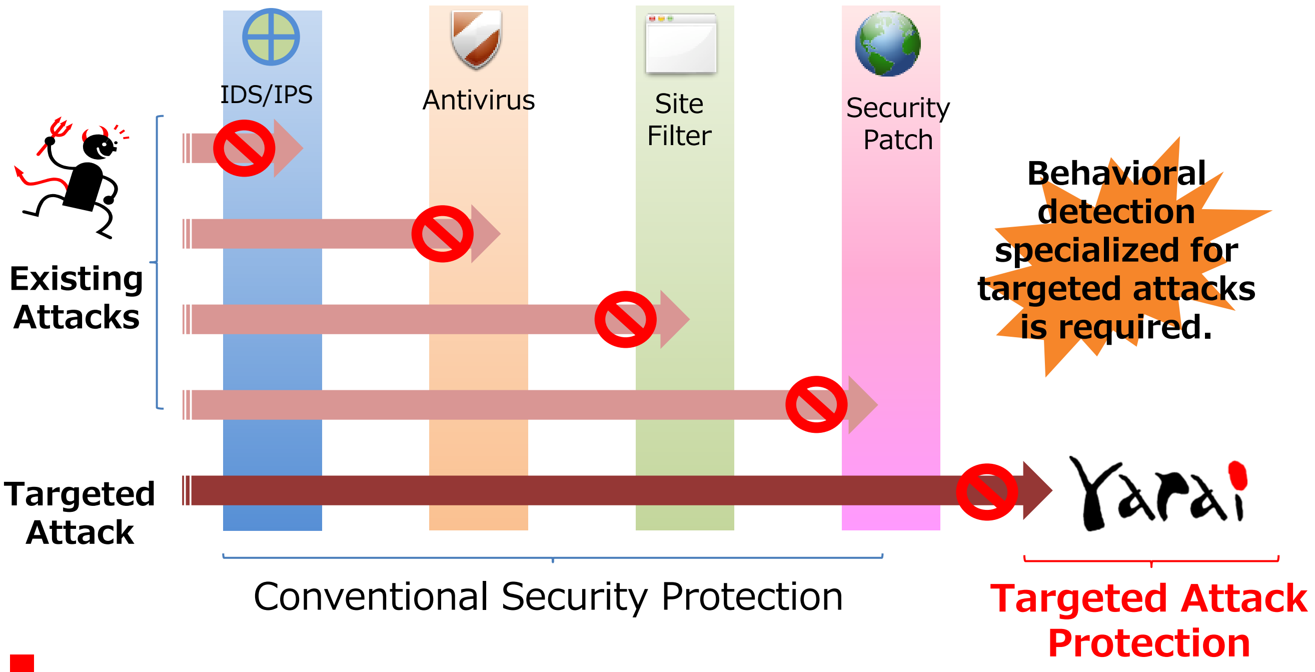
Targeted Attack Protection Software

FFRI yarai

"FFRI yarai" Targeted Attack Protection Software, Developed in Japan

Conventional security protection cannot provide full protection against targeted attacks.


IDS/IPS
Antivirus
Site Filter
Security Patch
Existing Attacks
Targeted Attack
Behavioral detection specialized for targeted attacks is required.
Yarai
Conventional Security Protection
Targeted Attack Protection

Five Behavioral Detection Engines of FFRI yarai

■ZDP Engine
Protects against virus attacks that target known and unknown vulnerabilities such as attacks when viewing emails or Web pages.Protects against arbitrary code execution vulnerability attacks by use of our original API-NX technology (Patent No. 4572259).

■Static Analysis Engine
Analysis performed without program operation. Detection is performed by using N-Static Analysis that incorporates numerous analysis methods including PE Structure Analysis, Linker Analysis, Packer Analysis, and Speculated Operation Analysis.

■Sandbox Engine
Runs programs on a virtual environment that includes a virtual CPU, virtual memory and virtual Windows subsystems.Detection is based on a combination of commands based on our unique U-Sandbox Detection Logic.

■HIPS Engine
Monitors the behavior of currently running programs. Our unique D-HIPS Logic detects behavior such as program intrusion, unusual network access, key logger and backdoor access behavior

■Machine Learning Engine
Monitors running programs based on big data related to malware that has been captured by FFRI Security.Behavioral characteristics in big data are extracted to detect malicious behavior in computer terminals by using machine learning to analyze such characteristics.

FFRI yarai Uses "Full Behavioral Detection" for Targeted Attack Protection

Five Unique Detection Engines

- ✓ Equipped with five unique detection engines to counter unknown malware without depending on pattern files

Prevent Code Execution Attacks

- ✓ Protection against unknown vulnerability (0-day) attacks
- ✓ Efficient operation with little load on your computer

Next-Generation Security Developed in Japan

- ✓ Technology developed in Japan, with a proven track record at government agencies, manufacturers, and critical infrastructure companies

Protection Range of Existing Security Measures and FFRI yarai

Yes: Supported
Partial: Partially supported
No: Not supported

	Antivirus software	IDS/IPS	Patch Management	**FFRI yarai**
Known Malware	**Yes**	**Partial**	**No**	**Yes**
Known Vulnerabilities	**Partial**	**Yes**	**Yes**	**Yes**
Unknown Malware	**Partial**	**Partial**	**No**	**Yes**
Unknown Vulnerabilities	**Partial**	**No**	**No**	**Yes**

Track Record of FFRI yarai Protection

Occurrence/ Report Date	Protection Engine Release Date	Unknown Threat (at the time) and Targeted Attack	FFRI yarai Detection & Protection Engine
July 2019	January 2019	“Sodin” ransomware	HIPS Engine
April 2019	May 2017	Malicious Excel File Impersonating Invoice or Delivery Slip	HIPS Engine
January 2019	March 2018	"Anatova" Ransomware	HIPS Engine
August 2018	March 2018	Malware using Windows task scheduler	Static Analysis Engine
July 2018	March 2018	“Emotet” malware	Sandbox Engine
April 2018	June 2017	“Satan” ransomware	Static Analysis Engine
April 2018	June 2017	“GandCrab” ransomware	HIPS Engine
March 2018	June 2017	“Panda Banker” banking malware	HIPS Engine
January 2018	May 2017	“SpriteCoin” ransomware	HIPS Engine
January 2018	May 2017	“Rapid” ransomware	Static Analysis Engine
December 2017	May 2017	“CoinMiner” cryptocurrency mining malware	HIPS Engine
December 2017	May 2017	Malware impersonating “Rakuten Card Co., Ltd”	HIPS Engine
October 2017	January 2017	“Bad Rabbit” ransomware	Static Analysis Engine
May 2017	October 2016	“WannaCry/WannaCrypt”ransomware	Static Analysis Engine
January 2017	September 2016	“Mirai”IoTmalware	Static Analysis Engine
June 2015	August 2014	"Emdivi" malware targeting the Japan Pension Service	(Not published)

* The release dates for protection engines are approximately 1 month to 1 year before the unknown threats or targeted attacks occurred. This means that "proactive technology" was used to detect and protect against future threats with a protection engine developed before such threats were even known.

* This protection record was obtained internally based on the results of verification against samples and does not guarantee the detection of all variants.

For assistance regarding products and service:

FFRI Security, Inc.
2F Shin-Tokyo Building
3-3-1, Marunouchi, Chiyoda-ku, Tokyo, JAPAN
100-0005
E-mail: sales@ffri.jp

Information about this product is also available on our website:
https://www.ffri.jp/en/index.htm

■ The content of this pamphlet is subject to specification and design changes without advance notification.

November 2019 Ver 2.00.07