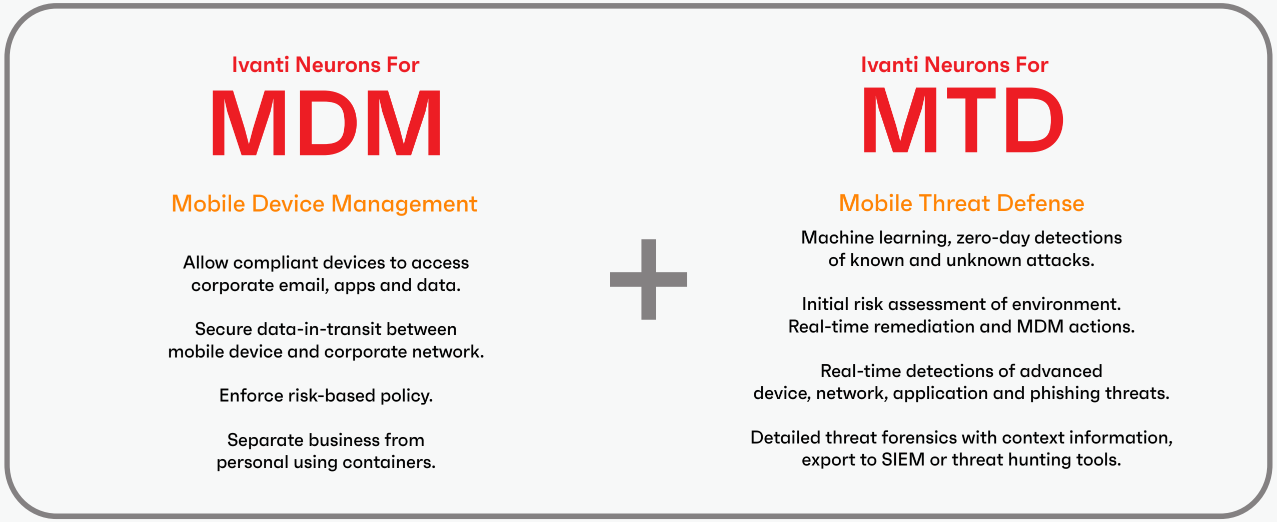
DATASHEET

Manage and secure your devices with Ivanti Mobile Security Solutions

Ivanti Neurons for Mobile Device Management and Ivanti Neurons for Mobile Threat Defense together offer comprehensive management and security features for all endpoints. They provide a secure environment for accessing and protecting data while ensuring that only authorized users, devices, apps, and services can access business resources. With comprehensive protection at every level, including device, network, and application, the solution defends against phishing attempts and prevents attacks before they can do harm.



Ivanti Neurons For
MDM
Mobile Device Management

Allow compliant devices to access corporate email, apps and data.

Secure data-in-transit between mobile device and corporate network.

Enforce risk-based policy.

Separate business from personal using containers.

+

Ivanti Neurons For
MTD
Mobile Threat Defense

Machine learning, zero-day detections of known and unknown attacks.

Initial risk assessment of environment. Real-time remediation and MDM actions.

Real-time detections of advanced device, network, application and phishing threats.

Detailed threat forensics with context information, export to SIEM or threat hunting tools.

The integrated solution provides IT security administrators with a way to safely enable both corporate owned devices and Bring Your Own Device (BYOD) and strike the balance between empowering mobile employees to be more productive with the device of their choice, while at the same time securing mobile devices and the organization against advanced threats.

With Ivanti's powerful endpoint protection solution, organizations can easily achieve real-time visibility into mobile risk, stay ahead of evolving mobile threats, and maintain regulatory compliance. The single Ivanti Go mobile client streamlines device enrollment and simplifies the deployment of enforcement policies, making it a comprehensive and elegant solution for organizations seeking to protect their endpoints.

Key benefits

Comprehensive device management

Ivanti Neurons for MDM provides organizations with a comprehensive endpoint security solution for their business that can manage and secure endpoints running iOS, iPadOS, Mac, Android, Windows, and Chrome operating systems. With Ivanti AppStation, business apps can be secured on contractor and employee devices without requiring device management, while easy on-boarding is achieved through full integrations with Apple Business Manager (ABM), Google Zero-Touch Enrollment and Windows AutoPilot. Furthermore, Apps@Work, an enterprise app storefront, streamlines app distribution and configuration, while iOS Managed Apps and Android Enterprise provide easy configuration of app-level settings and security policies..

Complete mobile device security

Ivanti Sentry provides a secure email gateway that manages, encrypts, and secures traffic between the mobile endpoint and back-end enterprise. In addition, App Threat Protection safeguards your apps from malicious threats such as phishing, ransomware, surveillance-ware, click-fraud, rootkits, jailbreaks and riskware. Device Threat Protection enforces policies to keep your devices secure with passcode protection, device encryption, and jailbreak detection, while Network Threat Protection ensures network safety from potential threats such as MITM attacks on both cellular and Wi-Fi networks, rogue wi-fi access points, ARP spoofing, and SSL attacks.

Data protection

Organizations can be at risk when employees use personal devices for work, as malicious or potentially harmful applications can be installed without proper security policies in place. Even seemingly harmless apps can expose sensitive corporate data through permissions abuse, which can be difficult for users to identify due to security fatigue on their devices. Such apps are often referred to as “leaky,” meaning that they can potentially expose sensitive data, endangering networks, user data, and business data.

Improve your organization’s security posture

Ivanti Neurons for MTD helps organizations improve their security posture by providing automatic scanning of new app installations for potential threats, ranging from exploits to vulnerabilities. This ensures that employees’ personal devices are not unknowingly introducing risks into the organization’s network. With MTD’s ability to send alerts to Ivanti Neurons for MDM, quick action can be taken to address any detected threat, enabling a swift and effective response to security threats. By working together to protect the organization’s assets, MDM and MTD help create a safe and secure Everywhere Work environment that instills employee confidence in their ability to work productively from anywhere.

Achieve 100% user adoption

Ivanti Neurons for MDM offers a comprehensive solution for managing and securing all devices, both corporate and BYOD, with ease. This streamlined approach to deployment ensures that security measures can be implemented without requiring user intervention, allowing organizations to focus on other priorities. By using the Ivanti Go app, administrators can easily and efficiently deploy Ivanti Neurons for MTD, ensuring that all users are fully protected from the potential threats of mobile devices. Achieving 100% user adoption becomes a simple task with this powerful solution.

Regulatory compliance

NIST 800.53

Special Publication 800-53, Revision 4, provides a more holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate – contributing to systems that are more resilient in the face of cyberattacks and other threats. Ivanti Neurons for MTD analyzes network connections and can accurately identify man-in-the-middle attacks, host certificate hijacking, hijacked SSL traffic, and TLS protocol downgrades.

NIST 800.124

NIST Special Publication 800-124 Rev. 2 section 4.2.3 states: "MTD systems are designed to detect the presence of malicious apps, network-based attacks, improper configurations and known vulnerabilities in mobile apps or the mobile OS itself." Ivanti Neurons for MTD provides comprehensive protection against the entire spectrum of mobile risk, which includes threats, vulnerabilities, and configuration risks across the four primary threat vectors - phishing, app, device, and network threats. In addition, the Ivanti platform uses artificial intelligence to analyze data from nearly 200 million devices and over 100 million apps to protect you from the full spectrum of mobile risk.

General Data Protection Regulation (GDPR)

GDPR offers a comprehensive framework for protecting EU citizens' data privacy and ensuring security by imposing strict procedural and technical requirements. Complying with GDPR necessitates adherence to data protection principles, such as data minimization, accuracy, storage limitation, and secure data processing. Ivanti provides essential security features that offer in-depth visibility into various mobile threats, vulnerabilities, and risky behaviors jeopardizing data security. With policy-based protection, Ivanti addresses mobile risks at scale, enabling organizations to establish policies for timely threat remediation, minimizing data-leak risks, and upholding user privacy.

Capability	Ivanti Neurons for MDM	Ivanti Neurons for MTD
Support for iOS and Android devices.	✓	✓
Provide initial vulnerability risk posture for OS/device, network, apps and phishing.	✓	✓
Detect if device has proper physical security enabled (pin code, device-level encryption).	✓ Basic	✓
Detect if device is jailbroken/rooted by user (using known hash values and file location).	✓	✓
Provide forensics into the tools and techniques of a device compromise or attack.		✓
Detect OS/Kernel and USB exploitations, profile/configuration changes, system tampering.		✓
Detect elevation of privileges attacks.		✓
Detect network attacks (man-in-the-middle, rogue Wi-Fi and cellular networks).		✓
Detect SSL stripping, fake SSL, attempts to intercept SSL traffic.		✓
Detect attackers conducting reconnaissance scans.		✓
Detect phishing, smishing, URL phishing, tiny URL, etc.		✓
Corporate app delivery and removal.	✓	
Secure corporate document sharing.	✓	
Secure line-of-business apps.	✓	

Capability	Ivanti Neurons for MDM	Ivanti Neurons for MTD
Detect malicious apps, known and unknown malware, dynamic threats using download and execute.		✓
Revoke access to non-compliant mobile devices.	✓	
Provide detailed mobile threat forensics.		✓
Enforce risk-based policy including lock or selective wipe for compromised devices.	✓	✓
Provide instant remediation once an attack is detected.		✓
Scan in-house developed apps for privacy and security concerns/risks.		✓
Receive privacy and security information from apps that have been installed on the device.		✓

Threat detection	Ivanti Neurons for MDM	Ivanti Neurons for MTD
Host-related critical and elevated threats		
Android device – possible tampering		✓
Abnormal process		✓
Developer options		✓
Device encryption	✓	✓
Device PIN	✓	✓

Threat detection	**Ivanti Neurons for MDM**	**Ivanti Neurons for MTD**
Host-related critical and elevated threats		
Device jailbroken / rooted MDM jailbreak/root detections are simplistic and easy to bypass. In addition, MDM does not provide any forensic visibility into the tools and techniques used in the attack.	✓	✓
Elevation of privileges		✓
File system changed		✓
Side loaded apps		✓
SE Linux disabled		✓
System tampering This is an advanced compromise of the device that may or may not use the additional step of jailbreaking or rooting the device.		✓
Suspicious iOS app		✓
Suspicious Android app		✓
Untrusted profile		✓
USB debug mode on		✓
Vulnerable Android version		✓
Vulnerable iOS version		✓

Phishing detection and prevention		
Always-on detection and blocking of phishing URLs.		✓
Time-of-click phishing detection stops phishing attacks in-motion.		✓
Network Related Critical & Elevated Threats		
MiTM		✓
MiTM - ARP		✓
MiTM – ICMP REDIRCT		✓
MiTM – SSL strip		✓
MiTM – fake SSL strip		✓
SSL/TLS downgrade		✓

About Ivanti

Ivanti makes the Everywhere Work possible. In the Everywhere Work, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 78 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work.
For more information, visit ivanti.com

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com