

secureletter.

26

Secureletter Inc.

AT A GLANCE

Business Type

Incorporated

Date of Foundation

June. 26, 2017

Number of Employees

26

Annual Sales(USD)

2019	2.3M
2020	3M
2021	3.7M

Capital(USD)

2019	0.3M
2020	0.3M
2021	0.3M

Certifications

-

MAJOR CUSTOMERS (%)

Korea

100%

HANA Bank

HANWHA Systems

CONTACT INFORMATION

Name	Daewon Kim	Mobile	+82-10-9060-6814
Gender	Male	Tel	+82-70-4285-1264
Division	CEO	Fax	+82-2-511-0904
Position	CEO	URL	www.secureletter.co.kr
City	Seoul	E-mail	dk@secureletter.co.kr
State	Seoul	Country	Republic of Korea
Address	2F, 223, Yeoksam-ro, Gangnam-Gu		

COMPANY OVERVIEW

CEO: Daewon Kim | **Established:** 06. 2017 | **Capital:** \$0.3M | **Team:** 3

Business: Wireless Intrusion Prevention System, Wireless Authentication Software

Secureletter is a specialized wireless security company and aims to challenge the world market in the field of wireless security beyond becoming No. 1 in Korea by strengthening our core competencies in the wireless solutions business and encouraging business expansion.

MAIN PRODUCT

[Service Product]

Anyclick AUS | Applicable to: Wireless Security

Anyclick AUS is a combined wire-wireless authentication system specializing in wireless security that protects internal infrastructure by blocking unauthorized users and terminal's access to a network through stronger user authentication and encryption and providing safe wireless data transmission.

This security technology is essential for implementing a safe wireless network. Thus the technology is stipulated in many security regulations and guidelines including the Security Recommendations of the National Cyber Security Center.

[Hardware Product]

DeepTrust AIR | Applicable to: Wireless Security

DeepTrust AIR is a Wireless Intrusion Prevention Solution to protect internal network by detecting and preventing a variety of intrusions that might occur within and beyond an organization and monitoring all wireless equipment that adhere to the WLAN Standards.

DeepTrust AIR WIPS provides the most comprehensive protection from all types of wireless threats, including Rogue APs, Soft APs, Honeypots, Wi-Fi DoS, Ad-hoc networks, Client misassociations, and Mobile hotspots.

DeepTrust AIR WIPS takes a fundamentally different approach by focusing on the fundamental threat vectors and vulnerabilities.

