Use case

Your devices, your data—your rules

Help secure the devices your organization depends on with mobile device management.

With more devices, there's a lot more to manage.

What happens when work takes place nearly everywhere? Employees carry sensitive data in their pockets. Every mobile device – whether corporate- or employee-owned – is a potential entry point for cybercriminals. Leaving these devices unmanaged can create blind spots and security gaps that can expose your organization to cyberthreats.

Challenges

The lack of a centralized mobile device platform can make it hard to enforce security policies, such as mandatory updates, complex passwords and secure configurations, across a diverse range of devices.

- **Inconsistent device management**
  Different regions and user groups often apply varying device security controls, creating gaps that attackers can exploit.
- **Mobile artificial intelligence (AI) exposure**
  The rapid adoption of generative AI (genAI) apps on mobile devices can increase the risk of sensitive data leaks, unauthorized sharing and exploitation by malicious actors.
- **Compromised devices**
  A single infected device can serve as a gateway into the network, leading to widespread breaches if not quickly contained.
- **Bring your own device environment**
  Use of personal devices to access company information adds risk and requires additional protections.

From blind spots to full visibility

Mobile device management (MDM) can help give your team the ability to control and manage your mobile devices from a central platform. It also helps ensure compliance with company security policies, regardless of where a device is used. With MDM, you can safeguard data, apply updates and quickly respond to lost devices or emerging threats.

Take a closer look at the data.

#1
Mobile device management is the first of the eight recommended best practices for mobile security.[1]

63%
of organizations that considered and rejected MDM experienced lost data in a security incident.[2]

70%
of mobile devices impacted by a cyberattack are personal, not corporate-issued.[3]

59%
of MDM users surveyed have defined and enforced genAI usage policies; that percentage drops to 45% among respondents that do not use MDM.[4]

71%
of MDM users surveyed automatically revoke mobile access privileges based on risk signals, compared with 57% of respondents that do not use MDM.[5]

verizon business

Solutions and benefits

A robust MDM solution is critical to help enhance policy enforcement and simplify device and software management. By gaining greater control over your devices, you can transform the way you protect your business from mobile threats.

Instant lockdown	Secure or wipe lost, stolen or compromised devices in real time to prevent unauthorized access, data theft and potential breaches.
Operational resilience	Strengthen organizational defenses by giving IT centralized control to enforce encryption, updates and compliance across all devices.
Ongoing security	Automate the onboarding and removal of devices for employees and contractors, ensuring these assets are protected from day one.
Access control	Block noncompliant or insecure devices from connecting to critical systems, reducing the risk of disruptions, breaches and regulatory violations.
AUP compliance	Establish and actively enforce an acceptable use policy (AUP) to help ensure all connected devices are used securely, comply with regulations and support a productive work environment.

What's the cost of a cybersecurity breach?

$6.3B+

In 2024 alone, more than $6.3 billion was transferred in Business Email Compromise scams.[6]

$115K

The median amount paid to ransomware groups in 2024 was a costly $115,000.[7]

Proven mobile security intelligence

The Verizon 2025 Mobile Security Index delivers an overview of the evolving mobile threat landscape. It transforms critical insights into actionable security strategies that let you benchmark your defenses, spot emerging risks and strengthen your mobile security posture. Get the report at verizon.com/mobilesecurityindex.

Why Verizon

Managing a mobile workforce is more complex than ever – but we can help make it simple. Verizon offers industry-leading MDM solutions to help you secure mobile devices connected to your network. Our portfolio includes:

- **Verizon Mobile Device Management:** Helps you manage and secure your mobile devices with remote, touchless onboarding and automatic device enrollment
- **Business Mobile Secure Plus:** Helps simplify mobile security with a single, easy-to-use unified endpoint management solution that combines MDM and mobile threat defense capabilities, helping safeguard your smartphones and tablets while keeping your teams productive

Let's build your mobile defense plan.

We're here to help your organization take control of your mobile devices. Contact your Verizon Account Representative, who can help you strengthen your mobile security defenses.

1. "2025 Mobile Security Index," Verizon, Oct 22, 2025. https://www.verizon.com/business/resources/reports/2025-mobile-security-index.pdf
2. Ibid.
3. Ibid.
4. Ibid.
5. Ibid.
6. "2025 Data Breach Investigations Report," Verizon, Apr 21, 2025. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf
7. Ibid.

verizon business