SOLUTION BRIEF

Secure and Transform Your Organization with FortiAI

Executive Summary

Artificial intelligence (AI) is already transforming many aspects of business, daily life, and society. It affects nearly all of us somehow—whether we are aware of its specific influence or not. Across industries, AI offers opportunities and challenges, and this is especially true for cybersecurity. Bad actors use AI-based attacks that move more quickly and are more difficult to stop. Organizations are adopting AI systems, but they are vulnerable and need to be protected, ironically, from AI-based (and other) attacks. Harnessing AI to fight cyberattacks offers several benefits and is critical for staying ahead of today's ever-evolving threat landscape. A few key examples of AI benefits include faster threat detection and response, the ability to extract more information faster from vast datasets, and helping close the cybersecurity skills gap with automation.

AI models and applications can pose significant risks if left unchecked.[1]

In essence, while AI offers unprecedented defensive capabilities for threat detection and response, its potential weaponization by adversaries necessitates robust security frameworks to ensure AI remains a tool for protection, not a source of vulnerability. Fortinet embeds diverse AI technologies in solutions across the Fortinet Security Fabric to deliver advanced AI-driven security and automation without additional complexity. FortiAI offers key differentiators across three main areas: protection against emerging threats and AI applications, automated security and network operations, and security for AI assets.

Using AI in Cybersecurity

The weaponization of AI by cybercriminals has significantly amplified the threat landscape. AI-powered attacks, including sophisticated malware, targeted phishing, and automated social engineering, pose escalating risks. Attackers leverage AI to accelerate attack speeds, enhance evasion techniques, and lower the barriers to entry for malicious activities, enabling large-scale attacks that can overwhelm traditional defenses. AI systems are also vulnerable, facing threats like data poisoning, model theft, and adversarial attacks designed to bypass security measures.

The good news is that AI can dramatically enhance threat detection and defense through autonomous AI agents, enabling swift responses without human intervention. Its ability to extract significantly more actionable intelligence from vast datasets enhances accuracy and detection. It enables organizations to defend at scale by automating security processes, significantly speeding up attack mitigation in real time. AI addresses the cybersecurity skills gap, allowing teams to prioritize strategic initiatives. The ability of AI to process complex data and detect intricate patterns enables rapid identification of diverse threats, including malware, ransomware, zero-day exploits, and AI-driven attack vectors. This streamlines operations, empowering teams to neutralize threats and strengthen security proactively.

What Is FortiAI?

FortiAI is our unique approach to delivering AI-powered innovations across the Fortinet Security Fabric. These capabilities are seamlessly embedded into our products, which are integrated into the Security Fabric. Unlike siloed point solutions that apply AI for specific tasks, FortiAI innovations provide intelligent, autonomous AI-driven protection across the Fabric, streamline operations, and enhance security for AI systems.

In the continuous battle against cyberthreats, FortiAI offers a decisive advantage. FortiAI doesn't just react; it anticipates. Delivering real-time, always-on protection empowers organizations to detect and respond to threats at warp speed. FortiAI automated security and network operations maximize availability and optimize user experience, ensuring seamless business continuity and productivity.

FortiAI delivers value in three key areas: protection against threats, even the very latest AI-driven threats, automation for NOCs and SOCs, and AI security.

FortiAI: Protection, Automation, and Security

With FortiAI, you can address the challenges of the AI-powered attack surface, streamline security operations with automated and autonomous AI, and protect your AI models and LLMs from threat actors.

FortiAI-Protect for proactive security

FortiAI-Protect uses real-time AI to block emerging threats, prioritize responses with contextual risk assessment, and minimize false positives. It detects hidden threats, including shadow AI, stops evasive attacks, and enforces secure AI usage through real-time controls and policies. FortiAI-Protect delivers:

AI-generated analysis and reports (68.2%) and AI-driven investigation and response recommendations (68.2%) are highly valued by C-Level leaders.[2]

- **Advanced AI protection:** Uses advanced AI analysis and threat intelligence to protect against a broad spectrum of new and evasive threats and intrusions
- **AI application detection and control:** Controls unauthorized AI (shadow AI) use, including GenAI use, to reduce security and compliance risks
- **Prioritization and reduced risk:** Prioritizes critical threat responses with contextual risk assessment, reducing false positives to near zero

FortiAI-Assist for operations

FortiAI-Assist optimizes network operations proactively and autonomously, automates security tasks, prioritizes threats and removes duplicates, hunts for hidden threats without the need for frequent human input, traces attack origins, and enriches threat intelligence. FortiAI streamlines operations, strengthens security, and reduces manual effort. FortiAI-Assist enables:

- **Proactive alert triage:** Analyzes logs, identifies patterns, and automates fixes in an autonomous network
- **Agentic AI reasoning:** Autonomous, AI-driven decision-making that analyzes and acts on threats or operational issues
- **AI-driven optimization:** Enhances network performance and resilience with predictive insights from correlated data

FortiAI-SecureAI for AI security

FortiAI-SecureAI safeguards AI infrastructure across networks, web and APIs, and clouds with layered defense, zero-trust access, data integrity protection, and deception for early detection. This ensures that comprehensive AI security is applied from the infrastructure to the data while maintaining compliance. FortiAI-SecureAI helps:

- **Secure AI models and systems:** Secures AI models and systems from poisoning and drift with ZTNA and network, web application, and API protection
- **Prevent data leakage:** Prevents confidential corporate data leakage from LLMs with DLP
- **Protect cloud AI workloads:** Monitors AI workloads with CNAPP

The FortiAI Advantage

Operating in real time, FortiAI secures and transforms organizations by proactively defending against emerging threats, enabling faster detection and response to threats, and automating security and network operations while maximizing network availability and optimizing user experience.

FortiAI offers key differentiators when compared to other AI-based cybersecurity solutions:

- **Embedded within a security fabric:** FortiAI is embedded across the Fortinet Security Fabric, providing real-time AI value across the platform, including enhancements for secure networking, unified SASE, and security operations.

- **Mature AI:** With 500+ patents issued and pending, FortiAI ML, now in its sixth generation, uses purpose-built ML models that leverage real-time data from millions of network, cloud, and endpoint sensors around the globe. This enables it to develop deep neural networks capable of sub-second classification and near-real-time remediation.
- **Automated and autonomous:** FortiAI automates network and security operations across the Security Fabric with autonomous AI (agentic AI). It analyzes without the necessity for frequent human input and provides unified control.

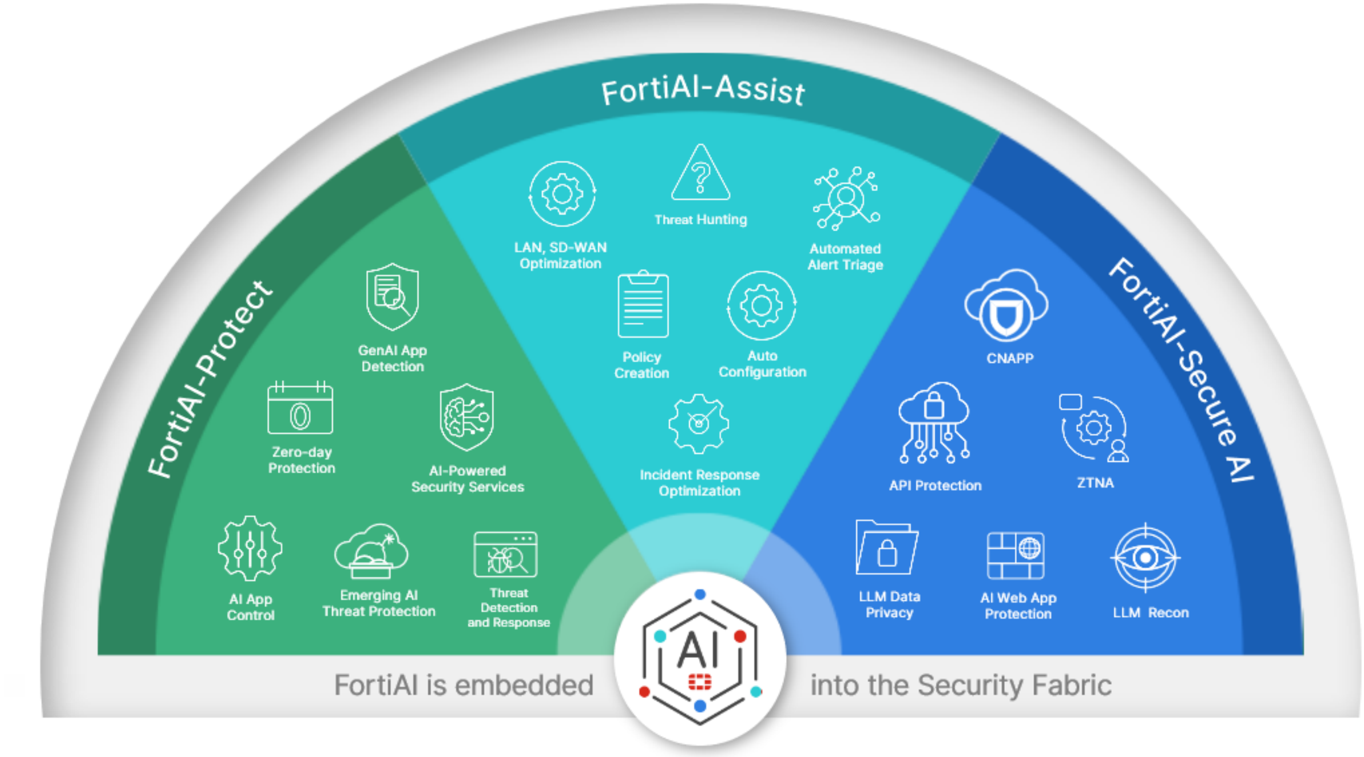

Figure 1: FortiAI capabilities across the Fortinet Security Fabric

Conclusion

FortiAI tackles the escalating complexities of modern cybersecurity, specifically addressing the unique challenges posed by emerging AI-driven cyberattacks, the persistent threat of zero-day vulnerabilities, increased operational complexity, and securing AI adoption.

With FortiAI embedded across the Fortinet Security Fabric, organizations are empowered to fight escalating AI threats with innovative AI, confidently embrace the transformative potential of AI, and unburden overwhelmed NOC and SOC teams.

[1] Avitah Litan, Tackling Trust, Rish, and Security in AI Models, Gartner, December 24, 2024.

[2] Monika Soltysik, Christopher Kissel, U.S. Threat Intelligence End-User Survey: From Insights to Action, IDC, February 2025.