



# Enhancing Public Sector Mobile Security:

Integrating Ivanti Mobile Device Management (MDM)  
and Lookout Mobile Threat Defense (MTD)



The Ivanti Neurons for MDM and MTD solutions give government organizations full control and visibility over their mobile devices, apps and cloud services, reducing the risk of security breaches.

### **Comprehensive Mobile Threat Defense**

Powered by Lookout Mobile Endpoint Security, Ivanti MTD provides advanced protection against mobile threats such as malware, phishing attacks and device vulnerabilities. It uses machine learning and threat intelligence to identify and block threats in real time.

Ivanti MDM complements Ivanti MTD's security features by enabling secure access to data and apps on any device across your organization, ensuring that only authorized users, devices, apps and services can access agency resources. This can help users work with the best endpoint devices for the job while preventing users from installing malicious apps or accessing risky websites.

Despite warnings from IT, an agency staff member, contractor, teacher or administrator might inadvertently click on a malicious link in a phishing email or text message on their phone. Ivanti Mobile Threat Defense would detect the threat and block the website, while Ivanti Mobile Device Management could prevent the employee from installing any malware that they download from the link.

### **Unified endpoint management and security**

By integrating the two solutions, you can manage and secure all your devices (laptops, desktops,

mobile devices) from a single platform. This simplifies administration and reduces complexity for IT teams.

You can also gain insights into the security posture of all your devices from a single interface. This helps identify and address potential risks more quickly and effectively.

For instance, you can use the integrated platform to see which devices are out of date on security updates, have non-compliant apps installed or are connected to risky Wi-Fi networks. You can then use this information to remediate these risks, resolving issues and security vulnerabilities proactively, predictably and automatically. No programming skills are required to automate common IT use cases beyond traditional Unified Endpoint Management.

### **Improved visibility and control**

With both solutions working together, you gain a comprehensive view of your mobile device security posture. This includes information about the devices themselves, the apps that are installed on them and the security threats that they are exposed to.

You can use this information to make informed decisions about how to manage and secure your mobile devices while preserving a great end-user experience. Ivanti Neurons for MDM provides the simplest onboarding and superior on-device experience, which improves user productivity.

For example, you can use combined visibility to identify which agency departments or user groups are most at risk from mobile threats. This information can then be used to target security awareness training or implement stricter security policies for these groups.

### **Improved visibility and control**

The integration between Lookout and Ivanti can streamline the deployment and management of mobile security solutions. This can save IT and compliance teams time and resources.

For example, you can use the integrated platform to automatically deploy Lookout Mobile Endpoint Security to all your mobile devices. Compliance is achieved automatically, without requiring end-user action. Administrators can also use the platform to manage security policies and settings for all your devices from a single place.

Security standards and certifications\*

- FedRAMP Moderate Authority
- CSA STAR
- SOC 2 Type II

\*Additional information on certifications can be found at: [ivanti.com/resources/security-compliance](https://www.ivanti.com/resources/security-compliance)


Learn more about how Ivanti can help you supercharge your MDM project: Visit [ivanti.com](https://www.ivanti.com)

## About Ivanti

Ivanti elevates and secures Everywhere Work so that people and organizations can thrive. We make technology work for people, not the other way around. Today's employees use a wide range of corporate and personal devices to access IT applications and data over multiple networks to stay productive, wherever and however they work. Ivanti is the only technology company that finds, manages and protects every IT asset and endpoint in an organization. Over 40,000 customers, including 88 of the Fortune 100, have chosen Ivanti to help them deliver an excellent digital employee experience and improve IT and security team productivity and efficiency. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit [ivanti.com](https://www.ivanti.com)

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".

**ivanti**

A vertical bar on the right side of the page, transitioning from red at the top to orange at the bottom.

For more information, or to contact Ivanti, please visit [ivanti.com](https://www.ivanti.com).