

The Fortinet logo, featuring the word "FORTINET" in a bold, black, sans-serif font. The letter "O" is replaced by a red square icon with a white grid pattern. A registered trademark symbol (®) is located at the end of the word. The background of the slide includes a light gray grid of dots in the top left, a red horizontal bar in the top right, and a teal rounded rectangle in the bottom right.

FORTINET®

FortiSOC – Unified, Automated, And Powered By Agentic AI

Why security operations is changing

FortiGuard Labs sees the pressure rising on every axis, and it is outpacing how most customers operate today



36K
scans / second

Attacks execute at machine speed, manual triage cannot keep up



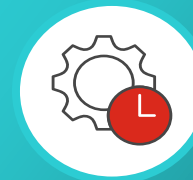
67%
of analyst capacity

Alert volume alone now consumes most of a team's day



~49%
uses living-off-the-land

Attackers abuse valid tools and credentials, signatures miss them



Hours
time-to-exploit

New vulnerabilities are weaponized in hours, not weeks

Customers will spend to reduce risk, cut alert noise, and cover the talent gap, the partner who frames the problem and solution first wins the project.

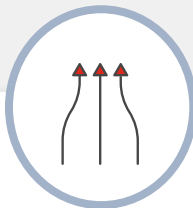
Customer Challenges

The SOC challenge is no longer detection alone; it is operational scalability.



More Threats, More to Protect, More Telemetry

AI-powered threats, cloud workloads, identity sprawl, APIs, and multivendor telemetry expand the SOC problem faster than teams can scale.



Too many handoffs and Blind spots

Disconnected detection, investigation, and automation workflows create duplicated work, slower decisions, and analyst fatigue



Buying and ops friction

Customers want faster time to value, easier operations, and flexible consumption without building another

MARKET SHIFT

Buying criteria shifting now

The market is rewarding unified platform experiences, faster time to value, simpler licensing, predictable operations, and embedded AI:

- From standalone tools to unified platforms
- Point integrations to common workflows
- Manual correlation to AI-powered investigation
- CAPEX-heavy refreshes to SaaS consumption
- From detection-only thinking to operational metrics/KPIs/outcomes

What customers ask	What it really means for the SOC
“Can we detect it?”	Do we have enough context to know what is real, related, and urgent?
“Can we respond faster?”	Can workflows execute consistently across tools without waiting on manual handoffs?
“Can we scale?”	Can we grow coverage and maturity without rebuilding the SOC architecture?



What customers are asking for

The same six requests keep surfacing — these conversations are already happening in your accounts.

Platform consolidation

Fewer tools and consoles; one place to operate

AI-assisted operations

Help triaging, investigating, and responding faster

Faster deployments

Outcomes in weeks, not a multi-quarter SOC project

Lower operating overhead

Predictable cost; less admin and tuning burden.

Managed services

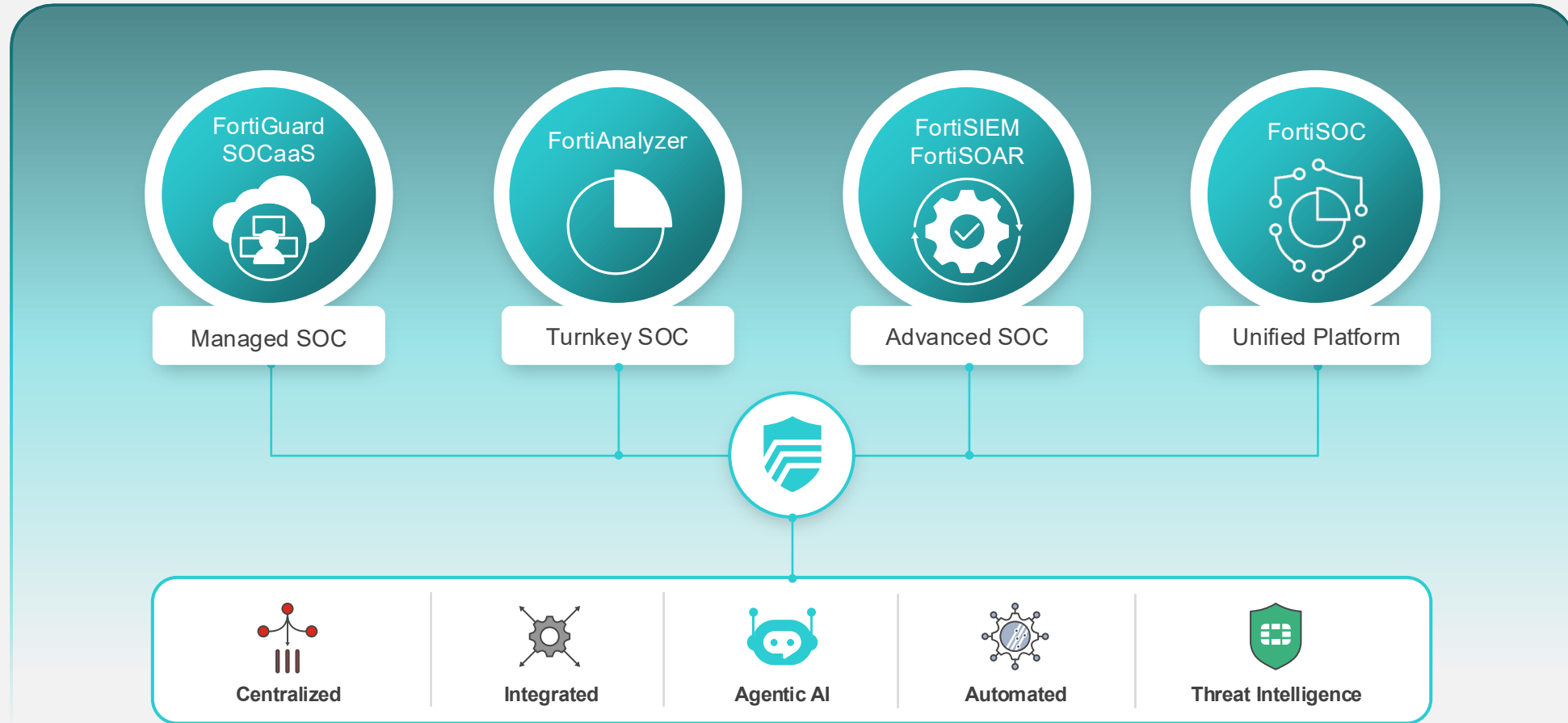
Someone to run it, co-managed or fully managed

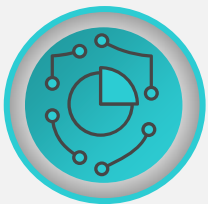
Faster outcomes

Measurable improvement in detection and response

Fortinet SOC Platform Portfolio

Choose from a unified platform, independent integrated solutions, or expert managed services





Introducing FortiSOC – One platform, total control



FortiAnalyzer

Analytics + Fabric Integration



FortiSIEM

Multi-vendor correlation at scale



FortiSOAR

Automation and Response



FortiTIP

Threat Intelligence for enrichment



AI/Agents

Assist and automate tasks



1 Platform, Zero Tool Sprawl

SIEM, SOAR, TIP, ITDR, and AI in a single cloud offering, eliminates multi-vendor complexity and accelerates time to value



Production-Ready from Day 1

Built-in best practices with preconfigured detection rules, escalation logic, and response playbooks developed from our SOCaaS operators

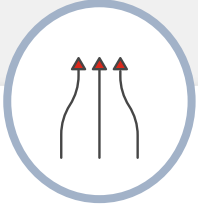


Elastic Delivery

One subscription, streamlined licensing, no hardware to maintain, customers deploy and grow on their terms.

Customer Problem to Fortinet Answer

WHY IT MATTERS



Too many handoffs & Blind spots

Disconnected detection, investigation, and automation workflows create duplicated work, slower decisions, and analyst fatigue



More Threats, More Telemetry, More to Protect, Less time to Respond

Cloud workloads, identity sprawl, and multivendor telemetry generate more signals than manual processes can prioritize, widening the gap attackers exploit.



Solution Fit, Buying Friction

Every organization operates at a different SOC maturity level, requiring adaptable deployment, automation depth, and integration flexibility.

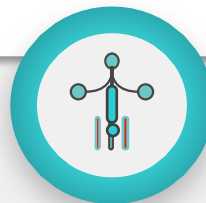
One Connected Platform

FortiSOC unifies analytics, SIEM, SOAR, TIP, and ITDR into one incident and workflow model.



Agentic AI + Automation

FortiAI-Assist helps triage, investigate, hunt, and coordinate response so teams scale action, not just headcount.



Built for Every Stage

Single subscription, unified experience, and faster time to value without giving up a path to broader SOC Platform adoption.



Analytics and detection on one data foundation



One normalized foundation

Every log usable on day one

All telemetry is ingested into one schema at ingest, with no connectors to stitch across query languages



Behavioral analytics & correlation

Find real threats, drop the noise

Cross domain correlation across firewall, endpoint, identity, and cloud surfaces multi stage attacks early



Identity threat detection

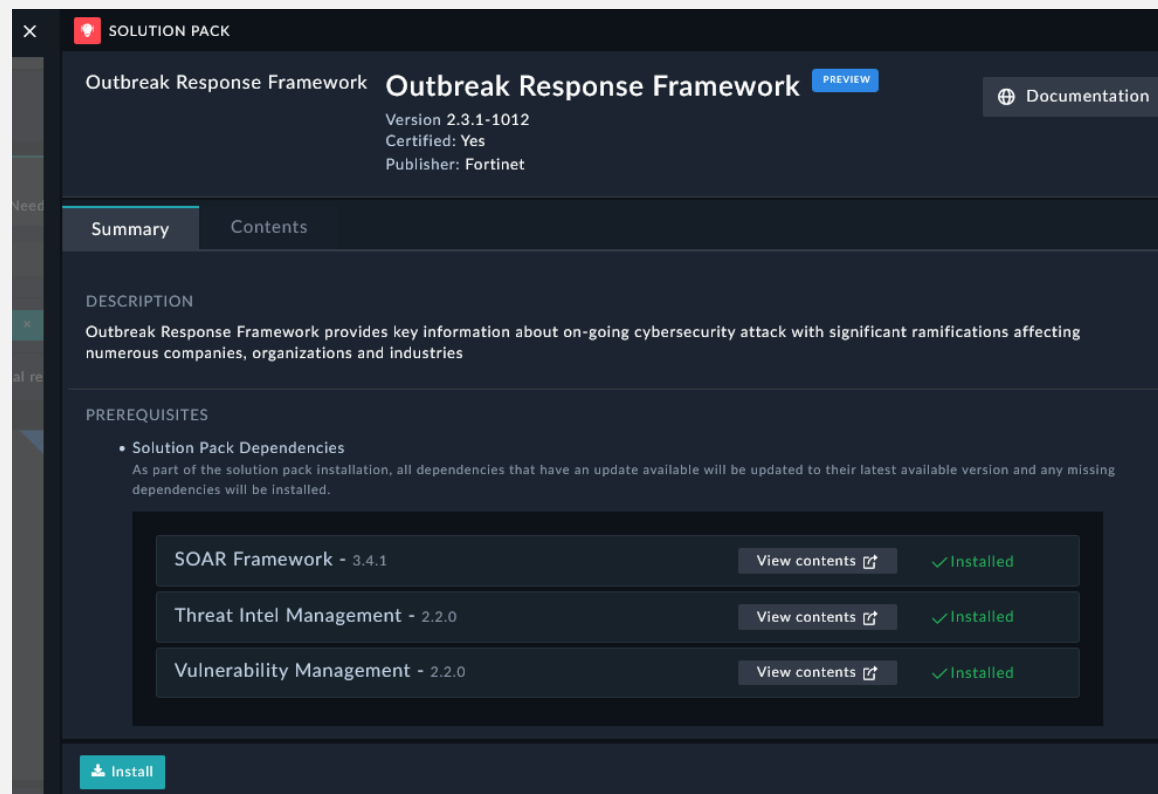
Follow the account, not just the IP

Identity context enriches every alert, so the team sees who and what is involved.



FortiGuard threat intelligence, built in

Native intelligence enriches detection and investigation automatically



Outbreak alerts and detection packs

Timely alerts and ready-made detection content for emerging campaigns



Preconfigured and auto downloaded

Threat content arrives and updates automatically, with nothing for the team to manage



Automatic enrichment

Indicators and context attach to alerts and cases as they form

Incident and SecOps management



Vulnerability and compliance

Stay audit ready

Track exposure and produce reporting aligned to PCI, HIPAA, ISO, and internal controls



Threat intel management

Feeds turned into action

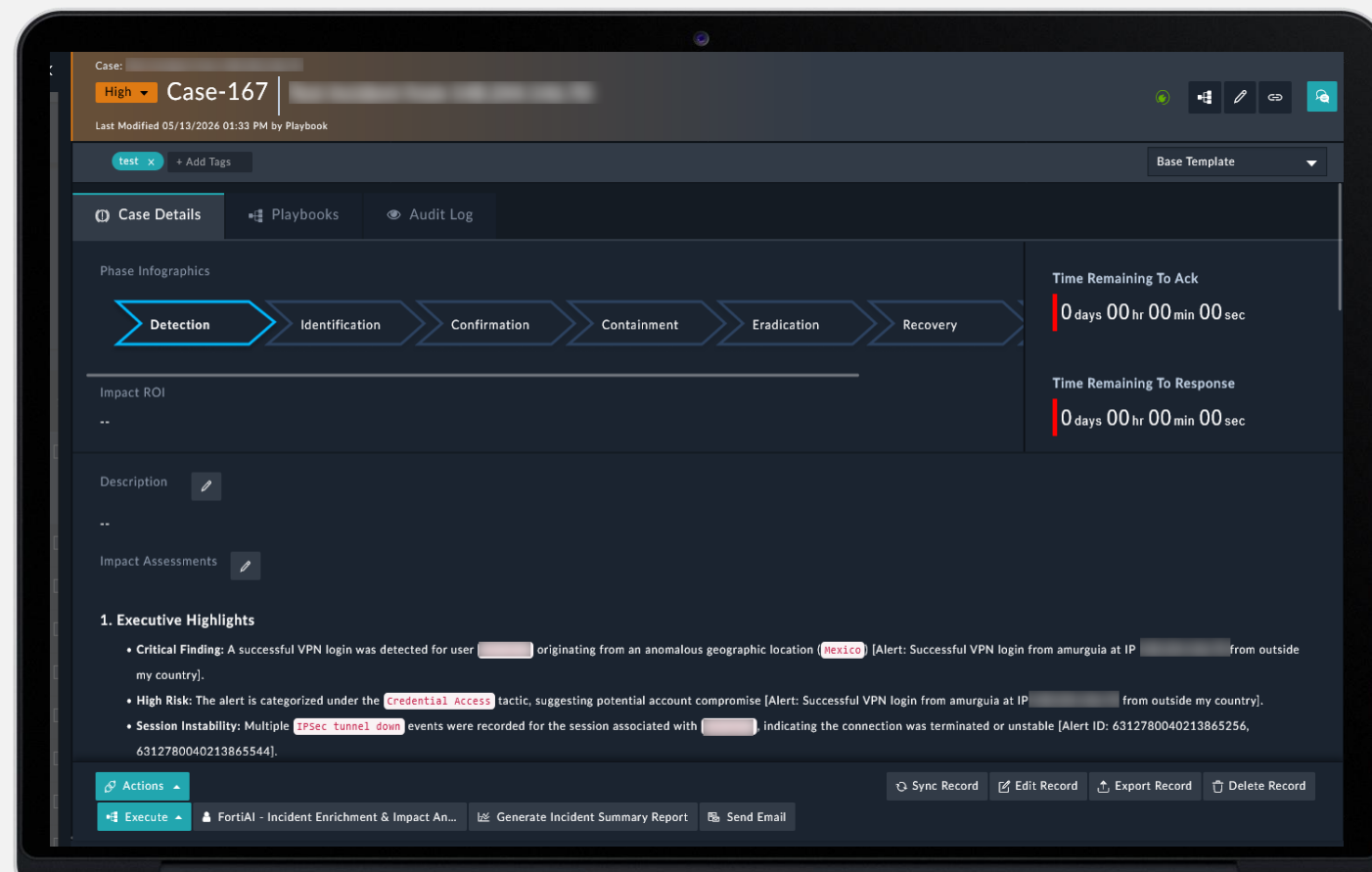
Ingest, validate, score, and operationalize internal and external intelligence into detection



Ops management and more

Run security and IT together

Network, application, service health monitoring, plus SOC metrics and performance tracking



Built-in Content Hub: Connect Everything, Automate Anything



900+ Connectors

Integrate hundreds of tools across Fortinet's Security Fabric and 3rd party vendors



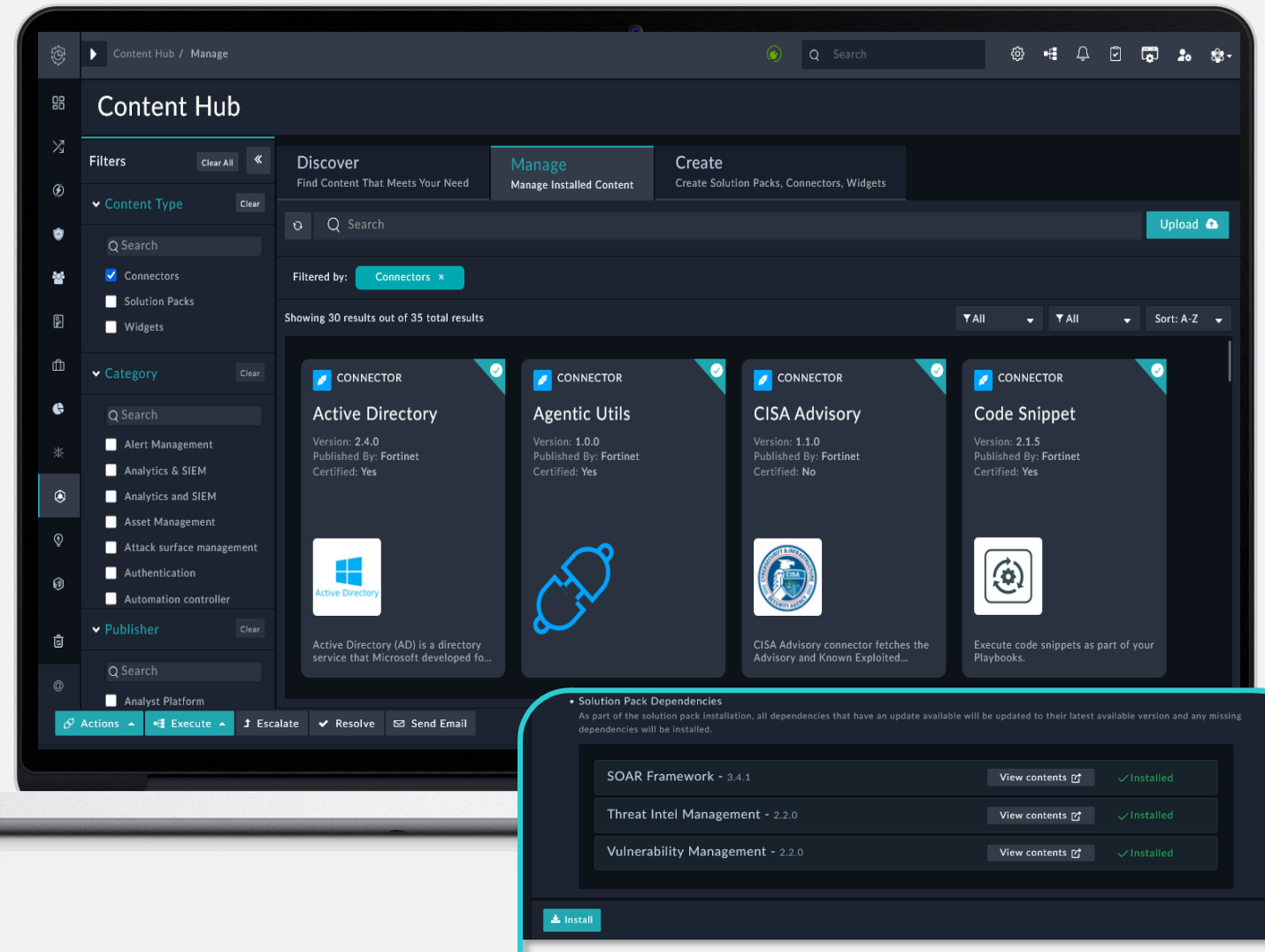
Automation for You

1,000s of preconfigured playbooks, detection, and correlation rules

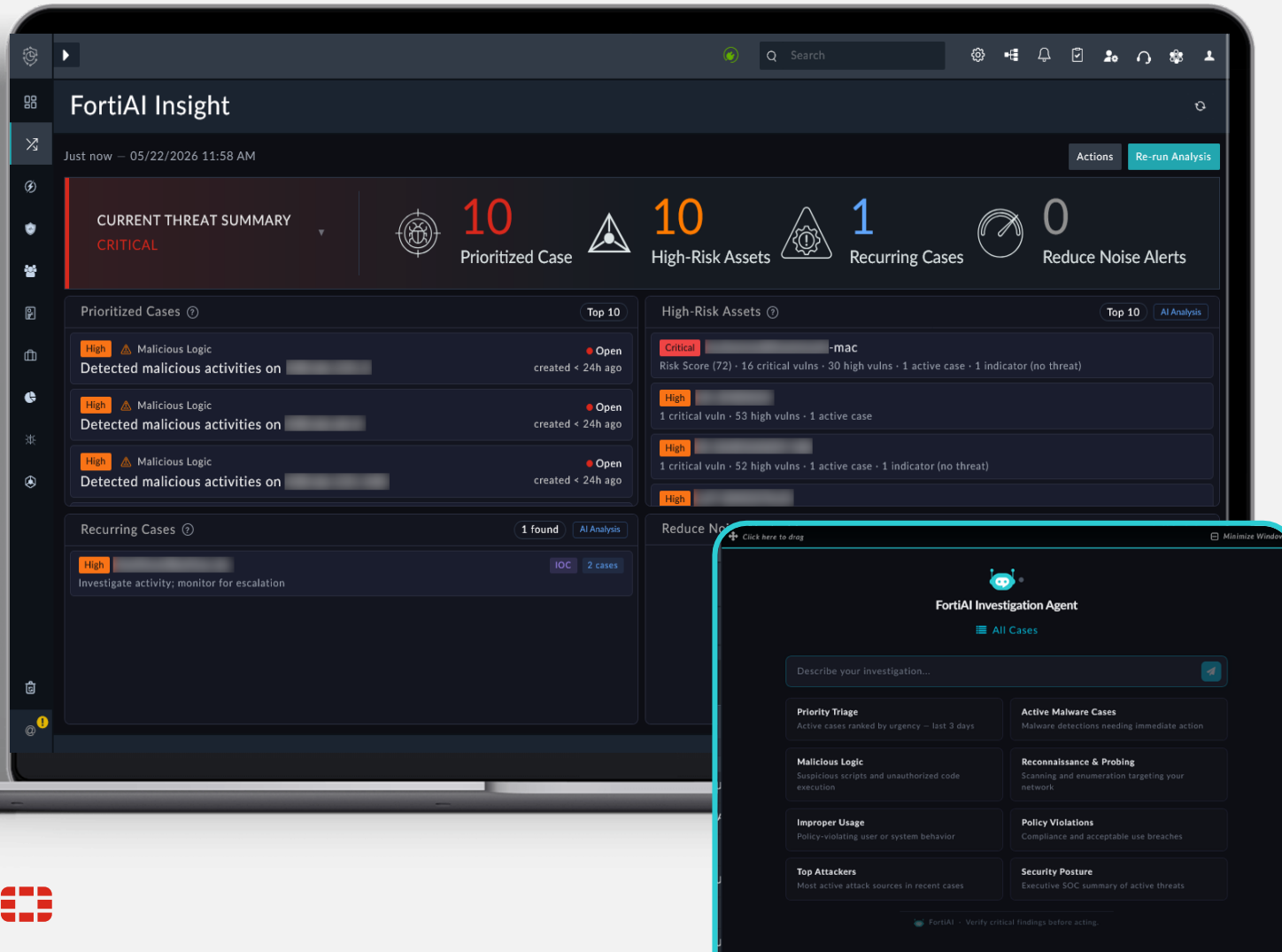


Jumpstart Operations

Built-in best practices with out-of-the-box solution packs developed by our SOCaaS operators



Agentic analysis, investigation, and response embedded across the SOC



Embedded AI

Applies AI directly across alerts, investigations, hunting, cases, and response workflows.



Attack Reasoning

Reasoning agent detects multi-stage coordinated attack campaigns and helps analysts focus on what matters.



Dynamic Response

Chooses the optimal response path dynamically and acts automatically with human oversight where required.



FortiAI: The Intelligence Layer Powering FortiSOC



FortiAI Insight

Start already prioritized

Surfaces prioritized cases, high risk assets, recurring attacks, and suppresses the noise



Investigation Agent

Investigate in plain language

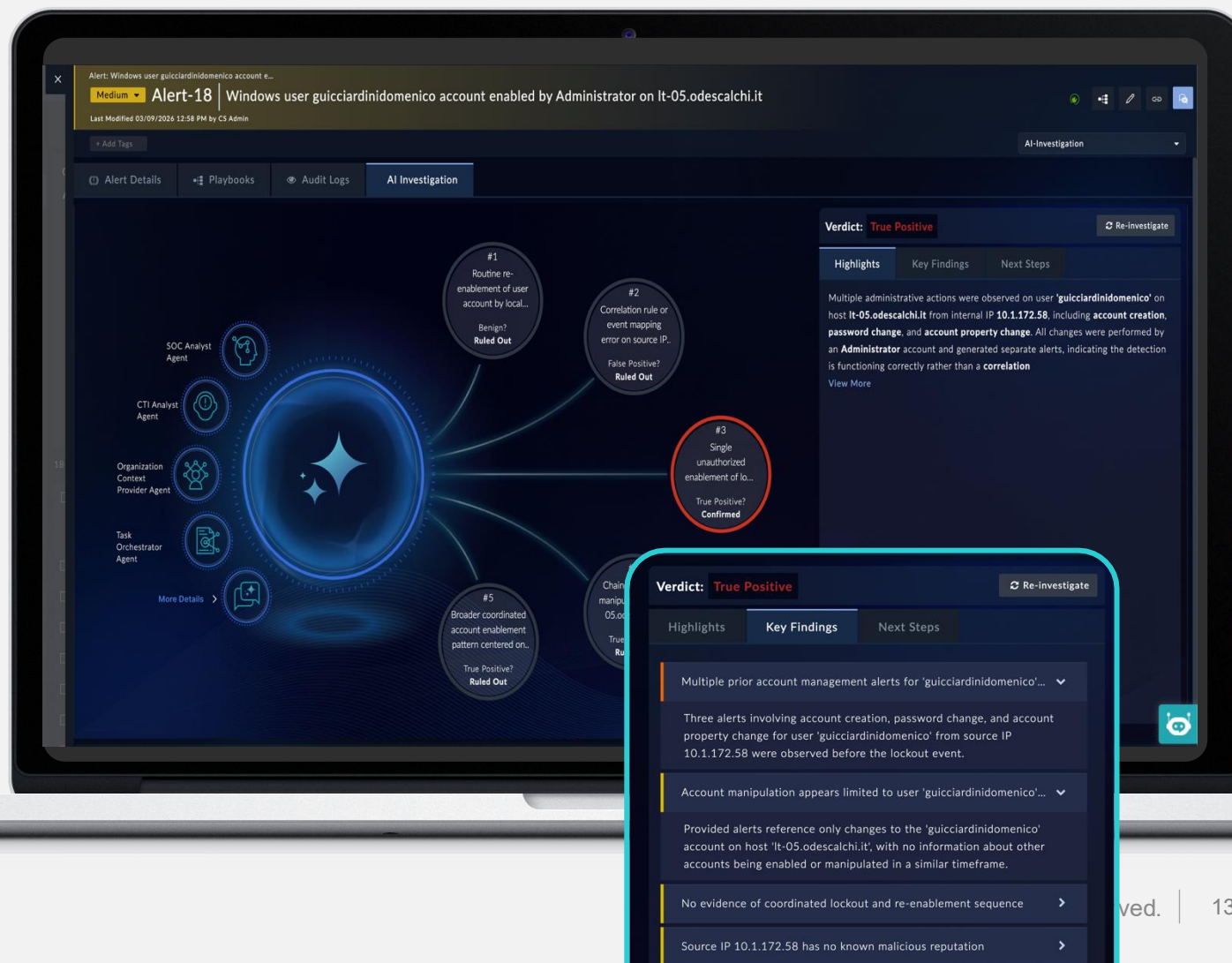
Multi agent analysis builds the timeline, reaches a verdict, and shows the reasoning behind it



Governed by design

Agentic, but in control

Secure proxy, shown reasoning, audit export, and analyst approval before any response action



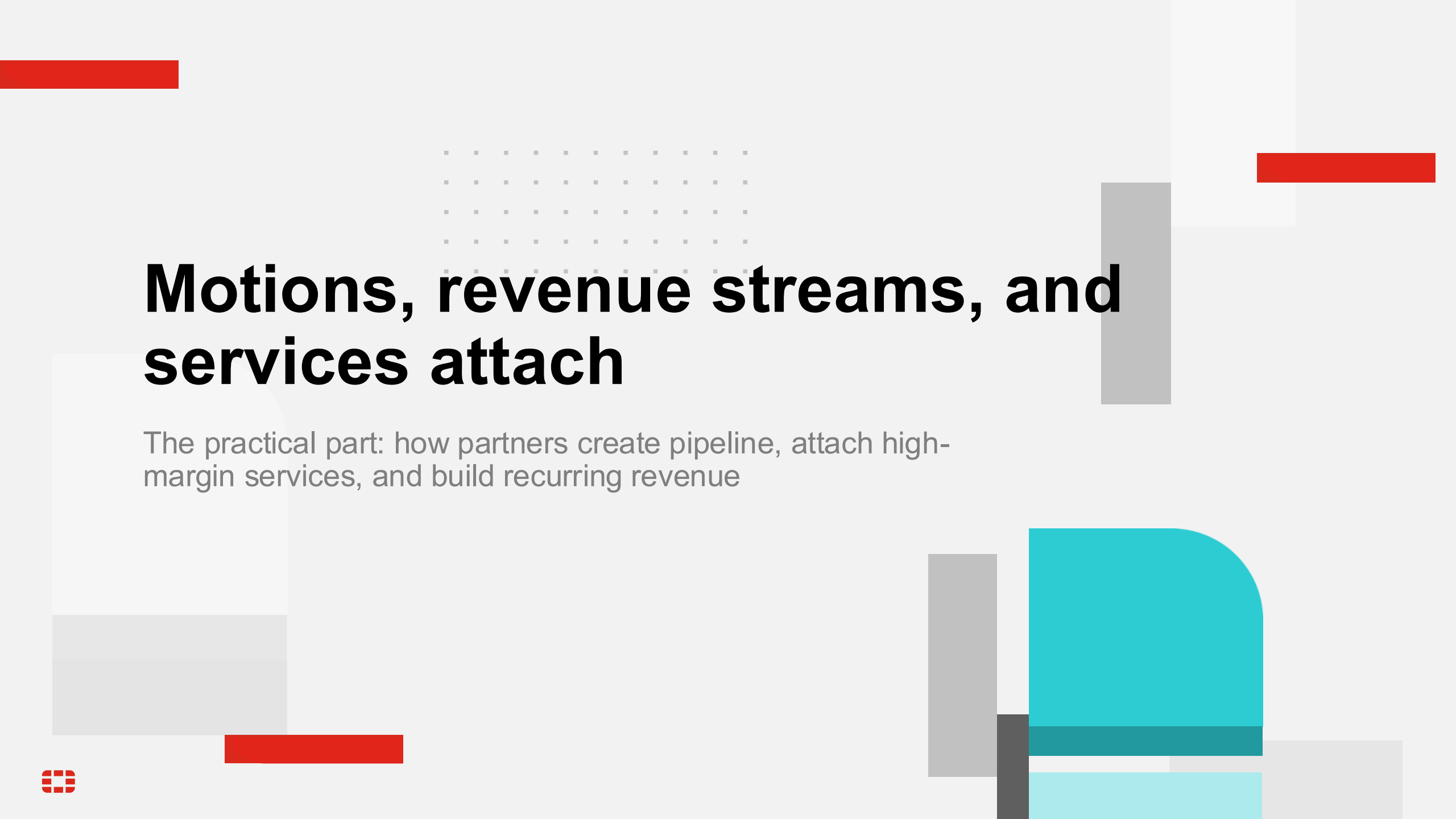
Base and Advanced, serving a broad market

From lean security teams to the advanced enterprise SOC

Capability	Core Capabilities	Advanced Capabilities
SIEM ingestion	Fortinet and curated third party	Full third party ingestion
Analytics	Core SIEM analytics and dashboards	UEBA and advanced analytics
Automation	Playbook editor and default playbooks	Full SOAR orchestration, AI assisted playbooks
Content Hub	Curated packs and connectors	Full access to the library
Threat intelligence	Enrichment and scoring	Enrichment and scoring
Identity threat detection	Not included	ITDR detections and playbooks
FortiAI assistant	Included	Included

Licensed by gigabytes/day. Start on Base for a fast, lean start. Upgrade to Advanced anytime by co term for the same data volume





Motions, revenue streams, and services attach

The practical part: how partners create pipeline, attach high-margin services, and build recurring revenue



What FortiSOC IS and IS NOT

FortiSOC is...

- A unified SaaS platform
- Based on FortiAnalyzer, FortiSIEM, FortiSOAR, technologies
- A new product in the SOC Platform portfolio
- Tiered licensing for Core and Advanced functionality
- Release 1 of a platform that will continue to add new functionality such as EDR and attack surface management.

FortiSOC is NOT...

- Multiple products in a portal
- Appropriate for all SOC customers and their technology needs
- An on-prem or private cloud solution
- A managed services offering
- A replacement for current Analyzer, SIEM, SOAR products
- A displacement for installed FortiAnalyzer



How FortiSOC Fits the Broader SOC Platform Story

Cloud simplicity for customers that want it. Deployment flexibility for customers that need it.

MATURITY FRAMEWORK

Turnkey / Core SOC

Fast start for lean or resource-constrained teams that need analytics, visibility, and built-in automation.

Advanced SOC

Broader correlation, deeper visibility, stronger orchestration, and higher-scale operations.

Managed SOC

Optional FortiGuard SOCaaS augmentation for after-hours coverage, offload, or co-managed operations.

FortiSOC

- SaaS-only cloud operating model
- Unified experience and single subscription
- Best for large deals prioritizing faster adoption and lower operational complexity
- Base and Advanced tiers map cleanly to maturity stages

Broader Platform

- FortiAnalyzer, FortiSIEM, FortiSOAR, SOCaaS
- Customer wants an on-prem SOC solution
- Incremental expansion of existing deployments
- Best for customers needing maximum deployment control or highly customized architectures
- Customers can coexist with, complement, or migrate into FortiSOC over time

FortiSOC follows **the same maturity framework** Fortinet SOC Platforms portfolio already provides. The difference is the operating model: FortiSOC delivers those capabilities through a unified cloud experience, while the broader portfolio continues to support on-premises, hybrid, and highly customized deployment needs.



Why FortiSOC is a partner opportunity

With FortiSOC partners earn margin, services, and annuity



Create pipeline

Consolidation and SIEM-modernization budgets are active now. Lead with the problem and you control the deal



Attach services

Assessments, migrations, onboarding, content, and tuning, high-margin services on every deal



Build annuity

Managed and co-managed operations turn one-time projects into recurring, defensible revenue

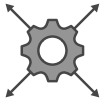
Every FortiSOC opportunity can carry product, services, and a managed annuity. The deals are larger, stickier, and more profitable than a point-product resale and they pull the rest of the Fabric with them

Channel: Who to Sell through

Partners need a clearer role than “resell the SKU”

Global / regional resellers

Use FortiSOC when customers want a cloud-first SOC platform with a simpler buying motion. Lead with faster adoption, lower operational complexity, and clear attach services.



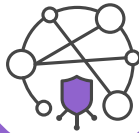
Service providers / MSPs

Use FortiSOC for customers that want managed or co-managed outcomes, especially when partners can attach onboarding, tuning, policy optimization, and operational support.



MSSPs

Position FortiSOC as a future-ready unified cloud SOC offer for provider-led use cases. *Dedicated MSSP capabilities are expected later; use a roadmap caveat where appropriate.



Fortinet install base

Target FortiGate, FortiAnalyzer, FortiSIEM, and SOCaaS-adjacent accounts that already trust Fortinet and are ready to simplify their SecOps operating model.



Onboarding, integration, data onboarding, content tuning, playbook customization, operational optimization, managed outcomes, and ongoing advisory services

Ideal customer profiles

Five profiles where FortiSOC wins, and the expansion behind each



Fortinet-centric
Already runs FortiGate
/ FortiAnalyzer /
FortiEDR

**Expand the
Fabric they own**



SIEM modernization
Legacy or costly SIEM
up for renewal

**Migration + cost
takeout**



Tool sprawl
Many point tools,
fragmented consoles

**Consolidation
play**



Wants simplicity
Lean team; wants
outcomes, not a
project

**Base tier + co-
managed**



Managed-ready
No 24x7 coverage;
alert fatigue

**Your MDR /
SOCaaS**

Buying triggers & pain points to listen for

When you hear these, the budget conversation is open, move to a discovery meeting

Event triggers

- SIEM / SOAR renewal approaching
- New CISO or security leader
- Recent breach or audit finding
- Merger, acquisition, or divestiture
- Cloud or compliance mandate

Pain signals

- Alert fatigue and false positives
- No 24x7 coverage or staffing gap
- Too many consoles; manual stitching
- Slow detection and response times
- Rising SIEM ingestion / license cost

Expansion openings

- FortiAnalyzer already deployed
- Fabric components without a SOC
- POV success ready to productionize
- Customer asking 'can you monitor it for me?'
- New use cases (OT, identity, cloud)

Discovery questions that qualify the opportunity

Ask across all three levels the answers tell you the motion, the use case, and the services to attach.

Executive

- What's the business cost of slow detection or a missed incident ?
- Is there board or compliance pressure on security operations ?
- What does your current SOC cost to operate, all-in ?
- Any M&A, audit findings, or cloud mandates in play ?

Technical

- What SIEM, SOAR, and EDR do you run today, and when do they renew?
- What are your data sources and daily ingestion volume?
- Who owns detection content and automation today?
- What are your cloud and data-residency requirements?

Operational

- How big is the team, and do you have 24x7 coverage?
- What are your MTTD and MTTR today?
- How many alerts per day, and what's the false-positive rate?
- Where does your team spend the most manual effort?

Objections & responses

The objections you'll hear — and the reframes that keep the deal moving.

“We already have a SIEM”

→ Great, when does it renew, and what does it cost to operate? Lead with modernization and a cost-takeout assessment; FortiAnalyzer can forward in, so it's a phased path, not a rip-and-replace

Isn't this just FortiAnalyzer rebranded?”

→ No. FortiSOC unifies analytics, SOAR, UEBA, threat intel, and FortiAI in one cloud console. FortiAnalyzer is one input to it — and a perfect on-ramp

“AI in the SOC feels risky”

→ FortiAI is governed: requests route through a secure proxy, every answer shows its reasoning and exports for audit, and any response action requires analyst approval

We're a Microsoft / CrowdStrike shop”

→ FortiSOC complements them — it ingests their data and adds cross-vendor visibility and predictable cost. You sell on top of what they own

We don't have the team to run it”

→ Then don't make them, co-managed or fully managed is the model. This is exactly where your managed practice or SOCaaS comes in

“Budget and timing are tight”

→ Start with a fixed-fee assessment and consumption-based licensing. Phase the rollout; prove value on a slice of data first

FORTINET®