Hardware security: How businesses can secure laptops and PCs

Tom Mangan
Staff

1 May 2023

Hardware security means thwarting cyberattacks everywhere – from the tiniest silicon chip on a laptop or PC to the server farms in the largest cloud data centers.

Getting your head around this concept takes some doing. Most security conversations center on creating strong passwords, authenticating users, and monitoring networks for signs of nefarious activity. We don't see as much talk about the threats hidden within a computer's silicon chips.

But these threats are real. Hackers can insert malicious code onto computer chips and gain access to sensitive data on a PC or laptop. Businesses crafting a sound cybersecurity strategy need to pay attention to PC security. Here are three ways to do that.

Educate yourself on hardware security threats

Effective cyber defense starts with network firewalls, authentication, and device monitoring. These are all essential and cannot be compromised. But there's a hidden vulnerability in the hardware of computing devices and the software that controls them.

Every computer, including smartphones, tablets, and PCs, has a circuit board with a CPU, memory chips, and a bus that helps them communicate with each other. Computers also have an operating system (such as Windows or MacOS) and firmware, code that tells the computer how to operate.

When a computer boots, it loads the operating system first. Historically, malware has attacked applications after the operating system loads. But attackers have also learned how to compromise computers before the OS starts working. This is why AMD recommends a "chip-to-cloud" approach to cybersecurity. Chip-to-cloud means every device is designed for maximum security, which is essential as more people adopt work-from-home lifestyles. Every remote computer is a security risk. And every company's computer hardware must be secure.

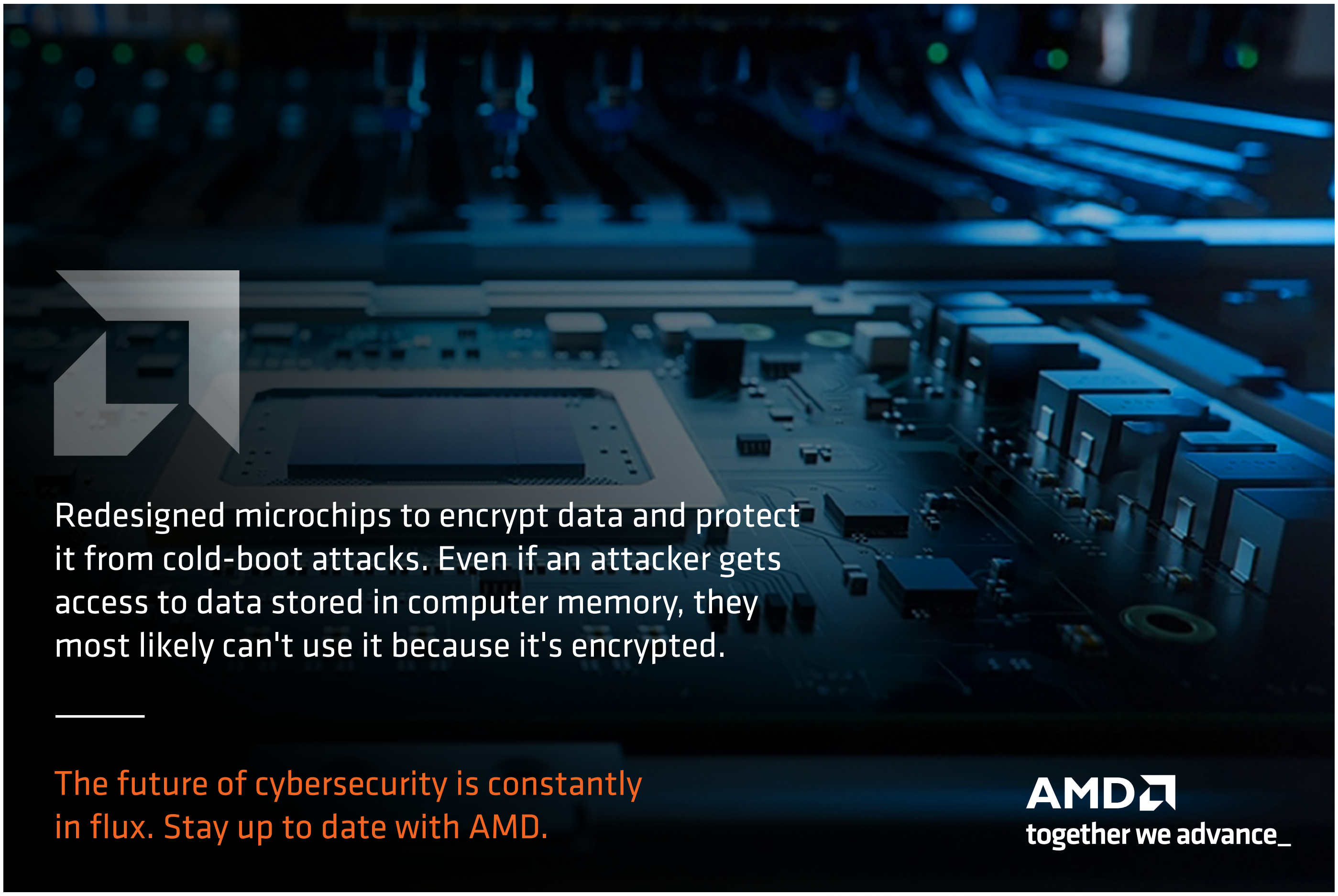
Fortunately, there's a global industry devoted to the software side of security. But your business cannot afford to overlook the hardware side.

Dig deeper on hardware security vulnerabilities

A cyberattack usually involves your adversary planting malware on a computer that will set bad actions into motion, such as stealing bank account numbers and passwords.

Most of these attacks target applications and operating systems, but there are other ways to cause trouble. One sneaky tactic is the "physical cold boot attack," which infiltrates computer firmware and memory before the operating system loads. This attack goes after data that a computer generates after it's turned on. It's almost comically easy to thwart a cold-boot attack: Just turn off your computer completely (that is, cut off the power supply) and then turn it back on.

What's not so comical is how people actually use their laptops and PCs, especially on the job. Most of us like to turn on our computers in the morning and leave them running all day. Some folks' computers do this for days or weeks.



Redesigned microchips to encrypt data and protect it from cold-boot attacks. Even if an attacker gets access to data stored in computer memory, they most likely can't use it because it's encrypted.

The future of cybersecurity is constantly in flux. Stay up to date with AMD.

Let's say your co-worker unknowingly clicks on an infected link, executing malware that launches a cold-boot attack. Their data will be at risk until they power their laptop back down. People would have to constantly turn their computers on and off all day to prevent cold-boot attacks. That's not remotely realistic.

These days, system memory needs real-time encryption, which protects against physical attacks even if a laptop is lost or stolen. Indeed, AMD has redesigned their chips with a feature called Memory Guard to encrypt data and protect it from cold-boot attacks. Even if an attacker gets access to data stored in computer memory, they most likely can't use it because it's encrypted.

Effective hardware security requires layers of protection between computer users and their data. The top layer is a third-party security application you'd purchase for tasks such as user authentication and endpoint management. The middle layers are for the operating system, CPU, memory, and the underlying silicon chip architecture. AMD, for instance, partners with Microsoft to secure Windows at the OS level along with the CPU, memory, and architecture layers (Memory Guard is one of these architecture layers).

The more layers of protection between you and your adversary, the better your chances of keeping your company's data secure.

Adopt hardware security best practices

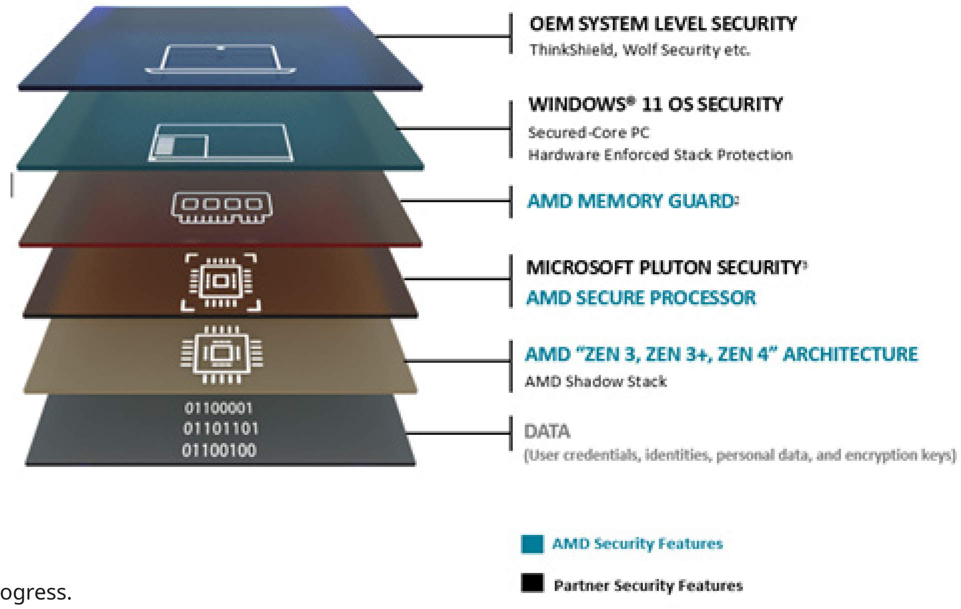
Here are some ways to ensure your PCs and laptops stay secure:

1. Start with a zero-trust approach

A robust cybersecurity strategy starts with a hard-to-breach perimeter around a business computer network (that is, a firewall). In the past, anybody who got past the perimeter was considered a "trusted" user. Then hackers started exploiting this trust by stealing passwords and creeping around networks to their heart's content.

A zero-trust security strategy acknowledges that people will break into a business network. It just doesn't give them any place to go. Every door has a lock, and every user must be verified before they get in. People have access only to the resources they need to do their jobs. Nobody is trusted by default.

Modern chips with encryption and protections like Microsoft Pluton – an encrypted CPU built in partnership between Microsoft and top chip manufacturers – are pillars of a zero-trust approach.


OEM SYSTEM LEVEL SECURITY
ThinkShield, Wolf Security etc.
WINDOWS® 11 OS SECURITY
Secured-Core PC
Hardware Enforced Stack Protection
AMD MEMORY GUARD[2]
MICROSOFT PLUTON SECURITY[3]
AMD SECURE PROCESSOR
AMD "ZEN 3, ZEN 3+, ZEN 4" ARCHITECTURE
AMD Shadow Stack
01100001
01101101
01100100
DATA
(User credentials, identities, personal data, and encryption keys)
AMD Security Features
Partner Security Features

*FIPS certification in progress.

2. Document your device fleet

You'll need to create an inventory of every device on your network and document its processor architecture. Look for laptops and PCs with older, unprotected chipsets, and consider replacing them.

3. Establish device replacement priorities

You may not have the budget to replace every PC or laptop in your fleet. Thus, you'll have to prioritize some devices over others. Devices with sensitive data such as company secrets or customer personal data should be replaced first.

Find out more on hardware security

Every new cyber defense tactic forces hackers to become more clever. And we can count on them to rise to the challenge.

It's hard enough keeping software patched to lock out hackers. Upgrading hardware is even more challenging: You may have to replace an entire computer to reduce the cyber risk. AMD has collected a series of reports and white papers on hardware security.

Find out more