3 ways to extend Zero Trust to the device level

Contents

In recent years, cybersecurity has **become a bigger strategic and budgetary priority** for organizations of all sizes — even those that are not in highly regulated industries. As many as **93% of businesses** are planning to increase their cybersecurity budget over the next year to shore up their defenses.

Cybercriminals are constantly adapting their tactics to evade defenses, forcing IT professionals and researchers to refine their security strategies based on the latest threats. The proliferation of devastating ransomware and phishing attacks, as well as the alarming appearance of fast-spreading malware such as **WannaCry** and **NotPetya**, likely played a role in elevating cybersecurity to a top-of-mind business concern.

Cyberattacks have been so successful in recent years that IT security has had to undergo a foundational shift. Previously, IT professionals focused on eliminating risk by setting up a strong perimeter of multi-layered defenses, but now the predominant philosophy has evolved to accept that ongoing risk is inevitable. Since organizations cannot stop threat actors from infiltrating systems, they must set up systems in a way that assumes everyone and everything trying to access data could be a threat. This philosophical shift in the industry has led to the widespread implementation of Zero Trust architecture.

However, as companies and government agencies enact Zero Trust, threat actors have noticed many commonly implemented protections focus solely on digital, rather than physical, IT security. While companies are focused on the "cyber" part of cybersecurity, threat actors are quietly finding ways to attack hardware and firmware.

Hardware-borne attacks rely on having physical access to the device being compromised, while firmware attacks can exploit firmware vulnerabilities either through a physical or remote attack — often targeting a perceived weak point in the supply chain. Either way, compromising a device's hardware or firmware can be difficult to pull off. The benefit for threat actors is these attacks are also hard for companies to detect and prevent, as they exploit common gaps in security programs.

Device-related attacks will continue to entice threat actors as long as companies continue to leave these gaps exposed. To get ahead of impending device-level attacks, organizations must extend Zero Trust to the physical layer of company hardware by:

1. gaining visibility into every piece of hardware connected to company systems
2. consistently scanning firmware code
3. leveraging hardware-based full disk encryption with partitioning

What is Zero Trust and why is it important?

Zero Trust — the concept of "never trust, always verify" any attempt to access data and systems — originated as a concept **as early as 1994**, but became more widely known because of a **2010 Forrester Research paper** that described the scaffolding for real-world implementation. Adoption of Zero Trust remained relatively slow before reaching a tipping point in 2021 when a confluence of factors drove greater adoption, including **an Executive Order** requiring Zero Trust Architecture within government agencies. Since then, adoption has tripled, and at least **61% of businesses now say they have enacted a Zero Trust initiative**.

Prior to Zero Trust, the prevailing cybersecurity model was based on establishing a multi-layered perimeter defense to keep threats from infiltrating an organization's network — an approach that was often compared to a castle with a moat. Any entities requesting access — including users, service accounts, network traffic and devices — were classified into one of two groups: trusted or untrusted. Once a user or device was verified as authorized, they were not required to re-authenticate before performing tasks within their authorized rights.

This model was developed during a time when enterprises still operated in a largely "closed" way, supporting users who only used corporate-owned devices that were solely connected to the company network, running and accessing services that were hosted and controlled on premise. As companies began to leverage cloud-based resources and virtual private networks (VPNs) to support remote and hybrid work, this legacy model was no longer adequate for keeping threat actors at bay.

While a strong perimeter defense remains vital to IT security, the Zero Trust model removes the idea that any authorized user or device can be deemed "safe" even after authenticating. Zero Trust requires re-authentication of every user and device before accessing enterprise resources.

The National Institute for Standards and Technology (NIST) defines Zero Trust in this way:

Zero Trust is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero Trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource.

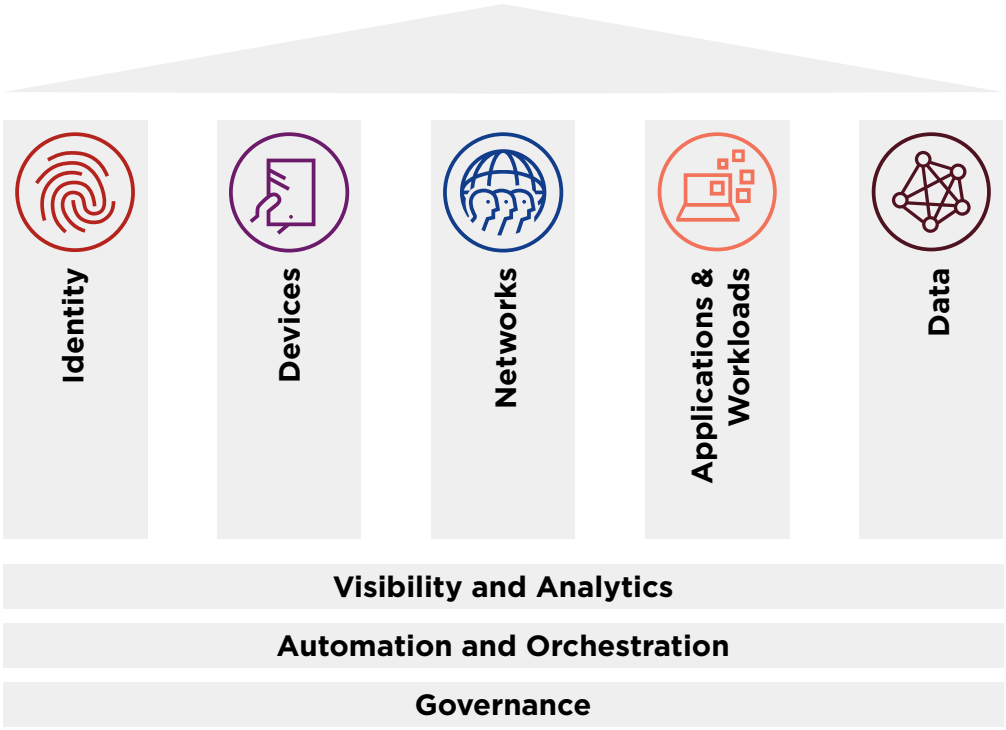


Figure 1: **Zero Trust Maturity Model Pillars**

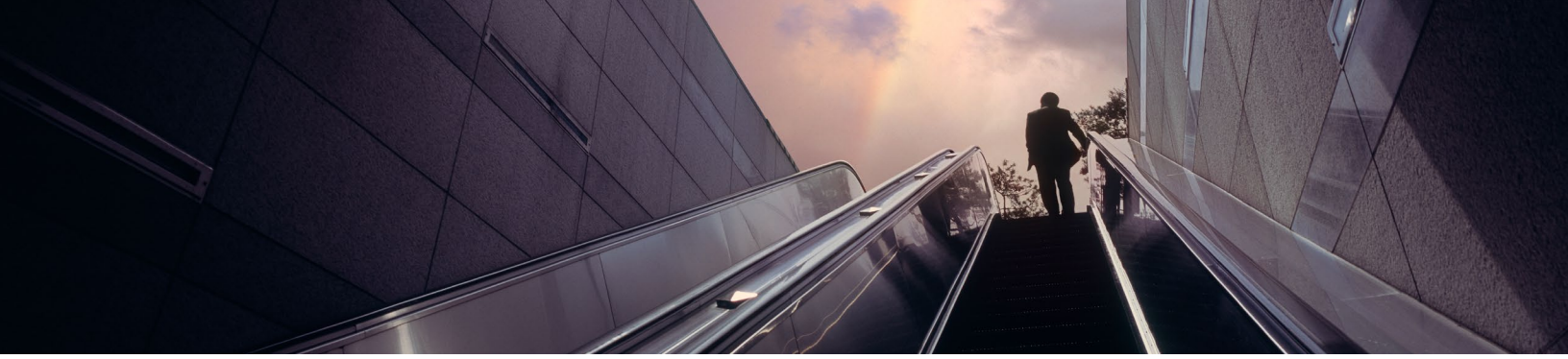
In a 2023 paper **Zero Trust Maturity Model**, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) detailed five pillars of the Zero Trust model: Identity, Devices, Networks, Applications & Workloads, and Data. This paper outlined that moving toward Zero Trust was an ongoing effort to continually mature cybersecurity protections, responses and operations over time, based on the latest threats.

The U.S. National Security Agency (NSA) followed up with **Advancing Zero Trust Maturity Throughout the Device Pillar** a cybersecurity information sheet that provided a deeper dive into the Device pillar. NSA issued this guidance because they found Zero Trust programs were often weakest at the device level, making them a growing target for attackers.

Device-level security is a common weak point because most organizations lack the right kind of technical insight into their devices. Endpoint protection solutions are vital for devices that can use them, but they work at the application or OS level. They do not provide insight into hardware, physical components, firmware or boot processes, and they typically cannot be used with IoT devices, network devices or many types of industrial operational technology.

While the call for Zero Trust at the device level is crucial, companies might still struggle to fully secure their systems from compromised devices. Standard cybersecurity solutions often miss these threats because the attacks are designed to bypass detection, or the systems themselves are only programmed to identify digital threats, not physical compromises.

To achieve true Zero Trust, companies need the ability to recognize and protect against hardware- and firmware-borne attacks, as well as data breaches resulting from physical access to a lost or stolen device.



Understanding common hardware attack threat vectors

Learning how hardware can be compromised is essential for protecting company devices. Here are three primary ways hardware attacks can happen:

Internal threats

With physical access to company hardware, employees and contractors are in a key position to implement hardware-borne attacks. **More than half** of insider-related incidents result from human error and negligence. However, as many as 26% of internal attacks are malicious and criminal.

Between August and November 2021, **numerous USB drives with malicious software** were sent to transportation, defense and insurance sector employees through the mail and UPS. These USB drives came with fake letters impersonating the Department of Health and Human Services and Amazon. The FBI issued a public warning identifying this as an attack from the FIN7 hacker organization, dubbing the attack "BadUSB."

BadUSB worked as an initial downloader for whatever malware the threat actor wanted to introduce — from credential grabbers to backdoors and ransomware. Researchers suspect the attackers were exploiting the rise of remote work, hoping to trick employees into installing malware on their home devices, compromising company networks.

BadUSB was not the only USB drive campaign targeting employees in recent years. In 2023, a hacker group known as UNC53 compromised at least 29 organizations in the United States, Europe and Asia by convincing staff to insert malware-infected USB drives into devices connected to company networks, unleashing a remote-access trojan called Sogu.

Along with USB storage drives, attackers also use various rogue devices to target internal victims. They can include peripherals such as speakers, mice or headsets. Typically, these devices fly under the radar of many security solutions. Spoofed peripherals are recognized by computers as legitimate devices (using legitimate VID/PID/ClassID), due to a lack of visibility into the physical layer.

Often, USB-borne malware is intended to spread beyond the initial site of compromise, setting off a chain reaction of compromised data and systems. The person inserting the USB device may have malicious intent or may be the victim of a social engineering attack. If an organization does not keep track of the USB devices and peripherals connected to company hardware, it cannot trace these events back to their origin, and further attacks may result.

To enact Zero Trust for devices, companies must ensure they can set company-wide restrictions that are automatically enforced around when and how USB ports are used and who can use them. Further, companies need the ability to recognize when peripherals are being plugged into any device on their network, as well as the ability to see who plugged in the device in case an investigation is needed.

Hardware supply chain compromise

Introducing a hardware-based threat during the manufacturing process is extremely difficult, however it can offer a big payoff for threat actors.

For example, a threat actor might intercept a digital device in transit from one factory to the next and insert a wireless keylogger device into the laptop's docking station. That will ultimately give the attacker access to every work conversation, password, product roadmap and any other sensitive company or personal data accessed from that device.

To mitigate this type of supply chain attack, it's important that companies have access to a bill of hardware components for every endpoint. A comprehensive bill of hardware should include:

With this in hand, security teams can then recognize any unexpected components or changes, such as the presence of a keylogger. Importantly, teams can use this bill of hardware components to assure the security of newly purchased devices, as well as maintaining visibility into any hardware compromises that occur throughout the device's lifespan.

Exploitation of existing vulnerabilities

Like any device, peripheral devices — such as mice and external cameras and speakers — sometimes contain security flaws that hackers can discover and exploit. Once those vulnerabilities have been discovered and reported by security researchers, companies should be able to intervene if an employee tries to use a compromised device. However, if companies don't have visibility into which devices their employees are using, it can be difficult to stop them.

In 2021, a **security researcher discovered** an alarming vulnerability within a Razer brand mouse. Using the mouse while on a company network gave the researcher access to administrative privileges that would allow him to do anything an administrator could do. An employee with malicious intent who knew about this vulnerability would be able to inflict an enormous amount of damage, from introducing malware to finding and exfiltrating sensitive company data they were unauthorized to access — simply by plugging in a mouse without the company knowing. To reduce overall risk, companies must have the ability to recognize when a device with a known vulnerability has been plugged into a company endpoint. Having this visibility enables IT teams to intervene before the vulnerability can be exploited.

Gaining visibility into hardware compromise is one important way to extend Zero Trust to the device level. But some threats target the chip-level code on devices, rather than the hardware. That is why organizations must also employ this second approach to device-level Zero Trust.

Experts sound the alarm: A call for Zero Trust to extend to physical device security

Regulatory organizations and top security researchers are calling government agencies and enterprises to enhance their security against physical device compromise.

U.S. Office of Management and Budget

In response to the May 2021 Executive Order on Improving the Nation's Cybersecurity, the Office of Management and Budget released its recommendations for Moving the U.S. Government Towards Zero Trust Cybersecurity Principles. One of its goals is to ensure the following:

"The Federal Government has a complete inventory of every device it operates and authorizes for Government use and can detect and respond to incidents on those devices. To enforce a Zero Trust architecture, agencies must monitor and assess the security posture of all of their authorized devices."

NSA

In October 2023, the NSA published a cybersecurity information sheet called Advancing Zero Trust Maturity Throughout the Device Pillar. It provides detailed recommendations for effectively addressing the device pillar of Zero Trust, saying:

"Continued cyber incidents have called attention to the immense challenges of ensuring effective cybersecurity across the federal government, as with many large enterprises, and demonstrate that "business as usual" approaches are no longer sufficient to defend the nation from cyber threats. The government can no longer depend only on traditional strategies and defenses to protect critical systems and data."

CISA

In its official Zero Trust Maturity Model guidelines, CISA includes device security as a pillar of Zero Trust architecture, saying:

"Agencies should secure all agency devices, manage the risks of authorized devices that are not agency-controlled, and prevent unauthorized devices from accessing resources. Device management includes maintaining a dynamic inventory of all assets including their hardware, software, firmware, etc., along with their configurations and associated vulnerabilities as they become known."

U.S. Department of Homeland Security and Department of Commerce

A joint draft report from the U.S. Department of Homeland Security (DHS) and Department of Commerce said firmware presented "a large and ever-expanding attack surface" for hackers to exploit, noting:

"Securing the firmware layer is often overlooked, but it is a single point of failure in devices and is one of the stealthiest methods in which an attacker can compromise devices at scale."

Microsoft

In March 2021, Microsoft's Security Signals report showed that more than 80% of enterprises had experienced at least one firmware attack in the past two years, saying:

"New data shows that firmware attacks are on the rise, and businesses aren't paying close enough attention to securing this critical layer. ...Attacks against firmware are outpacing investments targeted at stopping them."

3 ways to extend Zero Trust to the physical layer

1 Gain visibility into every piece of hardware connected to company systems to assess risk and protect against hardware-borne attacks, including both internal and supply chain threats.

Most organizations struggle to keep track of the hardware connecting to their network and systems, and it's understandable why. The average enterprise now manages about **135,000 devices** — many of which are at risk because they have become undetectable by company IT software.

With limited ability to track even company-owned devices, IT teams often have no way of knowing when an employee plugs in a harmless USB peripheral — or a compromised device. Furthermore, they have little to no ability to recognize product tampering that happens during the manufacturing process, especially since threat actors are skilled at evading detection.

To improve their Zero Trust maturity posture against hardware-based attacks, enterprises must prioritize gaining comprehensive visibility into the devices connecting to their systems. Additionally, they need the capability to identify and validate the integrity of these devices, detecting any potential tampering attempts.

51% of malware attacks are designed for USB devices.

In 2024, **Honeywell's USB Threat Report** showed 51% of all malware attacks were designed for USB devices. That is an almost six-fold increase from the 9% reported in 2019.

The rising number of USB-borne malware attacks has surprised security researchers. USB attacks were previously considered outdated because they required physical access, social engineering or the exploitation of supply chain vulnerabilities — all of which are challenging and risky for attackers.

The fact that more than half of malware attacks are targeted for these devices demonstrates threat actors' willingness to take on additional risk to achieve the greater rewards of exploiting physical devices.

2 Consistently scan firmware code to identify device vulnerabilities, misconfigurations, threats and compromises, needed updates and unauthorized changes.

Like hardware, firmware vulnerabilities were long underestimated by companies and only recently recognized as a major threat vector. Firmware is code installed on a device's chip during the manufacturing process to **tell the hardware how to run**. As TechTarget describes it, "Hardware makers use embedded firmware to control the functions of various hardware devices and systems, much like a computer's operating system (OS) controls the function of software applications."

In recent years, thought leaders including Microsoft and the U.S. Department of Homeland Security have deemed firmware compromise a growing threat. Microsoft revealed that, as of 2021, **80% of enterprises** had experienced at least one firmware attack in the prior two years. In 2018, **LoJax** became the first known malware to successfully infiltrate the UEFI code of its targets' devices. Several other high-profile firmware vulnerabilities have also been exposed by threat researchers in coordinated disclosure with the affected device makers, including **LogoFAIL**, **Spectre, and Meltdown**, bringing greater attention to the dangers of unsecured firmware.

Types of firmware

Firmware can be sorted into three categories based on the level of hardware integration:

Low-level firmware — Considered an intrinsic part of a device's hardware. Resides on read-only chips such as ROM and cannot be rewritten or updated. One-time programmable memory.

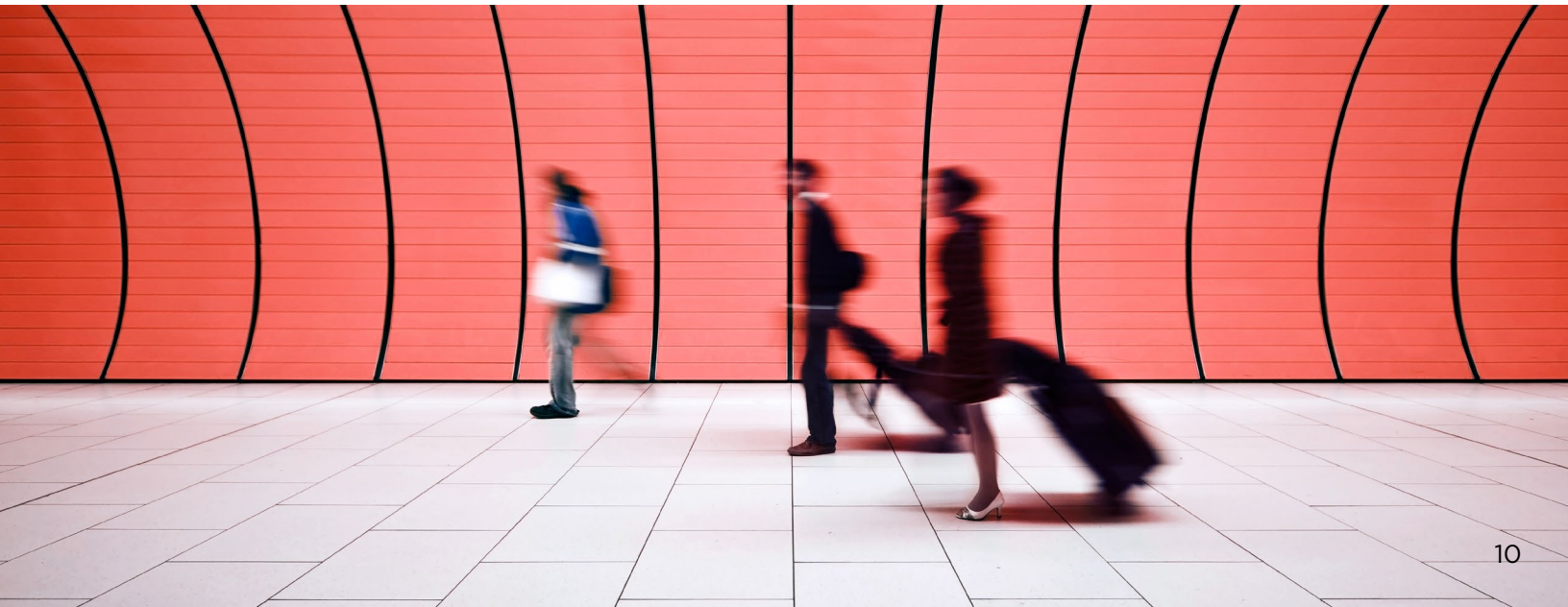
High-level firmware — Allows updates and is more complex than low-level firmware. In a computer, high-level firmware resides on flash memory chips.

Subsystem firmware — Often comes as part of an embedded system. Can be updated and is more complex than low-level firmware. For example, a server's power subsystem is a **piece of server hardware** that functions semi-independently from the server.

Source: **What is Firmware? Definition, Types and Examples (techtarget.com)**

There are a few ways firmware can be targeted by attackers. If devices are not implementing their Secure Boot functionality, threat actors can subvert the operating system when the device boots. In addition, vulnerabilities in the system UEFI or BIOS — like LogoFAIL — can grant attackers complete control over a device. Importantly, the same concerns apply to individual components within the device, including drives, processors, network adapters and more.

Having visibility into these components is crucial for companies to identify whether they are using devices with known vulnerabilities — or to identify suspicious changes to firmware. To improve an organization's Zero Trust maturity rating, they must verify that all firmware on devices connecting to company systems is what it says it is. This ability gives companies a way to understand a device's overall risk profile to set appropriate access rules for that device and prioritize updates.



There are a few common situations where companies may be particularly vulnerable to firmware-related risks:

- **Remote work and BYOD:** With the rise of remote work and BYOD, companies need the ability to audit the security posture of a variety of unmanaged devices, including employee laptops and routers, but also the company's networking and VPN infrastructure. Home routers have been targeted by **a number of large-scale, state-sponsored attacks** attempting to "extract passwords, intellectual property, and other sensitive information and to lay the groundwork for potential intrusions in the future."

  In addition, **CISA has issued a public alert** about vulnerabilities in popular corporate VPNs, including Citrix and Pulse Secure. As more company traffic runs through VPNs, it is important that organizations can ensure their infrastructure has not been compromised.

- **New device purchases:** While Zero Trust should mean that users and devices are presumed to be compromised until proven otherwise, companies may forget to apply this principle to new devices. However, the same supply chain vulnerabilities that apply to hardware-borne attacks also apply to firmware. Attackers with supply chain access may modify firmware with malicious implants that empower them to subvert higher-layer controls.

  Companies must remember to extend Zero Trust to new devices as well by scanning and verifying the firmware of all devices — ideally before purchasing them, but certainly before giving them wider access to company systems.

- **Firmware updates:** Device firmware needs to be updated on a regular cadence, as well as when new patches have been released to fix vulnerabilities. However, it is important to verify the firmware updates are behaving as expected, as there have been instances where **firmware used insecure updating practices** that could enable an attacker to intercept the update traffic and remotely deliver a malicious update instead of the intended version. Similarly, attackers have been able to **infiltrate a device maker's update** and deliver malware through the company's legitimate update tool.

  In each of these cases, organizations need the ability to detect vulnerable update processes and monitor for abnormal firmware behavior.

3 Leverage hardware-based full disk encryption with partitioning to protect data at rest on devices.

Forrester Research's **2023 State of Data Security** report showed that lost or stolen devices cause 17% of breaches. But only 7% of security decision makers are concerned about this type of breach, likely because they do not realize the prevalence or severity.

Data at rest on devices can be vulnerable to prying eyes, whether the device has been lost, stolen, seized or searched, or simply left unattended. When a device falls into the wrong hands, threat actors are skilled at bypassing security measures to gain access to files and other confidential information stored on devices. That can lead to data exfiltration, identity theft, intellectual property theft and corporate financial loss.

Stolen devices can also lead to network compromise. If an employee's device contains access credentials, they can be used to infiltrate the organization's network for a variety of nefarious purposes, such as spreading malware, exfiltrating or deleting data and more.

Lost and stolen devices put organizations and individuals at risk

Device theft and loss occur more frequently than companies might expect — leading to **17% of data breaches**. In an effort to protect their reputations and maintain their security, companies do not always report the incidence of lost and stolen devices, but a few alarming device losses have made the headlines in recent years:

Olympic insider misplaces computer and memory sticks

In February 2024, a City Hall engineer working on the Paris 2024 Olympics **reported a missing bag containing a computer and two memory sticks**. The engineer did not know whether the bag had been lost or stolen. The devices reportedly contained non-sensitive internal notes and transportation data, however this loss highlighted the risks of exposing proprietary and sensitive information stored on employee and contractor devices.

Chicago Public Schools loses $23 million in devices

During the 2021-22 school year, Chicago Public Schools reported the loss of **11% of their district-owned devices**, totaling 77,000 laptops and mobile devices. This figure included devices that were lost, stolen or untrackable by the school district's inventory system but may be recoverable. It is unknown whether the losses led to data breaches.

UK government loses thousands of laptops and mobile phones

In 2020, **the UK government revealed** there had been 2,004 incidents of lost or stolen devices among its employees in the preceding year. Alarmingly, most of the missing devices belonged to the Ministry of Defense (767) or the tax authority HMRC (288). Further, 10% of the missing devices reportedly were not encrypted. It is unknown whether these losses led to any data breaches.

Detection-based endpoint security solutions are an important security component, but if they are bypassed by adversaries, the damage can be substantial. To improve Zero Trust protection against physical device breaches, organizations need to look at data security on the device in a new way.

- **Companies must focus on prevention, not just detection:** Zero Trust is based on the idea that breaches will happen. It is vital that company security solutions be able to stop attackers from gaining access to important data by leveraging MFA for file and storage access.
- **Protection should live as close to the data as possible:** To fully embrace Zero Trust for data protection, companies need hardware-based, full disk encryption. This type of protection improves upon software-only solutions and policy-based data loss prevention by placing the protection directly in the storage and individual files.

  It delivers the added benefit of reducing the impact on system performance compared to software full disk encryption. Full-disk encryption even gives organizations the ability to create encrypted partitions within a hard drive to make highly classified information invisible to attackers or other prying eyes.
- **Companies need visibility into data access:** Often, when a device is lost, stolen or otherwise accessed by an unauthorized user, it is difficult to know whether data has been breached, and if so, which data. This makes it more difficult to identify compromised assets and prepare for collateral damage, such as follow-on attacks from stolen credentials.

  Hardware-based data encryption creates data logs to provide irrefutable documentation of activity so companies can know which sensitive data has fallen into the wrong hands. As with hardware-borne attacks and firmware attacks, having visibility into breaches affecting data at rest is a key component of achieving Zero Trust maturity.

Beware of “evil maids”

Today’s remote workers can do their jobs from anywhere — meaning company data travels everywhere. What happens when an employee with a high clearance level steps away from their device in a public setting — or even in their own hotel room? Unattended devices are a recognized threat vector for prying eyes, ranging from nosey neighbors to more sophisticated threat actors.

These more purposeful attacks on unattended devices are sometimes known as “evil maid” threats, originating from the idea that a hotel maid with a nefarious agenda could compromise a guest’s unattended device without that guest even knowing it.

Having hardware-level full disk encryption, along with visibility into which on-device data has been accessed and when, gives companies a strong defense against evil maid attacks and similar breaches of unattended devices.

Implementing Zero Trust for your devices

For any organization, reaching Zero Trust maturity across all five pillars — identity, devices, networks, applications and workloads and data — will be an ongoing journey, rather than a point-in-time project. The task is so vast, in fact, that many enterprises will be tempted to begin by shoring up the pillars they see as most critical. That will mean some organizations leave device-level security on the backburner, believing it to be less urgent.

However, the truth is that hardware attacks are no longer fringe cases. They represent one of the most pressing emerging threats to company data and networks and must be considered a critical priority for modern Zero Trust strategies.

No Zero Trust strategy can succeed without the help of automation and AI. Legacy technology — like legacy security architecture — is no longer up to the challenge of defending against today's most devastating threats, including hardware- and firmware-borne attacks. Look for toolsets, such as the Lenovo ThinkShield suite, that provide supply chain assurance, ongoing hardware and firmware visibility and the ability to automate key processes such as security scans and updates. Having the right technology will substantially improve your ability to achieve Zero Trust maturity and defend against emerging threats.

Stay ahead of the coming wave of hardware-borne attacks, and act now to implement Zero Trust defenses at the device level.

About Lenovo

Lenovo (HKSE: 992) (ADR: LNVGY) is a global technology powerhouse serving millions of customers every day in 180 markets. Focused on a bold vision to deliver smarter technology for all, Lenovo has built on its success as the world's largest PC company by further expanding into growth areas including software. Whether it's supporting hybrid work environments, enabling smart homes, empowering small and medium-sized businesses, revolutionizing AI gaming experiences, or enhancing digital learning, Lenovo Cloud and Software's portfolio of innovative solutions empower our customers to thrive in the ever-evolving digital landscape. Lenovo's world-changing innovation is building a more inclusive, trustworthy and smarter future for everyone, everywhere. To find out more, **visit our website**.

Discover how Lenovo's ThinkShield solutions can support your organization's efforts to implement Zero Trust at the device level.

Learn more