Secure Mobility Modernization for State & Local governments and Education Organizations

Equipping state & local government and educational employees with the tools they need to work in the field is essential for effective public service delivery. In today's dynamic work environment, the ability to connect teams, whether at a central office, a remote site or in the community, is key to serving constituents well. But managing the devices that make mobile work possible can be challenging.

Just one lost device or unsecured connection can have a serious impact on your organization's network and the sensitive data it holds. Ivanti Neurons for Mobile Device Management (MDM), Ivanti Neurons Platform and Ivanti Mobile Threat Defense work together to give state local and education (SLED) organizations a single, seamless platform for managing and securing mobile devices regardless of location.

Manage devices everywhere with Ivanti Neurons for MDM

As an endpoint-agnostic solution, Ivanti Neurons for MDM lets agencies manage iPhones, iPads, Macs, Android devices, Windows laptops, Chromebooks and PCs, Zebra devices, Oculus headsets and more — in one unified platform.

- **StateRAMP-aligned compliance:** Ivanti Neurons for MDM supports StateRAMP compliance requirements, helping your organization meet state and jurisdiction-specific security standards. The Ivanti Neurons for MDM is FedRAMP Moderate Authorized and "in process" for FedRAMP High Authorization.
- **Comprehensive device management:** Secure and manage your organization's entire fleet of devices through a centralized platform that streamlines operations and enhances security posture.
- **Advanced security controls:** Implement robust security measures, including policy enforcement, strict access controls and government-grade encryption to protect sensitive constituent and agency data across all devices.
- **Secure bring-your-own-device (BYOD) implementation:** Deploy BYOD programs with advanced security features, including data segregation, remote wiping capabilities and self-service device enrollment.
- **Simplified administration:** Empower lean IT teams with an intuitive management console while providing employees with secure self-service options to boost enrollment and lower administrative burden.
- **Operational efficiency:** Reduce IT workload through automated device provisioning, configuration management and security updates that align with state & local IT modernization goals.
- **Multifactor authentication enforcement:** Ensure strong multi-factor authentication is applied across all devices used for government work, protecting access to sensitive systems and constituent data.

Ivanti Neurons Platform

Ivanti Neurons Platform is a cloud-based platform designed for coordinated outcomes across IT and Security operations. The recommended starting point is Autonomous Endpoint Management (AEM) because it turns visibility into action quickly. Customers use AEM to reduce manual work through automation, bots and self-healing, improving endpoint stability and freeing IT and security teams to focus on higher value work. Ivanti Neurons Platform coordinates people, automation and AI through common data, governance and workflows, so capabilities can scale consistently across IT and Security.

- **Proactive AI capabilities:**
  Delivered through a unified agentic framework, the Ivanti Neurons Platform embeds AI-driven automation at the core of platform workflows. AI helps predict issues, guide prioritization, automate action and continuously learn from real operational data to improve outcomes.
- **Invisible, automated security:**
  Reduces risk and supports continuous resilience without disrupting day-to-day IT operations.
- **Unified and Actionable Data:**
  A cloud native data foundation that enables IT and Security teams to share data in real time without complexity. With native integrations, teams can connect AEM, Exposure Management, IT Service Management, Network Security and third-party tools, creating a continuously updated, lifecycle-aware data foundation for informed decision making and automation.
- **Flexible open ecosystem:**
  Large integration networks, vendor-agnostics and flexible migration options help you future-proof and innovate faster.
- **StateRAMP-aligned compliance:**
  Supports StateRAMP compliance requirements, helping your organization meet state and jurisdiction-specific security standards. The Ivanti Neurons Platform is “in process” for FedRAMP High Authorization.

Ivanti Mobile Threat Defense

Ivanti Mobile Threat Defense adds continuous layers of security to each device, detecting and remediating threats in real time. This real-time threat intelligence gives state & local agencies and education organizations visibility into threats across all devices. Ivanti Mobile Threat Defense helps IT and Security teams combat risks and make informed decisions to protect their networks and the constituents they serve.

- **Comprehensive security architecture:** Leverage real-time malware detection, network threat monitoring and sophisticated application security controls and behavior monitoring.
- **Continuous protection protocol:** Maintain robust security measures during network disruptions, ensuring field personnel — including public safety officers, building inspectors and social workers — remain protected even when offline.
- **Machine learning (ML) powered threat detection:** Harness ML to automatically identify and mitigate mobile security threats before they impact your agency's operations or expose constituent data.
- **Configure devices for compliance:** Set device configurations to automatically enforce the Criminal Justice Information Services (CJIS), Family Educational Rights and Privacy Act (FERPA), and agency-specific security requirements across all mobile devices, while automatically maintaining detailed compliance documentation for audits and oversight reviews.

Ivanti Neurons for MDM, Ivanti Neurons Platform and Ivanti Mobile Threat Defense: Better together

Ivanti Neurons for MDM, Ivanti Neurons Platform and Ivanti Mobile Threat Defense combine to create a stronger solution for SLED IT teams looking to automate managing and securing a wide variety of devices at scale. Together, they deliver a comprehensive mobile security solution that streamlines operations while maximizing protection.

Use cases

- **Device deployment and onboarding:** Ivanti Neurons for MDM allows organizations to achieve near 100% adoption of the solution. Device setup and configuration are quick and efficient, and Ivanti Mobile Threat Defense works alongside it to ensure each device meets required security standards from day one. Deployment occurs without end-user interaction, so there are no “accept” or “allow” buttons to click.
- **Lost device protection:** Ivanti Neurons for MDM provides remote data wiping capabilities for lost or stolen devices, while Ivanti Mobile Threat Defense provides critical protection for field workers handling sensitive case files, law enforcement data and personally identifiable information (PII).
- **Protection on personal devices:** Many agencies already use Ivanti Neurons for MDM to enable staff to use their personal devices. Ivanti Mobile Threat Defense adds enhanced threat detection, protecting critical agency, student and constituent data.
- **AI that works for you:** The Ivanti Neurons Platform connects insight to action by assessing issues with AI and resolving them through governed automation. AI in the Ivanti Neurons Platform is grounded in trusted, lifecycle-aware platform context provided by the platform’s operational systems of record for assets, endpoints and configuration state across IT and Security.
- **Application management:** Ivanti Neurons for MDM provides centralized control over application distribution and permissions, and Ivanti Mobile Threat Defense safeguards devices by monitoring applications forsecurity risks and suspicious behavior.
- **Zero Trust adherence:** Conditional access controls in Ivanti Neurons for MDM let agencies fine-tune access control inputs, such as device, app, network, geographic region and more. In the event of improper access, Ivanti Mobile Threat Defense adds additional layers of protection through threat detection and remediation.
- Visibility across IT and Security: The Ivanti Neurons Platform aggregates and normalizes data from devices, service workflows and security telemetry into actionable insights. Gain real-time visibility and control across your entire IT ecosystem to strengthen performance and compliance.

SLED organizations need IT solutions that are both powerful and secure. The combination of Ivanti Neurons for MDM, Ivanti Neurons Platform and Ivanti Mobile Threat Defense delivers a secure-by-design infrastructure that helps agencies outpace emerging threats, increase employee productivity and improve constituent service delivery, while maximizing efficiency and cost avoidance. With Ivanti, state & local agencies and education organizations can confidently embrace IT mobility, knowing their data and devices are protected.

For more information about Ivanti's modern state & local government IT solutions, visit **ivanti.com/industries/state-local-government**

or more information about Ivanti's innovative educational IT solutions, visit **ivanti.com/industries/education**

ivanti

For more information, or to contact Ivanti, please visit ivanti.com.