Privacy-i EDR

Next-Generation Antivirus Solution

SOMANSA

Detecting & Preventing Malware Variants In Real Time
Next-Generation Antivirus Solution
Privacy-i EDR

1 Overcoming the Limits of Traditional EDR Solution

- **Fileless malware** uses legitimate tools to execute a cyber attack. Since it does not rely on files and leaves no footprint, it is challenging to detect/remove filess malware via a traditional pattern detection mechanism.
- **Ransomware attack** starts by infecting a single endpoint, and then its variants eventually impact an entire business network. Ransomware can be prevented only via a behavior detection engine.

2 Preemptive Detection & Prevention

- It is demanding to protect data from threats only by a single-engine pattern detection solution since the solution does not provide up-to-date information of malware variants & has limited ability to respond to zero-day, fileless malware and ransomware.
- **Only EDR**, which identifies malicious activities based on the causes and effects of events, can detect and preempt security threats in real time.

2 Steps of Preemptive Threat Prevention
: Pattern & Behavior Detection Engines

Threat Occurrence

Zero-day exploit
Spam
APT
PowerShell
Ransomware

Step 1 Antivirus Engine

Antivirus Protection
via Pattern Detection Engine

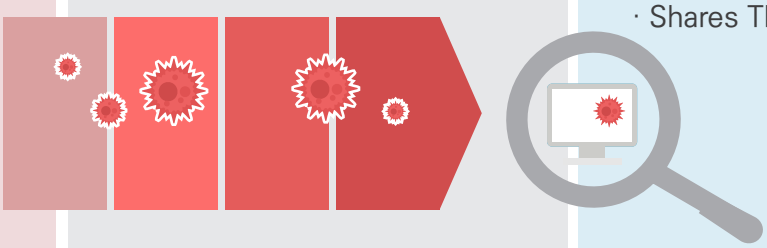
· Detects and blocks malwares by filtering and matching them against signatures in the database

Initial access of malware is difficult to detect due to the absence of related data

Step 2 Behavior Detection Engine

Endpoint Detection and Prevention
via Behavior Detection Engine

· Detects and prevents abnormal behaviors by using acutal data
· Conducts post intrusion investigation & analysis
· Reduces ricks of Zero-Day Attacks
· Shares Threat Intelligence (TI)



Overcoming The Limitations of Post-Breach Response, Developing An Automation Solution Specialized In Preemptive Prevention

1 2 Steps of Malware Detection (Malware Block Rate of 99.6%) : Pattern & Behavior Detection Engines

	Detection Methods	Block Rate
Results	Pattern Detection Engine	94.3%
	Behavior Detection Engine	5.3%
	Total	99.6%

* Test above was conducted by Somansa itself.

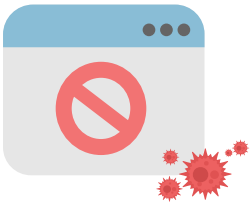
Step 1 Detects and blocks malware·ransomware·viruses by **filtering security threats** & **matching them against signatures in the database** via Pattern Detection Engine

Step 2 **Analyzes malicious behaviors** & **identifies malwares** via Behavior Detection Engine

① Preemptive blocking of malicious threats

② Prevents malware variant/fileless malware

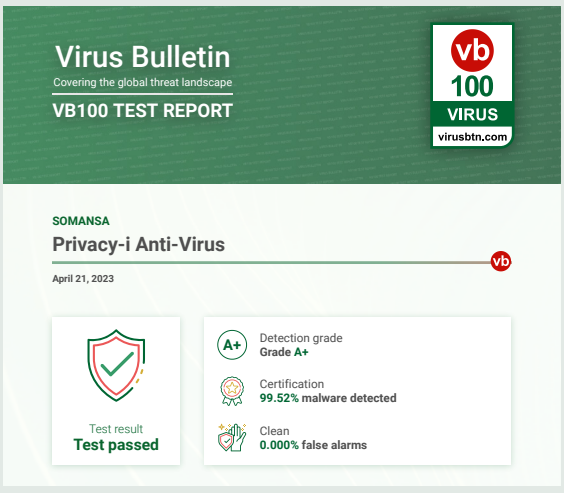
2 Real-Time Data Isolation and Recovery



- Detects every file stored in desktop and isolates malicious files.
- Minimizes data loss by detecting an abnormal behavior as soon as it attempts, preventing data encryption and recovering to the recent data.

3 Awarded Virus Bulletin's VB100 Certification

Recorded False Positive Rate of 0%, Detection Rate of 99.52% & Received the highest grade of A+



Results of VB100 Testing	
On 100 Thousand Malicious Samples	Result (%)
False Positive Rate	0%
Detection Rate	99.52%

Global Leader of
Data Protection & Secure Web Gateway
With 27 Years of Security Technology

One of Top 3 Major Banks in Korea

Successfully Built 15,000 Employee sized Endpoint Agents

- Built multiple solutions in one single agent, reducing overhead
  (Malware and Ransomware Blocking)
- Built Endpoint Infrastuctures for work-from-home

One of Top 10 Construction Companies

Successfully Built 12,000 Employee sized EDR Agents

- Provided Intelligent Threat Detection & Integrated Protection
- Built and implemented Endpoint EDR
- Shortened the doubled time for searching personal data

Somansa Customers In Various Industries

Government Institution

Advanced Security of Endpoints

Public Facilities Corporation

Improved Protection of Sensitive Data

Credit Card Company

Provided Ransomware Protection for Endpoints

Top-Rated Malware · Ransomware Prevention Solution

Technology Features		Somansa	CrowdStrike
Common Malware Prevention	TI (Threat Intelligence)	O	O
	AV (Anti-Virus)	O	O
Unknown Malware Prevention (Malware Variant, Zero-day)		O	O
Specialized Ransomware Analysis		O (more than 30 types of ransomware)	△
Client Side Exploit Prevetion		O (more than 30 types of exploit)	O
Detection of Malware Using Mitre ATT&CK		O	O
Fileless Threats Prevention		O	O
Single Agent Integration		O	X
Alternative to Single Antivirus Solution		O	O
Protection in Closed Network		O	X

3003 N. First St., Suite 301 San Jose, CA 95134, United States
TEL (408) 701-1302 FAX (408) 383-9089 EMAIL edr@somansa.com
www.somansatech.com

Visit Website