SOC 3.0 Sådan transformerer Agentic AI it-sikkerhed

Tommy Pedersen

Systems Engineer Fortinet Danmark

~$whoami

Tommy Pedersen

Team Lead, Systems Engineering Channel

- 25 års+ erfaring indenfor IT
- Arbejdet på alle sider af bordet; Kunde, Konsulent og Producent
- +10 år med salg og channel

Kontakt:

https://www.linkedin.com/in/pedersentommy/

tpedersen@fortinet.com

© Fortinet Inc. All Rights Reserved.

Challenges of a SecOps Teams

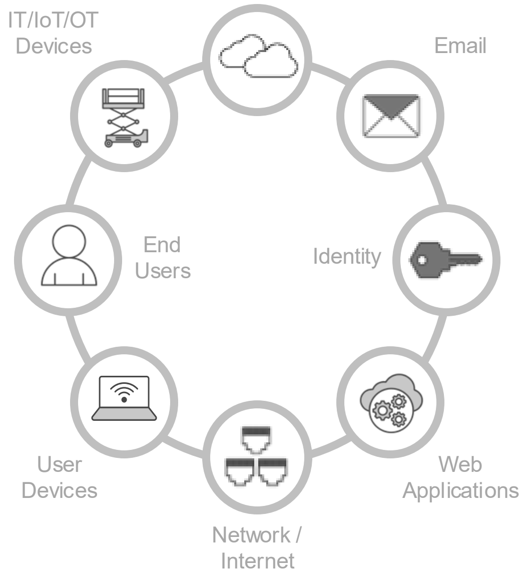
Evolving Threats, Expanding Attack Surface and Complex Alerts

Threat Landscape

- Industrial Ransomware
- APT Threat Actors
- Supply Chain Attacks
- New Vulnerabilities
- Long-lived Exploits
- Cloud Risks
- Insider Risks
- Cyber-physical Attacks

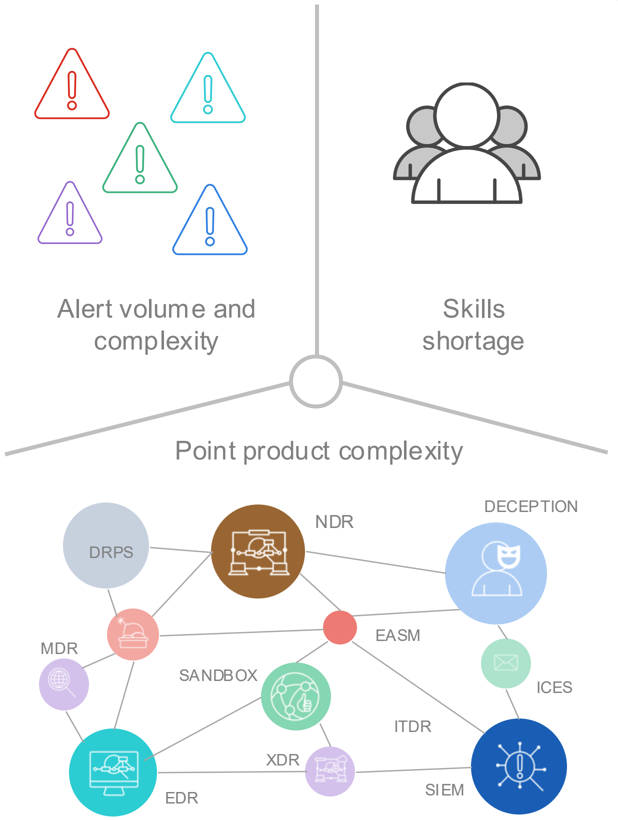
Speed and sophistication to cyber attacks

Attack Surface



Broad and dynamic area to continually monitor

SecOps Workload



Alert volume and complexity

Skills shortage

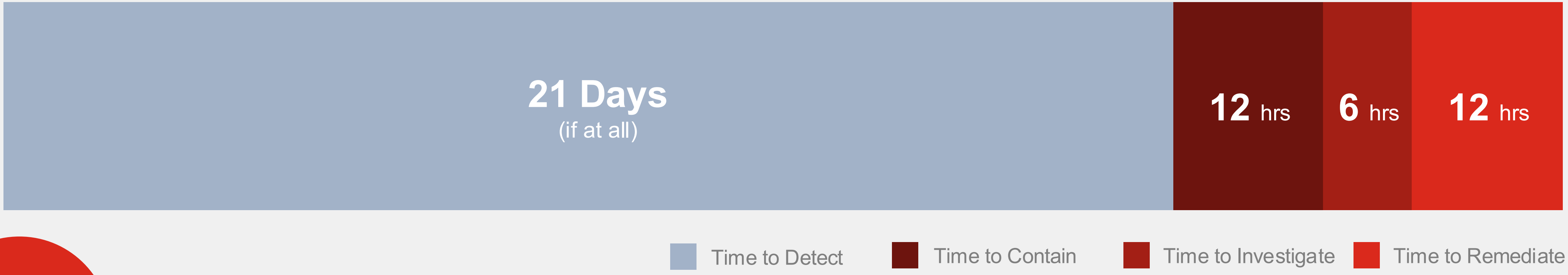
Point product complexity

On average, organizations have nearly 50 security tools in their environments, with some exceeding 140. – IDC Research

© Fortinet Inc. All Rights Reserved.

When Attackers Get in, They Stay Longer and Cost You More

Average time from detection to remediation



52%

of organizations report SecOps is harder than two years ago, citing threats, attack surface, volume/complexity[1]

SEC Rule

4 Days

to disclose material of a cybersecurity incident

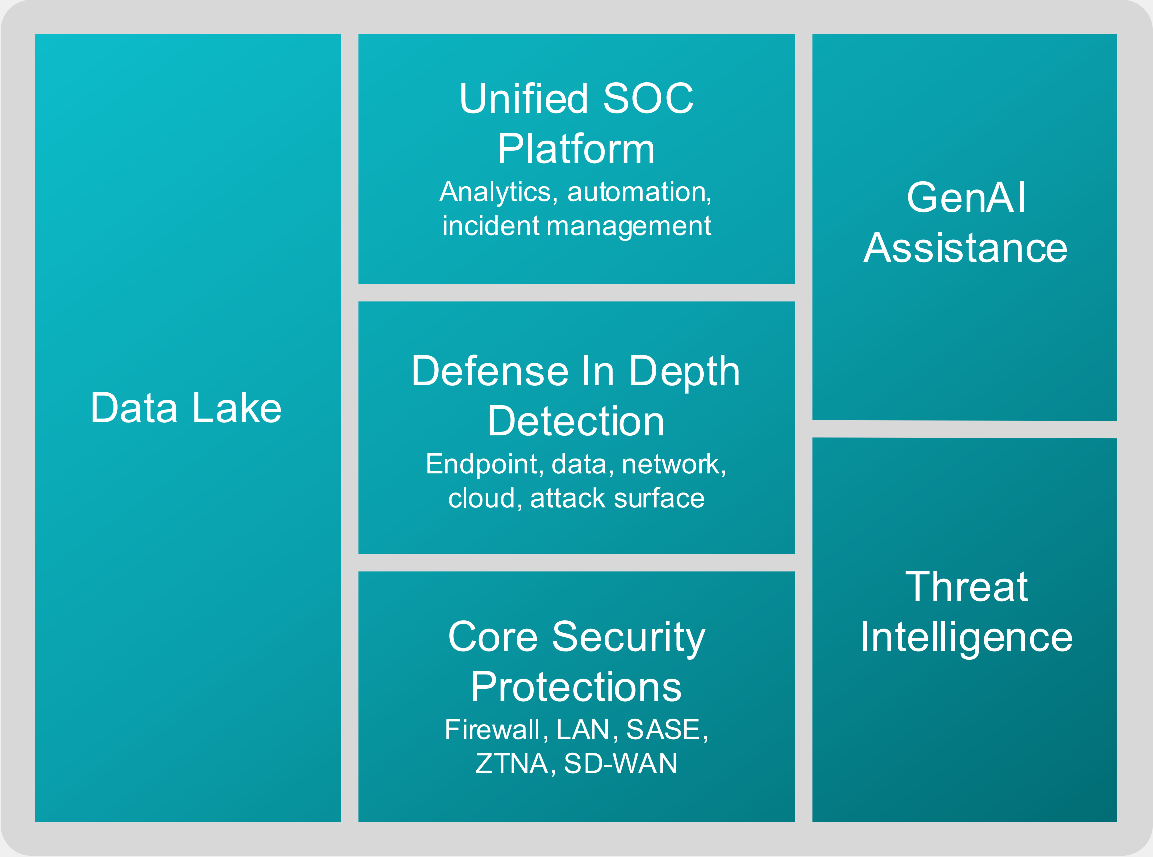
$9.4M

Avg breach cost

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

© Fortinet Inc. All Rights Reserved.

Needs of Today’s Security Team



Data Lake

Unified SOC Platform
Analytics, automation, incident management

Defense In Depth Detection
Endpoint, data, network, cloud, attack surface

Core Security Protections
Firewall, LAN, SASE, ZTNA, SD-WAN

GenAI Assistance

Threat Intelligence

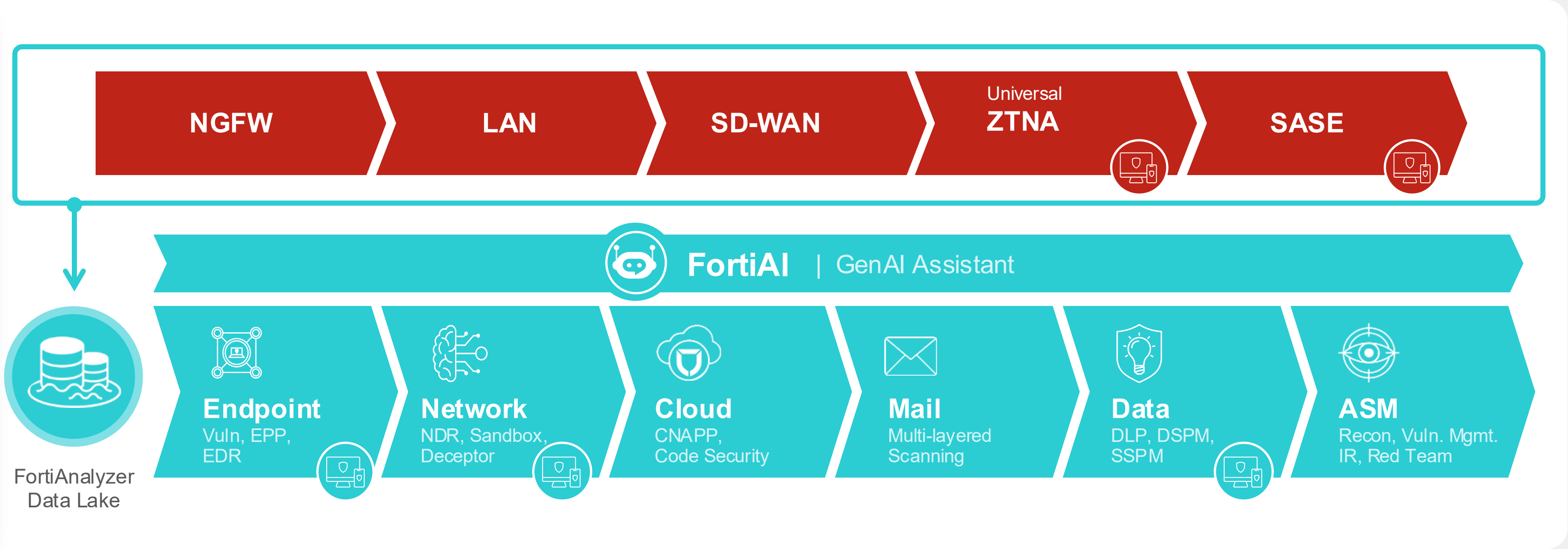
- A centralized, scalable data lake
- Enterprise-wide event collection
- Advanced detection to identify stealthy attacks
- Automation to speed response
- Rich threat intelligence feeds
- GenAI to aid analysts and streamline tasks
- Consolidated and flexible solutions for any size company and security team

© Fortinet Inc. All Rights Reserved.

Transforming SOC Capabilities for AI-Driven Cyber Defense

Centralizing security and networking data to enhance visibility, orchestration, and automation

Transform Insights into Outcomes with the Fortinet Security Fabric



NGFW

LAN

SD-WAN

Universal ZTNA

SASE

FortiAnalyzer Data Lake

FortiAI | GenAI Assistant

Endpoint
Vuln, EPP, EDR

Network
NDR, Sandbox, Deceptor

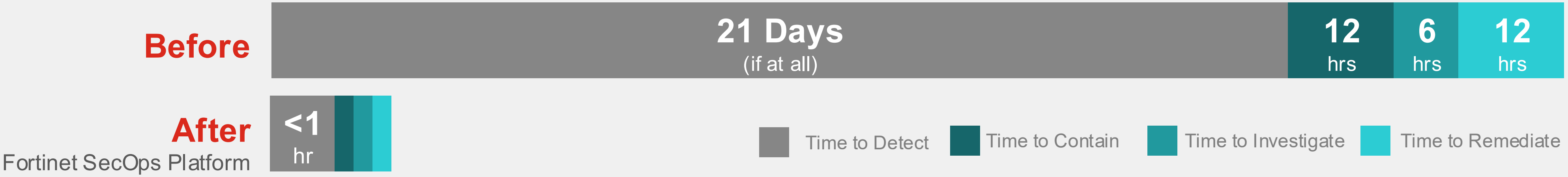
Cloud
CNAPP, Code Security

Mail
Multi-layered Scanning

Data
DLP, DSPM, SSPM

ASM
Recon, Vuln. Mgmt. IR, Red Team

Speed the time to fully investigate and remediate incidents from 18.5 hours to an average of 10 minutes.



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

© Fortinet Inc. All Rights Reserved.

Accelerating Product Development & Evaluation of SOC technology..

Meru Networks

Bradford Networks

ENSILO

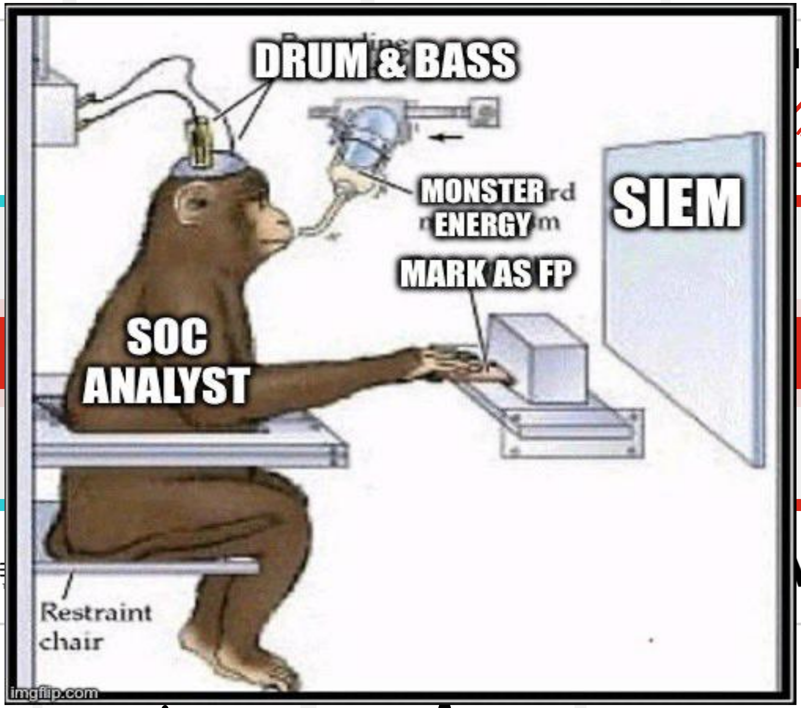
OPAQ

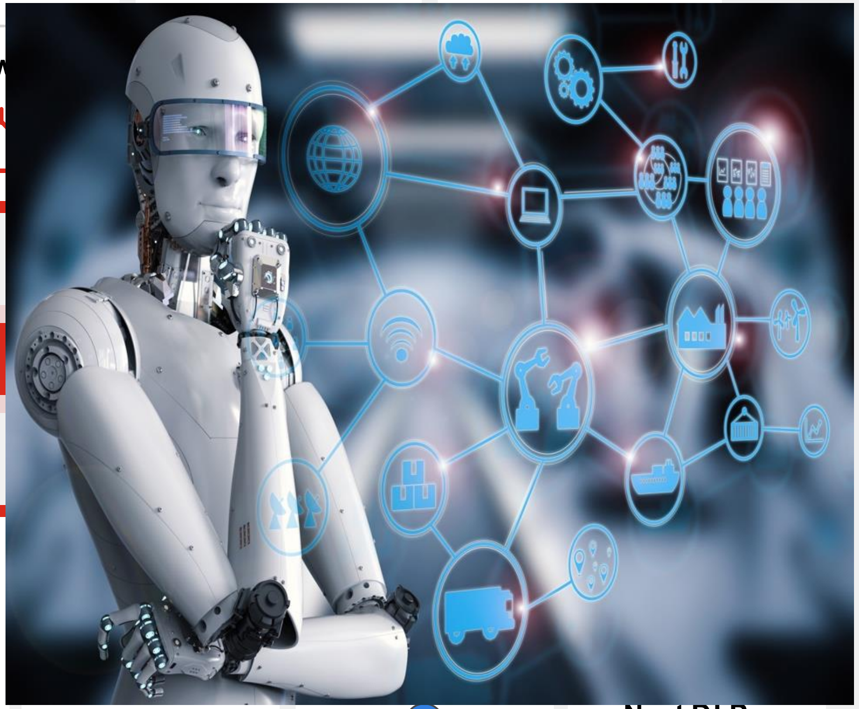
SHIELDX

LINKSYS

VOLON

LACEWORK

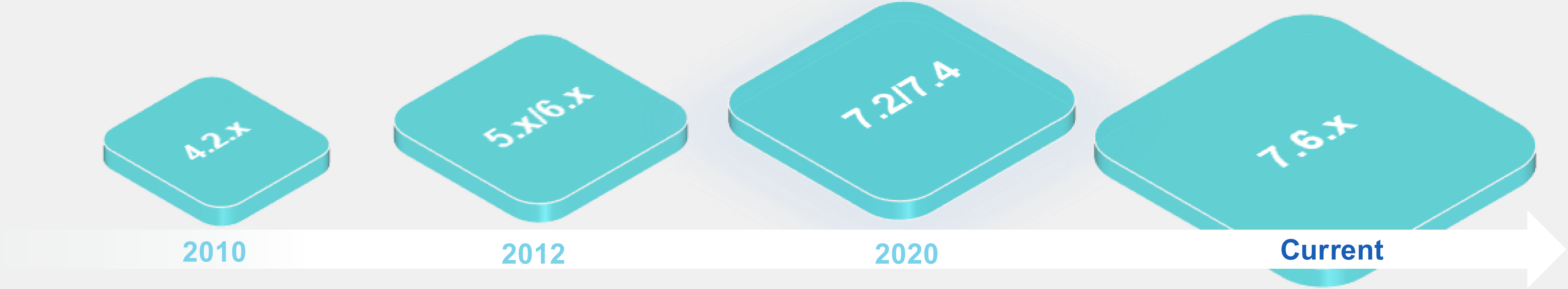




Next DLP

© Fortinet Inc. All Rights Reserved.

FortiAnalyzer Evolution



Capabilities

- Alerting FortiGate Logging
- Reporting

- FortiGuard IoC
- Security Fabric logging & analytics
- Security Fabric reporting
- SIEM for Security Fabric
- Incident Response framework

- FortiGuard Outbreak
- Advanced analytics for OT
- SIEM framework for 3rd-party
- SOAR framework
- Compliance reporting framework
- FortiAnalyzer Fabric

- Incident Analysis Workflow
- Enhanced Threat Intel
- Security Automation Content Packs
- ClickHouse support
- FortiAI Assistant

Platforms

VM

Appliance

aws Azure

PaaS

FAZ-BD Appliance

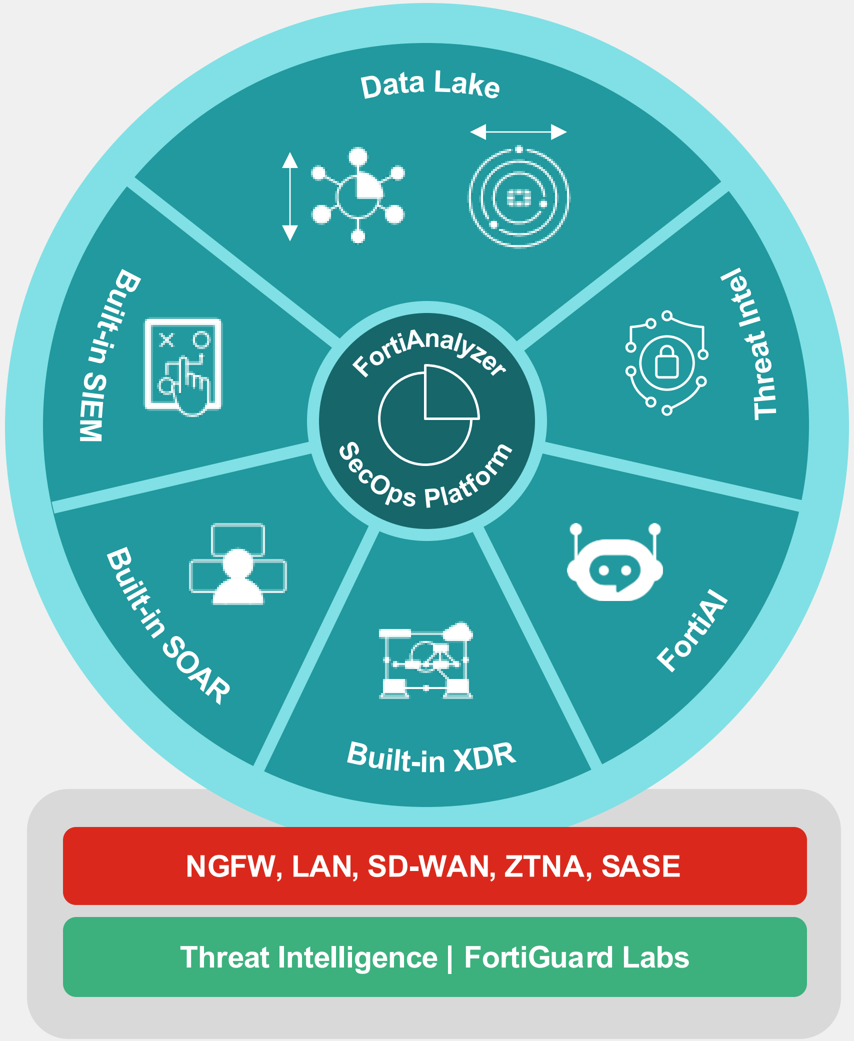
FAZ-BD VM

© Fortinet Inc. All Rights Reserved.

AI-Driven SecOps Platform

FortiAnalyzer: Essential turnkey capabilities for the lean security team

Appliance Virtual Machine Cloud Big Data



Unified Data Lake

Provides a single view of logs, incidents, configurations, and alerts

Native Threat Intelligence

Real-time FortiGuard Labs intelligence, including Outbreak Detection and Indicator of Compromise (IoC)

Built-in SOC Automation

Includes SIEM, SOAR, and XDR capabilities with pre-configured content

Embedded GenAI-Assistant

Integrates FortiAI, GenAI assistance to enhance efficiency and response

Flexible Deployments

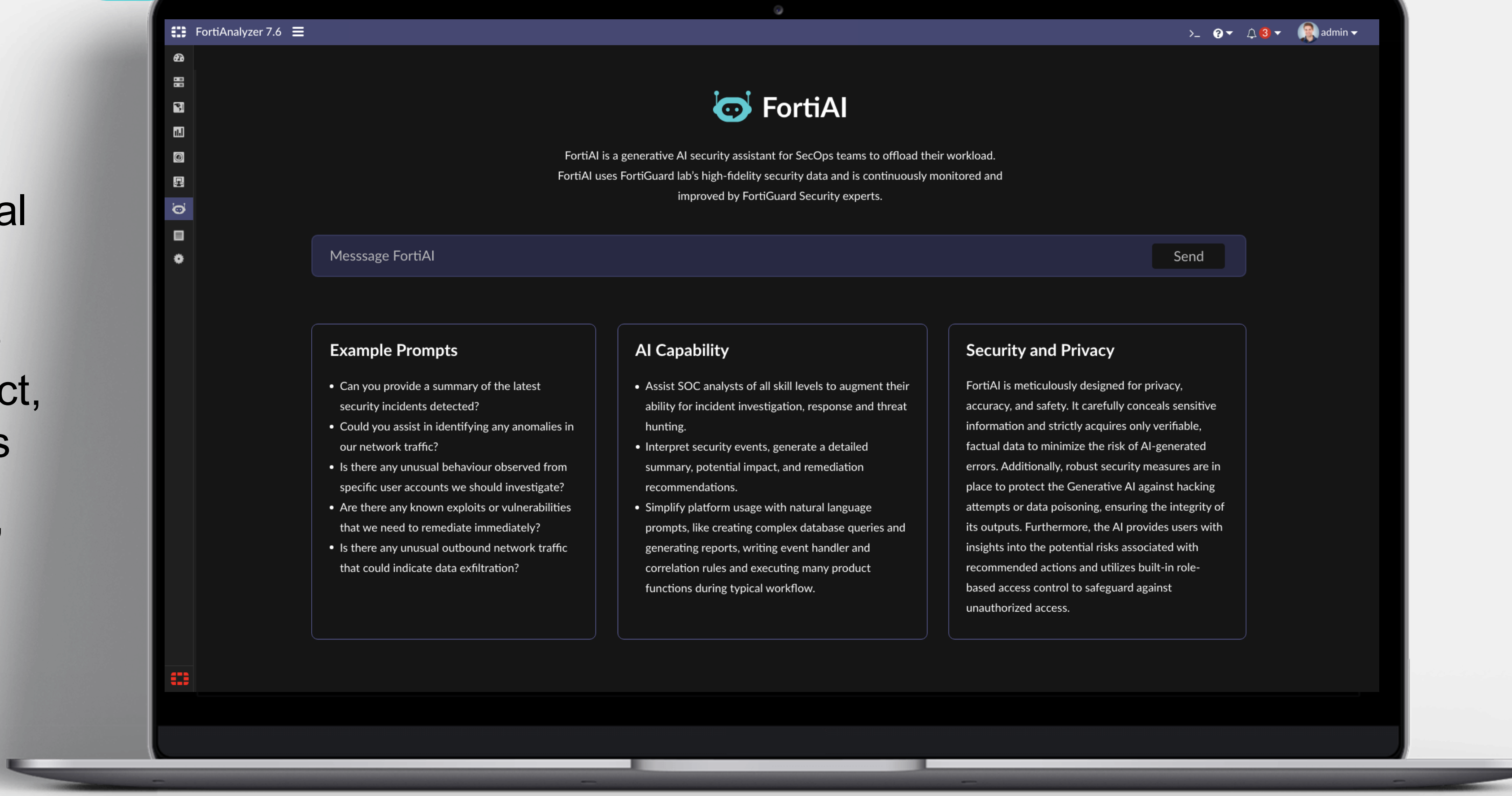
Offers lightweight deployment options through horizontal big data scale with appliance, VM, or cloud deployment options

© Fortinet Inc. All Rights Reserved.

FortiAI Assistant

Generative AI Augmented SecOps

- Reduces Security Operations workload
- Simplify platform usage with natural language prompts
- Interpret security events, generate summaries, assess potential impact, and remediation recommendations
- Create complex database queries, reports, event handlers and SIEM detection rules



FortiAI

FortiAI is a generative AI security assistant for SecOps teams to offload their workload. FortiAI uses FortiGuard lab's high-fidelity security data and is continuously monitored and improved by FortiGuard Security experts.

Example Prompts

- Can you provide a summary of the latest security incidents detected?
- Could you assist in identifying any anomalies in our network traffic?
- Is there any unusual behaviour observed from specific user accounts we should investigate?
- Are there any known exploits or vulnerabilities that we need to remediate immediately?
- Is there any unusual outbound network traffic that could indicate data exfiltration?

AI Capability

- Assist SOC analysts of all skill levels to augment their ability for incident investigation, response and threat hunting.
- Interpret security events, generate a detailed summary, potential impact, and remediation recommendations.
- Simplify platform usage with natural language prompts, like creating complex database queries and generating reports, writing event handler and correlation rules and executing many product functions during typical workflow.

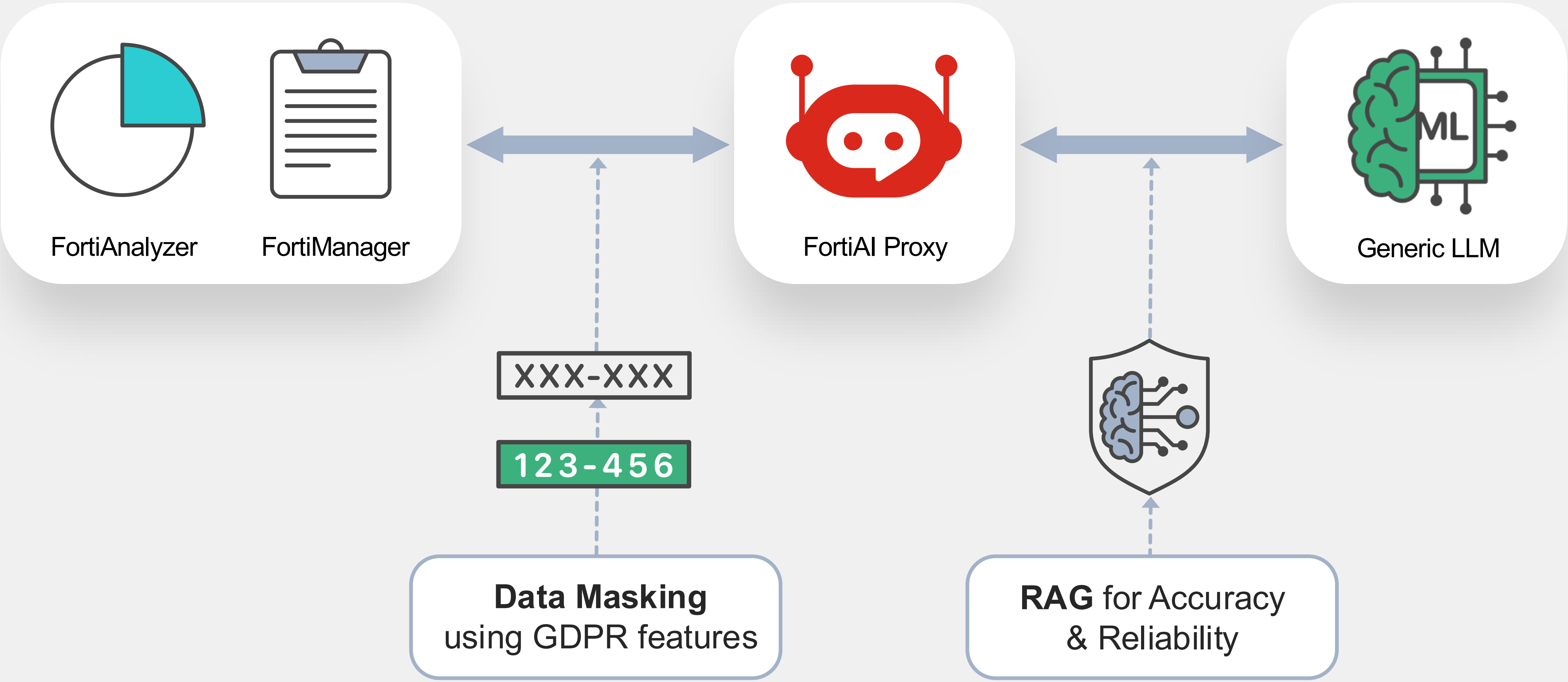
Security and Privacy

FortiAI is meticulously designed for privacy, accuracy, and safety. It carefully conceals sensitive information and strictly acquires only verifiable, factual data to minimize the risk of AI-generated errors. Additionally, robust security measures are in place to protect the Generative AI against hacking attempts or data poisoning, ensuring the integrity of its outputs. Furthermore, the AI provides users with insights into the potential risks associated with recommended actions and utilizes built-in role-based access control to safeguard against unauthorized access.

© Fortinet Inc. All Rights Reserved.

FortiAI Proxy & Data Privacy

Generative AI Augmented SecOps



FortiAnalyzer

FortiManager

FortiAI Proxy

Generic LLM

XXX-XXX

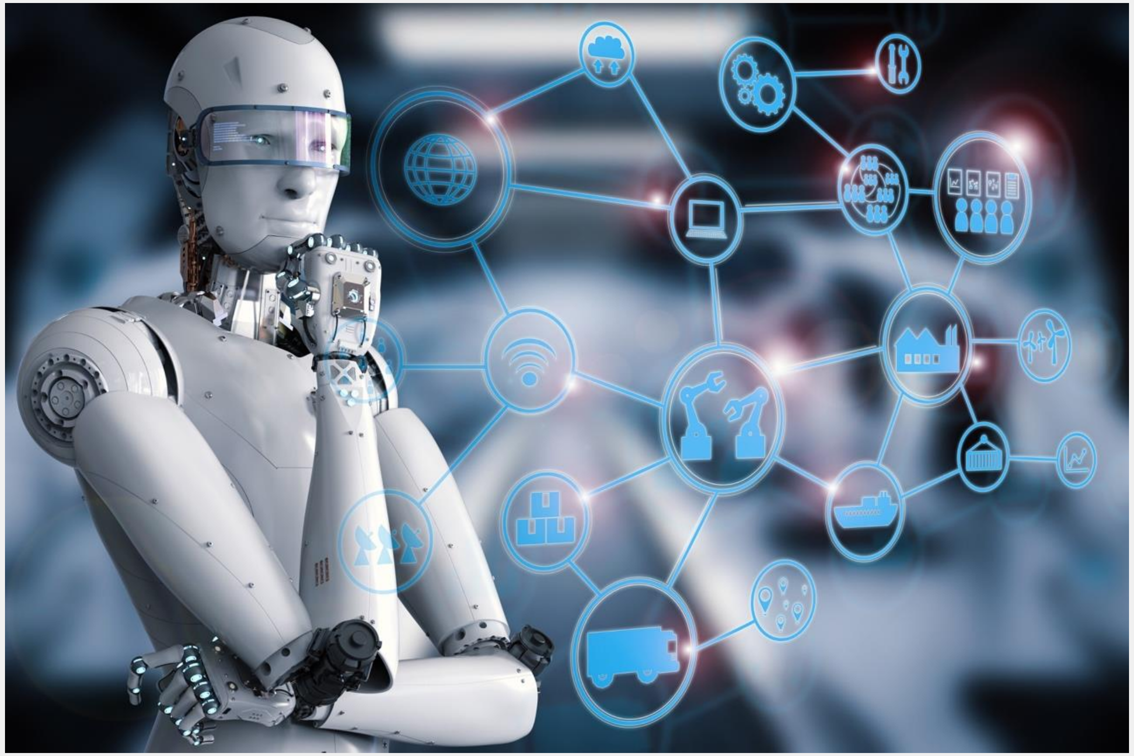
123-456

Data Masking
using GDPR features

RAG for Accuracy
& Reliability

© Fortinet Inc. All Rights Reserved.

Fortinet Hosted LLM (Agentic AI)

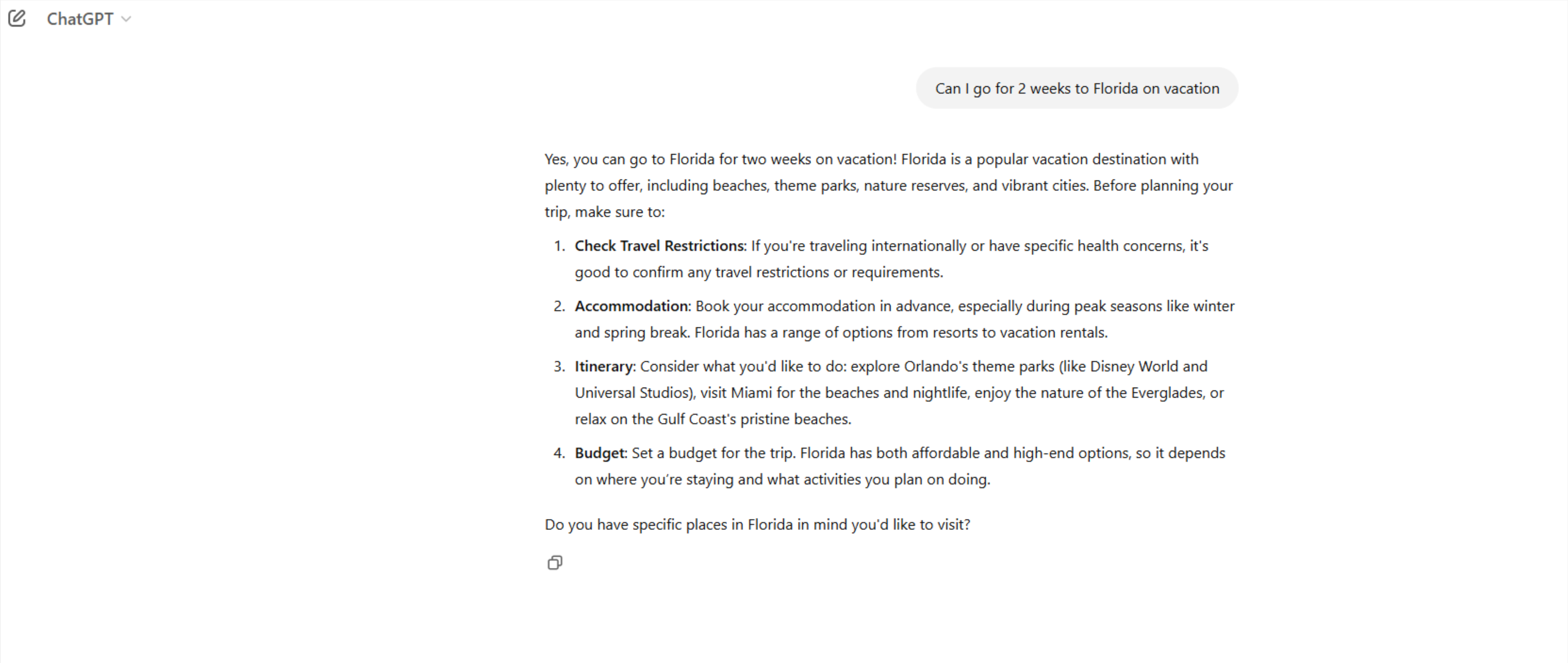


Agentic AI operates in four key stages:

1. **Perception:** It gathers data from the world around it.
2. **Reasoning:** It processes this data to understand what's going on.
3. **Action:** It decides what to do based on its understanding.
4. **Learning:** It improves and adapts over time, learning from feedback and experience.

© Fortinet Inc. All Rights Reserved.

Is this correct?



Can I go for 2 weeks to Florida on vacation

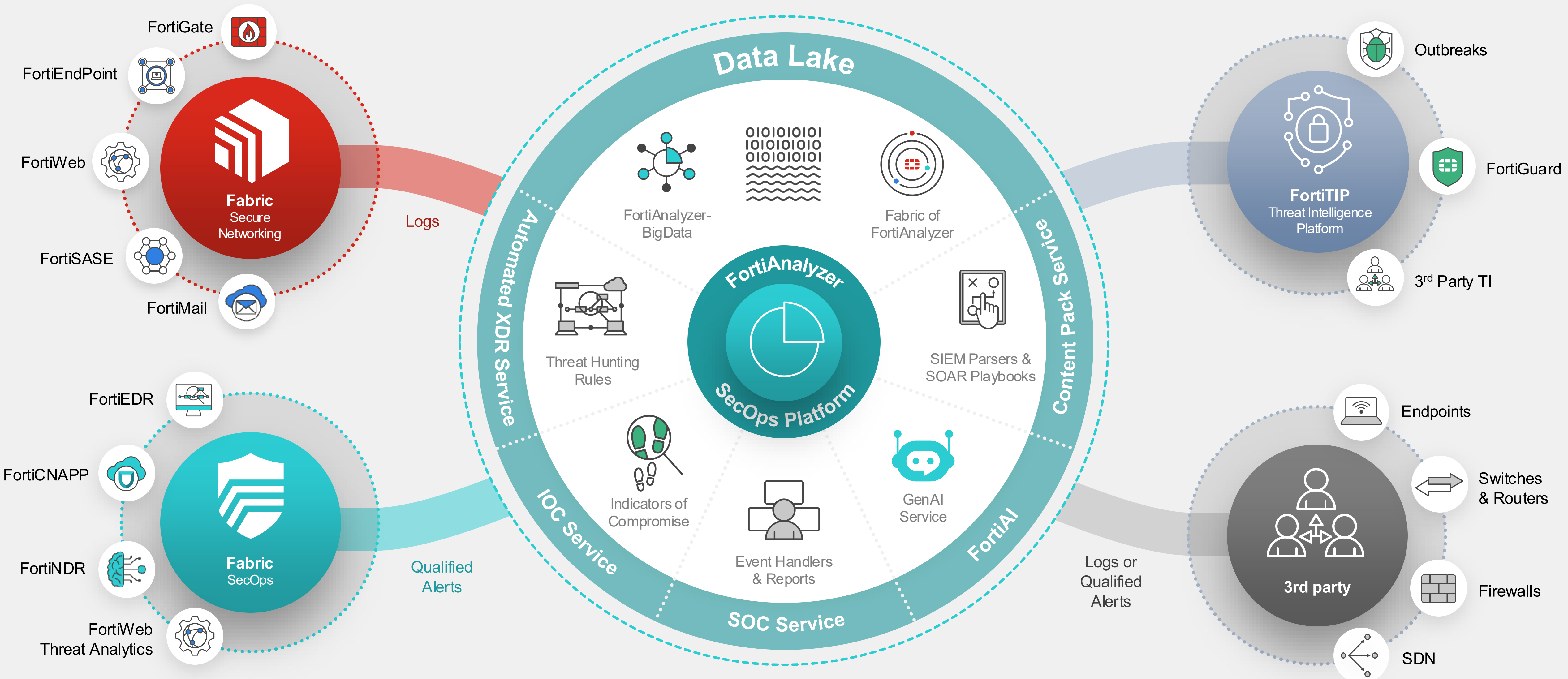
Yes, you can go to Florida for two weeks on vacation! Florida is a popular vacation destination with plenty to offer, including beaches, theme parks, nature reserves, and vibrant cities. Before planning your trip, make sure to:

1. **Check Travel Restrictions**: If you're traveling internationally or have specific health concerns, it's good to confirm any travel restrictions or requirements.
2. **Accommodation**: Book your accommodation in advance, especially during peak seasons like winter and spring break. Florida has a range of options from resorts to vacation rentals.
3. **Itinerary**: Consider what you'd like to do: explore Orlando's theme parks (like Disney World and Universal Studios), visit Miami for the beaches and nightlife, enjoy the nature of the Everglades, or relax on the Gulf Coast's pristine beaches.
4. **Budget**: Set a budget for the trip. Florida has both affordable and high-end options, so it depends on where you're staying and what activities you plan on doing.

Do you have specific places in Florida in mind you'd like to visit?

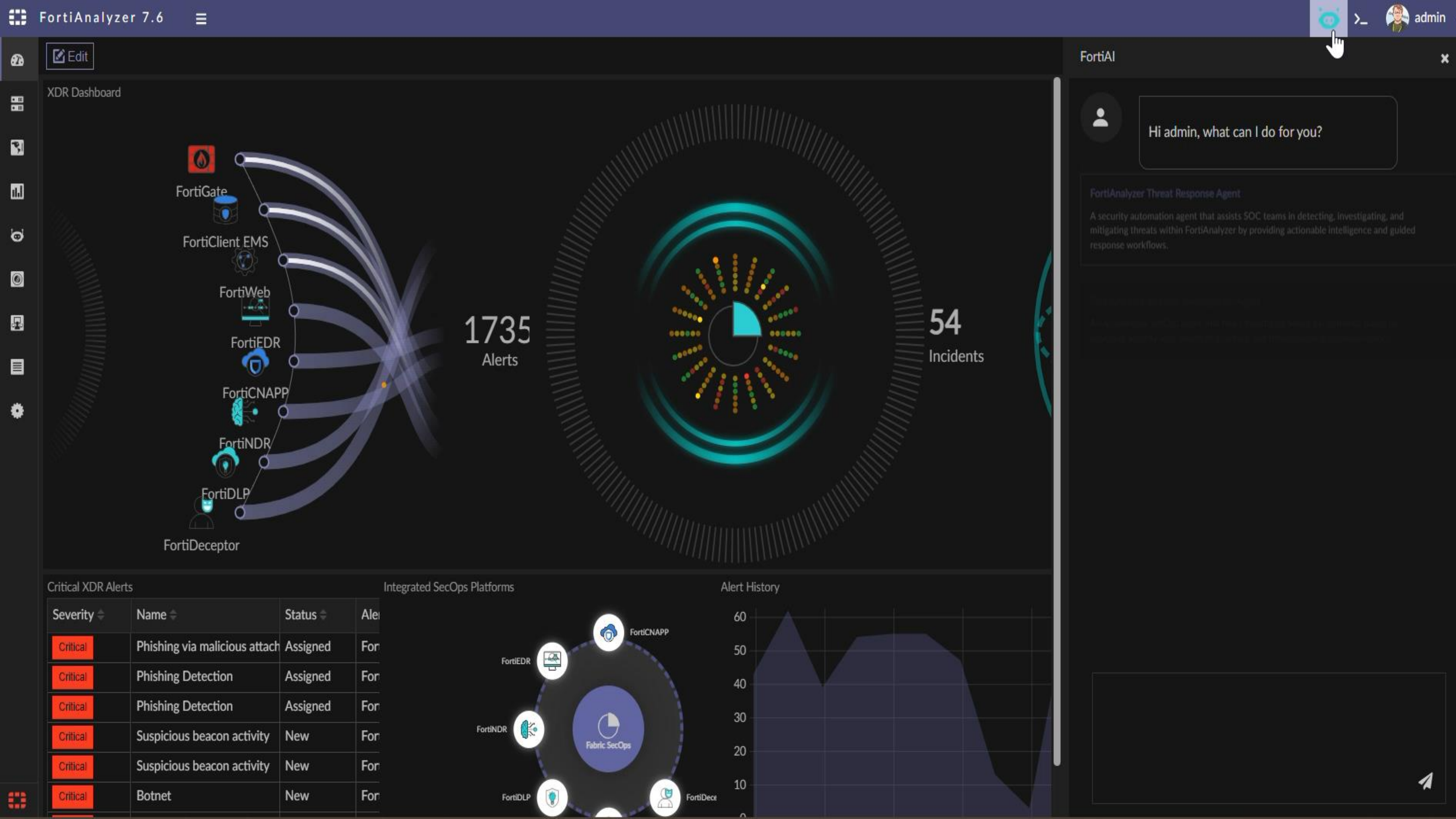
© Fortinet Inc. All Rights Reserved.

FortiAnalyzer: A Complete SecOps Platform



© Fortinet Inc. All Rights Reserved.

Say Hello to your new SOC Analyst “Steve”



Hi admin, what can I do for you?

FortiAnalyzer Threat Response Agent

A security automation agent that assists SOC teams in detecting, investigating, and mitigating threats within FortiAnalyzer by providing actionable intelligence and guided response workflows.

Critical XDR Alerts

Severity	Name	Status	Ale
Critical	Phishing via malicious attach	Assigned	For
Critical	Phishing Detection	Assigned	For
Critical	Phishing Detection	Assigned	For
Critical	Suspicious beacon activity	New	For
Critical	Suspicious beacon activity	New	For
Critical	Botnet	New	For

Turnkey 24/7 Security Monitoring with FortiGuard SOCaaS

- Fortinet Security Experts
- AI-Powered Technologies
- FortiGuard Labs
- Rapid Deployment

Acknowledge Alerts In
2.5
Minutes

Triage Critical Alerts
5-12
Minutes

Average
15
Minutes MTTR

Detect

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

Respond

Fortinet security experts will notify teams in as little as 15 minutes and provide insights into what happened, why it happened, and what steps to take to remediate the incident.

Improve

A cloud-based portal with intuitive dashboards, on-demand reports, and quarterly meetings with Fortinet Security Experts allowing users to drill into incidents, report up the chain.

*Purchased as a separate FortiGate add-on SKU

© Fortinet Inc. All Rights Reserved.