



Mobile Device Manager: Defense when and where you need it.

The mobile explosion

iPhones, iPads, Androids, BlackBerries...Devices of all types are flying off the shelves and landing in your workplace. Employees are bringing them to the office in record numbers and expecting you to manage them.

Beyond Consumerization of IT, lines of business are getting in on the action: They're developing apps for their favorite devices, whether for iPad-toting CXOs, ruggedized tablet-carrying warehouse operators, or smartphone-equipped sales road warriors.

The enterprise in your pocket

Employees slip your enterprise into their pocket every time they leave the office with a mobile device. From their devices they access the corporate network, business applications, and your most sensitive enterprise data whenever and wherever they need to. No one knows better than you how this can open your enterprise to risk. Jailbroken devices, unenforceable passcode policies, and non-compliant mobile apps are just a few problems that can jeopardize sensitive data, expose the enterprise to mobile threats, or push you out of compliance with corporate or regulatory policies, risking hefty penalties.

nForce Mobile Device Manager

nForce is the leader in secure mobile device management, with real-time defense across devices, apps, and the network, and enterprise-grade, on-premise and cloud secure mobile device management offerings. nForce Mobile Device Manager, our on-premise solution lets you secure and manage the most comprehensive array of mobile devices, gain visibility into and control over mobile apps, and shield the corporate network from mobile threats.

Mobile device security

Configure and set static and dynamic, context-aware policies based on role, device type, and whether the device is company-issued or personally-owned. Maintain a complete inventory of all authorized devices, discover and block rogue or non-compliant devices, and keep corporate data secure by locking and wiping them in the event of loss or theft. And when employees leave, decommission and selectively wipe the devices, removing corporate apps and data while leaving personal data and content intact.

Application security

Blacklist, whitelist, and block mobile apps that negatively affect employee productivity or break with company

policy. Offer secure access to—and all communications between—employees and enterprise applications with mobile app tunnels. Set dynamic, context-aware application policies, such as blocking employee access to select apps during specified times (e.g., no Facebook during work hours).

Network security

Gain visibility into mobile network traffic and behavior by device, user, system, or application, as well as insight into insider threats such as unauthorized access, leakage of sensitive corporate data, and mobile compliance violations. Protect the corporate network from mobile and insider threats through integration with security information and event management systems. Monitor device and mobility performance and troubleshoot issues to keep employees productive.

Truly enterprise-grade

Scale without fear! Our scale-out architecture and high availability enable us to support some of the largest production deployments in the world, with more than 65,000 devices for a single customer. With a failover strategy that includes active-active clustering and server and data redundancy throughout the system, nForce Mobile Device Manager has you covered.

nForce Features:

STAGE	FEATURE	BENEFIT	ADVANCED	PREMIUM	
Configure	Enable corporate email	<ul style="list-style-type: none"> Configure devices in an enterprise, policy-based way 	●	●	
	Set Wi-Fi, VPN, proxy server, and access point node	<ul style="list-style-type: none"> Enforce compliance with SOX, HIPAA and corporate data and system access policies 	●	●	
	Disable features and apps such as camera, YouTube, Safari, or iTunes		●	●	
	Disallow multi-player gaming or in-app purchases.		●	●	
	Define and enforce OS and patch levels		●	●	
Provision	Provision devices rapidly	<ul style="list-style-type: none"> Rapidly activate thousands of users 	●	●	
	Encrypt profiles	<ul style="list-style-type: none"> Maintain consistency across all deployed devices, with auditing and reporting 	●	●	
	Lock profiles		●	●	
	Distribute apps via the enterprise app store		●	●	
Secure	Enforce passcodes	<ul style="list-style-type: none"> Protect corporate data in event of device loss/theft 	●	●	
	Integrate with two-factor authentication	<ul style="list-style-type: none"> Claw back corporate data after employee departure 	●	●	
	Locate device	<ul style="list-style-type: none"> Prevent unauthorized access to corporate network and business applications 	●	●	
	Lock device	<ul style="list-style-type: none"> Protect corporate network from mobile threats 	●	●	
	Auto-lock device after inactivity period	<ul style="list-style-type: none"> Disable or limit access to device functions or applications based on context 	●	●	
	Wipe full device	<ul style="list-style-type: none"> Gain visibility into mobile device usage and access; integrate into popular SIEM applications 	●	●	
	Selectively wipe device	<ul style="list-style-type: none"> Gain visibility into mobile device usage and access; integrate into popular SIEM applications 	●	●	
	Auto-wipe device after failed login attempts	<ul style="list-style-type: none"> Enable secure file synchronization and provide content- and context-aware mobile DLP that is integrated with leading enterprise collaboration software 	●	●	
	Ascertain passcode history	<ul style="list-style-type: none"> Enable secure file synchronization and provide content- and context-aware mobile DLP that is integrated with leading enterprise collaboration software 	●	●	
	Block jailbroken or rooted devices from corporate network			●	
	Enable mobile app tunnels				●
	Use Secure Mobile Gateway to block unauthorized or non-compliant devices				●
	Use secure mobile gateway to perform app blacklisting/whitelisting				●
	Gain actionable mobile security intelligence and integrate with SIEM				●
	Set dynamic defense context-aware policies				●
Protect sensitive data with Enterprise Mobile DLP*				●	
Track	Detect user, device, system, or service issues by reporting and alerting on statistics, including OS, carrier, phone number, storage, applications, encryption, profiles, battery, and jailbroken status	<ul style="list-style-type: none"> Reduce wireless expenses by optimizing service plans against traveling employees Negotiate wireless service contracts with better visibility and more intelligence 	●	●	
	Maintain inventory of asset details, including employee-owned vs. company-issued, hardware version, SIM ID, IMEI and serial number	<ul style="list-style-type: none"> Protect corporate data and potential device misuse by retiring inactive devices+C9 	●	●	
	Track service details on roaming, location, user inactivity, and expenses		●	●	