WedgeCND™

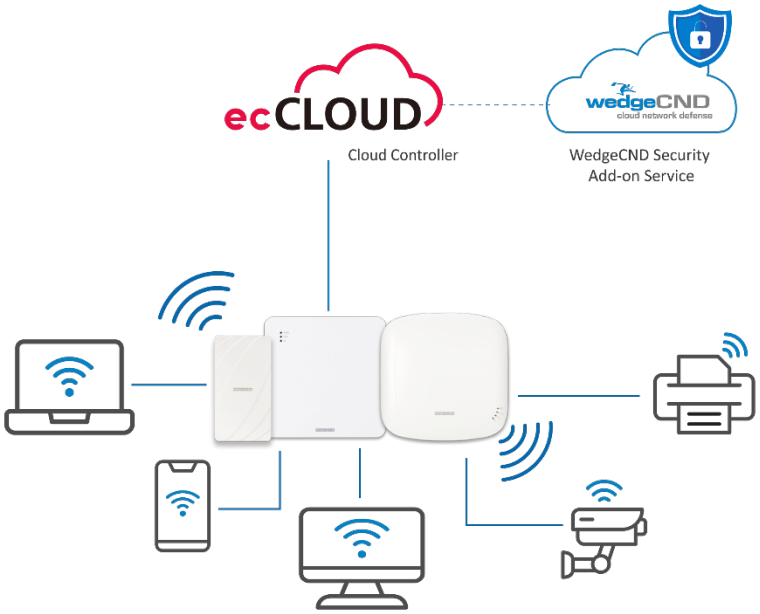
Wedge Security Addon

INTRODUCTION

Wedge Cloud Network Defense™ (WedgeCND™) is a cloud-managed, cloud-enforced security service offering that provides a vast array of optimized Security-as-a-Service (SECaaS) features typically not only available to SMEs and work from home (WFH) users, it also enables effective security solutions for any cloud-connected computing devices, providing scalability, flexibility and accuracy for and any locations using Wi-Fi Access Point while still maintaining privacy.

Wedge Security Addon is a value-added service provided by ecCLOUD that allows networks and endpoints connected to Access Point devices to be protected by WedgeCND.

When Wedge Security Addon is enabled for an Access Point device on the ecCLOUD, Internet access from the Access Point device will automatically be protected by WedgeCND. All types of threats, such as malware, ransomware, phishing, malicious websites, will be filtered and the network and endpoints behind the Access Point will receive clean Internet traffic.



APPLICATION

- EAP101
- EAP102

SUBSCRIPTION

- Low-cost
- Monthly Payment
- Pay to Go

FEATURES

ADVANCED MALWARE PROTECTION	
Anti-virus	• Signature and heuristic based antivirus with dual antivirus engines to detect most of known malware, such as Viruses, Trojans, Worms, Backdoors, etc.
AI Anti-malware	• Artificial intelligence machine learning based malware detection for unknown and never-seen-before malware, such as APT, Zero-day, Ransomware etc.
Malware Analyzer	• Sandbox based malware detection for greyware and suspicious code, data and files
WEB FILTER	
Malware sites	• Malicious content including executables, drive-by infection sites, malicious scripts, viruses, trojans, and code
Spyware and Adware	• Spyware or Adware sites that gather or track information and popup unsolicited ads
Bot Nets	• URLs and IP addresses, which are determined to be part of a Bot network, from which network attacks are launched. Attacks may include SPAM messages, DOS, SQL injections, proxy jacking, and other unsolicited contacts.
SPAM URLs	• URLs contained in SPAM
Phishing and Other Frauds	• Phishing, pharming, and other sites masquerading as reputable sites, usually obtain personal information from users
Proxy Avoidance and Anonymizers	• Proxy servers and other methods to gain access to URLs in any way that bypasses URL filtering or monitoring
Keyloggers and Monitoring	• Software agents that track a user's keystrokes or monitor their web surfing habits
Confirmed SPAM Sources	• Spam Sources includes Tunneling Spam messages through proxy, anomalous SMTP activities, Forum Spam activities
IDPS	
DoS	• Detect and block Denial-of-Service attack
SQL Injection	• Prevent from compromising SQL-based RDBMS
Exploit	• Prevent from exploits on different applications, including PDF readers, Microsoft RDP, Windows Media Player, VNC Server, Java-based programs, JavaScript, etc.
BOT Command & Control	• Inspect traffic from a list of botnet command and control servers
Critical Infrastructure Protection	• Inspect insecure data transfer methods and known vulnerabilities of various SCADA software packages, such as PcVue, Sunway ForceControl, Siemens FactoryLink, etc.
VoIP	• Methods of compromising phone servers via flooding (DoS or DDoS), buffer overflow, or session hijacking

*ecCLOUD will be supported in 2022, H1