
XPERTS26

XPERTS26

Cacería de Amenazas en la Nube

Una sola Plataforma para proteger las aplicaciones

Disclaimer

Fortinet Confidential

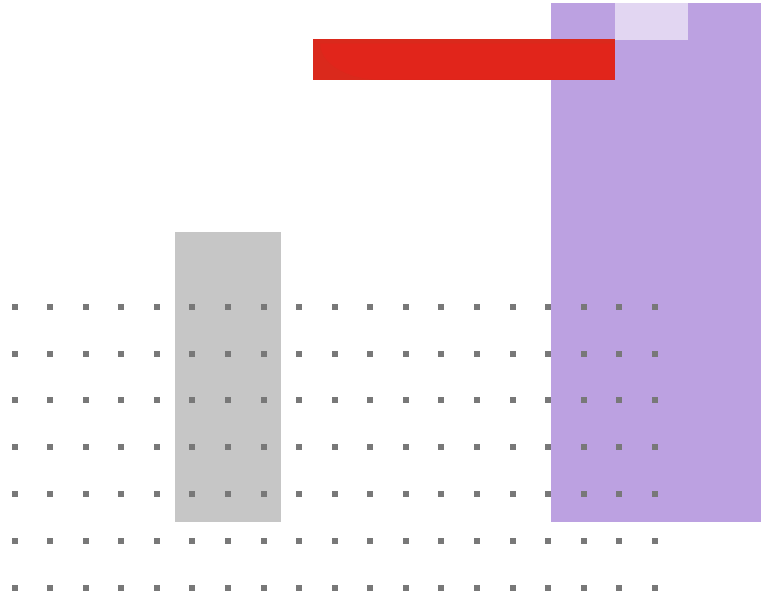
This document contains confidential material proprietary to Fortinet, Inc.

This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside Fortinet, Inc. without prior written consent of Fortinet, Inc.

This information is pre-release and forward looking and therefore is subject to change without notice.

The purpose of this document is to provide a statement of the current direction of Fortinet's product strategy and product marketing efforts.

Please note that this Product Roadmap is neither intended to bind Fortinet to any particular course of product marketing and development nor to constitute a part of the license agreement or any contractual agreement with Fortinet or its subsidiaries or affiliates.



Carlos Montes

Systems Engineer

David Zambonino

Cloud Subject Matter Expert - LATAM

AGENDA

Three acts. One investigation.

01

ACT I · THE CASE

Why detection got harder.
What AI changed.
What it costs when you miss.

02

ACT II · THE KIT

FortiAnalyzer as your workbench.
FortiGuard as your intel.
FortiAI as your co-investigator.

03

ACT III · THE HANDOFF

One breach.
Fifteen days.
Four hunts. Your turn.

45 minutes of briefing. 3h 15m of hunting.

01 / ACT I

The Case

Why this. Why now.

Your customers' attackers already use AI.

Phishing at LLM speed

Grammatical, personalized, native-language lures.
No more typos.

Autonomous agents

Multi-step recon, exploit chaining, session hijack — without a human in the loop.

Crime-as-a-service LLMs

WormGPT. FraudGPT.
Rented by the hour.
No jailbreak required.

Attackers operate in minutes. Defenders still think in days.

REALITY TWO · THE DEFENDER SIDE

Attacks accelerate. Analysts don't scale.

Evolving Threat Landscape

Attackers now move faster than human analysts can investigate.

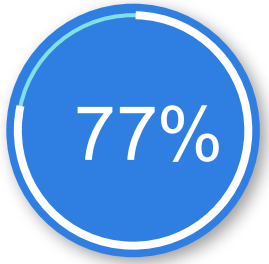
Expanding Attack and Risk Surfaces

External Threats

25+

New exploitable paths per week across cloud, OT, identities, and remote endpoints.

Insider Risks



Percent of organizations that experienced 1 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.

More surface. More tools. Fewer people. Same 24 hours.

THE DWELL-TIME ANCHOR

You have four days to disclose. You take twenty-one to find it.

- Average time from detection to remediation

Time to Detect Time to Contain Time to Investigate Time to Remediate

52%

of organizations report SecOps is harder than 2 years ago[1]

SEC Rule

4 Days

to disclose material cybersecurity incident

$9.4M

Avg Breach Cost

Source: Enterprise Strategy Group, 1. ESG Research, SOC Modernization Survey, January 2025.

The silent epidemic.

Your compute. Their wallet. And it's rarely just about the coins.

CRYPTOMINING

Legitimate. Disclosed. Consensual.

Opt-in compute solving cryptographic puzzles for a block reward. Bitcoin, Monero, Ethereum Classic. A business model — not a breach.

CRYPTOJACKING · malicious cryptomining

Malicious. Silent. Unconsented.

Malware-dropped or browser-injected mining that runs on your hardware without consent. Same coin. Stolen compute.

+20%

Cloud cryptojacking incidents, YoY

Sysdig 2025

+450%

Cryptojacking activity vs prior year

IBM X-Force

500

New mining instances every 20 sec

Sysdig

17K+

Exposed Open WebUI hosts at risk

Sysdig

The miner is rarely the whole story. It's the canary.

Same foothold → ransomware. data theft. access sold to the next buyer.

Sources: FortiGuard Labs · Sysdig 2025 Cloud-Native Security Report · IBM X-Force · Wiz Threat Research.

THE AI ON BOTH SIDES

Fortinet has been doing AI since 2005. This year it learned to talk.

Since 2005	6th gen	500+	15+ yrs	3.1T
FORTIGUARD LABS	ML ENGINE	AI PATENTS	IN PRODUCTION	ATTEMPTS BLOCKED · 2024

MACHINE LEARNING

Detects patterns at scale

- FortiGuard Labs
- FortiNDR
- FortiWeb
- FortiAppSec
- FortiSandbox
- FortiCNAPP runtime

Learns from 496M+ sources. Flags what doesn't fit.

GENERATIVE AI

Answers in plain English

- FortiAI-Assist (FortiAnalyzer/ FortiGate)
- FortiCNAPP AI Assist
- FortiAI in FortiGate / FortiOS

Summarizes incidents. Drafts hunts. Writes business impact.

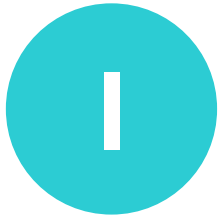
"ML detects the pattern. GenAI explains it. Today you'll use both."

02 / ACT II

The Kit

Your workbench. Your intel. Your co-investigator.

FortiAnalyzer. Your case room.



Ingest

Every log. Every source. One table.

Hunt

Saved queries. Pivoted investigations. Ad-hoc.

Correlate

Event handlers. IOC feeds. Cross-source.

Respond

Playbooks. Connectors. Automated actions.

Explain

FortiAI-Assist. Incidents in plain English.

One pane. Five verbs. Every hunt you'll run today lives here.

EXPANSION PATHS

Start here. Grow into here.

One platform. Three upsell motions. Zero rip-and-replace.

START HERE

FortiAnalyzer

one data lake · one schema · every hunt.

INCLUDED IN FORTIANALYZER · NO SEPARATE LICENSES

Unified Data Lake	Logging & Reporting	Incident Management
XDR · built-in	*SIEM · built-in*	*SOAR · built-in*

GROW INTO

FortiTIP

Threat Intelligence Platform

Curated feeds.

stix/taxii · virustotal

FortiSIEM

Enterprise SIEM

Compliance-grade.

multi-tenant · nist 800-53

FortiSOAR

Full Orchestration

Playbooks & cases.

itsm · complex playbooks

FortiSOC

Unified Cloud SOC

SIEM + SOAR in one.

ueba · tip · itdr · case mgmt

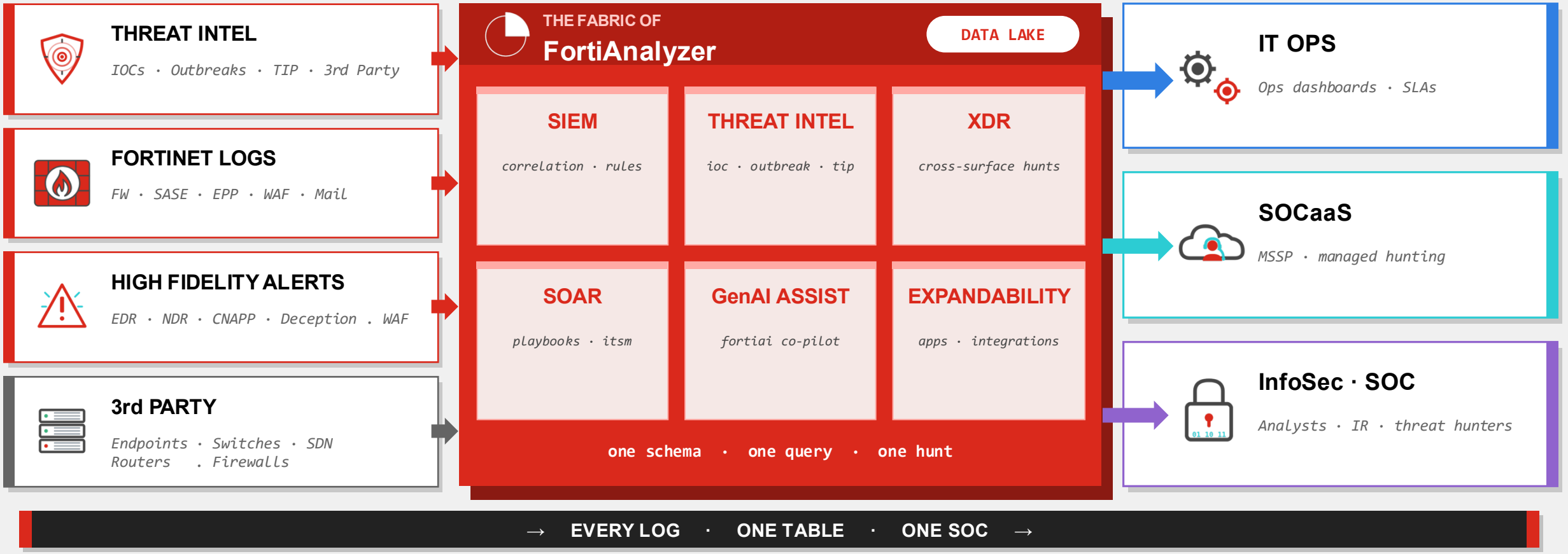
BETA · AVAILABLE TODAY

Same data lake. Same schema. Three directions to scale.

THE FABRIC OF FORTIANALYZER

Every log. One table. One SOC.

Fortinet logs, third-party telemetry, high-fidelity alerts and threat intel — one fabric, three audiences.



Remember the 50+ tool sprawl? This is the answer.

THE INTEL LAYER

Intel that ships with the box — and intel the box keeps learning.

FortiGuard Labs

Built-in. Always on.

- Built-in signatures
- IOC feeds
- MITRE ATT&CK mappings
- Updated continuously

Outbreak Alerts

Real-time bulletins.

- Active campaigns surfaced
- Ransomware variants
- New exploit kits
- Pushed into FortiAnalyzer

FortiTIP

Decision support.

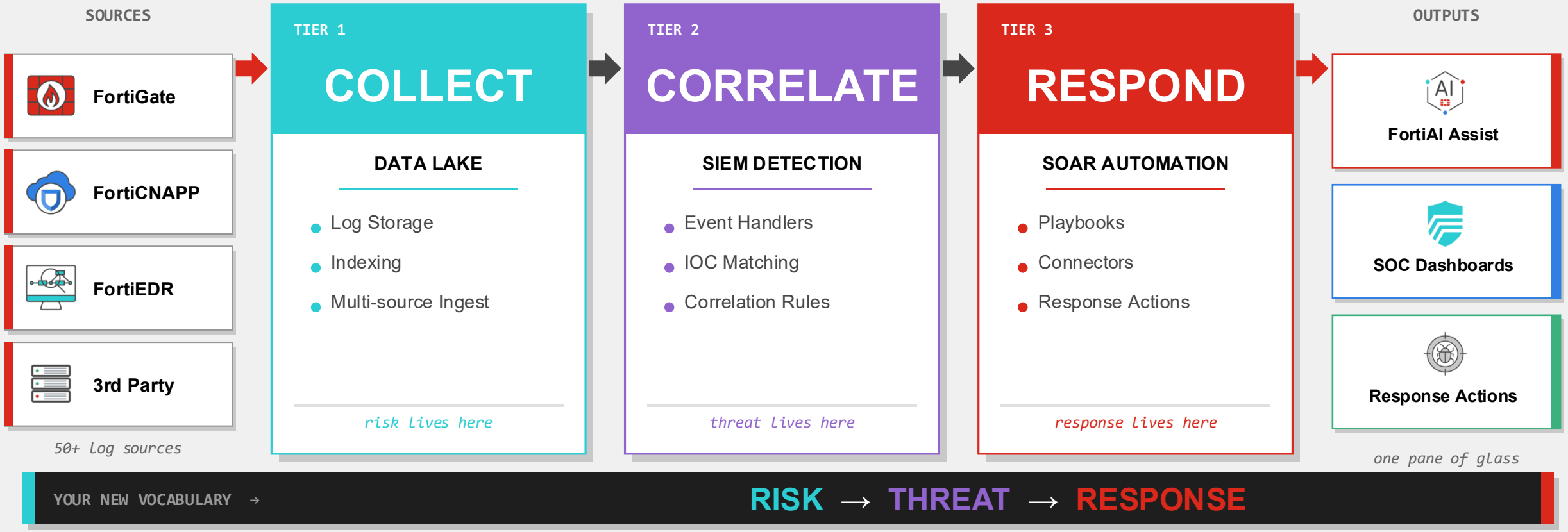
- Aggregates FortiGuard
- STIX / TAXII ingestion
- VirusTotal integration
- Third-party CTI

The data lake has context before you ask your first question.

THE ARCHITECTURE

Collect. Correlate. Respond.

Three verbs. One FortiAnalyzer. AI across every stage of the pipeline.



02B / SUB-ACT

The CNAPP Umbrella

One platform. Three pillars. You hunt through one.

THE CNAPP UMBRELLA

One platform. Three pillars. You hunt through runtime.

FortiCNAPP unifies CWPP · CSPM · CDR. Today's lab runs on the runtime pillar.

FortiCNAPP

Cloud-Native Application Protection Platform

CWPP | CSPM | CDR

CWPP

ACTIVE

Cloud Workload Protection

RUNTIME — inside the workload

- Processes
- Network activity
- File writes
- Identity behavior

FortiCNAPP · runtime module

ON in your lab. Every flag is runtime evidence.

CSPM

CONTEXT

Cloud Security Posture

POSTURE — what's configured wrong

- Misconfigurations
- Policy drift
- Compliance gaps
- IAM role posture

FortiCNAPP · posture module

Off in lab. In the picture for customer talks.

CDR

CONTEXT

Cloud Detection & Response

DETECT — attacks in motion

- Anomalous API calls
- Credential / session theft
- Privilege escalation
- Lateral movement

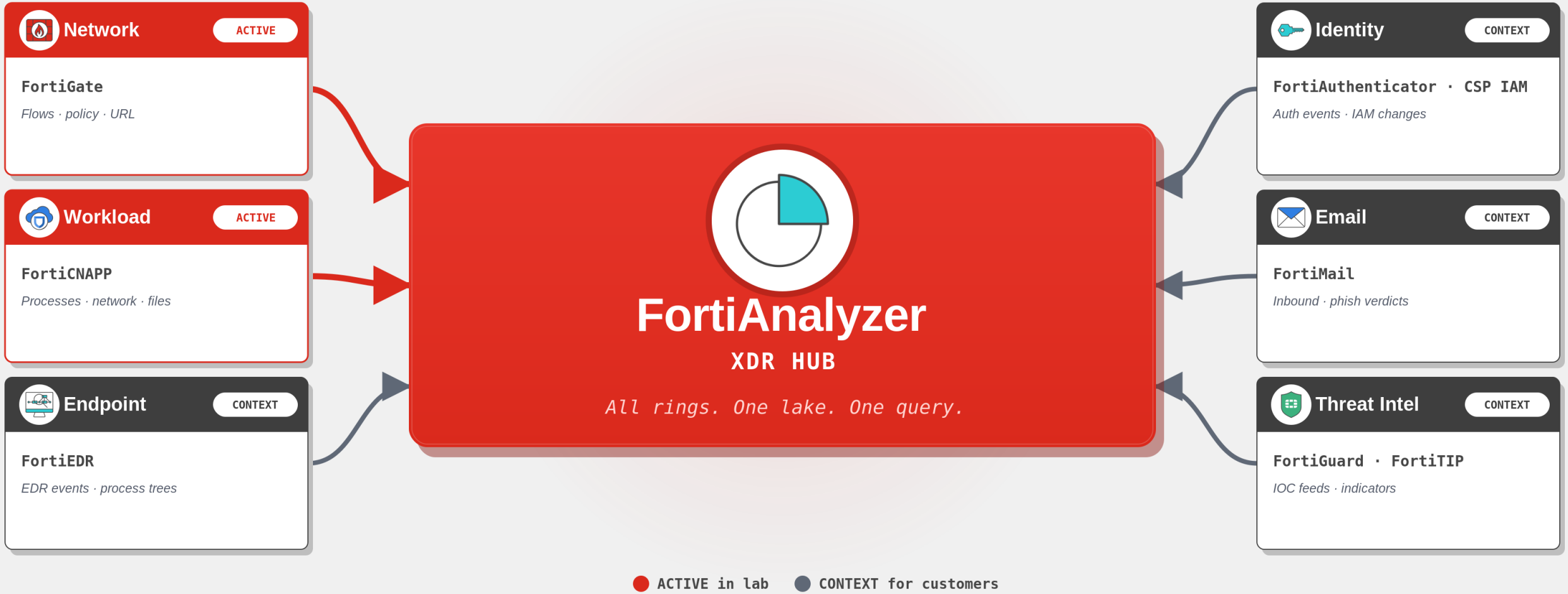
FortiCNAPP · CDR module

Off in lab. In the picture for customer talks.

CNAPP = CWPP + CSPM + CDR (+ CIEM). One FortiCNAPP. Today → runtime.

FortiAnalyzer IS the hub.

Six rings → one correlation. XDR is the outcome.

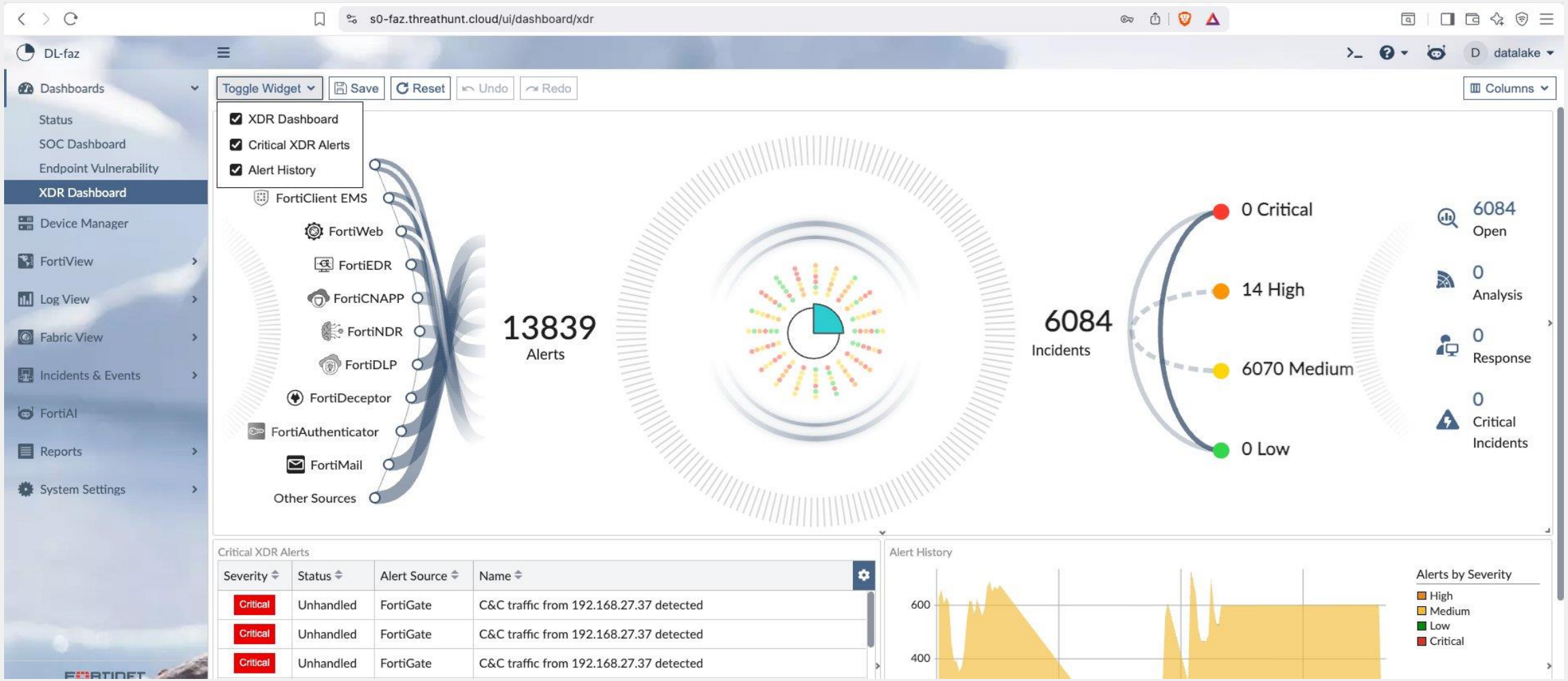


XDR is not a separate product. It's what FortiAnalyzer does when the sources line up.

FortiAnalyzer IS the hub.

Six rings → one correlation. XDR is the outcome.

XDR is not a separate product. It's what FortiAnalyzer does when the sources line up.



The analyst at your side.

INTELLIGENT TRIAGE · INSTANT CONTAINMENT · AUTONOMOUS RESPONSE

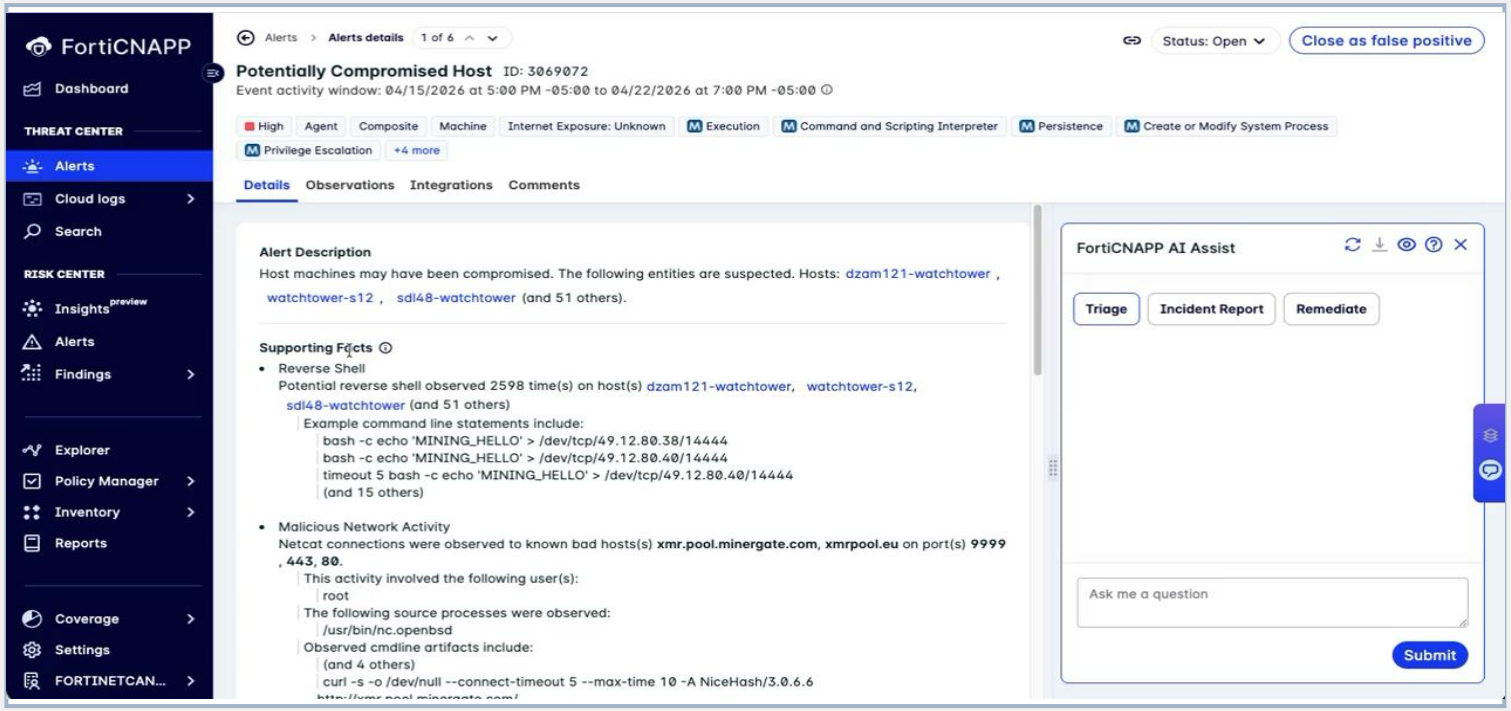
YOU ASK

FortiAnalyzer FortiAI

"can you triage incident IN00000004"

6 words. lowercase.

FORTIAI ANSWERS



Also in the lab — FortiCNAPP AI Assist triages runtime alerts on the host itself. Two assistants, same hunt.

One question. Ten million events. Fifteen seconds.

The analyst at your side.

INTELLIGENT TRIAGE · INSTANT CONTAINMENT · AUTONOMOUS RESPONSE

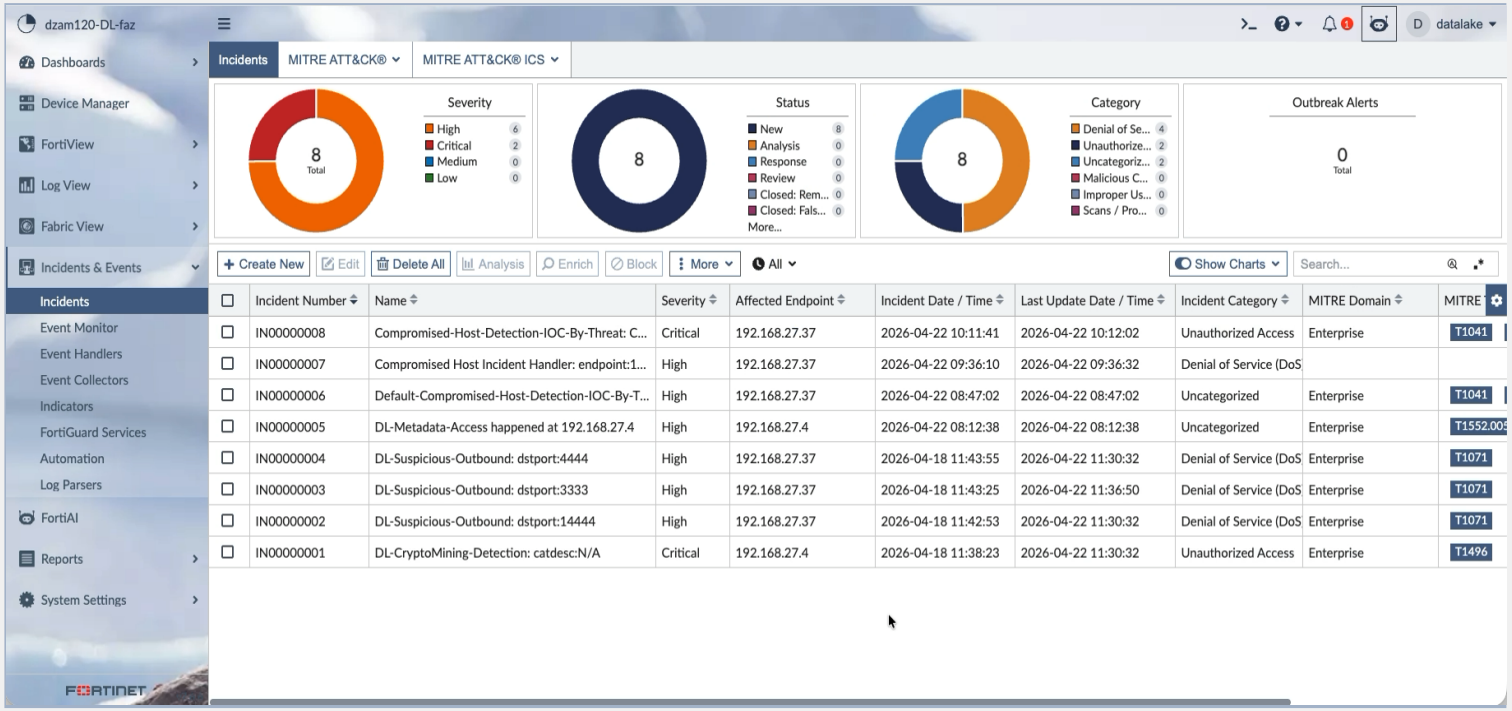
YOU ASK

FortiAnalyzer FortiAI

"can you triage incident IN00000004"

6 words. lowercase.

FORTIAI ANSWERS



Also in the lab — FortiCNAPP AI Assist triages runtime alerts on the host itself. Two assistants, same hunt.

One question. Ten million events. Fifteen seconds.

What a cryptojacker looks like to a hunter.

Three signals. One process. Five MITRE techniques in the chain.

COMPUTE

CPU pinned. Unusual child of a web user.

`process=xmrig · uid=www-data · path=/tmp/.cache/`

NETWORK

Stratum protocol. 5-minute beacon cadence.

`tcp/14444 · dns=pool[.]hashvault[.]pro · TLS-SNI mismatch`

PERSISTENCE

Survives reboot. Lives in two places.

`cron @reboot · systemd --user unit · IMDS-harvested keys`

MITRE ATT&CK CHAIN

T1496	Resource Hijacking
T1071.001	App Layer · Web
T1053.003	Scheduled Task · Cron
T1552.005	Unsecured Creds · Cloud IMDS
T1098	Account Manipulation

```
$ crontab -l
@reboot /tmp/.cache/xmrig --url=49.12.80.38:14444 --pass=x --cpu-max-threads-hint=60 --donate-level=0 -B
```

Five TTPs. One process. Three hours to catch them all.

What you learn here maps to real customer scenarios.

Match the scenario · pick the tier · lead with the right qualifier.

Customer scenario	FortiAnalyzer tier	FortiAI-Assist role	Primary qualifier to ask
Lean team · single-site · needs visibility	FAZ 400F / 1000F · or FAZ-VM	Incident summarization	*"Who reads the alerts today — one person or a rotation?"*
Mid-market · hybrid · compliance-driven	FAZ 3000F / FAZ-VM + FortiTIP	Triage + threat intel pivot	*"Which regulators or frameworks are you audited against?"*
Enterprise · multi-tenant · mature SOC	FAZ 3700F / FAZ-VM + FortiSIEM	Full triad (Triage · Containment · Response)	*"How many business units share the SOC, and do they keep data separate?"*
MSP / MSSP · multi-customer	FAZ-VM clusters	Per-tenant summarization	*"How do you partition tenant data and report per-customer?"*
Cloud-first · workload-heavy · shared-responsibility	FortiCNAPP + FAZ-VM	CWPP AI Assist + FortiAI-Assist	*"Do your runtime workloads outnumber your on-prem assets?"*

Fortinet's Security Operations architecture FortiAnalyzer Ordering Guide FortiCNAPP Ordering Guide FortiSOC Ordering Guide

Five scenarios · five qualifiers · one lab that earns you the right to ask them.

Six questions that qualify the deal before you quote it.

Ask these in order. Every answer narrows the tier.

VOLUME

01

How many Fortinet and non-Fortinet log sources feed your SOC today?

Maps to FAZ model family and ADOM count.

02

What retention window do you need — and for which data classes?

Drives storage sizing and archive strategy.

TEAM

03

Who investigates alerts — a dedicated SOC, a rotation, or an MSSP?

Decides FortiAI-Assist story: summarization vs. full triad.

04

How are you measured — MTTD, MTTR, dwell time, or audit posture?

Anchors the ROI slide in numbers they already track.

SCOPE

05

Do you need multi-tenancy, per-ADOM isolation, or per-customer reporting?

Enterprise · MSSP · regulated BU split.

06

Where do your runtime workloads live — on-prem, cloud, or both?

Pulls FortiCNAPP into the story when cloud-heavy.

FORTINET FIT GUIDE

FAZ 400F / 1000F · or FAZ-VM

Single-site SOC. Starter analytics. AI-Assist = summarization.

FAZ 3000F / 3700F / FAZ-VM + FortiTIP

Hybrid. Compliance-driven. Full AI-Assist triad + threat intel.

FAZ-VM + FortiCNAPP

Cloud-first. Per-tenant. CWPP AI Assist on the workload.

Lead with the qualifier. Let the tier follow.

Six questions. Three tiers. Zero guesswork on the first call.

PRESALES · DEAL VELOCITY

Three phases. One proof. Four resources.

1 DISCOVER

~1 WEEK

Qualifier calls. Telemetry audit. Tier recommendation.

2 PROVE

~2 WEEKS

FAZ-VM trial. Ingest their logs. Run two hunts live.

3 DEPLOY

~2–4 WEEKS

HW / VM procurement. ADOM setup. Day-1 rulepack.

15 days → 3h 15m

THE POV NUMBER

What today's lab proved.

The same compression is the POV story: your prospect's dwell time, halved or better.

DOCS

FortiAnalyzer Admin Guide

Deployment, ADOMs, report packs, sizing reference.

docs.fortinet.com

COMMUNITY

Threat Hunting Forum

Peer hunts, query recipes, FortiAI prompt patterns.

community.fortinet.com

OUTBREAK

FortiGuard Outbreak Alerts

Live IOC feeds tied to active campaigns.

fortiguard.com/outbreak-alert

PARTNER

Fortinet Partner Portal

NFR licenses, POV kits, deal registration.

partnerportal.fortinet.com

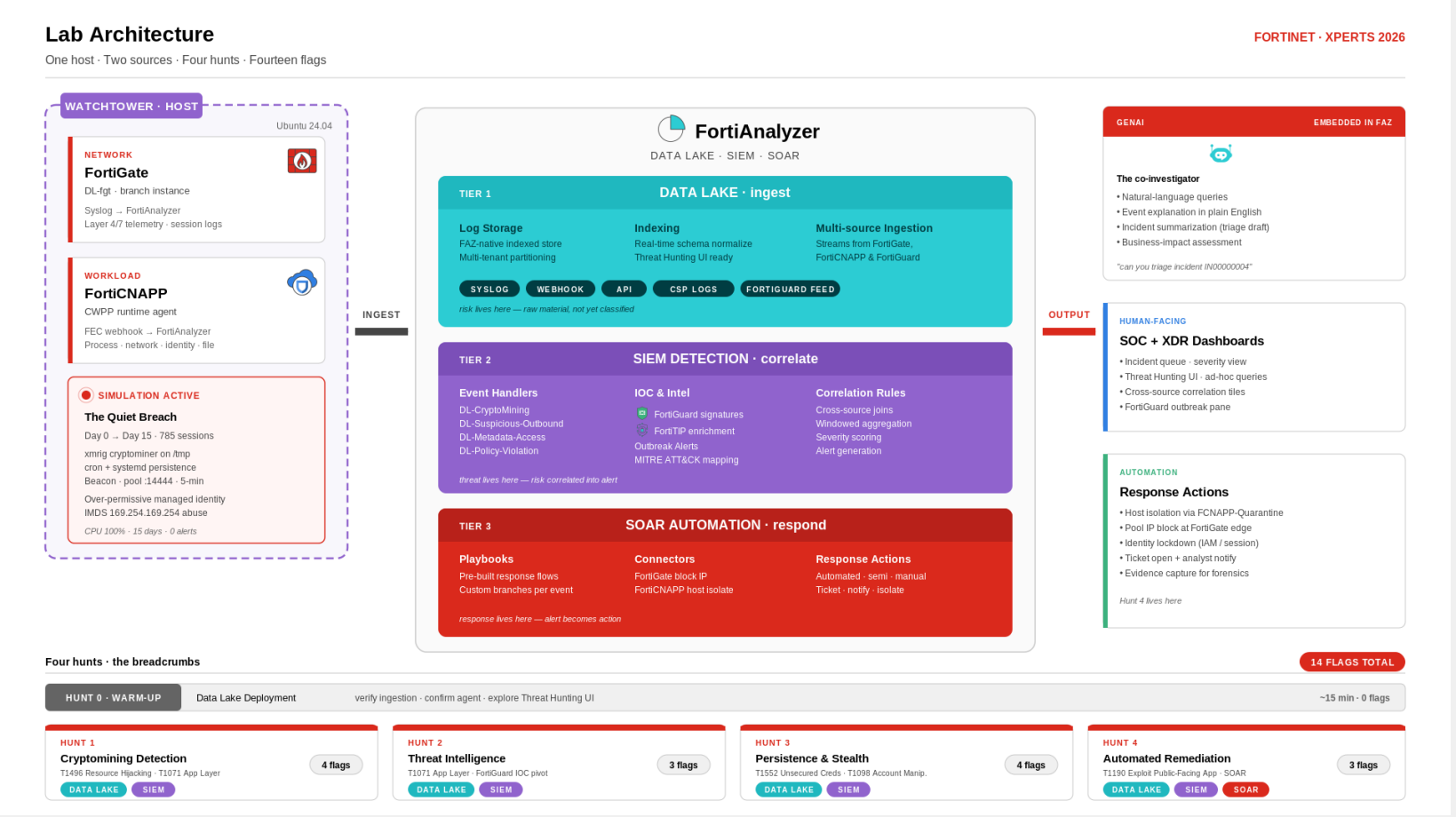
Discover · prove · deploy. Every tile above is a door you can open tomorrow.

03 / ACT III

The Handoff

Fifteen days. Three hours and fifteen minutes.

This is where you'll hunt.



One host. Two sources. Four hunts. Fourteen flags.

Lab Architecture

One host · Two sources · Four hunts · Fourteen flags

FORTINET · XPERTS 2026

WATCHTOWER · HOST

Ubuntu 24.04

NETWORK

FortiGate

DL-fgt · branch instance

Syslog → FortiAnalyzer
Layer 4/7 telemetry · session logs

WORKLOAD

FortiCNAPP

CWPP runtime agent

FEC webhook → FortiAnalyzer
Process · network · identity · file

SIMULATION ACTIVE

The Quiet Breach

Day 0 → Day 15 · 785 sessions

xmrig cryptominer on /tmp
cron + systemd persistence
Beacon · pool :14444 · 5-min

Over-permissive managed identity
IMDS 169.254.169.254 abuse

CPU 100% · 15 days · 0 alerts

INGEST

FortiAnalyzer

DATA LAKE · SIEM · SOAR

TIER 1 — DATA LAKE · ingest

Log Storage
FAZ-native indexed store
Multi-tenant partitioning

Indexing
Real-time schema normalize
Threat Hunting UI ready

Multi-source Ingestion
Streams from FortiGate,
FortiCNAPP & FortiGuard

SYSLOG · WEBHOOK · API · CSP LOGS · FORTIGUARD FEED

risk lives here — raw material, not yet classified

TIER 2 — SIEM DETECTION · correlate

Event Handlers
DL-CryptoMining
DL-Suspicious-Outbound
DL-Metadata-Access
DL-Policy-Violation

IOC & Intel
FortiGuard signatures
FortiTIP enrichment
Outbreak Alerts
MITRE ATT&CK mapping

Correlation Rules
Cross-source joins
Windowed aggregation
Severity scoring
Alert generation

threat lives here — risk correlated into alert

TIER 3 — SOAR AUTOMATION · respond

Playbooks
Pre-built response flows
Custom branches per event

Connectors
FortiGate block IP
FortiCNAPP host isolate

Response Actions
Automated · semi · manual
Ticket · notify · isolate

response lives here — alert becomes action

OUTPUT

GENAI — **EMBEDDED IN FAZ**

The co-investigator

- Natural-language queries
- Event explanation in plain English
- Incident summarization (triage draft)
- Business-impact assessment

"can you triage incident IN00000004"

HUMAN-FACING

SOC + XDR Dashboards

- Incident queue · severity view
- Threat Hunting UI · ad-hoc queries
- Cross-source correlation tiles
- FortiGuard outbreak pane

AUTOMATION

Response Actions

- Host isolation via FCNAPP-Quarantine
- Pool IP block at FortiGate edge
- Identity lockdown (IAM / session)
- Ticket open + analyst notify
- Evidence capture for forensics

Hunt 4 lives here

Four hunts · the breadcrumbs

14 FLAGS TOTAL

HUNT 0 · WARM-UP	Data Lake Deployment	verify ingestion · confirm agent · explore Threat Hunting UI	~15 min · 0 flags

HUNT 1
Cryptomining Detection — 4 flags
T1496 Resource Hijacking · T1071 App Layer
DATA LAKE · SIEM

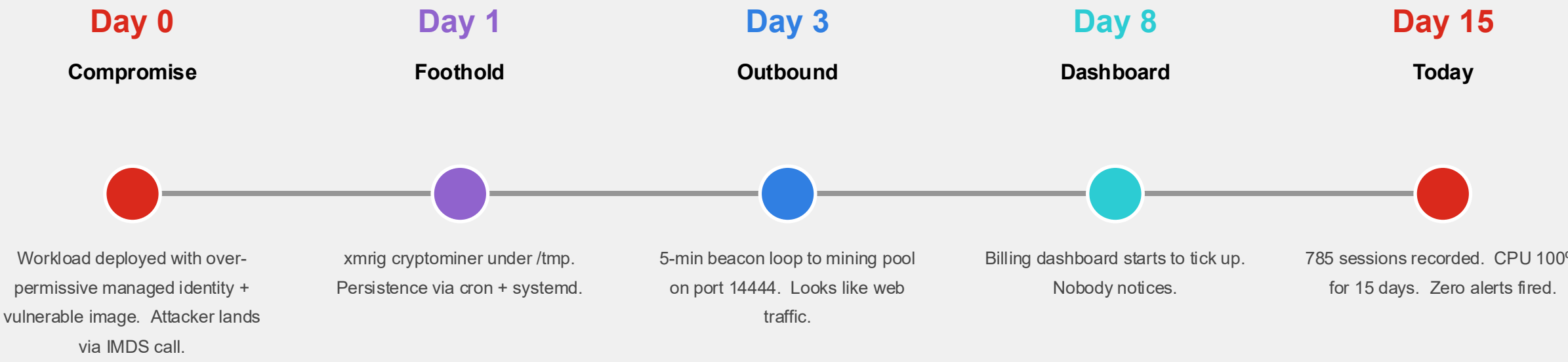
HUNT 2
Threat Intelligence — 3 flags
T1071 App Layer · FortiGuard IOC pivot
DATA LAKE · SIEM

HUNT 3
Persistence & Stealth — 4 flags
T1552 Unsecured Creds · T1098 Account Manip.
DATA LAKE · SIEM

HUNT 4
Automated Remediation — 3 flags
T1190 Exploit Public-Facing App · SOAR
DATA LAKE · SIEM · SOAR

THE SCENARIO

The Quiet Breach.




```
$ ps -ef | grep xmrig   →   www-data  /tmp/.cache/xmrig --url=49.12.80.38:14444 --donate-level=0 -B
```

> *"Are we already compromised, and we just don't know it yet?" — the CISO.*

FOUR HUNTS · FOURTEEN FLAGS

Here's where the evidence lives.

HUNT 0 · before you start · Data Lake Deployment · verify ingestion · explore Threat Hunting UI (~15 min)

1 Cryptomining Detection

4 flags

Find the miner. Find the beacon.

T1496 Resource Hijacking
T1071 Application Layer Protocol

2 Threat Intelligence

3 flags

Pivot on the pool IP. What does FortiGuard already know?

T1071 Application Layer Protocol

3 Persistence & Stealth

4 flags

How did it survive reboot? Where else does it hide?

T1552 Unsecured Credentials
T1098 Account Manipulation

4 Automated Remediation

3 flags

Isolate the host. Contain the identity. Close the loop.

T1190 Exploit Public-Facing Application

No step-by-step here. The lab guide has those. These are the headlines.

15

DAYS

Nobody caught it. You have 3h 15m.

Let's see what AI-assisted hunting can do.

Now let's hunt.

LAB URL

https://canada.amerintlxperts.com/ai/Security_Data_Lake/

Credentials in your handout. Hunt Zero starts now.

You have 3h 15m. Beat the attacker's dwell.

THANK YOU

Questions?

Keep in touch· **dzambonino@fortinet.com**

FORTINET · XPERTS 2026


FORTINET