



***winbond***  
**TrustME<sup>®</sup> Security Solution**

## ***Vision Statement***

以綠色半導體技術豐富人類生活的隱形冠軍

***Be a hidden champion in providing sustainable  
semiconductors to enrich human life.***

***winbond***



# WINBOND'S TrustME<sup>®</sup>

## Application Scope

Winbond introduced the first certified Secure Flash to protect connected devices across several markets



### Automotive



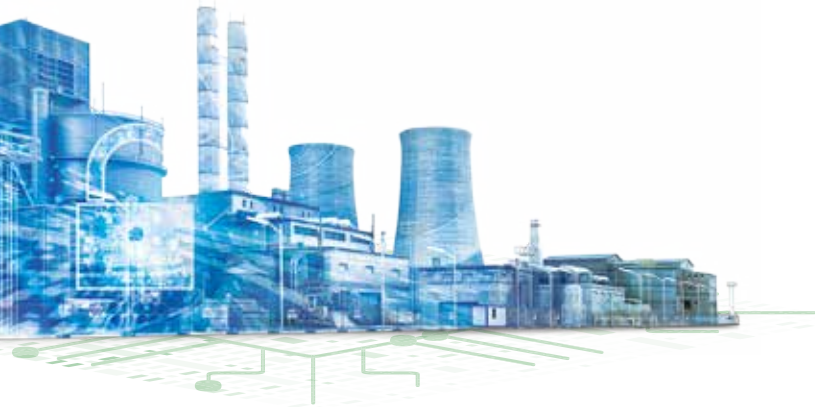
GPS



Wi-Fi



Cloud



### Industry 4.0



Sensors



Robots



Servers



### IoT



Smart Camera



Smart Door Locks



Home Energy Console

## A Leading Specialty & Secure Memory Supplier

---



A heavy investment on security infrastructure and technology



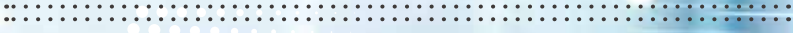
All manufacturing sites are certified for Common Criteria EAL 5+ products



Active participation in standard bodies and security forums

**winbond**  
威邦电子

# W75F



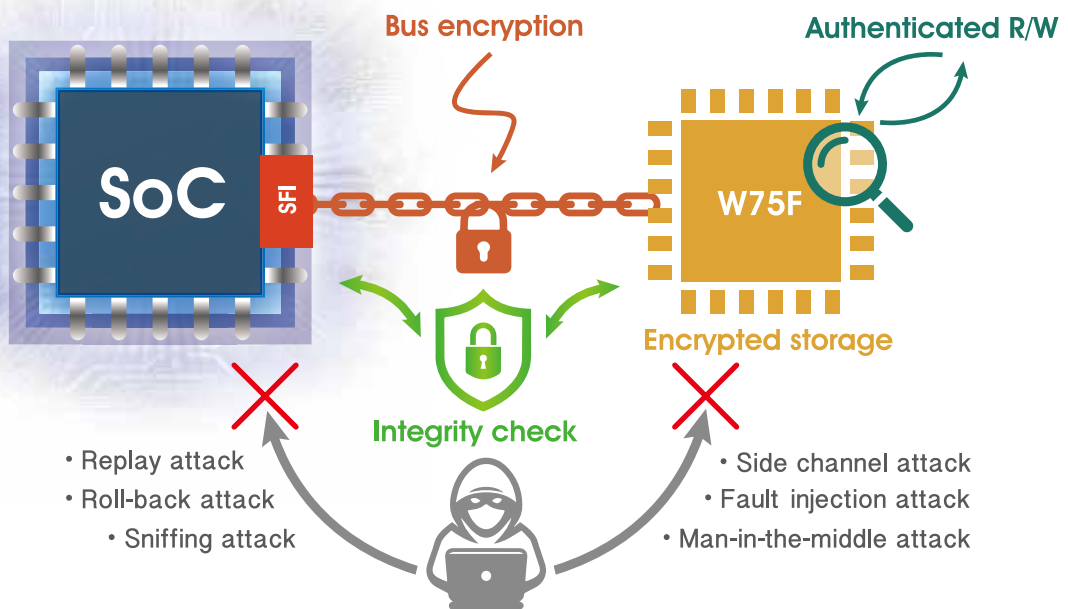
## Winbond TrustME® W75F Certified Secure Flash Solution



Winbond's W75F Secure Flash Solution is the first secure flash memory device to gain a Common Criteria (CC) EAL5+ certificate. It can be used for secure eXecute-in-Place (XiP) and can protect the confidentiality and integrity of code and data in IoT devices, integrated UICC, integrated Secure Element , Artificial Intelligence (AI) platforms, integrated Hardware Security Modules (HSM) for automotive subsystems. The W75F provides the industry's most secure external storage for code and data. It offers a dependable solution for manufacturers of connected devices who want to defend their products against threats such as replay, roll-back, man-in-the-middle, sniffing, side-channel attack and fault injection attack.







- The world's first Secure Flash device, Common Criteria EAL5+ certified
- Bolt-on security for IoT, Automotive and Artificial Intelligence (AI) platforms
- Complementary solution for Arm®v8-M and Arm®v8-A TEE sub-system
- In-band integrity check protects the interface
- Flexible secure memory architecture

| Flash Density                | Product Series | Voltage    | Certificate | Feature   | Package                  |
|------------------------------|----------------|------------|-------------|---|--------------------------|
| 4M bit<br>16M bit<br>32M bit | W75F           | 1.65-1.95V | CC EAL 5+   | <ul style="list-style-type: none"> <li>• Secure eExecute-in-Place (XiP)</li> <li>• Tamper and SCA/DPA Resistant</li> <li>• Code and Data Confidentiality and Integrity</li> <li>• Mutual Authentication with SoC</li> <li>• Secure SPI Quad/Octal Interface</li> <li>• Shared Memory Architecture for Multiple-Domains</li> <li>• AEC-Q100 with AG2 Qualification Available or Upon Request</li> <li>• 21 MByte/sec Secured and Authenticated Throughput</li> <li>• 100,000 Program/Erase Cycles</li> <li>• 20-year Data Retention</li> <li>• Temperature Range : -40°C to 105°C</li> </ul> | WQFN32<br>5x5mm<br>WLCSP |

## KGD

We also offer KGD (Known Good Die) products. For further information please contact: [TrustME@winbond.com](mailto:TrustME@winbond.com)





**Premium Content Protection**

- Usage of individual secret key per title
- Limiting number of playbacks/shares



**Internet of things (IoT)**



**Electronic Wallet**

- Mobile payment
- Software secure solution



**Secure Boot**

- Protect boot code from modifications
- Secure execution storage vs. Root-of-Trust e.g. TPM



**Winbond TrustME®**



**Support AG2 (Automotive)**



**Biometric Information Authenticity**

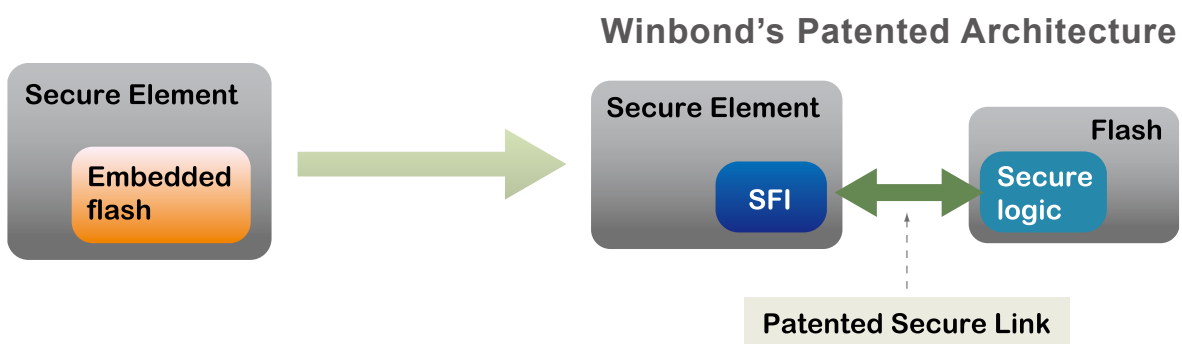
- Fingerprint storage



**GSMA Remote Provisioning**

- Support OTA technology to lower international roaming switching cost between countries
- GlobalPlatform UICC Card Architecture
- 32-bit CPU based on the Arm® SecurCore™ SC000™





### Uniquely Paired Secure Controller and Secure Flash Memory

- Added digital logic to flash device to protect secure flash interface and create secure link between integrated IP and flash
- Flash device from Winbond as a security companion device

### Cost Effective, Two Separate Devices

- Standard flash memory process
- Standard CMOS process for the controller

### Scalable Large Flash Density to Enable Application Innovation

| Flash Density      | Product Series | Voltage   | Clock (MHz) | Feature  | Package  |
|--------------------|----------------|-----------|-------------|--|--|
| 2M Byte<br>4M Byte | W76S           | 1.65-3.6V | 100         | <ul style="list-style-type: none"> <li>• 32-bit CPU based on Arm® SecurCore™ SC000™ Core</li> <li>• 32KB RAM</li> <li>• 2MB/4MB Secure Flash</li> <li>• Compatible with Java Card Specification 3.x</li> <li>• Crypto Accelerators for 3DES, AES, RSA, ECC, SHA, TRNG</li> <li>• GSMA Remote Provisioning Specifications Compliant</li> <li>• GlobalPlatform UICC Card Architecture Support</li> <li>• AG2 Support</li> <li>• SWP, SPI, ISO 7816, I2C, GPIOs</li> <li>• Temperature Range: -40°C to 105°C</li> <li>• CC EAL5+ Certificate</li> <li>• EMVCo Approval</li> <li>• CFNR Certificate</li> </ul> | <ul style="list-style-type: none"> <li>• WQFN32 5x5 mm</li> <li>• WSON12 4x4.2 mm</li> <li>• SON8(MFF2) 6x5mm</li> <li>• WSON8 4x4.2 mm</li> </ul> |

Contact us: [TrustME@winbond.com](mailto:TrustME@winbond.com)



## Winbond TrustME® W77Q Secure Flash

### SpINOR Flash Compatible Memory Enabling Comprehensive, End-to-End Security

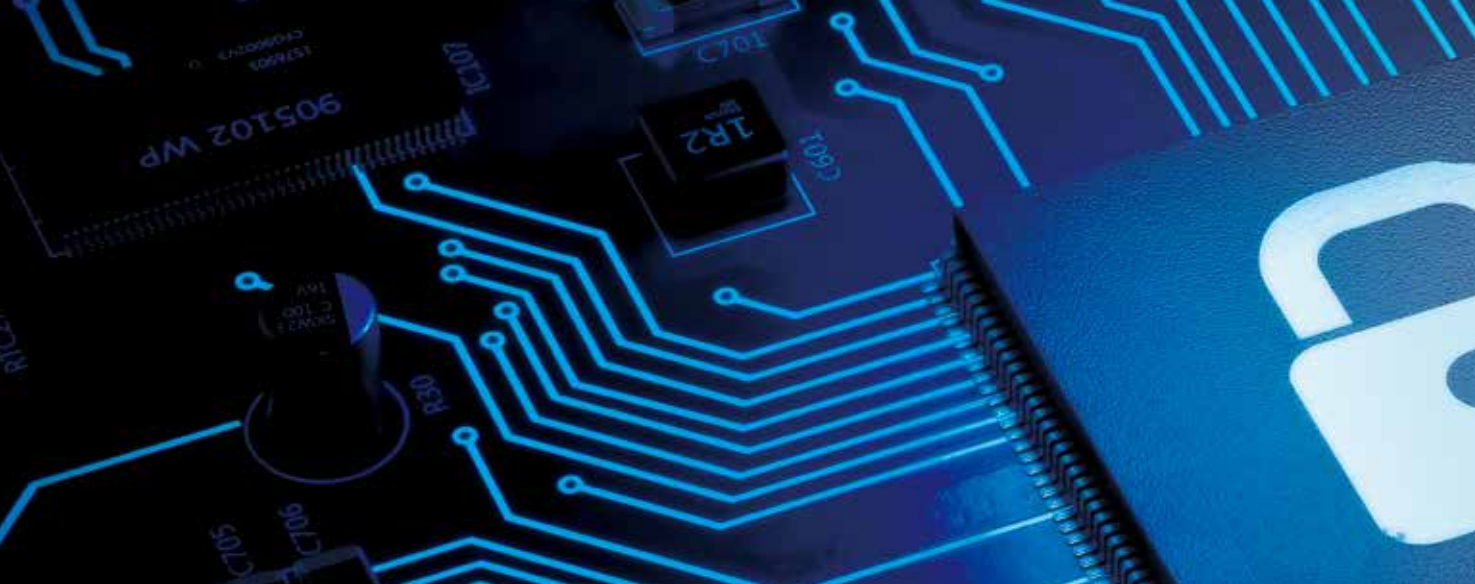
W77Q series of Secure Flash memory devices is a drop-in replacement for standard flash devices. It supports secure boot and system level resilience, and provides strong protection for operations such as over-the-air updates and device authentication. The new W77Q enables hardware root-of-trust and secure, encrypted data-storage and transfer capabilities. It ensures robust and secure over-the-air updates with end-to-end secure channel between the updating authority and the IoT device equipped with W77Q, even when the host processor is compromised.

| Flash Density | Product Series | Voltage    | Clock (MHz)  | Feature   | Package <sup>1</sup>                                    |
|---------------|----------------|------------|--|---|---|
| 32 Mbit       | W77Q           | 1.65-1.95V | 66MHz at Double Transfer Rate/<br>133MHz at Single Transfer Rate | <ul style="list-style-type: none"> <li>• Hardware-based Root-of-Trust engine</li> <li>• Device attestation</li> <li>• Cryptographically secured write protection</li> <li>• Secure code updates with anti-rollback</li> <li>• Secure boot from Flash (Root-of-Trust) with fast execution</li> <li>• Secure eXecute-in-Place (XIP) of boot and application code</li> <li>• Authenticated watchdog timer</li> <li>• Authenticated and encrypted data transfer between the Flash and the host</li> <li>• Secure over-the-air update with end-to-end secure channel between the updating authority and W77Q even when the host processor is compromised</li> <li>• Secure interface:               <ul style="list-style-type: none"> <li>§ Replay Protection Monotonic Counter (RPMC)</li> </ul> </li> <li>• Incremental security               <ul style="list-style-type: none"> <li>§ In-field fail safe configuration update</li> <li>§ Secure symmetric key management</li> </ul> </li> <li>• Secure unique device ID</li> <li>• 20-year data retention</li> <li>• 100,000 program/erase cycles</li> <li>• Operating temperature range of -40°C to 105°C</li> </ul> | SOP16 (300-mil)<br><br>WSON8 (6x5)<br><br>24-ball TFBGA |

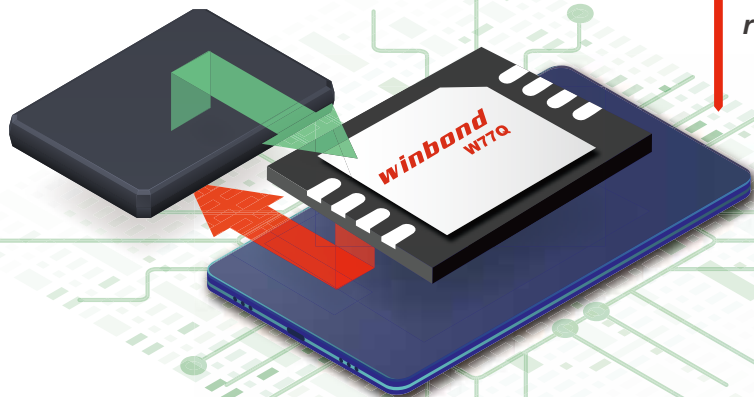
1. For other package and density, please contact: [TrustME@winbond.com](mailto:TrustME@winbond.com)

### KGD

We also offer KGD (Known Good Die) products. For further information please contact: [TrustME@winbond.com](mailto:TrustME@winbond.com)



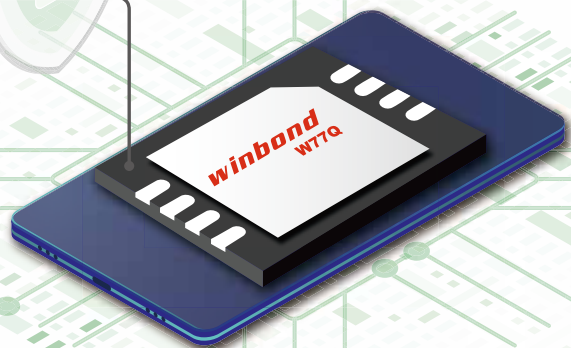
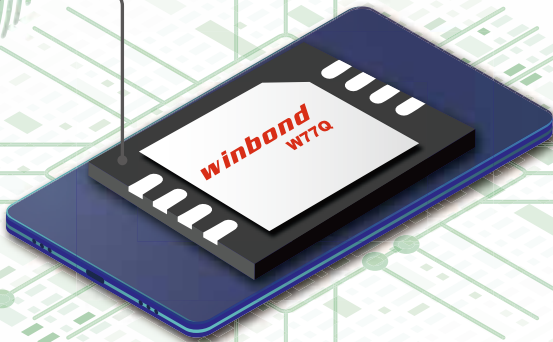
100% electrical and functional drop-in replacement for standard serial flash  
Fast integration path with no need to redesign board or SoC



Secure over-the-air update support

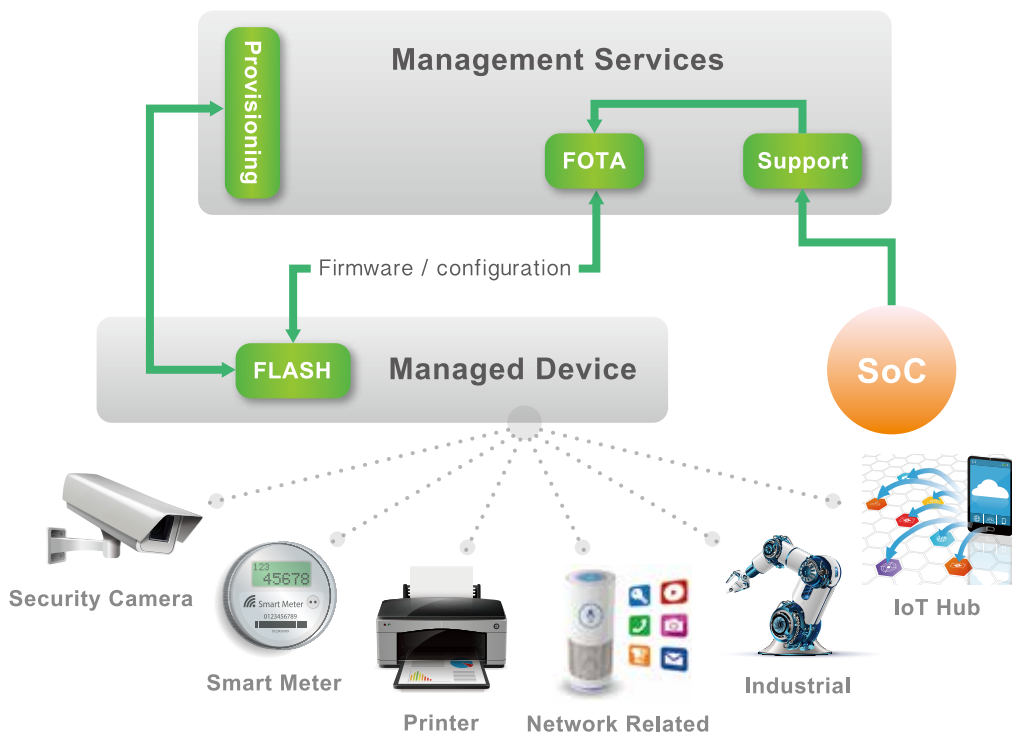


**Advanced security features**  
Automatic code and data authentication and fallback



**Secure storage and  
advanced security functions**

# ARCHITECTURE OVERVIEW



## Root-of-Trust Secure Flash Memory

- Self code integrity check and secure boot
- Hacking detection
- System recovery (Resilience)

## End-to-End Security Architecture

- Even with unsecure or compromised host processor
- Secure firmware over-the-air update
- Remote memory configuration for high / substantial / basic security demand

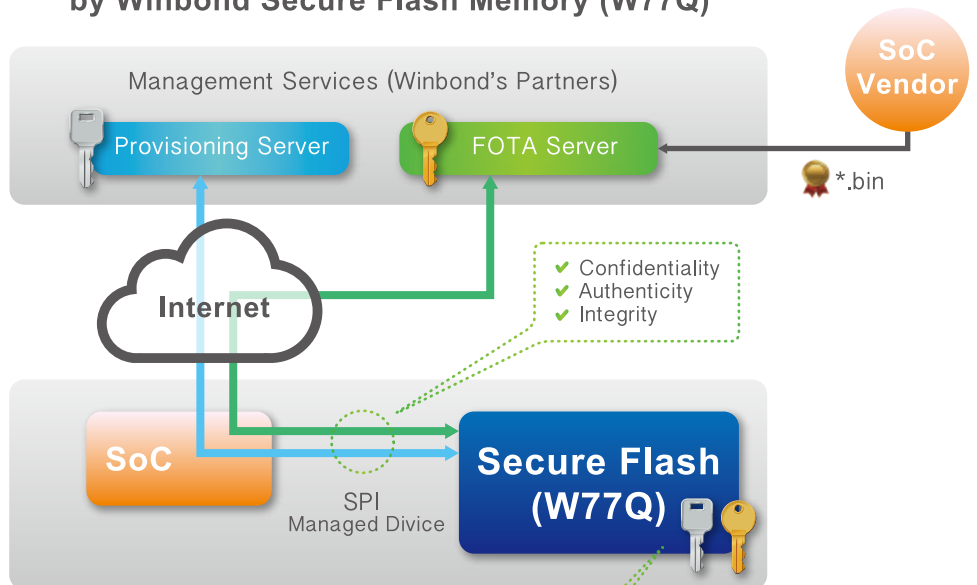
## 3rd Party Certified and Trusted Memory

- CC/EAL2 (in progress)
- SESIP (in progress)

## Drop in Replacement

- Compatible with standard flash memory
- Enables incremental security

**End-to-End Security Application Example  
by Winbond Secure Flash Memory (W77Q)**







## Business Benefits

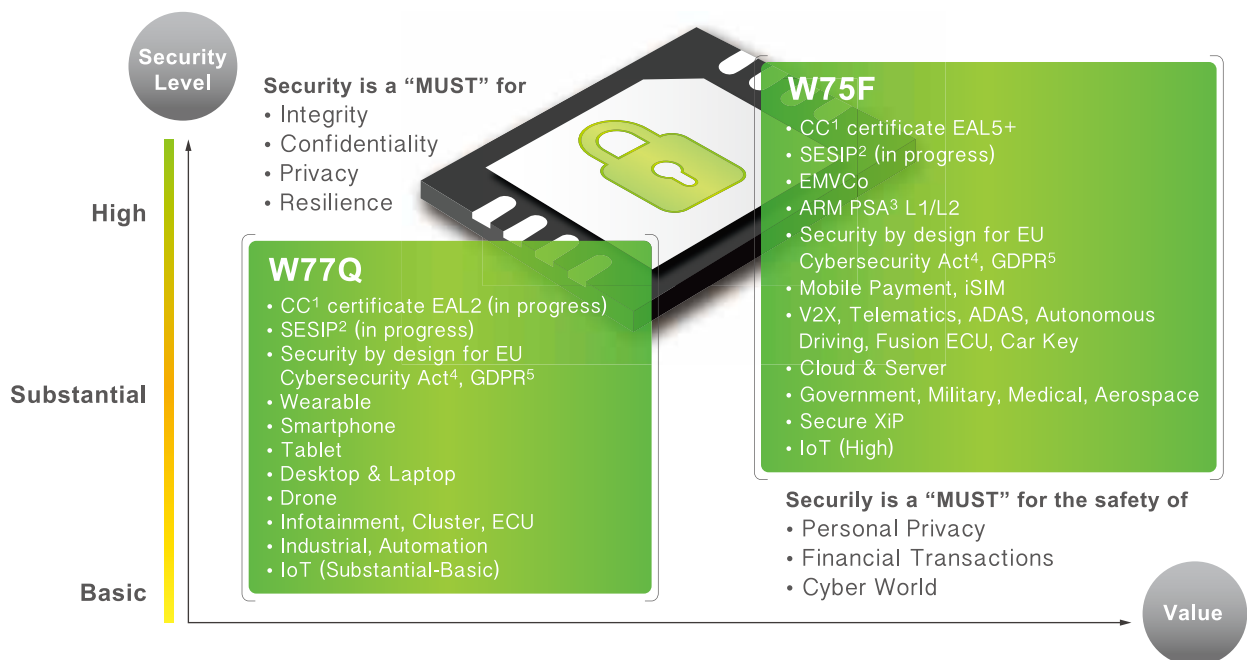
.....

- Drop-in replacement for standard flash
- Fast-time-to-market product development
- System resilience with protection, detection and recovery



# Winbond's Portfolio Addresses All Levels of Resilience And Protection

W75F and W77Q can satisfy the composition certification scheme to save customer's effort and expedite time-to-market



1. Common Criteria (CC) for Information Technology Security Evaluation
2. The Security Evaluation Standard for IoT Platforms (SESIP) defines a standard for trustworthy assessment of the security of the IoT Platforms
3. Arm's Platform Security Architecture
4. The EU Cybersecurity Act establishes an EU-wide cybersecurity certification framework for digital products, services and processes.
5. The General Data Protection Regulation (EU) 2016/679 (GDPR)





# *winbond*

## WORLDWIDE SALES OFFICE

### Winbond Electronics Corporation -CTSP Site

No. 8, Keya 1st Rd., Daya Dist.,  
Central Taiwan Science Park,  
Taichung City 42881, Taiwan  
Tel : 886-4-2521-8168

### Jhubei Office

No. 539, Sec. 2, Wenxing Rd., Jhubei City,  
Hsinchu County 30274, Taiwan  
Tel : 886-3-567-8168

### Taipei Office

2F., No.192, Jingye 1st Rd., Zhongshan Dist.,  
Taipei City 10462, Taiwan  
Tel : 886-2-8177-7168

### Winbond Electronics Corporation America

2727 North First St., San Jose,  
CA 95134, U.S.A.  
Tel : 1-408-943-6666

### Winbond Electronics (Suzhou) Limited

Room 1206, Kingboard Plaza (Building B, 12 floor),  
No.505, Guangming Road, Huaqiao Town,  
Kunshan City, Jiangsu Province, China  
Te : 86-512-8163-8168

### Winbond Electronics (Suzhou) Limited -Shenzhen Branch office

8F Microprofit Building, Gaoxinnan 6 Road,  
High-Tech Industrial Park,  
Nanshan Dist. Shenzhen, P.R. China  
Tel : 86-755-3301-9858

### Winbond Electronics (H.K.) Limited

Unit 9-11, 22F, Millennium City 2,  
378 Kwun Tong Road, Kowloon, Hong Kong  
Tel : 852-2751-3126

### Winbond Electronics Corporation Japan

Shin-Yokohama Square Bldg. 9F 2-3-12 Shin-Yokohama,  
Kouhoku-ku, Yokohama, kanagawa 222-0033, Japan  
Tel : 81-45-478-1881



[www.winbond.com](http://www.winbond.com)