A GOVERNMENT TECHNOLOGY PAPER

Palo Alto Networks and LevelBlue

A Holistic Approach to Modernizing Network and Remote Workforce Security

Government agencies face an uphill battle in modernizing their legacy security systems while balancing security, cost, and operational efficiency. Many organizations struggle with rigid budget constraints, aging infrastructure, and a growing attack surface—all while needing to support an increasingly remote workforce. Traditional approaches to security are no longer sustainable, leaving agencies vulnerable to advanced threats, compliance risks, and inefficiencies.

Public sector organizations also face unique challenges compared to private enterprises. State and local governments often manage aging IT infrastructure that is not designed for the demands of cloud computing or remote access. Many agencies operate legacy applications that are difficult to secure and maintain, leading to increased vulnerability to ransomware attacks. For example, municipalities managing public utilities frequently rely on outdated security controls, making them prime targets for cybercriminals seeking to disrupt essential services. Law enforcement agencies handling criminal justice data must comply with strict security mandates such as those required for Criminal Justice Information Services (CJIS), but many still struggle to implement modern Zero-Trust frameworks that prevent unauthorized access.

A strategic approach to modernization should include both updates to security technology and guidance from a trusted third-party advisor, such as a managed security services provider (MSSP), who can help to simplify this transition. MSSPs provide technical assessments and planning expertise, strategic support for risk and compliance management, and continuous monitoring, all of which can help agencies navigate the complexities of cybersecurity without overburdening their internal teams.

Accelerate security modernization by partnering with an MSSP that can:

- Assess legacy systems
- Design security migration strategies
- Incorporate automated monitoring
- Promote proactive risk management
- Provide compliance expertise

Converging Network and Security with SASE

Traditional network models are insufficient for modern government agencies that support remote employees, distributed offices, and cloud-based applications. Agencies such as state transportation departments managing traffic control systems and digital tolling infrastructures require high-speed, low-latency network connectivity that integrates security without disruption. Public universities supporting hybrid learning environments need flexible, cloud-based security architectures that protect faculty, students, and research data across multiple locations.

MSSPs can offer secure access service edge (SASE) solutions that unify networking and security by integrating SD-WAN, ZTNA, and real-time threat prevention into a single framework. This approach enables secure, optimized traffic routing, consistent security enforcement, and improved network resilience for government entities. Agencies leveraging managed SASE services benefit from a future-proof security model that adapts to evolving infrastructure needs and cybersecurity threats.

Enhancing Cybersecurity with Next-Generation Firewalls

Sophisticated firewall capabilities help secure data and ensure trusted access to the network. These firewall solutions provide application visibility, policy enforcement, and advanced threat intelligence to prevent data breaches.

MSSPs can provide managed firewall services that include real-time rule adjustments, cross-platform firewall integration, and incident response support to help agencies secure sensitive data while maintaining operational efficiency. By leveraging next-generation firewall capabilities, government entities can improve network visibility, prevent unauthorized access, and enforce compliance-driven security policies tailored to their specific needs.

Security and Cloud Environments

MSSPs simplify hybrid cloud security by providing centralized policy enforcement, end-to-end visibility, and real-time compliance monitoring. With continuous 24/7 monitoring and proactive threat intelligence, government organizations can confidently adopt cloud services while ensuring data integrity, availability, and security.

Beyond securing cloud migrations, MSSPs provide ongoing security management, automated policy enforcement, and compliance auditing, reducing the operational burden on government IT teams. This enables agencies to improve cloud security postures, respond rapidly to emerging threats, and maximize long-term security investments.

Marrying Services and Technology for Better Outcomes

Keith Thomas, Practice Lead for Cybersecurity Operations at LevelBlue, emphasizes the risks of agencies managing modernization efforts alone.

“Going through these kinds of transitions creates new risks and broadens your vulnerability landscape,” Thomas says. “Partnering with an MSSP helps government agencies transition from legacy systems while maintaining a strong, comprehensive, and proactive security posture.”

Agencies such as state transportation departments managing traffic control systems and digital tolling infrastructures require high-speed, low-latency network connectivity that integrates security without disruption.

> **One of our customers was on an MPLS network, and auditors told them they lacked the security necessary to meet PCI requirements across their 1,800 locations. They had 18 months to correct the issue. We built and rolled out a full SASE solution—integrating SD-WAN and Security Service Edge services—to all 1,800 locations, helping them achieve PCI compliance within 12 months."**
>
> — **Keith Thomas,** Practice Lead for Cybersecurity Operations, LevelBlue

LevelBlue has a longstanding history of managing public sector security environments and working with government agencies at the federal, state, and local levels to navigate complex cybersecurity challenges. With more than three decades of experience providing managed security services tailored to public sector needs, LevelBlue understands the compliance requirements, operational constraints, and evolving threat landscape that agencies face daily.

Through its deep and longstanding partnership with Palo Alto Networks, LevelBlue enables agencies to leverage best-in-class security technology alongside expert, hands-on managed services. This collaboration ensures that agencies benefit from deeply integrated security solutions, including Prisma SASE, ZTNA, and next-generation firewall capabilities, tailored specifically for public sector needs.

Palo Alto Networks provides the cutting-edge security technology that agencies require to protect their networks, while LevelBlue delivers the operational and advisory expertise to implement, manage, and optimize these solutions. This partnership helps agencies reduce complexity, strengthen security postures, and maintain continuous compliance with government regulations, ensuring mission-critical systems remain protected against emerging threats.

A Strategic Approach to Security Modernization

Government agencies must modernize their security infrastructure to keep pace with the digital transformation of public services. A holistic, managed approach, guided by LevelBlue and Palo Alto Networks, ensures a secure and efficient transformation. By leveraging their combined expertise, public sector organizations can navigate the complexity of security modernization, optimize resources, and establish a resilient, future-ready security posture—ensuring their mission-critical operations remain protected in an ever-evolving threat landscape.

Government agencies must modernize their security infrastructure to keep pace with the digital transformation of public services.

This piece was written and produced by the Government Technology Content Studio, with information and input from Palo Alto Networks and LevelBlue.

Produced by Government Technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

www.govtech.com

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyber threats so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

At Palo Alto Networks, we're committed to bringing together the very best people in service of our mission, so we're also proud to be the cybersecurity workplace of choice, recognized among Newsweek's Most Loved Workplaces (2023, 2022, 2021), with a score of 100 on the Disability Equality Index (2023, 2022) and HRC Best Places for LGBTQ Equality (2022).

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it. We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision-making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk so you can focus on your business. Cybersecurity. Simplified.

Contact us to learn more or speak with your LevelBlue sales representative.

ADOBESTOCK/AI GENERATED