

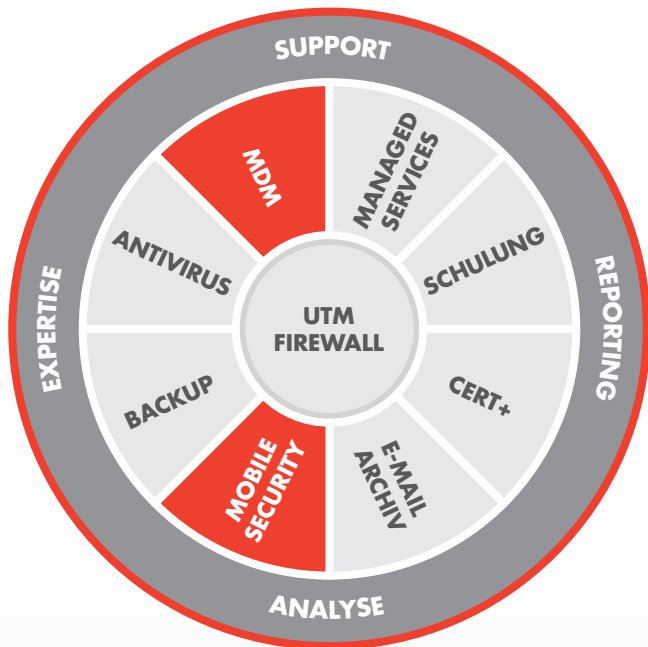
• @ • SECUREPOINT

SECUREPOINT MOBILE SECURITY

VIRUS PROTECTION AND MOBILE DEVICE MANAGEMENT

Securepoint Mobile Security combines powerful mobile device management (MDM) with the security of cloud-based Securepoint NextGen UTM firewalls.





SECUREPOINT UNIFIED SECURITY

Unified Security means ensuring network security at all levels. Just as in a car, where headrest, seatbelt, and crumple zone work together to achieve maximum safety, individually effective IT security measures combine to form a robust security infrastructure.

Take a comprehensive approach to IT security with Unified Security by Securepoint.

Surf safely

Keeps mobile devices secure on the go as they are on the corporate network, removing malicious code, blocking dangerous URLs, and enforcing corporate policies.

Encrypted connections only

When a mobile device leaves the secure corporate WLAN, it establishes an encrypted connection to geo-redundant cloud firewalls and is protected in unsecured/open WLANs.

Perfect combination for mobile security

More and more smartphones, tablets and notebooks are being used in the classroom or as mobile workstations. This often undermines all the protective mechanisms of a secure network (UTM firewall, network virus scanner, etc.) as well as corporate policies. In the worst case, if employees leave the corporate network with mobile devices, companies lose complete control.

Device Protection - Cloud Firewall

As soon as a mobile device leaves the company's secure WLAN, all data traffic is encrypted (VPN) and redirected to highly available Securepoint NextGen cloud firewall clusters. This ensures that communication and surfing remain secure even in open and insecure WLANs.



Mobile Device Management

For schools, businesses, and government agencies: Conveniently manage mobile devices via a central web interface and control apps, functions and user profiles.

Easy startup

The cloud solution is ready for immediate use and activated in just a few minutes. The enrollment process for individual devices is deliberately kept simple and intuitive.

The port filter settings implement the policies that apply to a company's mobile devices. The integrated web security additionally prevents access to dangerous websites, malicious code, etc. already in the data stream, regardless of the device.

Securepoint Mobile Security provides true security for Android and iOS/iPadOS devices as well.

MDM for enterprises, schools and government agencies

Settings and restrictions can be combined, defined and transferred to the devices via the Mobile Device Management web interface. Finding, locking and deleting lost devices is also possible. Apps can be easily installed, deleted or blocked. Depending on the device type, deep restrictions can be defined (e.g. for camera, messenger, app store, etc.).

The implemented restrictions per device can be viewed in the admin portal. The solution is available for Android and iOS/ iPadOS devices. It offers excellent value for money through user-based bidding.

System requirements

The current system requirements for Securepoint Mobile Security - Device Protection and Mobile Device Management (MDM) can be found at:

www.securepoint.de/mobile-requirements

The perfect match for mobile safety

Analysis and reports

Securepoint Mobile Security provides excellent options for evaluation and allows the administrator to navigate through the results in real time. Thanks to the integrated pseudonymization, the user reference can be masked out to ensure EU DSGVO compliance for this evaluation.

Mobile Security - Device Protection

- Secure Internet traffic even in public and open WLANs
- Control over websites (+SSL) and services
- Provider-independent
- Zero Hour Protection - malware (incl. Crypto Trojans), drive-by downloads, phishing and advanced persistent threats
- Access points georedundant and guaranteed in Germany
- Device-independent protection (TCP/IP)
- Protects smartphones, tablets and laptops
- True protection for iOS/iPadOS and Android devices.
- SMB-optimized security solution

Mobile Device Management (MDM)

- Central management via web interface
- Settings such as camera, passwords, and more. define
- Finding, locking and deleting devices
- Mail and WLAN management
- Google Android Enterprise incl. Work-Container
- Google accounts, app notifications and wallpapers from iOS profiles. Manage out of
- Apple DEP (Device Enrollment Program) and VPP (Volume Purchase Program)
- Supports Apple School Manager, Classroom app and shared iPads
- Hosted and maintained by Securepoint

Mobile Security and Data Protection

According to the European Data Protection Regulation (GDPR), lost data and data leaks can result in heavy fines (up to 20 million euros or up to 4% of a company's annual global turnover).

Securepoint Mobile Security reliably secures your mobile devices. All data traffic is routed exclusively in encrypted form to German data centers, where it is monitored by Securepoint NextGen cloud firewalls. Encryption also protects your data in public and free WLANs.

Überreicht durch Ihren Securepoint-Partner

Subject to changes and errors. As of: 14.02.2024.

 **SECUREPOINT**

Securepoint GmbH • Bleckeder Landstraße 28 • D-21337 Lüneburg • Tel.: 04131 2401-0
www.securepoint.de • info@securepoint.de