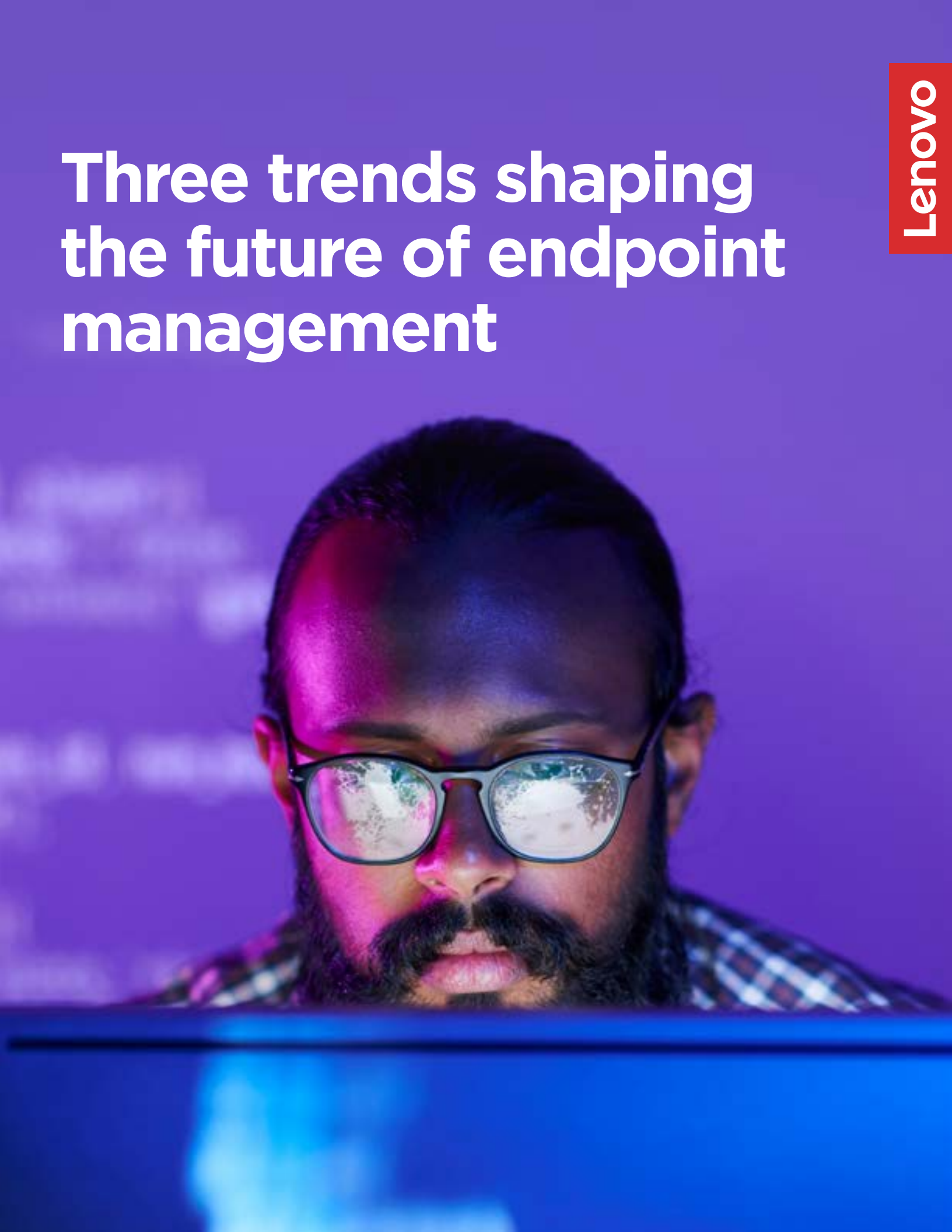
Three trends shaping the future of endpoint management



Endpoint management is at a turning point

Endpoint management has never been more critical for businesses both large and small. The average enterprise now manages about **135,000 devices**, and nearly half are at risk because of either an outdated OS or because they are no longer detected by the organization's IT department.

Meanwhile, as the boundaries between digital work and life are often blurred, corporate endpoints are exposed to a growing number of potential cyber threats. **Half of workers** surveyed use their company-owned devices to check personal email, shop online (32%), and access their personal social media accounts (28%). Moreover, **24% have allowed a friend or family member** to borrow their work device to check personal email, and **7% have visited illegal streaming sites**.

IT teams are well aware that company-issued devices are subject to this kind of risk exposure. However, it is becoming more concerning as cyber threats continue to rise and evolve. The new wave of free and low-cost generative AI tools is enabling **hackers to leverage GPTs** to easily create malicious software. Further, threat actors are turning their attention to new vectors, including device firmware. Addressing these threats will require a combination of employee training and Unified Endpoint Management (UEM) solutions.

Although IT teams understand the need to keep up with security-related patching and to document and manage the lifecycle of each device, many have found it challenging to do so. This is because most of these tasks require physical proximity to devices and manual updates that mean restarting employee devices in the middle of the workday. Improvements in UEM automation are alleviating some of this burden, unlocking new opportunities to not only keep endpoints more secure and visible, but also to begin other optimizations that keep devices operating in peak condition.

In this ebook, we'll cover how factors including the evolving threat landscape, remote work, net-zero pledges, and advancements in automation are all converging to shape the future of endpoint management in three key ways.

1 A focus on firmware security to preempt attacks

Firmware attacks are on the rise, and security professionals are taking note. In 2021, Microsoft found that **80% of firms** globally had experienced at least one firmware attack in the past two years.

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. The report went on to note:

> **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.**

Firmware vulnerabilities can present themselves in a few ways. Most often, they arise because of simple human error rather than malicious intent. However, they may also be created — or exploited — during the hardware manufacturing process.

Most modern IT manufacturers have built global supply chains to deliver more powerful technology at lower prices. To guarantee the integrity of their technology throughout manufacturing and minimize firmware vulnerabilities, companies need to establish a secure supply chain. Device makers should have processes in place for identifying and addressing security risks for intelligent components; ensuring suppliers are following exemplary security protocol; and providing auditable security help to customers.

Firmware attacks can manifest in a variety of forms, including malware, BIOS/UEFI rootkits, remote exploitation of firmware vulnerabilities, physical tampering, management backdoors and supply chain attacks. Fortunately, many of the most well-known firmware vulnerabilities — including LogoFAIL, Thunderspy, Spectre and Meltdown — have been discovered by security researchers and were not necessarily exploited by malicious attackers.

Upon discovery of these vulnerabilities, device manufacturers have worked quickly to release patches. However, for the average organization, patching firmware vulnerabilities can still take from **6-9 months**. In the meantime, the device's risk level is at an all-time high because the vulnerability has been publicized.

There can be a few reasons for this delayed response, but most commonly, IT teams have been reluctant to interrupt employee productivity. Patching often requires manual updates, physical access to the device and a device restart after installation. Because firmware has not historically been considered a major threat vector, many organizations have not prioritized these updates as part of their regular security routine.

What is changing:

Modern UEM solutions now have the capability to deliver security-related firmware updates as well as regular system updates — and to do so remotely and during off-peak work hours. IT teams can quickly roll out BIOS/UEFI security updates across their entire fleet and automate them for future deployment alongside regular system updates. Additionally, tech teams can leverage a modern UEM's reporting capabilities to ensure updates were implemented successfully.

Reputable device makers have had zero-trust supply chain security protocol in place for years, but enterprises are beginning to better understand the value of buying devices that are built by a heavily vetted supply chain. Continuing to do so will help reduce endpoint risk exposure.

Infamous firmware vulnerabilities

Hidden within device firmware can be vulnerabilities — weaknesses that hackers exploit to gain unauthorized access, steal data or disrupt operations. Let's explore some of the most infamous firmware vulnerabilities that have shaken the tech world in recent history.

LogoFAIL

A set of two dozen vulnerabilities discovered in 2023 within the UEFI code of many devices. Security researchers found they could rewrite the device logo that appears when a system boots, inserting malware that was delivered when the device booted. Major device makers released UEFI security updates as part of a coordinated disclosure.

Thunderspy

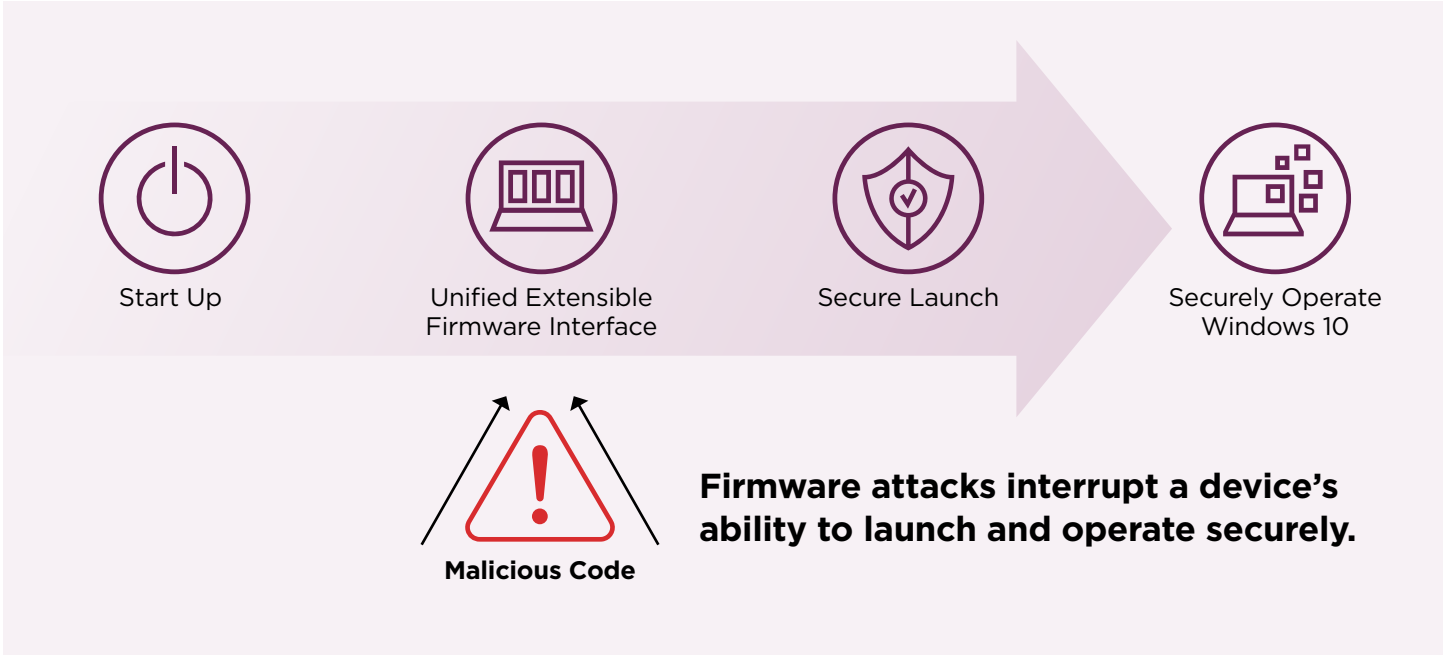
An attack developed by a security researcher in 2020 that demonstrated how hackers could launch an "evil maid" attack on unattended devices, gaining full access to their data within about five minutes. Using Thunderspy required the attacker to have physical access to the device to connect to the PC's Thunderbolt chip, so it was not deemed a significant threat. However, it provided a clear example of why supply chain security is vital for protecting device components.

Spectre and Meltdown

The names given to different variants of the same underlying vulnerability in most computer chips manufactured before 2017. The vulnerability was not patchable at the hardware level, so vendors released software patches to work around the problems.

FinSpy

A commercial spyware used by law enforcement and government agencies around the world, first discovered by the wider public in 2011 when it was referenced in WikiLeaks documents. Among other attack vectors, it can be loaded from UEFI and Master Boot Record (MBR) components.



Source: Microsoft: **Guarding against supply chain attacks—Part 2: Hardware risks (microsoft.com)**.

2 A prioritization of automated application patching to reduce the risk of data breaches

Firmware patching may be a newer priority for IT teams, but application patching has been a key focus for many years. Companies spend about **320 hours a week** on vulnerability response — equivalent to eight workers devoting full-time focus to application patching. Still, about **60% of data breaches** originate from a known, unpatched vulnerability.

Similarly, **one-third of ransomware attacks** originate with an unpatched vulnerability. In 2022, an estimated 55% of those incidents were caused by two vulnerabilities that had patches available — **ProxyShell**, a chain of exploits targeting three known vulnerabilities in Microsoft Exchange Servers, and **Log4Shell**, a vulnerability found in a common Java-based logging library used in a variety of applications.

Furthermore, there is evidence that ransomware breaches that start in this way are far more devastating for the victims than breaches that start with compromised credentials. Ransomware breaches that exploit unpatched vulnerabilities have four times higher overall attack recovery costs ($3M vs. $750k for compromised credentials) as well as a slower recovery time (45% took more than a month vs. 37% for compromised credentials).

There are a **number of factors** that can make patch management challenging for IT teams, including the vast number of patches released every day; the continued use of legacy and unsupported technology; a lack of visibility into vulnerabilities; and the ever-expanding number of software and systems many IT teams are managing.

More than half of organizations say they are at a disadvantage in responding to vulnerabilities because they use manual processes.

In addition, many teams follow risk-based prioritization of patches, where the vulnerabilities deemed most critical receive the swiftest attention. However, this can lead to presumably "lower-risk" vulnerabilities remaining unpatched and, sometimes, forgotten over time — until an attacker finds and exploits them.

What is changing:

Modern UEM solutions have significantly improved their ability to help IT teams effectively manage application patching. They can maintain a catalog of hundreds of application patches to ensure a wide range of vulnerabilities are easy to identify and remediate.

Along with this advancement, IT teams now have the opportunity to leverage UEM capabilities to scan all company endpoints to identify which applications are installed. They can then set up remote, automated patching of those applications during off-peak work hours, reducing the burden on IT team members and eliminating the need to interrupt employee productivity.

3 An opportunity to reduce energy consumption through power management

Although remote work has reduced overhead costs for many companies, the number one driver of energy consumption in the commercial sector is still **computers and office equipment**. A **survey of UK businesses** showed that, for more than half of companies, energy bills account for roughly 25% of business costs.

In conjunction with cutting those costs, many companies want to reduce their energy consumption to work toward **net-zero pledges**. According to the World Economic Forum, a critical mass of the largest companies and countries in the world have committed to net-zero goals, hoping to contribute to achieving climate stability.

Taking even basic measures to reduce energy consumption — such as leveraging digital solutions that monitor and control usage — can yield energy savings of **up to 40%**. However, many companies have not prioritized doing so in the past, often because other IT initiatives took precedence.

What is changing:

Modern UEM solutions now make it easy to program schedules for multiple power management options. Teams can set rules as to when singular or multiple company devices should power off and on, as well as sleep, hibernate or wake.

Teams can also use their UEM to schedule a switch from electric to battery power during peak hours of the day. These advanced features are expanding the utility of enterprise UEM solutions and making power management much more approachable to implement.

The average wattage of a company laptop

In February 2024, sustainability researchers and consultants Eco Cost Savings **published their findings** on the average power consumption of laptops, based on their study of 1,084 devices. They found:

- Laptop wattage for non-gaming PCs typically ranges from 30W to 200W, with the most common wattage being 65W.
- On average, laptops only use 0.34W in Off mode, 0.78W in Sleep mode, 2.45W in Long Idle mode and 5.91W in Short Idle mode.
- With typical usage, laptops consume 55.45 watt-hours (0.055 kWh) per day, 1,686.6 watt-hours (1.69 kWh) per month and 20,238.8 watt-hours (20.24 kWh) per year.
- It costs $3.04 per year to power a laptop, on average.

For companies with hundreds of thousands of endpoints on-site, reducing laptop energy usage can equate to significant savings each year.

Strong IT leadership is vital in this new era

At this critical turning point for enterprise endpoint management, today's IT leaders are called upon to not only be technical experts but also strategic negotiators. They must be forward-thinking, navigating the challenges and opportunities that AI presents.

It is difficult to overstate the importance of enacting an endpoint strategy that sets IT teams up for success as risk exposure increases and threats continue to escalate. For many organizations, this will mean seriously reevaluating their tools, practices and priorities to build a modern endpoint management strategy from the ground up.

IT leaders who can adopt flexible, solution-oriented approaches will build a strong foundation to address future challenges. Progress begins with acknowledging the challenges we face and then tackling them with practicality and confidence.

How Lenovo Device Manager helps

Lenovo Device Manager, or LDM, is a cloud-based endpoint management solution that simplifies device and app management for IT admins. Developed by Lenovo engineers for Lenovo devices, LDM enables IT to centrally manage and secure their fleet.

Empower your IT team with LDM:

Effortless updates

Automate firmware, drivers, BIOS and software updates.

Centralized management

Monitor all devices from a central console.

Detailed device insights

Gain real-time data on device performance and health.

Scalable solution

Manage a growing number of devices with ease.

Energy optimization

Schedule rules to automatically manage power consumption.

When evaluating UEM options, explore solutions designed specifically for your devices by the original equipment manufacturers (OEMs). LDM makes it easy to begin streamlining and automating firmware and system updates, applying security patches, and instituting power management rules — across all your applicable devices. We leverage a constantly updated repository to deliver patches seamlessly through our UEM solution, ensuring your systems are always protected with the latest security updates.

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 expanding into growth areas including software. Whether it's supporting hybrid work environments, enabling smart homes, empowering 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**.