App Guard was developed for the Pentagon 26 years ago and is also used within the U.S. government



App Guard has been designated as a recommended solution by the Japan Hospital Mutual Aid Association.

In recent years, there have been numerous instances of cyberattacks and ransomware attacks targeting medical institutions, resulting in prolonged suspensions of medical services; consequently, medical institutions are required to implement even more robust security measures. The Japan Hospital Mutual Aid Association has recognized App Guard as the optimal product for protecting hospitals from cyberattacks.



App Guard Industrial

Cyberattack Mitigation for IoT Embedded Systems App Guard Industrial

Examples of App Guard Industrial Deployments (Already Implemented or Currently Under Evaluation)

Precision equipment manufacturers, logistics companies, machinery manufacturers, food processing companies, packaging manufacturers, POS and kiosk terminals at all stores of a convenience store chain





Cutting Edge Co., Ltd.

1-9-6 Kaji-Cho, Chiyoda-Ku, Tokyo 101-0044, JAPAN

sales@cut-edge.jp

https://cuttingedge-tech.jp

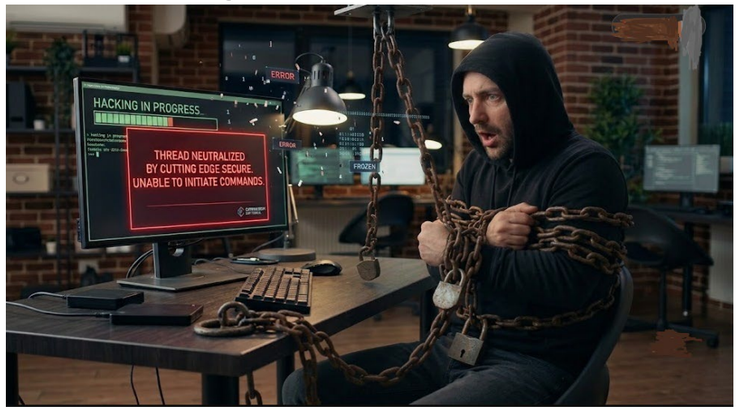
Contact to

2026-11-11

ゼロトラスト型エンドポイントセキュリティ APPGUARD

CUTTING EDGE

This is what the world needs right now.
It is the only solution in the world that has never suffered a cyberattack in 26 years.



1. **Even if a cyberattack manages to infiltrate through a vulnerability, it can't do anything!**
2. **Whether you plug a virus-infected USB drive into your PC or run a suspicious attachment, it’s impossible for malware to run!**
3. **It will only launch applications that have been explicitly authorized.**
4. **No specialized knowledge, no dedicated staff, and no need for 24hours/365-day monitoring!**
5. **All you have to do is install the app on your PC or server and select the apps you want to allow.**
6. **Used by the U.S. government, the Pentagon, the Japanese government, the Ministry of Defense of Japan, and others!**
7. **A last-resort solution for neutralizing and preventing cyberattacks that has never been breached in 26 years!**



This is a cyberattack blocking solution—developed and patented 26 years ago for the U.S. Department of Defense (the Pentagon)—that can neutralize cyberattacks. Customers in the United States and Japan who have implemented this application have never been breached by a cyberattack in the past 26 years. Right now, this solution is urgently needed around the world.

Main features of App Guard





This does not apply to phishing scams.
Phishing is a type of fraud in which scammers send emails pretending to be from major online retailers, delivery companies, and other organizations. They trick recipients into clicking on embedded links that lead to fake websites, where they steal sensitive information such as credit card numbers and account details (user IDs, passwords, etc.). Unlike cyberattacks, phishing relies on victims voluntarily entering their personal information; therefore, the only effective defense is for individuals to exercise extreme caution.

Major Differences Between App Guard and Antivirus Software

Product	App Guard	Antivirus Software
Purpose	Prevent them from doing bad things	Find the virus
Virus Detection	NG	Good
Virus Removal	NG	Good
Preventing Malware Creation	Good	NG
Preventing Malware Execution	Good	NG
Device Hijacking	Good	Good/NG

Antivirus software identifies, detects, and removes only viruses based on reported incidents. However, because attackers always stay one step ahead until security updates are released, the software is unable to stop these attacks and is completely ineffective against unknown threats.
App Guard, on the other hand, allows only authorized applications to run; since an attacker's application is not authorized, it is frozen and prevented from launching. App Guard restricts the attacker's freedom of action and prevents them from achieving their objectives. It can counter any type of intrusion attack, regardless of whether it is new or old, its nature, or the attack method used.

App Guard does not have a removal feature. However, if you use Microsoft 365, the included Defender—which is free—works to detect and remove viruses. By using App Guard and Defender together, you can take advantage of antivirus capabilities and achieve the greatest possible protection against cyberattacks.

Major Differences Between App Guard and EDR

Product	App Guard	EDR
Purpose	Preventing a Successful Attack	Assuming a breach will occur, this supports rapid response after the breach
Introduction and Tasks	Just install it on your PC or server and select the apps you want to allow	The work of having specially trained engineers constantly monitor and collect logs,and continuously record and store behavioral data such as communications and process execution
Methods	Preventing Unauthorized Actions	Threat Detection, Correlation, and Analysis
Technical Specialist	Not needed	Number of technical specialists providing 24-hour, 365-day monitoring: At least 6 to 10
Annual Cost	1. Annual license fee + management fee: Required every year: Very low 2. Implementation and management fee: Required only in the first year: Very low	1. Labor costs for at least 6 to 10 specialized engineers: Very high 2. Training costs for engineers: Very high 3. EDR license and other expenses: Very high
Outsourcing Services	None	1. In-house staff required at the time of service implementation: 1–2 people 2. Annual license fees + monitoring fees: Very expensive 3. Operating costs: Very expensive
Remarks	Since there is no need to install the application on every PC and server within the company—for example, it can be installed only on the PCs of three specific users, such as the CEO, an engineer, and an accountant—the solution offers flexible scalability and helps keep costs down.	The costs of installing applications on all company PCs and servers, as well as the costs of the technicians who monitor them, are extremely high; however, EDR is an approach based on the assumption that a cyberattack will occur.

EDR is an approach based on the assumption that a breach will occur, designed to support rapid response after a breach. It requires several staff members—who have received specialized training in defense, detection, and response to attacks—to monitor the system 24 hours a day, 365 days a year. Consequently, it incurs very significant expenses, including personnel costs and training costs for skill development. Furthermore, since the methods of defense and response in the event of an
On the other hand, with App Guard, all you need to do is install the software on your computer or server and select the applications you want to allow—no specialized knowledge or dedicated staff is required. Since only approved applications can be opened, malware and other threats are effectively frozen and cannot launch. As a result, App Guard works behind the scenes to stop cyberattacks and keep you safe without you even noticing.