelligence is dangerous.



VISIBILITY

Your AI is Only as Smart as the Data It Can See

43 Tools?
Your AI connects to maybe 6



90% Blind Spots
Threats hide here

Blind AI
is not security, it's a risk

Confident but Wrong
Model analyzes 10% of the context

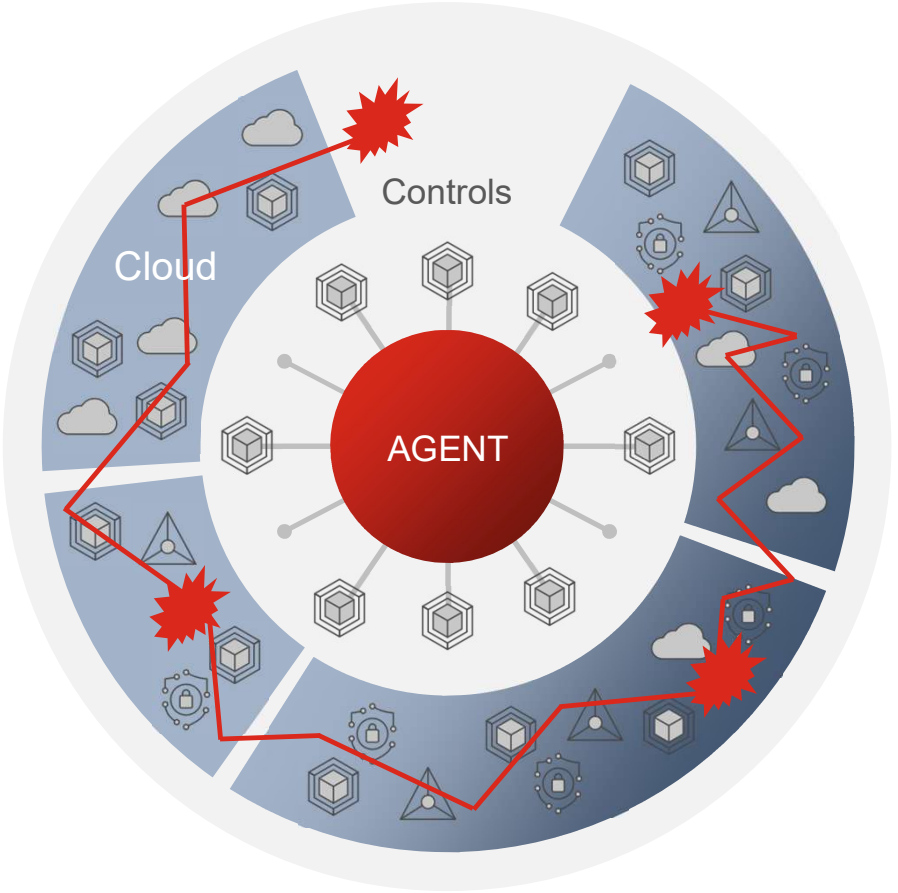
Exfiltration
Hidden between the tools

An Agent That Controls 20% of Your Environment

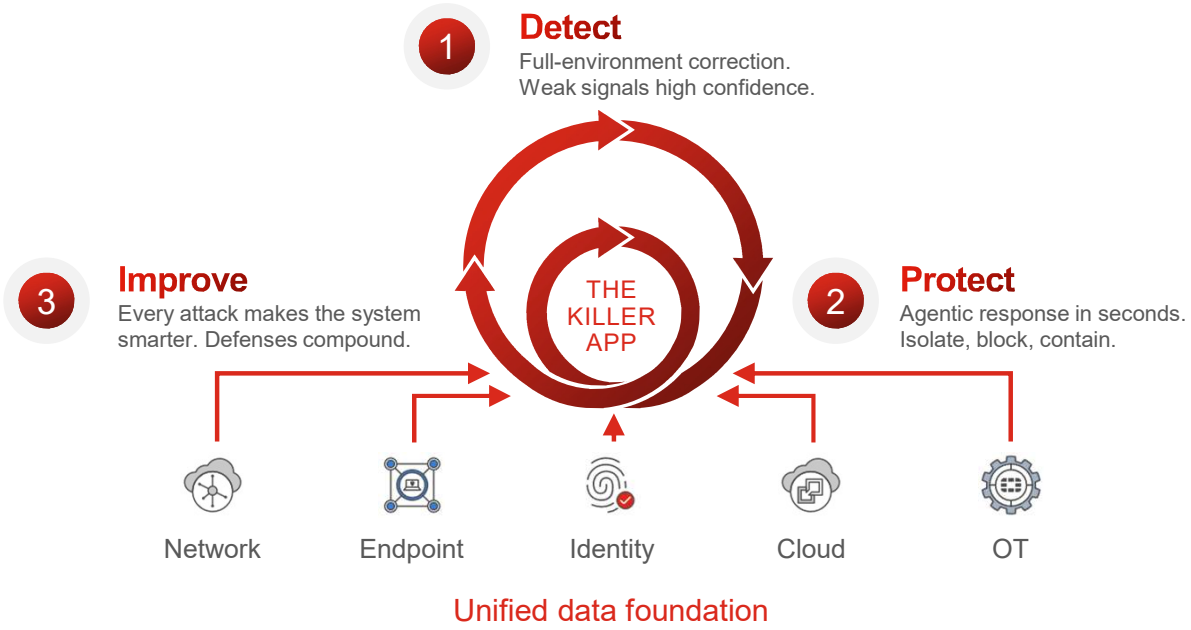
… is not an agent. It's a risk

Automated Incompetence

If your agent only sees the endpoint, it isolates the laptop while the attacker moves laterally through the cloud. In a fragmented stack, an agent reports "Success" while the breach continues.



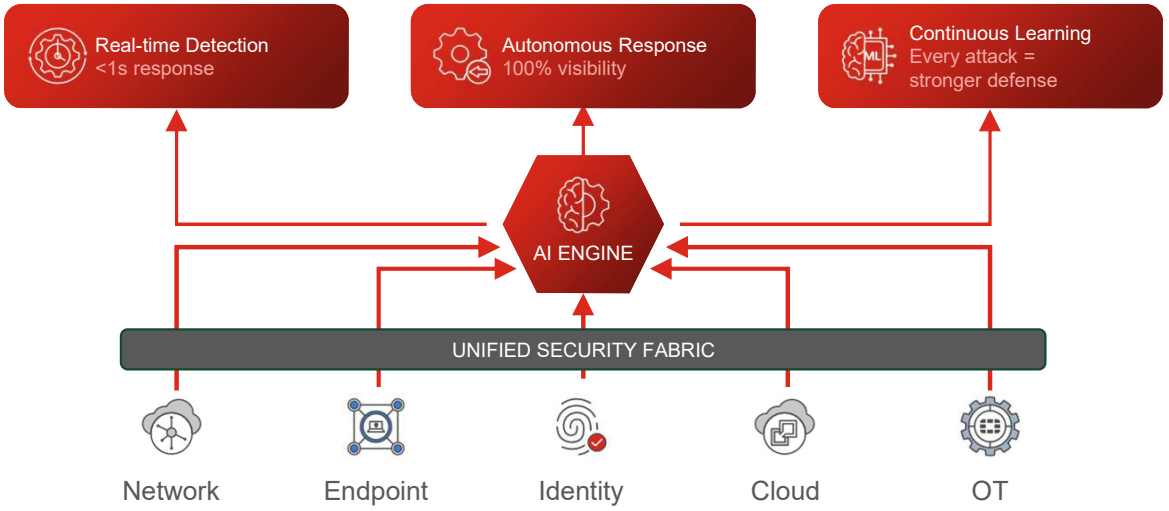
The Killer App



- The “Improve” loop flips the asymmetry.
- In a unified platform, the defense gets smarter with every attack.
- Attackers must keep innovating. Defenders accumulate advantage.
- The platform, and agentic loop are the great unlock. The “Killer App.”

Platform Isn’t a Purchasing Preference

It's an architectural requirement



The platform isn’t where you deploy AI. It’s what makes AI work.

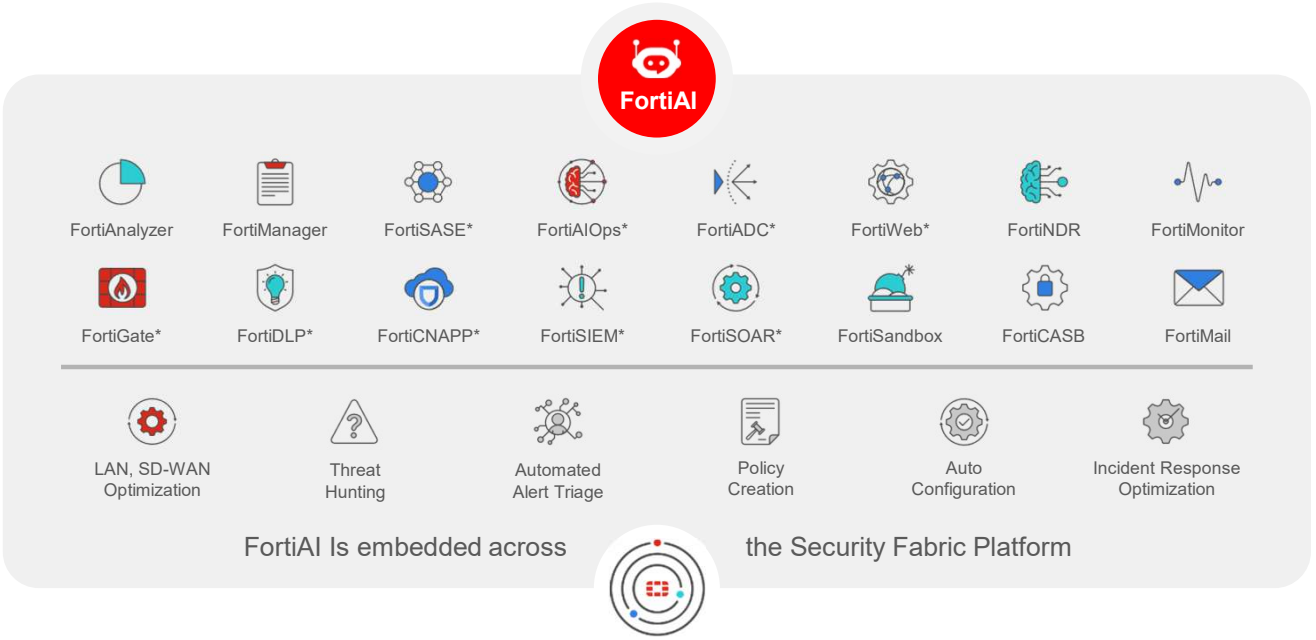
The Detect-Protect-Improve loop requires:

- Unified data — every signal, every domain, one model
- Integrated controls — act everywhere, not just where you have APIs
- Continuous learning — the system improves with every attack

The Most Integrated

AI powering
20+
Solutions

with
500+
Patents*

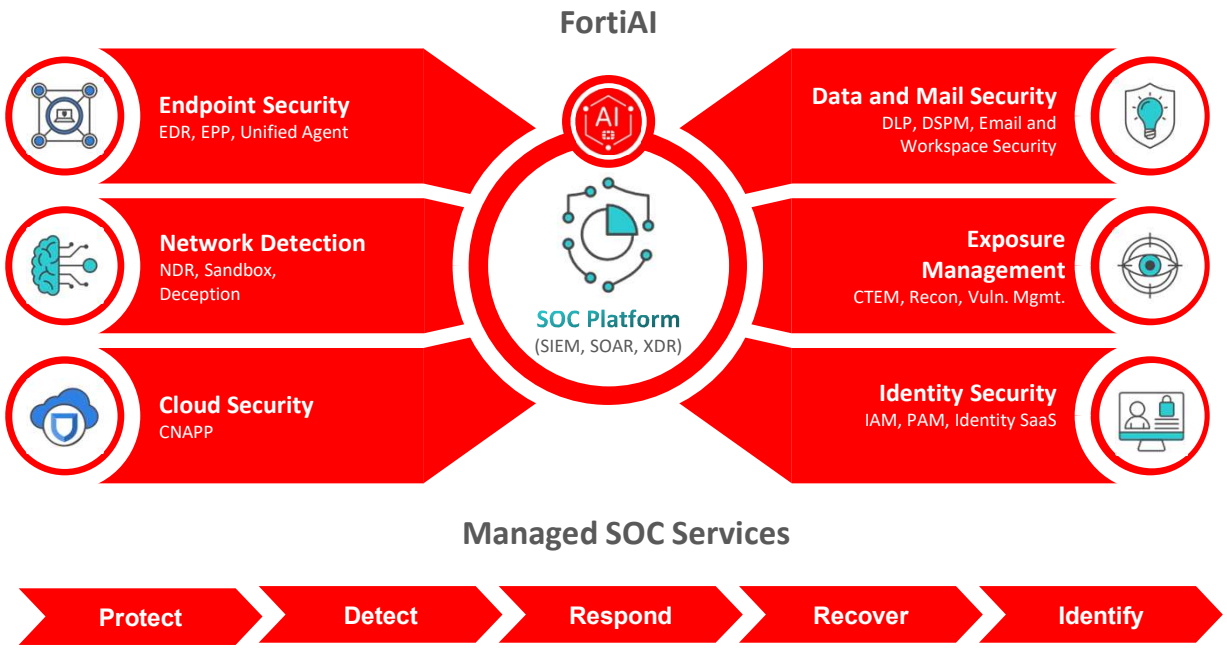


*Registered and Pending

Broadest Security Operations

Operate across the full SOC lifecycle with speed, scale, and automation

- End-to-End Coverage
- Detect Earlier
- Respond Faster
- Connect Everything
- Automate Anything
- Scale as You Grow
- Reduce TCO



Purpose-Built for Every Stage of the Security Operations Journey

	Start Anywhere	Automate Anything	Deploy with Flexibility
How Fortinet delivers	The only vendor offering a continuous maturity path from managed to Advanced SOC Platform.	The industry's most adaptable automation, delivering up to 99% faster response.	The lowest TCO, delivering scalable cloud, hybrid, and on-prem models.
Customer benefit	Improved security posture, simplified operations and coverage throughout the entire SecOps journey.	Automate anything, connect everything at scale to accelerate threat response and optimize operations.	Reduce overhead, complexity, and enable SOC capabilities for any requirement.
Proven results	**86%** Increase in productivity	**85%** Fewer false positives	**99%** Reduction in manual processes

Turnkey SOC: FortiAnalyzer

Essential turnkey capabilities purpose-built for lean teams

Unified Data Lake

Centralized log collection with a unified view and single source of truth.

Native Threat Intelligence

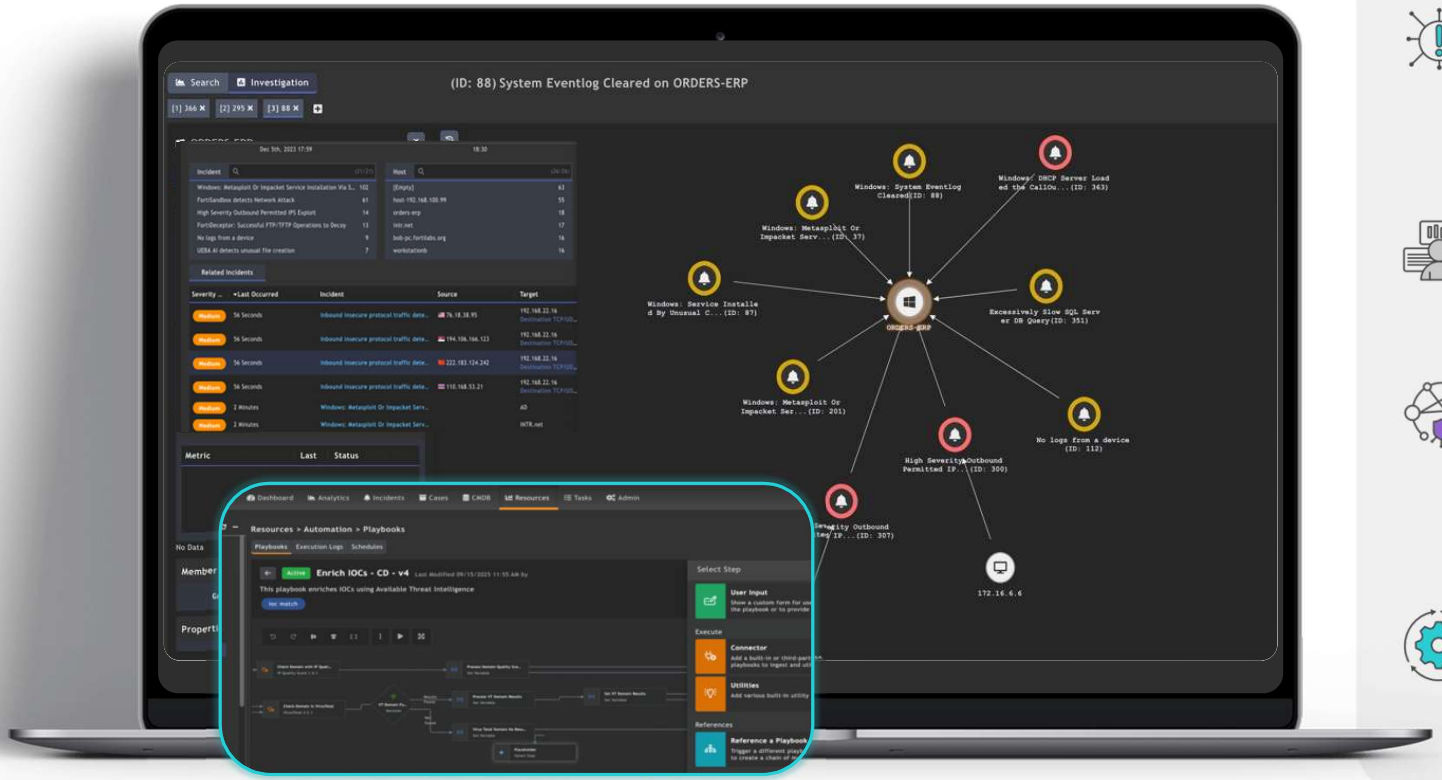
Surface threats with FortiGuard Labs intel, outbreak detection, and IoC tracking.

Built-in SOC Automation

Ready-to-deploy XDR, SIEM, and SOAR capabilities with prebuilt content.

Advanced SOC: FortiSIEM and SOAR

Connect anything, automate everywhere



Working together or independently to power the Enterprise & MSSP SOC

Enterprise Threat Detection

Multivendor event collection, behavioral threat detection, and comprehensive SIEM features.

Incident Management

Rich analyst features optimized and automated to prioritize and respond to attackers in real-time.

SecOps Functions and Management

Vulnerability and compliance management, threat intel and hunting, operations management, and much more.

Automation Everywhere

Native SOAR automation in SIEM and full SOAR platform for any SecOps / NOC / IT workflow.

Managed SOC: FortiGuard SOCaaS

Security monitoring and incident handling managed 24/7

Detect

Let Fortinet monitor and investigate alerts 24/7, notifying you when something is important and needs attention.

Respond

Fortinet experts will alert teams in 15 minutes and provide insights on the incident and remediation steps.

Improve

Cloud portal with intuitive dashboards, on-demand reports, and quarterly meetings with Fortinet experts.

FortiSOC: Unified Cloud SOC

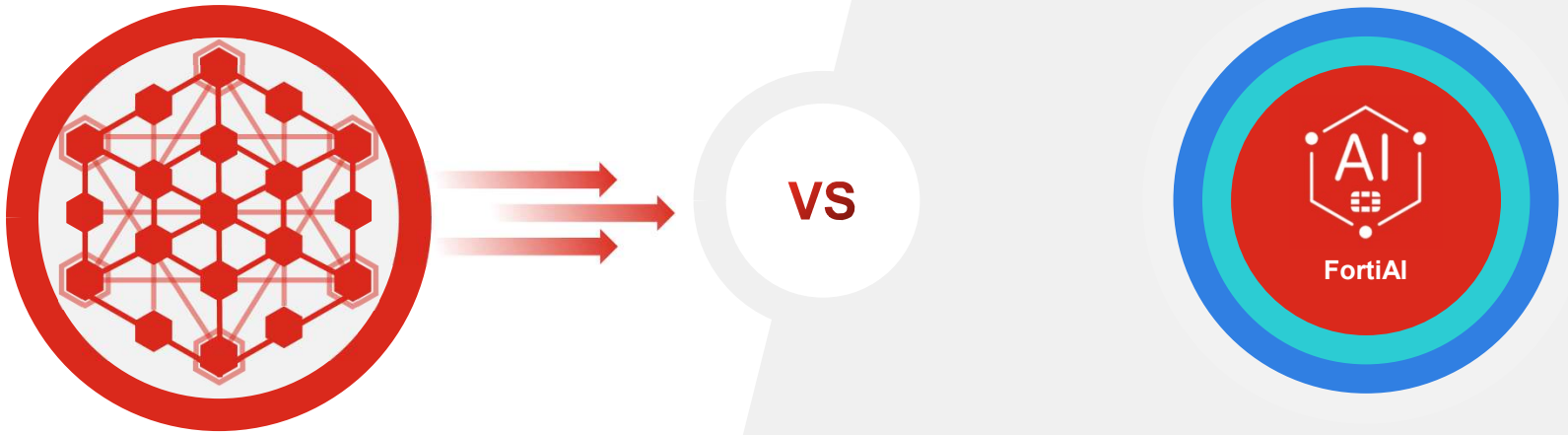
Consolidates Analyzer, SIEM, SOAR, TIP, UEBA, and Agentic AI into a single cloud-delivered service

FortiSOC

- Unifies users, assets, and behaviors into a single source of truth.
- AI analyzes and correlates alerts to surface what matters most.
- Automates response to disrupt attacks at machine speed.
- Single cloud service and license simplifying deployment and SOC scale

Winning in the AI Era Starts with the Platform

Companies that move to Fortinet will have defense that compounds in value



Attacker

Agentic Unified Defender

The companies that win won’t have the best AI. They’ll have the best platform for AI.

Thank you