

SOLUTION BRIEF

Securing Today's Public Sector Networks

Fortinet Improves Efficiency and Protection

Executive Summary

State and local governments and educational institutions (SLED) face several cybersecurity problems: increasing attacks, new vulnerabilities with digitalization, a shortage of skilled security staff, and budget constraints. The Fortinet Security Fabric offers integrated, comprehensive cybersecurity to guide operational and defense strategies for public sector entities of all sizes.

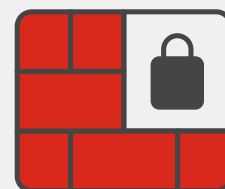
Cybersecurity Designed for the Needs of Modern SLED

State and local governments deal with the same cybersecurity issues facing federal institutions (greater network complexity, an expanding attack surface, a rising number of cyber incidents), but often with smaller operating budgets. Even when funds allow for increased headcount, the persistent global shortage of skilled talent leaves most security teams under-resourced. In the United States alone, there are roughly 500,000 unfilled cybersecurity jobs.² To make matters worse, outdated security infrastructure can inhibit the adoption of new digital tools, such as migrating services to the cloud or deploying smart technologies for increased efficiency.

The potential fallout of a successful cyberattack may include operational disruptions, civilian service outages, loss of sensitive and private information, negative impacts on press and public relations, financial and legal obligations, and even, in extreme cases, endangering public safety.

As their attack surfaces expand, organizations often scramble to cover security gaps using point products that do not communicate with one another. This fragmented approach decreases visibility, delays threat responses, and creates operational inefficiencies. Overlapping software and hardware license costs are also wasteful.

To protect public sector organizations, Fortinet offers a comprehensive cybersecurity solution that helps maximize resources and minimize the attack surface. The Fortinet Security Fabric integrates modern solutions for centralized visibility, network controls, and simplified IT management. This helps public institutions balance available resources while addressing critical use cases for protecting modern networks.



The importance of robust cybersecurity practices at the state and local levels cannot be overstated. Strong cybersecurity measures are essential for safeguarding sensitive information and infrastructure and maintaining public trust and confidence.¹



Government agencies are the third most-targeted sector for ransomware attacks.³

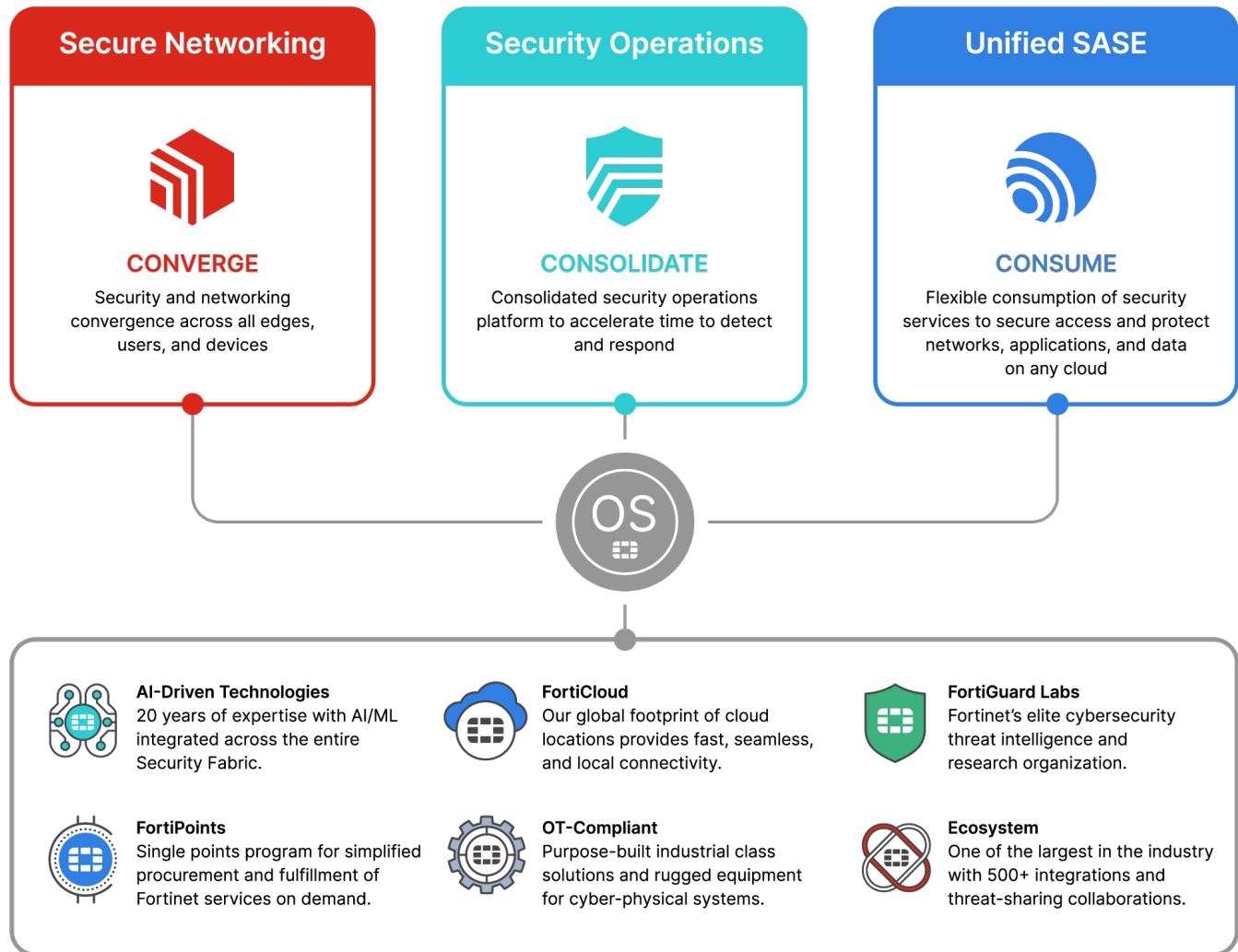


Figure 1: Fortinet Security Fabric

Enable Broad Integration

Fortinet Unified SASE is a single-vendor solution that combines critical networking and security technologies delivered from the cloud. Consolidation and integration help optimize budgets and reduce complexity.

Enforce zero-trust policies: Fortinet combines universal zero-trust network access (ZTNA) and strong vulnerability management with FortiGuard AI-Powered Security Services to ensure consistent policies, endpoint protection, and secure access.

Protect applications: Seamless integration with leading cloud providers and other Fortinet security solutions enables modern application protection and holistic, full-stack cloud security, including context-rich actionable insights and threat detection analytics.

See everything, end to end: Full visibility across users, networks, applications, and the cloud helps institutions understand performance data, respond to incidents, and resolve issues faster.

Transform faster: Fortinet offers unmatched performance, resilience, and scalability to help organizations safely grow while adopting new tools and technologies.

Streamline network management: Centralized management of networking and security policies, efficient cloud security operations, and prioritized risk mitigation can boost IT team productivity, enhance network reliability, and increase ROI.

Streamline Security Operations

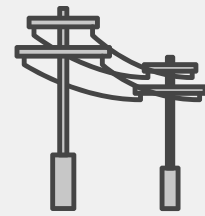
Coordinated cyber and physical security threats are evolving faster than some organizations can manage. The Fortinet Security Fabric supports automation that streamlines security operations and reduces the burden on IT teams. The Fortinet Security Operations platform includes AI-augmented sensors and advanced analytics to help organizations proactively disrupt attacks, investigate incidents, and respond to emerging threats.

Detect threats with AI: Deploying machine learning, deception techniques, and deep learning across domains can uncover attacks humans can't see.

Protect more of the attack surface: Monitoring users, devices, networks, email, applications, cloud services, and the dark web exposes blind spots in defenses.

Integrate and automate: Broad security integration helps instantly share threat intelligence across the organization and automate responses to coordinated attacks.

Investigate and respond: Generative AI assistance is embedded into analyst workflows to improve and accelerate incident management and threat detection.



Cyberattacks against critical infrastructure targets jumped 30% last year, according to recent data from the House Committee on Homeland Security.⁴

Centralize Network Security

State and local governments also handle essential functions like elections, issuance of identification, and law enforcement. Centralizing network security management enhances visibility, provides granular control, and ensures consistent security policies. Fortinet unites best-in-class solutions to help organizations centralize cybersecurity management, saving time and money. Fortinet Secure Networking is the industry's sole converged networking and security platform, empowering AI-driven defense, enhancing productivity, and improving user experience.

Unify firewalls: Fortinet hybrid mesh firewalls unite security and management for greater operational efficiency, stronger security, and comprehensive visibility.

Secure modern wireless networks: FortiGate Next-Generation Firewalls include SD-WAN capabilities, and LTE/5G controls for a secure and enhanced user experience.

Enforce ZTNA universally: FortiGate is the only network security solution in the industry with ZTNA enforcement to enable explicit application access.

Streamline management and automate networking: Centralized management consolidates provisioning and oversight of networking and security products, while network automation improves efficiency and functionality to reduce complexity.

Ensure consistent web security everywhere: Fortinet incorporates web filtering, antivirus, anti-malware, anti-botnet, encryption inspection, data loss prevention, and more to ensure secure internet and private access.

Protect Critical Infrastructure

Government entities may depend on operational technology (OT) systems for critical infrastructure and services like energy grids, water utilities, public transportation, and communication with first responders. As sensitive OT control systems connect to common IT-based systems, opportunistic attacks against public sector OT systems have sharply increased. As an extension of the Security Fabric, the Fortinet OT Security Platform offers efficient and unintrusive security and compliance for OT environments.

Protect operations with purpose-built OT solutions: Many Fortinet security solutions include specialized features explicitly designed for sensitive OT environments.

Stay ahead of risks with threat intelligence: Fortinet actively monitors more than 70 OT protocols and tracks over 500 signatures of known vulnerabilities in OT environments.

Strengthen security with seamless integration: Fortinet's open ecosystem extends the advantages of the Security Fabric to OT. This helps organizations provide advanced end-to-end security across their entire infrastructures.



Empowering Cybersecurity Resilience for Public Institutions

The Fortinet Security Fabric helps public sector organizations deploy and manage modern security and networking technologies efficiently, even with limited resources. In addition, Fortinet solutions meet government compliance requirements such as FISMA, NIST, and CJIS. With a single interface, teams can oversee their entire infrastructure. This makes it easier for education and government organizations to protect modern networks from cyberthreats today and as they evolve in the future.

For more information, visit our website or contact us at sled@fortinet.com.

¹ ["Public Sector Impacts of NIST Cybersecurity Framework 2.0,"](#) Government Technology Insider, May 8, 2024.

² ["Cyber Threat Snapshot,"](#) U.S. House Committee on Homeland Security, November 12, 2024.

³ Ibid.

⁴ ["Cyber Threat Snapshot,"](#) U.S. House Committee on Homeland Security, November 12, 2024.



www.fortinet.com