SAMSUNG

SSD

Using Secure Solid-state Drives (SSD) to Guard against Today's Cyber Threats

Technology Paper

Rapidly Evolving Threat Landscape

Because storage devices and media are the ultimate resting place of data, they have been a focus point of many nefarious actors (threat agents). As storage drive capacities have soared into multi-terabyte ranges, this storage can be a real treasure trove in the wrong hands. Data has become the "coin of the realm" in many organizations and market sectors, so the incentives to acquire it, exploit it, damage it, etc. for malicious purposes (i.e., intentional and malevolent acts or actions) by internal and external threat agents have increased exponentially.

Cybercrime is forecasted to cost the world $9.5 trillion USD in 2024, according to Cybersecurity Ventures.[1]

Contemporary attackers have access to tools and kits (e.g., ransomware as a service) that were only available to nation states and organized crime in the past; in short, attackers have caused bigger impacts with fewer technical skills, resulting in extortion, data theft, stolen intellectual property, and significant reputational damage. More advanced attackers now employ a wide range of very sophisticated attacks against information and communications technology (ICT) platforms and their individual components in their pursuits of data. Some of these attackers are already employing artificial intelligence to help them identify vulnerabilities and weaknesses in products (hardware and software) as well as protocols and interfaces used in these products.

Responding to the Threat Landscape

It is generally safe to say that the security community is in a defensive posture that attempts to respond to current or perceived threats. A core element of this response is active vulnerability management and patch management that help eliminate or mitigate known attacks. For zero-day events (i.e., not previously seen), reliable and timely cyber threat intelligence (strategic, tactical, operational, and technical) can provide early warnings that enable an organization to take proactive, protective actions or to help mitigate attacks that are already happening.

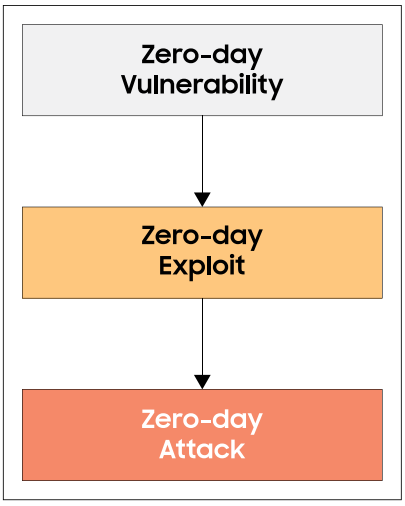

Figure 1

A wide assortment of security-oriented standards have been developed for the protection of information and ICT by formal standards development organizations (see table for examples). While compliance with these standards is often voluntary, they can be directly or indirectly invoked as part of statutory or regulatory requirements at the local, national, and/or regional (e.g., EU) level. From a legal perspective, many of these standards are recognized as best practices for which conformance can be a way of demonstrating *due care.*

In addition, a significant number of industry associations are also involved in the development of specifications that are relevant to storage security. The relationships, interactions, and interdependencies between the formal standards development organizations and industry associations add another dimension of complexity (see table 1).

Some organizations are seeking alternatives to reactive defenses and are looking to more proactive approaches like zero trust security. With zero trust security there is no implicit trust of users or system and the operating environment is assumed to be hostile

[1] https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024

International	International Organization for Standardization (ISO) International Electrotechnical Commission (IEC) International Telecommunication Union (ITU) Institute of Electrical and Electronics Engineers (IEEE)
Regional	European Committee for Standardization (CEN) European Committee for Electrotechnical Standardization (CENELEC)
National	US National Institute of Standards and Technology (NIST) Korean Agency for Technology and Standards (KATS) British Standards Institution (BSI) German Institute for Standardization (DIN) Singapore Standards Council (SSC) Standards Council of Canada (SCC)

Table 1

and fully compromised. All users and systems are required to be authenticated, authorized, and their access continuously validated prior to being granted access to data or resources. System security configurations and maintenance patches, or the absence of current patches, can also impact granted access. Such an architecture, when implemented correctly, has been shown to prevent data breaches. In addition, when attacks are successful the damage is typically limited in scope.

Another alternative is the use of confidential computing, which goes beyond protecting data in-motion and data at-rest by adding protection for data in-use (active data undergoing analysis, change, or other manipulation). This protection is accomplished through the use of hardware-based, attested[2] Trusted Execution Environments (TEE), providing assurance of data integrity, data confidentiality, and code integrity. During computation, these TEEs prevent unauthorized access or modification of applications and /or data thereby always protecting data.

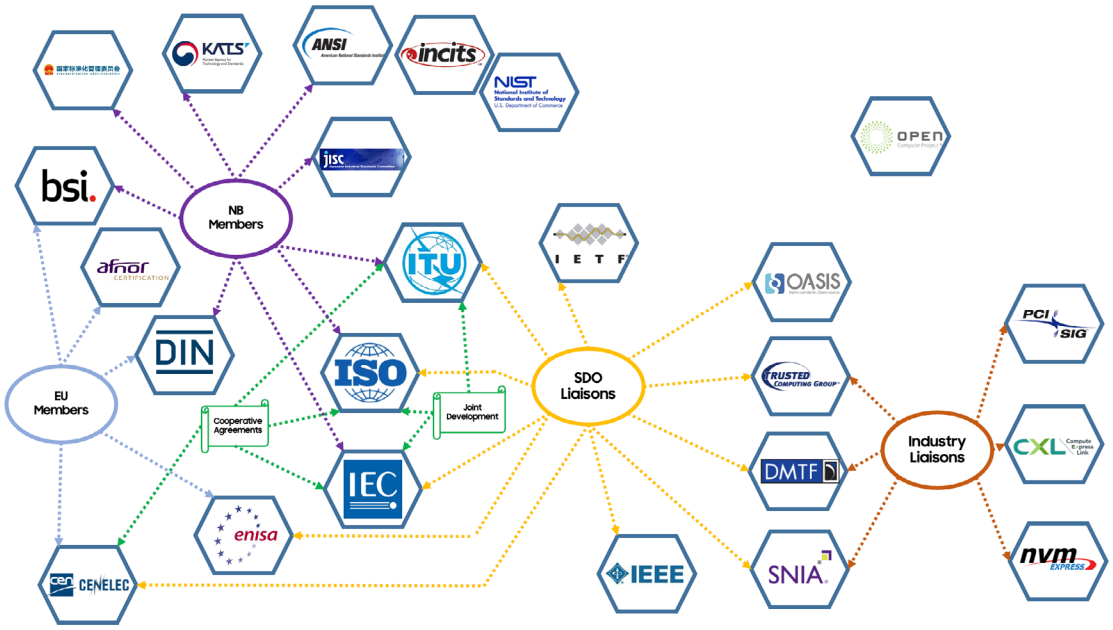

Figure 2

[2] The goal of attestation is to prove to a remote party that firmware, operating system, and/or application software are intact and trustworthy.

Securing Solid-state Drives (SSD)

Basic SSD Security

Storage drives have evolved from devices that simply record and retrieve data to systems that actively participate in the protection of data. Using the Trusted Computing Group (TCG) *Security Subsystem Class (SSC): Opal*, Version 2.02 as a representative example, the following security functionality is commonly available:

- **Drive locking**
  This feature prevents access to user data at-rest until the correct authentication key is presented to the drive. Once configured, the drive automatically locks when it is powered down. Additional locking controls can be enabled to control firmware downloads.

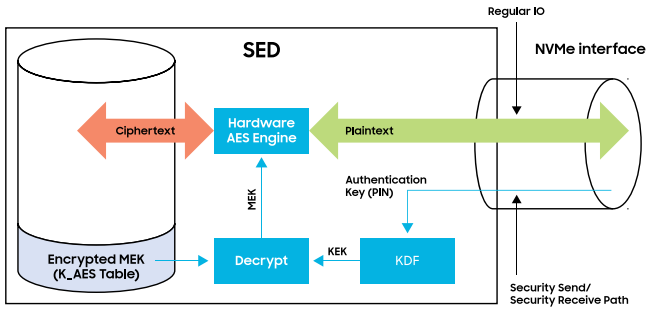

Figure 3

- **Internal encryption and key management**
  This feature ensures all user data written to self-encrypting drives (SED) are encrypted by the drive before being written and decrypted by the drive when data are read. The TCG *Storage Architecture Core* Specification requires compliant drives to use the Advanced Encryption Standard (AES) as the encryption algorithm in one of several block cipher modes of operation (XTS, CBC, GCM, etc.). However, the US National Security Agency (NSA) Commercial National Security Algorithm Suite (CNSA Suite) Version 1.0 further constrains the acceptable algorithms for encryption, signing, and integrity checking that can be used for all "national security systems" (software and hardware that will be run by defense or intelligence agencies). While all data at-rest are protected, it is important to note that data in transit between the host and drive are not encrypted.

- **Media sanitization**
  This feature, as defined by ISO/IEC 27040:2024[3], eradicates some or all of the user data stored on the drive using a clear or purge sanitization technique as specified in IEEE 2883-2022[4]. From a sustainability perspective, this data eradication is a prerequisite to drive reuse.

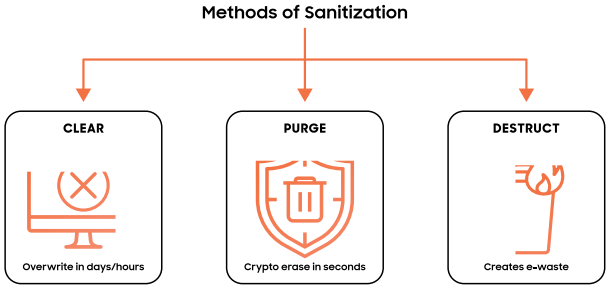

Figure 4

With these capabilities activated correctly, organizations are afforded protection against data breaches due to lost or stolen drives as well as having efficient data eradication capabilities when the drives are to be removed from service.

Samsung SSDs, including models PM1743 and PM9D3a, are compliant with TCG Opal SSC Version 2.02 and include drive locking functionality along with XTS-AES-256 encryption. In addition, the cryptography (algorithms and parameters[5]) used in Samsung SSDs are in compliance with CNSA Suite 1.0. Samsung SSDs also include IEEE 2883-2022 compliant media sanitization that uses cryptographic erase for purge-based sanitization operations.

SAMSUNG

SSD and Platform Trust

Many organizations have a supply chain in which third-party organizations develop hardware/software components that are used in the development of their products. Supply chain attacks (e.g., counterfeit systems and components, vulnerable components, and implanted backdoors) are an increasing reality that affect organizations and their customers. As a mitigation strategy, some organizations and vendors have adopted a platform security architecture that goes beyond applications and operating systems to also include functions and services provided by the underlying layers (i.e., the platform). The platform[6] includes the hardware and firmware components necessary to initialize components, boot the system, and provide runtime services implemented by hardware components (i.e., necessary for the system to operate).

Platform firmware and its associated configuration data are not only critical to the trustworthiness of a computing system, but much of this firmware is highly privileged in the system architectures. A successful attack on platform firmware could render a system inoperable, perhaps permanently or requiring reprogramming by the original manufacturer, resulting in significant disruptions to users. Other sophisticated malicious attacks could attempt to inject persistent malware in this firmware, modifying critical low-level services to disrupt operations, exfiltrate data, or otherwise impact the security posture of a computer system.

To help address these issues, additional security features and capabilities are being integrated in modern SSDs, including:

- A hardware Root of Trust (RoT)[7] in the form of highly reliable hardware, firmware, and software components that perform specific, critical security functions that serve as the trust anchor for many of the drive's security features. At a minimum, the RoT hardware-based controls can provide a foundation for establishing platform integrity assurances. For example, a RoT may execute a "trusted boot" process that ensures any software running on a device is trustworthy.

- Secure boot to ensure the SSD only runs authentic firmware and measured boot to collect/report measurements (digests) of code being loading. Secure boot is anchored to an immutable RoT and it prevents unauthorized software (e.g., malware) from taking control of the device. With TCG Device Identifier Composition Engine (DICE) devices can make authoritative statements to establish device identity and make claims about itself (e.g., its state, configuration, date, coding, etc.). Collected measurements can be used for attestation purposes.

- Remote device that enables an SSD to provide verifiable evidence of its identity and operating state in response to a host challenge to establishing trust with the SSD. This evidence is in the form of claims, including hardware identity, software image, security-relevant configuration, operating environment, etc. Within SSDs, the DMTF Security Protocol and Data Model (SPDM) is instrumental in delivering these device claims, along with authentication and provisioning of hardware identities, measurement for firmware identities, session key exchange protocols to enable confidentiality with integrity protected data communication and other related capabilities.

With these capabilities, organizations can determine the trustworthiness of SSDs used within their systems and infrastructure as well as verifying this trustworthiness throughout the life of the SSDs.

Samsung SSDs, including models PM1743 and PM9D3a, have hardware RoTs and support for TCG DICE. When used in conjunction with supported SPDM, this capability enables a host/platform to automatically verify the authenticity and integrity of the hardware and software state of the SSD.

[3] ISO/IEC 27040:2024 (2nd Ed.), Information security – Security techniques – Storage security
[4] IEEE 2883-2022, IEEE Standard for Sanitizing Storage
[5] Key size, modulus, or curves.
[6] As described by NIST Special Publication 800-193 Platform Firmware Resiliency Guidelines.
[7] According NIST SP 800-193, a Root of Trust (RoT) is an element that forms the basis of providing one or more security-specific functions, such as measurement, storage, reporting, recovery, verification, and update. A RoT is typically just the first element in a Chain of Trust (CoT) and can serve as an anchor in such a chain to deliver more complex functionality.

Future Directions for SSD Security

The storage industry continues to explore and develop security capabilities focused on having storage serve as a last line of defense in protecting data. Current efforts include:

- Secure communications that are unsusceptible to eavesdropping or interception between SSDs and the systems to which they are connected. In the past, SSD connections to systems transferred data and commands without secure communications; when needed, sensitive data were encrypted prior to being stored on the SSD. However, recent specifications from the Peripheral Component Interconnect Special Interest Group (PCI-SIG™) for the PCI Express™ (PCIe™) optional Integrity and Data Encryption (IDE) feature and the DMTF SPDM optional secure sessions feature may change this in the future. Both PCIe IDE and SPDM can protect transmitted data and commands, using AES-256 encryption, between systems (host and VMs) and SSDs.

- Fine-grain encryption and external key management. Most TCG Opal compliant SSDs have the ability to use multiple, internally generated and managed media encryption keys (MEK) that are associated with defined Logical Block Addressing (LBA) ranges (typically no more than 1024 such LBA ranges). Recent enhancements to the NVM Express™ (NVMe™) specification and collaboration with the TCG on multiple specifications[8] have resulted in publication of Key Per I/O (KPIO) functionality. KPIO allows a host to securely inject a finite number (few hundred to a few thousand) of MEKs into a key cache that the SSD is then able to use in subsequent reads and writes, which include a key tag (specifies an entry in the key cache). Using KPIO, a host has complete control of the lifecycle of the MEKs (MEKs are removed from the SSD on a power cycle of the SSD) and can employ an almost limitless number of MEKs as long as the host ensures that the MEKs are injected into the key cache prior to use. A promising use case involves having each VM on a system controlling its own MEKs that get used on some number of SSDs.

- Conventional/classic asymmetric cryptographic algorithms (RSA, ECC, DH, etc.) base their security on one of three hard mathematical problems: the integer factorization problem, the discrete logarithm problem or the elliptic-curve discrete logarithm problem. However, these algorithms are under serious threat by the recent relatively rapid advancement in the capabilities of quantum computing and will be effectively completely broken when a Cryptographically Relevant Quantum Computer (CRQC) becomes a reality. In anticipation of a CRQC, NIST is specifying quantum resistant cryptography that includes the CRYSTALS-Kyber (FIPS 203), CRYSTALS-Dilithium (FIPS 204), and SPHINCS+ algorithms (FIPS 205); the FALCON algorithm is anticipated in late 2024. In addition, the US Government (NIST and NSA) has issued guidance (e.g., use of CNSA Suite 2.0) that quantum-resistant algorithms must be fully deployed in Government systems within the 2030-2033 timeframe, which means the supply chain is expected to be ready in the 2026-2027 timeframe. For symmetric key encryption, the guidance is to basically double the key size, so AES implementations are expected to use 256-bit keys. CNSA 2.0 does not require a transition from SHA-2 to SHA-3, but SHA-3 is used in at least one of the quantum-resistant algorithms.

- Trusted Execution Environments (TEEs) and secure enclaves are technologies often associated with confidential computing to protect data in-use (i.e., securely isolate workloads). Extending these concepts to virtual machines (VM), specifically TEE VMs (TVM), where a portion of one or more devices are assigned to the TVM, it is necessary to establish and maintain a TEE for the composition. Building upon security foundations of DMTF Component Measurement and Authentication (CMA)/ SPDM and PCIe IDE for a secure interconnect between the host and a device, the PCIe TEE Device Interface Security Protocol (TDISP) can be used to establish and maintain a trust relationship between a TVM and a device.

Many of these capabilities are covered in recent specifications and some are still in draft form. Samsung is actively tracking and/or participating in these developments and adjusting the Samsung SSD security functionality to counter evolving threats and meet customer requirements.

Trust but Verify

The implementation of security features and capabilities within storage systems is of increasing importance to organizations around the world. Many of these organization (e.g., government, financial, energy, telecommunications, and other markets) seek assurances that storage technology has passed rigorous security testing by appropriate third-parties (e.g., an accredited lab), that the test results have been validated, and that the product can be used to secure sensitive information.

The following are the more common forms of security validation and certification programs relevant to SSDs:

- Formal certification schemes with established security evaluation criteria have been establish for cryptographic modules as well as for the entire suite of security capabilities of product. International cryptographic module certifications (e.g., South Korea, Japan, Malaysia, Spain, and Turkey) are possible based on ISO/IEC 19790 and ISO/IEC 24759; in the US and Canada these standards are used with modifications specified in the NIST SP 800-140x documents as part of the FIPS 140-3 Security Requirements for Cryptographic Modules. Four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments are specified along with the security requirements covering areas related to the secure design, implementation and operation of a cryptographic module.

- Common Criteria for Information Technology Security Evaluation, often referred to as Common Criteria (CC), is an international set of specifications (e.g., the ISO/IEC 15408 series) and guidelines designed to assess information security products and systems; CC serves as a basis for internationally–recognized certifications of products security capabilities. To help with consistency across a specific technology type (e.g., firewalls), a Protection Profile (PP) or collaborative PP (cPP) may be developed by a government to specify both functional and assurance requirements; products undergoing evaluation can claim conformance to one or more PP/cPP. Under the Common Criteria Recognition Arrangement (CCRA), all member countries agree to recognize each other's Common Criteria certificates, which allows developers to access the global marketplace regardless of where their product is certified. The latest version of Common Criteria (CC:2022 Release 1) is relatively new and an industry transition from version 3.1 is underway. As an example of the importance of CC, the EU Cybersecurity Act introduces an EU-wide cybersecurity certification framework for ICT products, services and processes; the new European Common Criteria-based cybersecurity certification scheme[9] (EUCC) is expected to handle a significant number of the certifications of ICT products destined[10] for the EU.

- TCG Storage Opal compliance for an SSD can be determined by subjecting such a device to a third-party validation of the TCG Storage Opal Family Test Cases, which are a set of tests that verify the correct behavior of a storage device. The TCG also offers a Storage Certification Program that starts with the Opal compliance validation and further includes the SSD successfully achieving Common Criteria certification with the Full Disk Encryption (FDE) Encryption Engine (EE) cPP included as part of the evaluation criteria.

Samsung SSDs, including models PM1743 and PM9D3a, are validated against the TCG Storage Opal Family Test Cases. In addition, these Samsung SSDs are either FIPS 140-2 or FIPS 140-3 validated or undergoing FIPS 140-3 validation. Common Criteria certification is not commonly required of devices like SSDs at this time, but Samsung has extensive experience with CC and mobile devices; CC certification of SSDs is something that Samsung is monitoring, including The EU Cybersecurity Act (Article 49 Regulation EU 2019/881).

[8] TCG Storage Key Per I/O SSC Version 1.00 Revision 1.41, September 1, 2023
[9] https://www.enisa.europa.eu/topics/certification
[10] Certification to the new EUCC will initially be voluntary, but the European Commission will periodically review the schemes' efficiency and use, and whether certification should be mandatory

Advancing the State of Storage Security

Storage security is complex in that it plays a role at many different levels. From an organizational level there are storage media handling and data protection requirements (e.g., ISO/IEC 27001 and NIST SP 800-53). From a platform level, there are technology-specific requirements for storage covered by standards such as ISO/IEC 27040:2024 and IEEE 2883-2022 along with a plethora of country-specific standards. These standards specify what needs to be addressed, and to a lesser degree, how to do it. At the component level, specific storage security mechanisms and capabilities are described in specifications from organizations such as the Trusted Computing Group, PCI-SIG, DMTF, NVM Express, CXL Consortium™, SNIA, etc.

Samsung actively participates in all the major industry activities associated with storage security (e.g., TCG, DMTF, OCP, PCI-SIG, etc.). Additionally, Samsung has provided key leadership in developing international storage security standards (e.g., ISO/IEC 27040:2024 and IEEE 2883-2022). Samsung also collaborates with the storage industry on industry best practices (e.g., SNIA encryption/key management[11] and Fibre Channel security[12] papers) and general storage security awareness (e.g., IEEE Computer Society, Computer article[13]).

Summary

The threat landscape is evolving and devastating attacks are occurring at a dizzying pace, exposing massive amounts of sensitive and high value data to data breaches and to possible data destruction (e.g., ransomware). Regulatory, statutory, and legal entities as well as standards development organizations and industry associations aim to mitigate or eliminate these problems through an assortment of activities and publications. To realize a benefit from these activities, product developers and consumers of these products need to adjust their strategies, approaches, and technologies in a timely manner.

As evidenced in this paper, Samsung is actively keeping abreast of storage security developments, tracking initiatives within key industry associations and formal standards development organizations. Samsung adapts the security capabilities of its SSDs to respond to the evolving threat and regulatory landscapes. Customer who avail themselves of Samsung SSD security capabilities are afforded additional tools in their arsenal to protect data.

[11] SNIA, Storage Security: Encryption and Key Management, September 2023, https://www.snia.org/educational-library/storage-security-encryption-and-key-management-technical-paper-2023

[12] SNIA, Storage Security: Fibre Channel Security, February 2024, https://www.snia.org/sites/default/files/technical-work/whitepapers/SNIA-FCIA-Storage-Security-Fibre-Channel-Security.pdf

[13] IEEE Computer Society, Computer, Self-Encrypting Drive Evolving Toward Multitenant Cloud Computing, February 2024, https://www.computer.org/csdl/magazine/co/2024/02/10417805/1Ua1C4FoH8k

AES	Advanced Encryption Standard
ASIC	application-specific integrated circuit
CBC	cipher block chaining
CNSA	The Commercial National Security Algorithm Suite (CNSA) is a set of cryptographic algorithms promulgated by the US National Security Agency (NSA)
DMTF	Organization that creates open manageability standards spanning diverse emerging and traditional IT infrastructures including cloud, virtualization, network, servers and storage.
ECC	Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.
FIPS	Federal Information Processing Standards (FIPS) of the United States that are a set of publicly announced standards that the National Institute of Standards and Technology (NIST) has developed.
DH	The Diffie-Hellman (DH) Algorithm is a key-exchange protocol that enables two parties communicating over public channel to establish a mutual secret without it being transmitted.
DICE	Device Identifier Composition Engine
GCM	Galois/Counter Mode
ICT	information and communications technology
IDE	Integrity and Data Encryption
IEEE	The Institute of Electrical and Electronics Engineers (IEEE) is a technical professional organization dedicated to advancing technology for the benefit of humanity through its publications, conferences, technology standards, and professional and educational activities.
LBA	logical block addressing
KEK	key encryption key
MEK	media encryption key
OCP	The Open Compute Project (OCP) is a collaborative community focused on redesigning hardware technology to efficiently support the growing demands on compute infrastructure.
RoT	Root of Trust
SPDM	Secure Protocol and Data Model
SoC	System on Chip
TCG	The Trusted Computing Group (TCG) is an organization formed to develop, define and promote open, vendor-neutral, global industry specifications and standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms.
TDISP	TEE Device Interface Security Protocol
TEE	trusted execution environment
TVM	TEE virtual machine
VM	virtual machine
XEX	Xor-Encrypt-Xor
XTS	XEX-based tweaked-codebook mode with ciphertext stealing

Table 2

For more information

For more information about the Samsung Semiconductor products, visit semiconductor.samsung.com.

About Samsung Electronics Co., Ltd.

Samsung Electronics Co. Ltd inspires the world and shapes the future with transformative ideas and technologies. The company is redefining the worlds of TVs, smartphones, wearable devices, tablets, digital appliances, network systems, memory, system LSI and LED solution. For the latest news, please visit the Samsung Newsroom at news.samsung.com.

Samsung Electronics Co., Ltd.
129 Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 16677, Korea **www.samsung.com** 1995-2021

SAMSUNG