BUILD STRONG SECURITY, STARTING FROM THE DEVICE-LEVEL

Physical threats to data security
and how to defend against them

Lenovo

TABLE OF CONTENTS

WITH ALL EYES ON ONLINE THREATS TO DATA SECURITY, IT'S EASY TO OVERLOOK PHYSICAL THREATS.

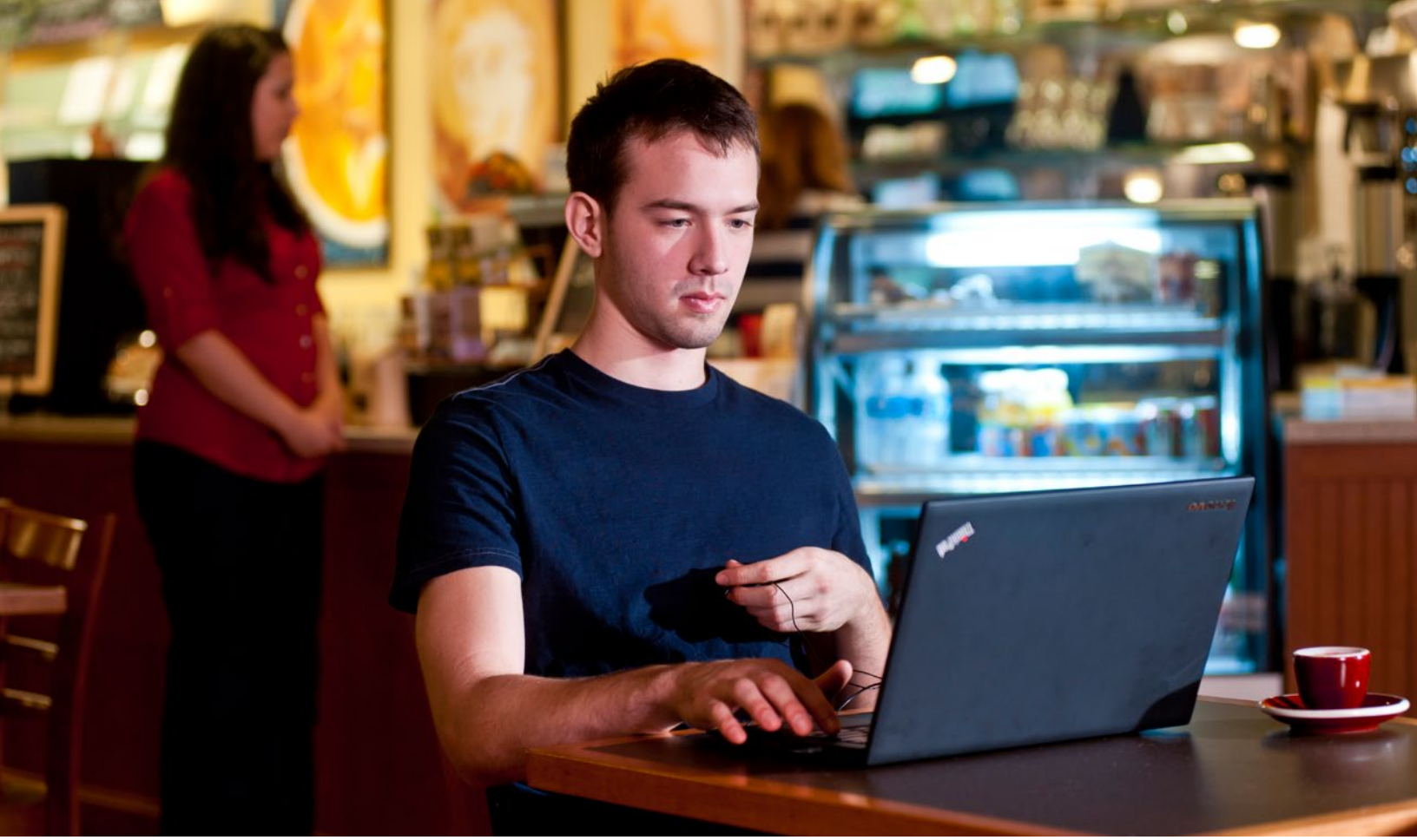
INTRODUCTION

At a time when tens of thousands of new malware strains are created every day,[1] it's natural to focus on the network as the main avenue of attack for data breaches. But with all eyes on online threats to data security, it's easy to overlook physical threats. And while these may not garner the attention or the headlines that viruses and other forms of malware do, they can be equally sinister—and every bit as dangerous.

In this eGuide, we'll look at physical security threats to which every computer—whether desktop PC, laptop or tablet—is vulnerable, and show you how to guard against them.

1/ First line of defense:

DEVICE SECURITY



THE EASIEST WAY TO TRY AND STEAL DATA? STEAL THE DEVICE THAT LEADS TO THE DATA.

Swiping a tablet off a tabletop in a crowded coffee shop, smashing a car window and grabbing a laptop that's in plain sight, and even just snatching a device from a work area when an employee leaves it unattended for a few moments—these are all examples of the simplest, most straightforward approach to getting at someone's data.

According to a recent survey, theft of mobile devices is one of the top five external threats to data for organizations today. Of the 22% of survey respondents who reported experiencing theft incidents, 16% said they had lost data as a result.[2]

It's not hard to see how this kind of data loss can happen. If the data on a device isn't encrypted, or the device doesn't have strong password protection, very little effort is required to gain access to data. Of course, more and more data is being stored in the cloud today, so there may be little to find on a hard drive. But the apps that lead to critical data in the cloud are still there—and if they're not protected by strong passwords, access to data may be way too simple.

ON THE DEFENSIVE:

WAYS TO THWART THIEVES

LOCK IT UP

For laptops, a lock slot to plug in a cable that will literally chain the device in place is a time-tested solution. There was a time when most laptops included this feature, but fewer do today—perhaps because as more data moves to the cloud, the degree of risk isn't considered as great. But since most device theft occurs from the workplace, adding this layer of physical security can only help.[3]

REMOTELY CONTROL AND SECURE

If you can't stop a laptop or tablet from being stolen, count on anti-theft technology like Absolute Computrace—now better known as Absolute Data & Device Security—to remotely disable the device and keep data from being accessed. Absolute Computrace enables IT to enforce compliance policies, identify at-risk devices, and take pre-emptive and reactive measures in case of a security incident. Computrace also provides investigations and recovery services in case of non-compliant or criminal activity.

PERSONALIZE PROTECTION

To ensure sensitive company data stays secure in the event of theft or loss, make sure your devices include biometric protection, like fingerprint and smartcard readers, to keep intruders out.

2/ ACCESS CONTROL SHOULD BE

MULTI-LAYERED

2 / ACCESS CONTROL SHOULD BE MULTI-LAYERED

Hackers take advantage of whatever pathways possible to access devices and data. While USB drives are quite useful for downloading data from a hard drive or uploading it to a computer, these same devices can provide an opening for someone on the attack. With a USB drive, stealing data from a computer is as simple as using its USB port to download files and then just slipping the drive into a pocket. After all, why steal the computer itself when an object the size of a thumb makes it so easy to just take the data?

And it's not just about taking data; it's also about leaving data behind that can wreak havoc with apps and systems. Warn your users: If they ever see a thumb drive on the ground, they shouldn't let curiosity lead them to plug it in to find out how much storage it offers or whether there's anything interesting on it. The same goes for USB giveaways from industry events. Chances are, nothing will happen. But one could end up exposing data or unknowingly uploading a virus.[4] **IS IT WORTH THE RISK?**

ON THE DEFENSIVE:

WAYS TO ACCESS VIA USB

JUST SAY NO

While it's not practical to completely prohibit the use of USB drives at work, it's possible to at least limit it. The National Institute of Standards and Technology (NIST) has a reasonable policy worth considering as a model.[5]

EXERCISE THE OPTION

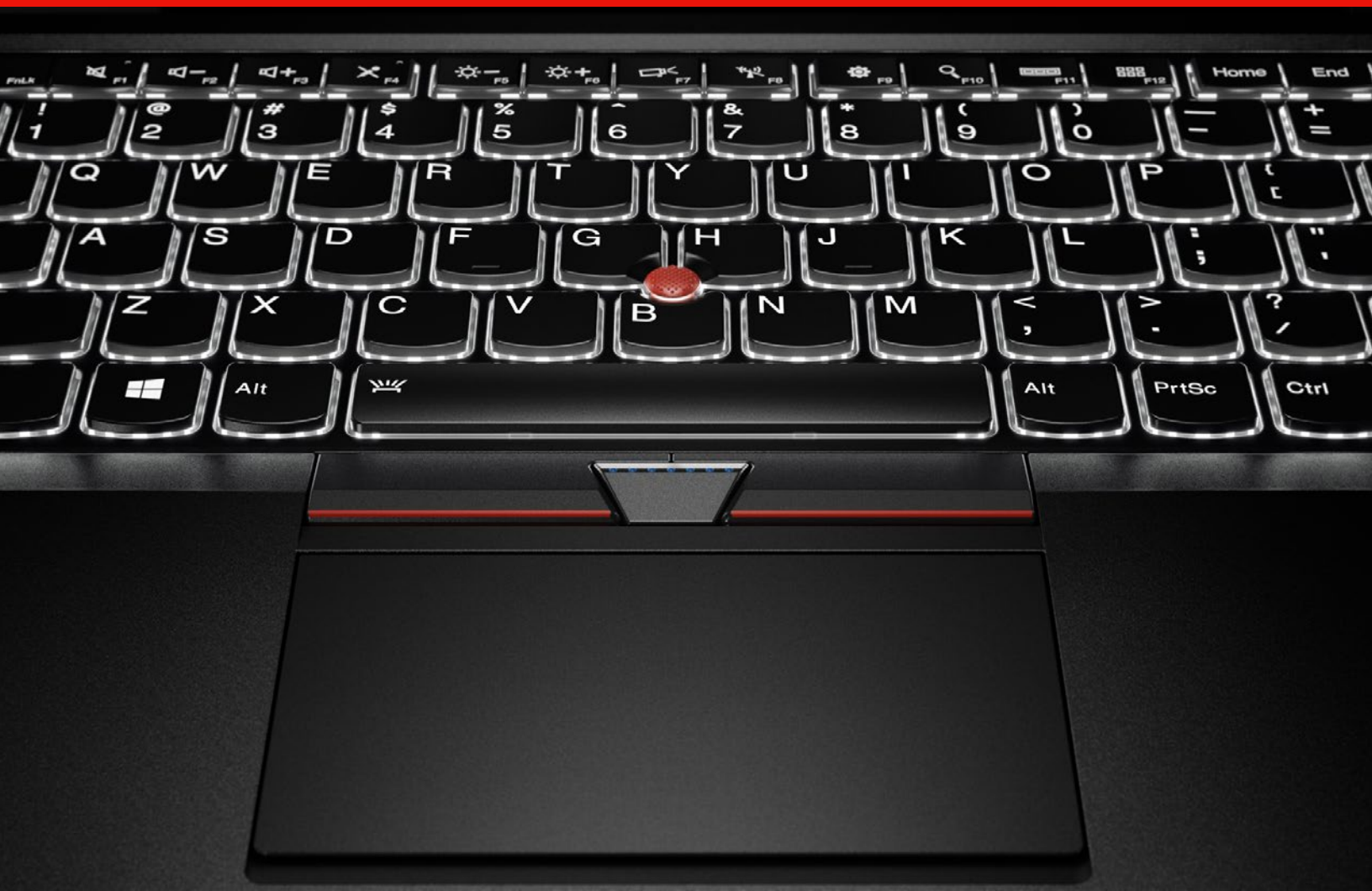
When limiting USB use by policy doesn't work, consider hardware that offers the option of disabling USB ports at the BIOS level.

EDUCATE USERS

Make sure your users understand the risks and know what not to do.

3/ ENDPOINT PROTECTION

IS KEY



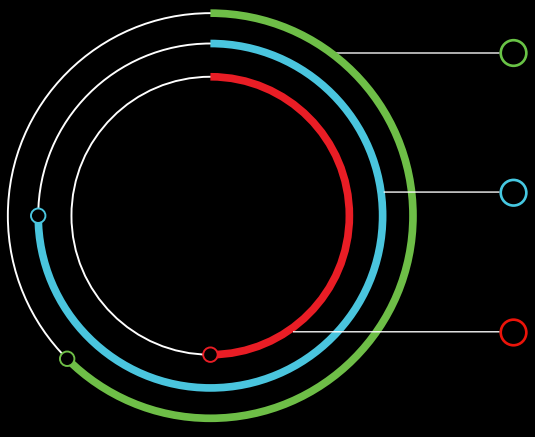
As long as a lost or stolen device is password-protected, there's nothing to worry about, right? Unfortunately, password protection is increasingly a contradiction in terms, as thieves get better at stealing passwords, hackers get better at cracking them, and users get worse about making them stronger or changing them often enough.

Statistics and data analysis have helped hackers develop new and faster algorithms for getting access to your accounts. How? Because statistics identify and study patterns—and users are notorious for using patterns when devising passwords that are "easy to remember." Basically, your users' easy-to-remember passwords are a hacker's dream.

While password protection does present at least some barrier to accessing data, it's often a barrier that's not difficult to breach. A 2015 study reveals 63% of all confirmed data breaches involved leveraging weak, default or stolen passwords.[3] One problem is that making passwords harder to guess also makes them harder to remember; changing them frequently has the same unwanted effect. This has led to the alarming news that almost three-quarters of people use the same password for more than one device or account, and almost half have at least one password they haven't changed in five years.[6]

Consider this, though: Someone can have the strongest password possible, but that won't matter if someone else sees it over his or her shoulder as they enter it. One thing that can help is having devices that make it easier to use strong passwords and harder for others to steal them. Even better, consider using computers that include authentication that's much more difficult to breach, like biometrics.

AS LONG AS A LOST OR STOLEN DEVICE IS PASSWORD-PROTECTED, THERE'S NOTHING TO WORRY ABOUT, RIGHT?



63% of all confirmed data breaches involved leveraging weak, default or stolen passwords.[3]

Almost 75% of people use the same password for more than one device or account.[6]

Almost 50% of people have at least one password they haven't changed in five years.[6]

ON THE DEFENSIVE:

WAYS TO SOLVE PASSWORD PROBLEMS

TAKE A PASS

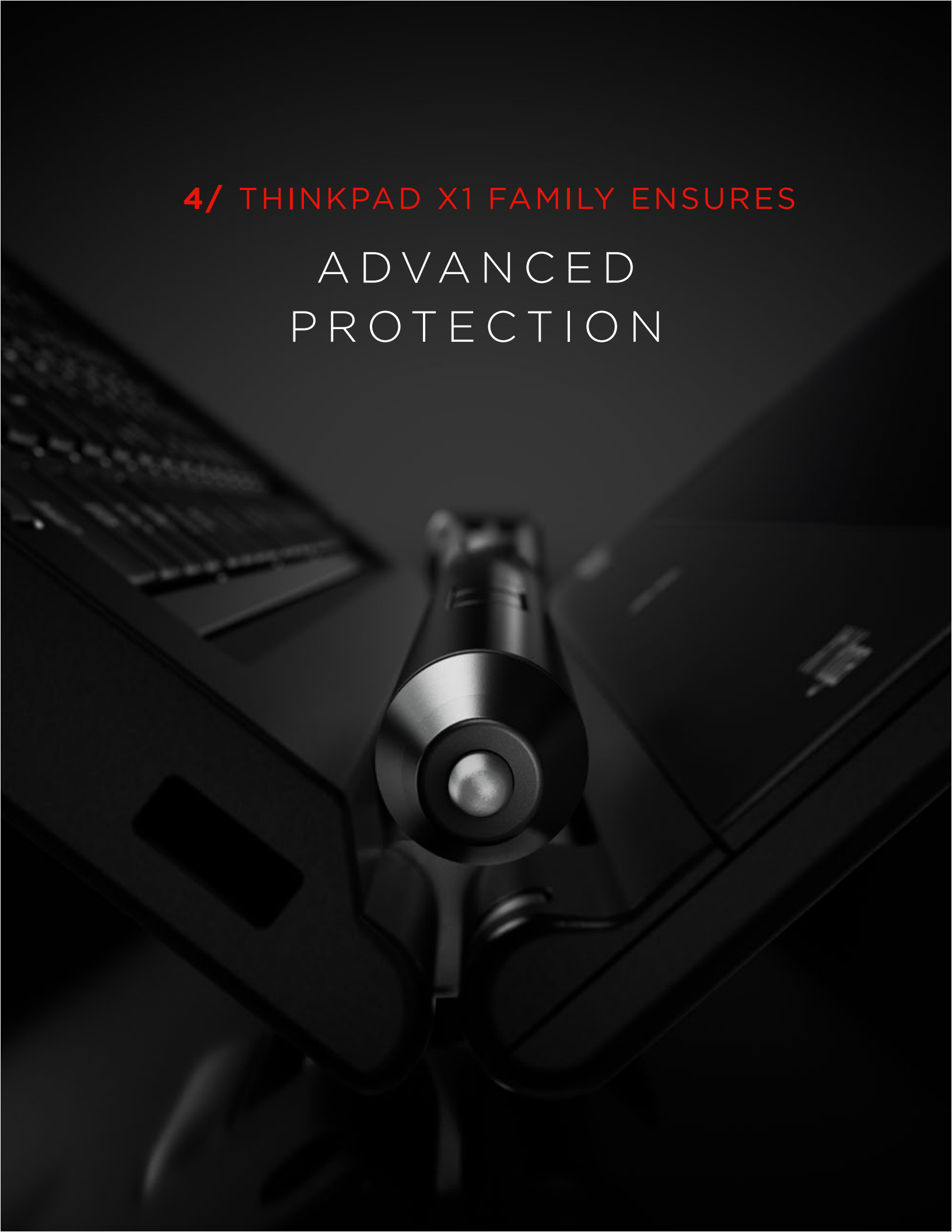
Instead of relying on passwords, consider computers equipped with fingerprint readers or other biometrics-based means of authenticating users.

EXTEND TO THE SOFTWARE-LEVEL

In addition to fingerprint readers, choose devices with Windows 10, which features Windows Hello facial recognition software to further protect data.

TAKE PRECAUTIONS

Consider everything from screens designed for privacy to computer-based encryption (so even if someone gets past the password, data will be unusable).



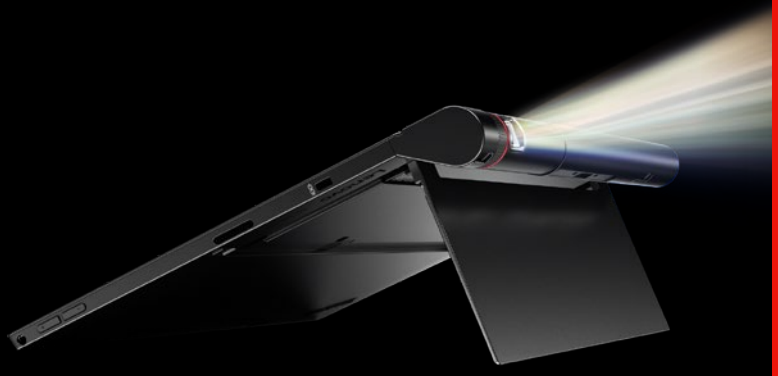
4/ THINKPAD X1 FAMILY ENSURES

ADVANCED PROTECTION

THINKPAD X1 FAMILY
ENSURES ADVANCED PROTECTION

The Lenovo ThinkPad and ThinkCentre X1 family delivers intelligently designed, advanced security across the spectrum of device types:

THINKPAD X1 TABLET



A thin, light tablet with a design that makes it easy to use as a laptop or projector, plus detachable keyboard that's available in a variety of colors

THINKPAD X1 YOGA

An ultra-light 2-in-1 with a stunning display, the fastest mobile broadband available, and four modes to work, present, create and connect

THINKPAD X1 CARBON

An ultrabook with carbon-fiber reinforced durability, all-day battery life, powerful storage performance and innovative docking options

THINKCENTRE X1

An all-in-one desktop PC with a sleek, ultra-thin design, the latest enterprise manageability and a brilliant wide-screen anti-glare display

Lenovo ThinkPad and ThinkCentre X1 security features include:

- Biometric-based authentication, including the ThinkPad X1 **TOUCH SENSOR FINGERPRINT READER**, which is more reliable and accurate than typical swipe readers, and also supports Windows Hello face/fingerprint recognition software
- Protection from prying eyes with **PRIVACY FILTERS** that utilize patented 3M microlouver privacy technology to darken the screen at specific angles, making it impossible for others to view
- **TRUSTED PLATFORM MODULE (TPM)** chip that stores encryption keys, passwords and digital certificates to secure hardware
- BIOS-based security capabilities including **BIOS PORT LOCK** to disable USB ports and a **USB BLOCKER** to identify and block different types of USB devices connected to the system
- Intel Anti-Theft technology featuring **ABSOLUTE DATA & DEVICE SECURITY** (previously known as Computrace) in the BIOS to enable remote lockdown of a lost of stolen device
- **SECURITY-LOCK SLOT** on the ThinkPad X1 Carbon ultrabook to attach a security cable lock

Want to know more about the ThinkPad and ThinkCentre X1 family?

DOWNLOAD THE SOLUTION BRIEF **SHOP NOW**

Intel Inside®. Extraordinary Performance Outside.
Powered by Intel® Xeon® processors.

[1] Pandalab Annual Report 2015.
http://www.pandasecurity.com/mediacenter/src/uploads/2014/07/Pandalabs-2015-anual-EN.pdf

[2] "IT Security Risks Survey 2014: A Business Approach to Managing Data Security Threats," *Kaspersky Lab*, 2014.
http://media.kaspersky.com/en/it_security_risks_survey_2014_global_report.pdf

[3] "2016 Data Breach Investigations Report," *Verizon*, 2016.
http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

[4] "Should You Plug That USB Drive Into Your Computer?" *Forbes*, October 30, 2015.
http://www.forbes.com/sites/ygrauer/2015/10/30/usb-drive-malware-security-homeland-security-cybersecurity/#2f5c71954391

[5] "USB thumb drive security best practices spelled out by NIST," *SearchSecurity and TechTarget*
http://searchsecurity.techtarget.com/USB-thumb-drive-security-best-practices-spelled-out-by-NIST

[6] "The passwords we never change: One in five people haven't changed password they use in a decade," *Daily Mail*, June 7, 2015.
http://www.dailymail.co.uk/news/article-3114675/The-passwords-never-change-One-five-people-haven-t-changed-phrase-use-decade.html