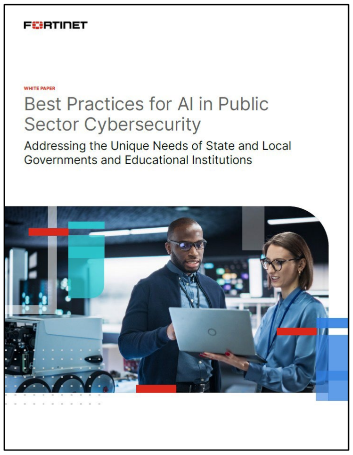
FORTINET

carahsoft



FORTINET

WHITE PAPER

Best Practices for AI in Public Sector Cybersecurity

Addressing the Unique Needs of State and Local Governments and Educational Institutions

Best Practices for AI in Public Sector Cybersecurity

Fortinet White Paper

Thank you for downloading Fortinet's Best Practices for AI in Public Sector Cybersecurity white paper. Carahsoft is the distributor for Fortinet's cybersecurity solutions available via NASPO, OMNIA, E&I and other contract vehicles.

To learn how to take the next step toward acquiring Fortinet's solutions, please check out the following resources and information:

For additional resources:
carah.io/FortinetResources

For additional cybersecurity solutions:
carah.io/CybersecuritySolutions

To set up a meeting:
Fortinet@carahsoft.com
866-468-3868

To purchase, check out the contract vehicles available for procurement:
carah.io/FortinetContracts

For upcoming events:
carah.io/FortinetEvents

For more information, contact Carahsoft or our reseller partners:
Fortinet@carahsoft.com | 866-468-3868

FORTINET

WHITE PAPER

Best Practices for AI in Public Sector Cybersecurity

Addressing the Unique Needs of State and Local Governments and Educational Institutions

Executive Summary

State and local governments and educational institutions face distinct cybersecurity challenges: constrained budgets, aging infrastructure, and a diverse user base. These factors create significant vulnerabilities, leaving organizations more susceptible to cyberattacks, particularly as malicious actors increasingly exploit AI to accelerate their tactics.

At the same time, AI can also serve as a powerful defense. By working with vendors that bring extensive public sector experience and solutions compatible with legacy systems, organizations can overcome critical barriers. Prioritizing ease of use, enabling diverse device management, automating detection and response, and upholding strong data privacy standards help close the gap between limited resources and rising threats.

Fortinet offers a suite of AI-powered solutions, such as FortiAI embedded in the Fortinet Security Fabric, designed to help protect state and local agencies and educational institutions. With the right strategy and tools, public sector organizations can harness AI to strengthen their defenses and reduce risk.

A startling majority, 82%, of K-12 schools experienced a cyber incident between July 2023 and December 2024.[1]

Understanding Public Sector Needs and Challenges

State, local, and educational organizations face a lot of the same challenges as other industries but many are unique to the public sector. Some of the most common hurdles are:

Resource and budget constraints

Public sector organizations often operate with limited budgets and small IT teams. AI solutions should be cost-effective, easy to manage, and reduce reliance on specialized staff.

Legacy systems

Integrating AI-powered security tools with existing, often outdated, infrastructure is essential. Solutions should work seamlessly with current systems without requiring major overhauls.

Diverse users and devices

Public sector networks must support a wide variety of users and devices. Educational networks, in particular, serve staff and students, each with different levels of cybersecurity awareness. This diversity increases the attack surface, so AI solutions should be user-friendly and minimize complexity for all end-users.

High volume of vulnerabilities

The combination of constrained resources, legacy systems, and diverse users increases the number of vulnerabilities and risk of cyberattacks, making AI-powered cybersecurity solutions critical for protection.

Best Practices for AI-Powered Security Solutions in the Public Sector

Fortinet has over 15 years of AI research experience, more than 500 AI patents, and multiple integrated solutions across its security and networking portfolio. Public sector organizations can strengthen cybersecurity by following these key implementation practices:

Select vendors with public sector expertise

Organizations should engage vendors that understand the unique constraints and challenges of state, local, and educational institutions. Look for cost-effective solutions that reduce alert fatigue, address skills gaps, and provide simplified management interfaces.

Confirm compatibility with legacy systems

AI-powered solutions should integrate seamlessly with existing infrastructure, minimizing disruption and reducing the need for costly upgrades.

Focus on user-friendliness

AI-powered tools should be intuitive and require minimal technical expertise to deploy and operate, accommodating the diverse skill levels of users across public sector organizations.

Enable diverse device management

AI-powered solutions and services should enhance network visibility and control over the multitude of devices connecting to public sector networks, improving security across all endpoints.

Automate detection and response

Solutions should support real-time detection and automated responses, helping address the cybersecurity skills gap and reducing the impact of attacks.

Provide comprehensive training and support

Vendors should offer extensive training and readily available support for AI-powered security solutions. Additionally, cybersecurity awareness training should be mandatory for all employees to mitigate human error.

Prioritize data privacy and compliance

Educational institutions should choose AI solutions that help them comply with regulations such as CIPA, COPPA, and FERPA. Across all public sector organizations, including state and local government, solutions should also support compliance with relevant state and local data privacy laws. Vendors should implement strong data anonymization practices to protect sensitive information.

Ensure E-Rate eligibility

K-12 schools and libraries should confirm that the AI-powered security solutions they are considering are eligible for E-Rate funding.

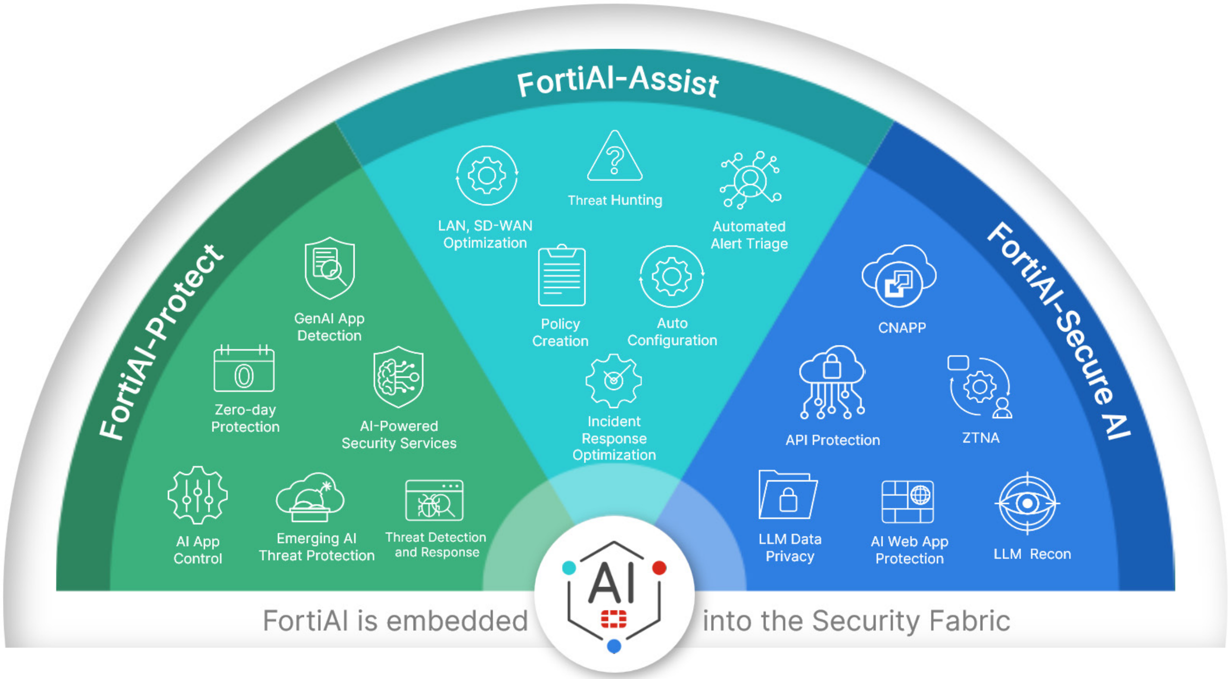


Figure 1: FortiAI embedded into the Fortinet Security Fabric

Addressing Challenges in AI Implementation

AI-powered solutions can be a valuable complement to public sector cybersecurity, but organizations must carefully navigate several challenges:

Data quality and privacy

Educational organizations should ensure AI models are trained on high-quality, anonymized data to improve accuracy and comply with privacy regulations such as FERPA.

Integration with legacy systems

CISOs and IT leaders should plan for phased AI deployments to ensure smooth integration with existing infrastructure and protect prior technology investments.

Human oversight

Cybersecurity teams must maintain human oversight to validate AI findings and make critical decisions ensuring AI supports, not replaces, expert judgment.

Continuous monitoring and updates

Cybersecurity teams should leverage regular threat intelligence reports and updates from their AI security solution vendors to stay protected against new and evolving cyberthreats.

FortiGuard Labs: The AI Engine That Drives Real-Time Threat Protection

FortiGuard Labs is Fortinet's global threat intelligence organization, consisting of over 1,000 experts using AI and machine learning (ML) to deliver real-time insights. Due to the sheer volume and velocity of cyberthreats today, AI-driven analysis to identify them is an absolute necessity to stay secure. FortiGuard Labs uses AI/ML at various stages of its threat intelligence life cycle for:

- Data collection and analysis: Data from millions of sensors and over 200 partners fuels AI-driven pattern recognition and anomaly detection.
- Deep behavioral analysis: This enables detection of sophisticated threats through application and traffic behavior.
- Predictive threat modeling: Emerging attack vectors are anticipated and mitigated.
- Global collaborations: Working together with organizations like INTERPOL, MITRE, and CERTS helps to disrupt cybercrime.
- Threat research: In addition to AI/ML, the data and analysis are also researched and analyzed by the FortiGuard Labs team.

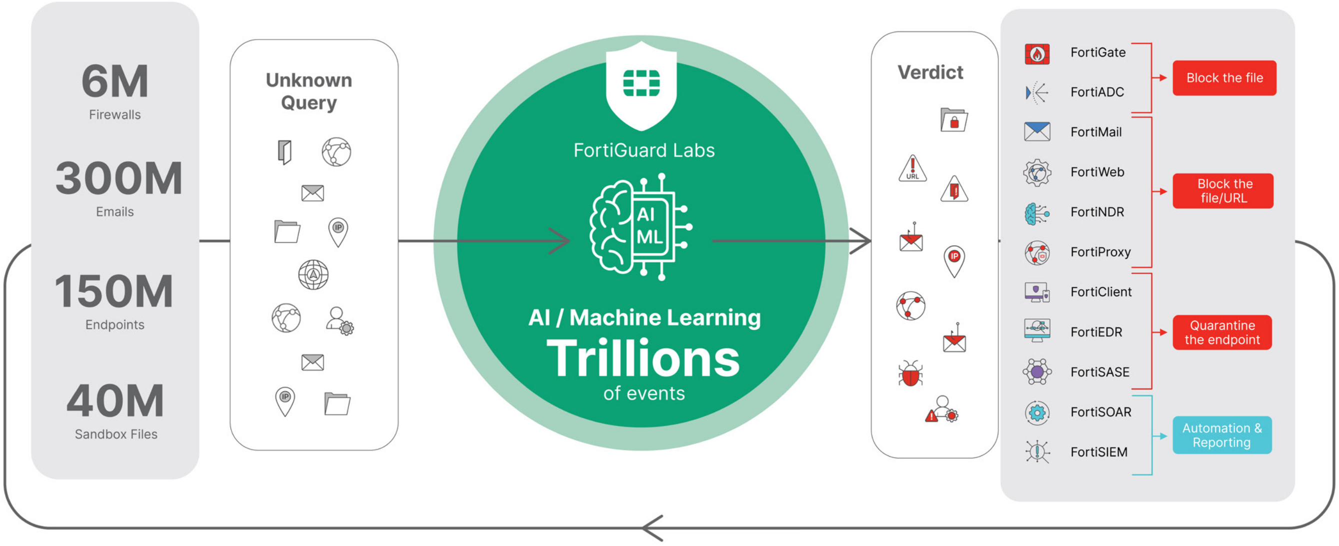


Figure 2: Early detection and response

AI-Powered Fortinet Security Solutions for Public Sector Entities

With Fortinet solutions, AI is not an add-on. It is embedded across our Security Fabric with more than 40 solutions. Fortinet uses a full stack of AI technologies, including AL, ML, deep learning, large language models (LLMs), computer vision, Generative AI, and agentic AI.

Key areas of AI implementation in Fortinet products include:

	Use cases	Products
Threat detection and prevention	Protects against ransomware, malware, phishing, evasive, and sophisticated AI-powered threats in the cloud, networks, and endpoints	FortiGuard IPS, FortiGuard Inline Malware Prevention for real-time inline protection, FortiMail, FortiSandbox for zero-day protection, and FortiEDR for endpoint monitoring
Automated incident response	Automates responses, troubleshooting, prioritizing incidents, and reduces alert fatigue	FortiSOAR for playbook automation, FortiAnalyzer for anomaly detection, FortiAIOps for automating troubleshooting, FortiGate for policy enforcement and protection
AI-powered threat intelligence	Delivers teal-time threat intelligence for real-time protection	FortiGuard AI-Powered Security Services and FortiAnalyzer
Identity and access management (IAM) with impersonation prevention	Defends against malicious insiders and impersonation	FortiToken for MFA and FortiAuthenticator for centralized access control
False positives	Improves the accuracy of threat detection and reduces false positives	FortiGate with FortiGuard Inline Malware Prevention Service, FortiSandbox, FortiEDR, and FortiAnalyzer
Decision-making	Correlates, prioritizes, and addresses security incidents faster with AI to improve and accelerate the decision-making process	FortiSIEM, FortiSOAR, and FortiAnalyzer
Endpoint security	Secures endpoint devices with real-time threat detection	FortiEDR and FortiClient
Automated risk mitigation	Automatically quarantines or blocks threats based on AI analysis	FortiSOAR, FortiGate, and FortiNAC
Network performance	Gains insight into, diagnoses, and optimize network health and performance proactively	FortiAIOps for network health and FortiManager for unified management

Stay Ahead of Threats with Fortinet's AI Capabilities

AI is essential for protecting public sector organizations against today's cyberthreats. FortiAI, integrated with the Fortinet Security Fabric, provides advanced, easy-to-deploy, and regulation-compliant solutions that help organizations bridge the gap between limited resources and increasing risks.

By following best practices and partnering with an experienced vendor like Fortinet, state and local agencies and educational institutions can secure their networks effectively without compromising performance or accessibility.

What is FortiAI?

FortiAI is our unique approach to delivering AI-powered innovations across the Fortinet Security Fabric. Unlike siloed point solutions that apply AI for specific tasks, FortiAI provides intelligent, autonomous AI-driven protection across the Security Fabric. This streamlines operations, and enhances security for AI systems.

[1] Anna Merod, 82% of K-12 schools recently experienced a cyber incident, K-12 Dive, March 10, 2025, https://www.k12dive.com/news/k-12-schools-experienced-cyber-incident-cis/741915.

September 26, 2025 2:22 PM / MKTG-2163-0-0-EN