

Fujitsu Security - Advanced Threat Prevention Solution

Fujitsu Advanced Threat Prevention solution analyzes program behavior to proactively protect against both known and unknown threats, observes the system events and blocks programs that exhibit malicious cyber activity.

Features

- Monitor malicious threats and behaviors of malware embedded in attachment files and network connection followed by an analysis of the potential threats.
- Generate regular reports with in-depth analysis of malware behaviors for a better understanding of the threats involved.
- Provide professional security advices on how to tackle and eliminate the malwares within the IT environment.

Fujitsu Advanced Threat Prevention Model

1. Threat Detection

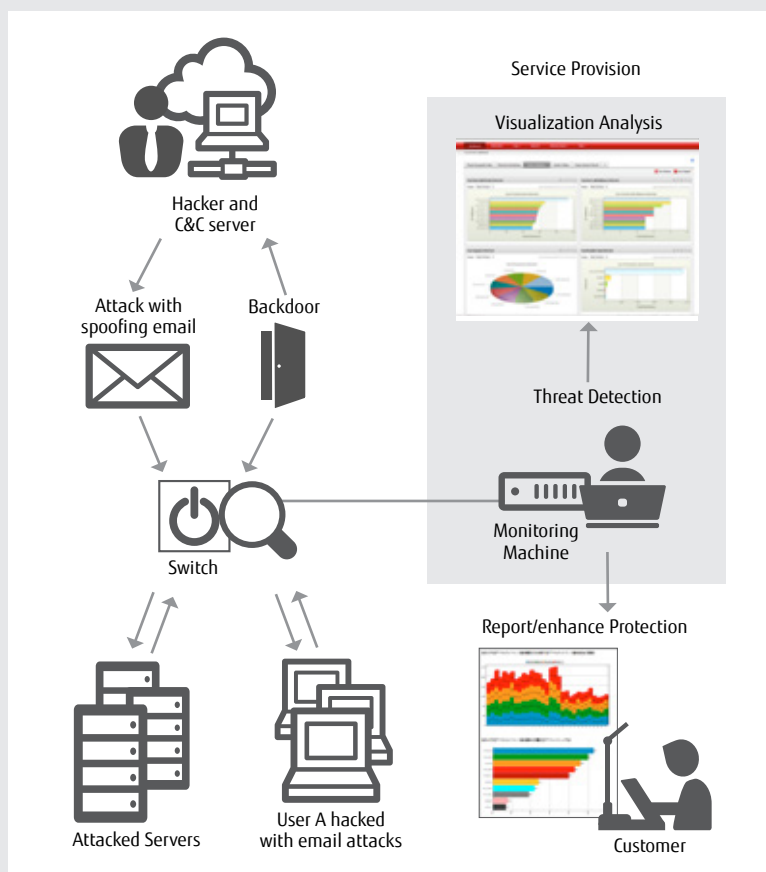
- Unknown malware that travels into internal system are detected; network monitoring observes network activities for malicious behavior that has circumvented trusted corporate traditional defenses.
- A team of security experts will diligently observe and monitor the activities within the IT environment so as to reduce potential risks of cyber threats

2. Threat Analysis

- Potential threats are efficiently analyzed by using both conventional rules and multi-layers of dynamic analysis
- Wide-range of analysis tools cover multiple types of attacks for multiple protocols

3. Customer support

- After the incidents are detected, Fujitsu provides correlation analysis and report to the customer for their immediate decision-making and action
- Fujitsu support team will respond swiftly to any queries about malware activities from the customer



- C&C server: Control server controls by sending out signs to infected computer after being attacked.
- Backdoor: It allows hacker to access secretly into computer without notification.

Why Fujitsu?

The explosion of more and more sophisticated cyber threats means the impact of doing nothing is huge. Fujitsu understands the challenges faced by enterprises nowadays- from not having enough insights of what's roaming behind their corporate systems to a lack of dedicated and skilled security team.

From early malware detection, fixing the programs that exhibit malicious activity to providing post attack support, Fujitsu brings a complete end-to-end suite of security solutions to our customers, ensuring a high level of protection against new, unknown, and emerging threats. We want to ensure organizations are better prepared by sharing insights and best practices into IT security from leading experts around the world.

Holistic security solution as a service



We provide security services and operation solutions based on customers' policies and security control requirements

Visualization and Analysis on Network



We continuously verify ICT status against threats in real time even for malwares that are unknown and difficult to detect

Threat Analysis and Control for Customer



We protect customer from threats through a dedicated system that generates comprehensive reports with professional security measure and solutions

Benefits

- Better understanding of potential cyber threats that could lead to business risks
- Reduction of operational expenses and time spent on blocking malware
- Establishment of anti-virus structure to reduce threat risks

Fujitsu Total Support

Leveraging on the advanced persistent threat and custom defense technology of Trend Micro, Fujitsu offers a holistic approach in tackling and managing malware activities - from detecting the threats at an early stage, analyzing the behaviors to providing advices and support on to how to stop the malware from disrupting your operations.

Service Name		Service Content	
Detecting Malware / Aftercare Support	Installation Service	Initial Setup, Operational Configuration	<ul style="list-style-type: none"> • Preparation of requirements including design and installation • Operations design
	Operation Service	Security Incident Notice	<ul style="list-style-type: none"> • Update and maintenance of APT at customer's site • Immediate incident notification • Supporting inquiries from detection results and reports • Updating information about new security development
		Advisory Report	<ul style="list-style-type: none"> • Quarterly report of detected malware
		Solution Support	<ul style="list-style-type: none"> • Inspection and analysis with prospective solutions against suspicious malware detected on network • **Update customer AV environment with custom signature against detected threat
		Incident Response Support	<ul style="list-style-type: none"> • Engineer support on-site to handle problems <p><i>This service only available for customers using Premium Onsite Response Support. For more details, please contact Fujitsu.</i></p>

** only applicable to officescan

What's next?

To find out more, contact:
 Email: info@sg.fujitsu.com
 Web: fujitsu.com/sg

Fujitsu Asia Pte Ltd

Nexus @ one north
 1 Fusionopolis Link, #04-01, Singapore 138542
 Email: info@sg.fujitsu.com
 Web: sg.fujitsu.com

Copyright 2015 Fujitsu, the Fujitsu logo, other Fujitsu trademarks /registered trademarks are trademarks or registered trademarks of Fujitsu Limited in Japan and other countries. Other company, product and service names may be trademarks or registered trademarks of their respective owners. Technical data subject to modification and delivery subject to availability. Any liability that the data and illustrations are complete, actual or correct is excluded. Designations may be trademarks and/or copyrights of the respective manufacturer, the use of which by third parties for their own purposes may infringe the rights of such owner.