PROTECT. PREVENT. PRESERVE.
Physical first level security solutions for IT & AV hardware interfaces & systems.
“THERE ARE ONLY TWO TYPES OF COMPANIES - THOSE THAT KNOW THEY’VE BEEN COMPROMISED AND THOSE THAT DON’T KNOW.”

Dmitri Alperovitch, Cyber Security Expert & Co-Founder of CrowdStrike
DATA SECURITY SOLUTIONS
THE BENEFITS OF PHYSICAL DATA PROTECTION

Data security solutions provide users with the tools to help prevent security compromises and deter unauthorised users from accessing ports that provide essential functionality to an application or store sensitive data that needs to remain confidential or secure.

There are a variety of ways to secure data digitally: like firewalls, anti-virus programs and bespoke security software, however physical blockers can be just as important in keeping data safe from compromise. Port blockers are visual deterrents that seamlessly fit into a variety of environments and provide a physical barrier to unauthorised access.

---

1 STRENGTHEN SECURITY

Port blockers serve as a great visual deterrent for threats to data. Plug these simple devices into a corresponding port and stop unauthorised users from inserting devices that could compromise security or data.

---

2 USER FRIENDLY

Quick and easy deployment allows multiple ports to be blocked and managed easily by system administrators. No training or software is required for installation and once installed the port blockers require virtually no maintenance.

---

3 EFFICIENT & SCALABLE

Low installation costs facilitate gradual deployment across an installation as budget allows. With virtually no maintenance costs and additional keys and locks available, these devices provide almost unlimited scalability.

---

4 SECURITY IN DEPTH

Combined with software solutions such as specialist programs and BIOS restrictions, port blockers provide an added layer of defence against data theft and compromises.
USB PORT BLOCKERS
TYPE C & TYPE A

USB Port Blockers are useful little devices that system administrators can use to physically prevent access to USB ports. USB Port Blockers allow locks to be inserted and removed from USB ports to stop unauthorised users from inserting pen drives, USB mass storage and mobile devices into shared workstations or devices with USB ports in public spaces.

QUICK GUIDE
FOR USING USB PORT BLOCKERS

01 A lock is attached to the key and inserted into a USB port.
02 The sliding mechanism on the key is then released leaving the lock in place.
03 To remove the lock the key is inserted into the lock and pulled back, simple!
Prevent tablets that are left in public environments, e.g. points of sales and classrooms, from being plugged in by unauthorised third parties.

Block access to USB ports on professional AV and IT systems, e.g. servers, matrices and switches.

Protect laptops from unauthorised access in workplaces.

Block ports on office PCs to help label unused ports or deny access.

APPLICATION EXAMPLES
FOR COMPATIBLE DEVICES
WITH USB C & USB A PORTS

▲ Block access to USB ports on professional AV and IT systems, e.g. servers, matrices and switches.

▲ Prevent tablets that are left in public environments, e.g. points of sales and classrooms, from being plugged in by unauthorised third parties.

▲ Block ports on office PCs to help label unused ports or deny access.

▲ Protect laptops from unauthorised access in workplaces.
USB TYPE C

The Type C Port Blocker Set allows locks to be inserted and removed from USB Type C ports. Available as a pack of 10 locks, or as a set of 1 key and 4 locks in a variety of colours.

PACK OF 4 LOCKS WITH 1 KEY
AVAILABLE IN SETS OF PINK, GREEN, WHITE, ORANGE, BLUE

PACK OF 10 LOCKS WITHOUT KEY
AVAILABLE IN PINK, GREEN, WHITE, ORANGE, BLUE
USB TYPE A

The Type A Port Blocker Set allows locks to be inserted and removed from USB Type A ports. Available as a single key, a pack of 10 locks, or as a set of 1 key and 4 locks in a variety of colours.

PACK OF 4 LOCKS WITH 1 KEY
AVAILABLE IN SETS OF PINK, GREEN, BLUE, ORANGE, WHITE

PACK OF 10 LOCKS WITHOUT KEY
AVAILABLE IN PINK, GREEN, BLUE, ORANGE, WHITE

KEY WITHOUT LOCKS
AVAILABLE IN PINK, GREEN, BLUE, ORANGE, WHITE
RJ-45 PORT BLOCKER

RJ-45 Port Blockers can be used to easily block open network ports and prevent users from connecting cables, devices or inserting foreign objects without permission. RJ-45 ports are ubiquitous in networked environments, by blocking these ports there is a first line of network security against viruses and other compromises. RJ-45 ports can also act as a visual cue, showing inactive or disconnected ports.

PACK OF 10 LOCKS WITH KEY
AVAILABLE IN SETS OF BLACK, GREEN, ORANGE, YELLOW

PACK OF 20 LOCKS WITHOUT KEY
AVAILABLE IN BLACK, GREEN, ORANGE, YELLOW

KEY WITHOUT LOCKS
AVAILABLE IN BLACK, GREEN, ORANGE, YELLOW
QUICK GUIDE FOR USING RJ-45 PORT BLOCKERS

01 A lock is attached to the key and inserted into a RJ-45 port.

02 The sliding mechanism on the key is then released leaving the lock in place.

03 To remove the lock the key is inserted into the lock and pulled back, simple!

APPLICATION EXAMPLES FOR COMPATIBLE DEVICES WITH RJ-45 PORTS

- Denies user access to Ethernet ports on desktop PCs in workplaces and schools.
- Deter users from using Ethernet outlet ports in corporate buildings.
- Mark RJ-45 ports on network switches to show deactivated or inactive ports.
- Restrict access or mark unused ports in a server room that contains a LAN.
SD PORT BLOCKER

SD Port Blockers can be inserted into SD card ports on memory readers, in cameras, and other devices. These devices provide a visual deterrent to anyone looking to copy data or viruses from, or to, an SD card. SD Port Blockers are available as a set of 1 key and 4 locks, or a pack of 10 additional locks.

PACK OF 4 LOCKS WITH KEY
AVAILABLE IN GREY

No. 40478

PACK OF 10 LOCKS WITHOUT KEY
AVAILABLE IN GREY

No. 40479

QUICK GUIDE
FOR USING SD PORT BLOCKERS

01 A lock is attached to the key and inserted into a SD port.

02 The sliding mechanism on the key is then released leaving the lock in place.

03 To remove the lock the key is inserted into the lock and pulled back, simple!
APPLICATION EXAMPLES
FOR COMPATIBLE DEVICES WITH SD PORTS

Block access to a desktop PC with SD port, stopping users from copying sensitive data or introducing viruses.

Limit access to memory ports on cameras to stop users from copying data or introducing new data onto a device.
Worldwide Offices

Germany
LINDY Electronic GmbH
Mainzheim
T: +49 6231 470050
info@lindy.de

United Kingdom
LINDY Electronics Ltd.
Stockton-on-Tees
T: +44 1642 754000
postmaster@lindy.co.uk

International
LINDY International Ltd.
Stockton-on-Tees
T: +44 1642 754020
postmaster@lindy.com

Italy
LINDY Italia Srl.
Oglieta Olona (VA)
T: +39 03911 801711
info@lindy.it

France
LINDY France
Mundolsheim
T: +33 1 88 29 06 66
france@lindy.fr

Portugal
Lidertronica, Lda
Lisboa
T: +351 1 851 05 50
lider@lidertronica.com

South Africa
Linkagio
Cape Town
T: +27 21 514 8800
support@linkagio.co.za

Australia
LINDY Australia Pty Ltd
Brisbane
T: +61 7 326 23033
info@lindy.com.au

Hong Kong
LINDY China Ltd.
Hong Kong
T: +852 9098 8920
info@lindy.com

China
LINDY Electronics Ltd.
Ningbo, Zhejiang
T: +86 574 8695613
info@lindy-china.cn

Taiwan
LINDY Asia Inc.
Taipei
T: +886 2 2937 1141
sales@lindy.com.tw

Indonesia
PT LINDY Teknik Indonesia
Jakarta
T: +62 21 5929706
info@lindy-indonesia.id

Japan
LINDY Sales Inc.
Tokyo
T: +81 3 8779 2989
support@lindy.co.jp

Lindy and the Lindy logo are registered trademarks of the Lindy Group in the UK and other countries. All other trademarks are property of their respective owners. Subject to technical modifications and other changes. The contents of this brochure have been prepared with great care. No warranty or liability is accepted for the completeness, correctness, or accuracy of the information. This brochure does not constitute a contractual offer and is solely for the purpose of providing (non-binding) Information. © Lindy Group

Publishing Date: 5/2019 en