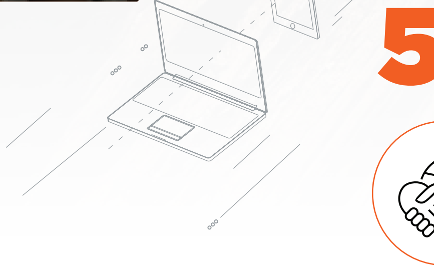
Lenovo

WORKFORCE MOBILITY SOLUTIONS

Lenovo's 360° approach to security is a cohesive mesh of features and technologies that deliver maximum protection in a business PC.

SOLUTION SETS

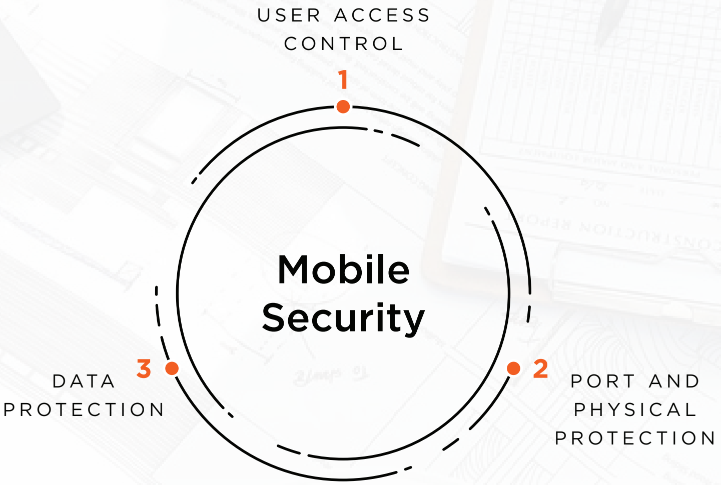
- MOBILE DEVICES
- MOBILE SECURITY



Windows 10 Pro

MOBILE SECURITY SOLUTION DATASHEET Ver 1.0

With the rise of the mobile workforce, the need to minimize security risks like device theft, data accessibility, and malware attacks is also increasing. Also, the sophistication of today's security threats require a comprehensive approach that keeps your business devices, networks, and data protected.



5 reasons why Lenovo is a difference maker

- Trusted around the world
- Expertise across categories
- Confidence in our products
- Business-boosting technology
- Flexible support network

USER ACCESS CONTROL

A dynamic workforce requires their IT team to monitor and protect their devices and networks against threats such as unauthorized access, ID theft, and hacking.

Lenovo's user access control technology protects the organization's devices and business ensuring only the right people have access to it.

Multi Factor Authentication (MFA) - For User Identity Protection

Fingerprint Reader with Match on Chip

- Match on Chip is the most secure implementation of fingerprint technology on a PC — it stores biometric credentials on a separate chip inside the hardware with 256-bit AES (Advanced Encryption Standard) encryption.
- Since image processing and secure matching takes place on the sensor chip and not in software, the user data remains protected from malware attacks.

Strengthen access control with Intel® Authenticate

- Intel® Authenticate stores biometric, security credentials, and IT policy engine in the hardware instead of the OS or third-party software. Since the data is captured, encrypted, matched, and stored in hardware, reaching it becomes harder even for the most advanced threats.
- This reduces exposure to software-level attacks such as password cracking, phishing, and screen scraping, strengthening identity protection on the PC.

IR Camera with Windows Hello - For Simple and Secure Facial Login

With **Windows Hello**, the optional IR camera on selected devices simplifies and secures the login process. **Windows Hello** face authentication uses a camera specially configured for near infrared (IR) imaging to authenticate and unlock the device. Also, the IR camera doesn't capture photos – this prevents spoofing and provides uncompromised security.

Smart Card Access - For Two-factor Authentication in One Step

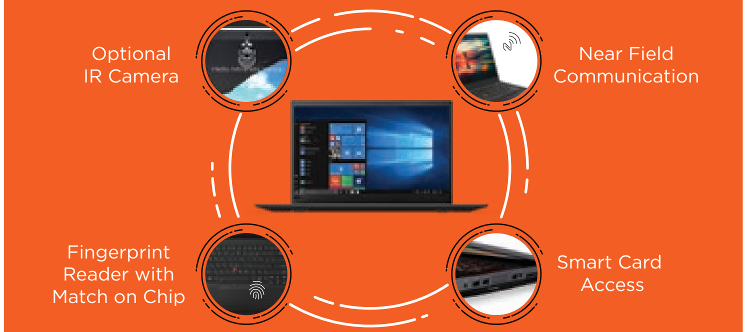
An intelligent way to manage access to multiple devices sans passwords, these tamper-resistant cards store the user's login information on an embedded chip. This user data can only be accessed through the smart card operating system with proper access rights. With a robust set of encryption capabilities including key generation, secure key storage, hashing, and digital signing, smart cards directly implement two-factor authentication, ensuring that devices are averse to threats.

Near Field Communication (NFC) - For Rapid Contactless Authentication

NFC is a type of radio communication standard, much like Bluetooth, WiFi, and other networking technologies. To snag the NFC signal to log in, the user needs to be physically close to the PC with the right NFC tag or a secondary device like their smartphone. Without the tag, it is impossible to hack into the device.

GET MORE FROM SECURITY SOLUTIONS

- **Windows Hello** is a convenient, enterprise-grade alternative to passwords that are designed for today's mobile-first world. It uses natural (biometrics), familiar (PIN), or a companion device as factors to validate a user's identity.
- Intel® Authenticate solution provides a simple self-service enrollment tool for end-users to quickly get started, eliminating calls to IT.
- The chips embedded in Smart Cards are extremely difficult to duplicate or forge. A variety of hardware and software capabilities detect and react to tampering attempts and help counter possible attacks.



A SMART APPROACH TO PROTECTION

- **Kensington® Cable Lock**
  - The push button design in the cable lock offers one hand operation for easy installation while the Kensington® T-bar™ secures the lock to your device.
- **Camera Shutter**
  - No more sticky notes for camera privacy! The physical camera shutter provides strong and easy camera security with just a flick.
- **ThinkPad Ultra Dock**
  - ThinkPad Docking Stations support PXE book, wake on LAN, and MAC address pass-through, simplifying asset management for IT managers irrespective of their location.

PORT AND PHYSICAL PROTECTION

Whether in the office or on the go, end user computing devices need protection not only at the software level but also at a physical level. Built-in port security features help protect against physical theft of data via the USB and other access ports on company PCs.

ThinkShutter Camera Privacy - For Privacy When You Need It

With the shutter built into the front-facing camera, protecting privacy just requires sliding the tiny cover to close the camera shutter — no more worries about anyone eyeing the user.

Kensington® Cable Lock - For Preventing Device Theft

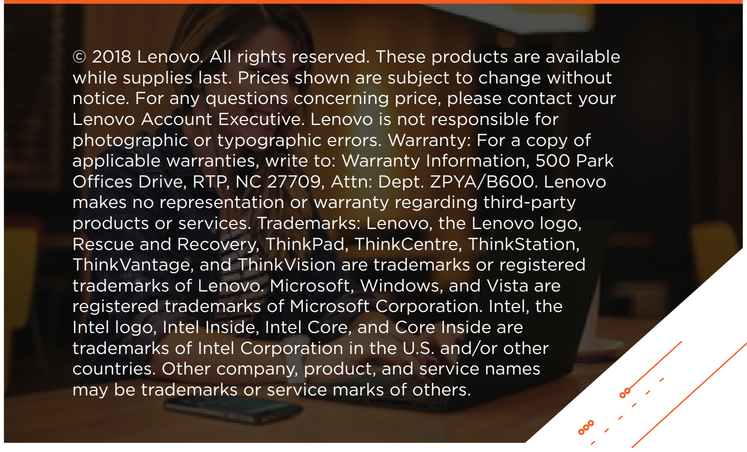
The Kensington® Cable Lock helps reduce theft and increase physical asset security protection for notebooks, notebook docking stations, desktops, and flat panel monitors. Standard on all Lenovo PCs, it allows customers to manage physical security access within the office premises.

ThinkPad Ultra Dock - For Innovative Dock and Device Security

This innovative docking solution is easy to connect and secures your system while you are away. A Security Lock conveniently secures both the device and your dock to the desk with a single key. It provides a driver-free convenient connection securely to a range of USB accessories and external displays.

COMPREHENSIVE APPROACH TO SECURING DATA

- **Windows 10 Mobile Device Management (MDM)** provides an alternative to traditional PC management processes where users can transition to Cloud-based management at their own pace.
- Intel® Active Management Technology (Intel® AMT) allows users to prevent unsolicited access by allowing remote wiping of the data on the drive with Intel® Remote Secure Erase if it falls into wrong hands.
- **BUFFERZONE**® enables employees to browse the net safely by opening the browser in a container in case a threat is detected. With detailed reporting and integration with SIEM and Big Data analytics, BUFFERZONE helps identify targeted attacks.
- **Coronet** can detect and evade unsafe wireless connections over both WiFi and Cellular networks. It requires no installation and ensures that only trusted devices, networks, and Cloud services can access your data.



DATA PROTECTION

To keep the business running smoothly and without disruption, it is essential to have secure, automatic, and efficient data backup. Lenovo's robust data protection tools enable easy and efficient data recovery and retrieval only by authorized personnel.

Fast Identity Online (FIDO) - For Robust Data Protection

FIDO-enabled authentication reduces dependence on user passwords by using hardware, mobile, and biometric-based authenticators. This simpler and safer approach prevents potential data threats like phishing, man-in-the-middle, and stolen passwords.

FIDO protocols are based on public key cryptography to access FIDO-enabled services, which creates a better security for accessing popular websites and online services.

Discrete Trusted Platform Module (dTPM) 2.0 - For Data Encryption

The embedded dTPM 2.0 chip enables and stores unique RSA encryption keys specific to the host system for hardware authentication. Tamper resistant technology keeps it unaffected by the malicious software.

Online Data Backup (OLDB) - For Safeguarding Your Critical Data

Lenovo's Online Data Backup is an easy-to-use, automatic online backup and recovery software solution. With this tool, organizations and user groups can share storage without the need for administrators to allocate capacity individually.

- Requires no capital expenditures for hardware; low upfront investment with minimal maintenance overhead
- Relative to tape-based approaches, OLDB is more efficient, less intensive for the operator, and not as prone to human error

Hard Drive Retention - For Retaining Sensitive Company Data

Lenovo Hard Drive Retention service allows customers to retain the defective hard drive that is replaced in the course of the Lenovo hardware warranty or maintenance services. If the internal hard disk drive (HDD) or internal solid state drive (SSD) fails during warranty, the service allows them to keep the failed hard disk drive to retain sensitive data within the organization.

BUFFERZONE® - For Sophisticated and Supreme Malware Protection

This next generation of endpoint security solution not only detects and blocks malware but also isolates suspicious applications and runs them in a completely isolated container. This creates a buffer that prevents malware from infecting the endpoint and your corporate network. Available from Lenovo, BUFFERZONE conveniently allows employees to browse the net and safely use removable media without risk to the organization.

Mobile Device Management

In-built Mobile Device Management: Windows 10 Mobile Device Management (MDM) support, lets you use Cloud-based management services* to control business and personal devices. Your employees get access to corporate applications, data, and resources from virtually anywhere on almost any device, while IT helps to keep your business information secure.
*Sold separately