Fujitsu continuously works on achieving safe and secure ICT to continue supporting customers and sustainable business.

The growing popularity of cloud computing and smart devices has seen the regions utilizing ICT expand and cyber-attacks grow more sophisticated and cunning by the day, so taking measures against the attacks to ensure safe and secure utilization of ICT has become a significant issue. Through appropriate countermeasures and operations, Fujitsu, which is comprised of approximately 300 companies worldwide, currently deals with several hundred million security events logged per day to detect threats in its own Intranet. To apply this expertise to the security measures of its customers and deliver integrated support, including enhanced systems and operations as well as education and training of companies’ personnel, Fujitsu has organized a line of products and services that follow its new “FUJITSU Security Initiative.”

| Security Solutions |

Currently, the environment encompassing information security is exposed to a variety of security risks, starting with external threats such as viruses and illegal access, and including cyber-attacks and data loss incidents which are increasing in conjunction with the widespread use of smart devices. Fujitsu’s track record of practical experience provides security solutions based on consistent beliefs and thorough in-house implementation under “the Fujitsu Enterprise Security Architecture (ESA)” and “our Security Management Framework (SMF).” Providing solutions requires integrating the necessary security solutions and conforming to the ESA in order to effectively support companies’ investments from a functional aspect. Presenting reference models based on internal practices enables customers to implement highly reliable solutions drawn from our track record.

**FUJITSU Security Initiative**

### Offerings

<table>
<thead>
<tr>
<th>Offerings</th>
<th>Cyber-Attack Countermeasures</th>
<th>Applications</th>
<th>Platforms</th>
<th>Network</th>
<th>Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consulting, Operations, Training</td>
<td>Global Managed Security</td>
<td>Common/Business Applications (authentication, access control, ID management)</td>
<td>Server, Storage, OS, MW (access control, designated user management, vulnerability management)</td>
<td>LAN/WAN (identification, access control, encryption, VPN, IDS/IPS, quarantine, malware detection, next generation FW)</td>
<td>PCs, Connected Devices, Thin Clients (authentication, access control, encryption, virus protection)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Loss Prevention</td>
<td>Anti-Virus</td>
<td>End-point Security</td>
<td>e-mail Security</td>
<td>Physical Security</td>
</tr>
<tr>
<td></td>
<td>Unauthorized Access Measures</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Assessment/Consultation</td>
<td>Security Operation</td>
<td>E-mail Security Enhancement</td>
<td>Mobile/Remote Access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Education and Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Products

- **FUJITSU Security Initiative**
  - **Consulting, Operations, Training**
  - **Applications**
  - **Platforms**
  - **Network**
  - **Endpoints**

### Main Models Offered

- **Global Managed Security**
  - Visualizes problem areas with the existing organization and processes, and while continuing to make use of conventional counter measures, provides optimal countermeasure solutions for the customer to respond to cyber-attacks, based on practical knowledge cultivated through numerous business talks and operation of in-house systems.
- **Security Governance**
  - Supports the realization of “information security governance” in the organization based on continuous security measures from the perspective of overall company activities including ICT.
- **Cyber-Attack Countermeasures**
  - Provides optimal measures to guard against new cyber-attack methods, while taking full advantage of conventional measures.
- **Smart Device Security**
  - Provides services for customers’ security concerns when using smart devices for business purposes.
- **Unauthorized Access Measures**
  - Realizes a security cycle including surveillance 24 hours a day, 365 days a year, as well as planning, establishing measures, implementing measures, auditing, and monitoring.
- **Data Loss Prevention**
  - Provides functions for drafting and establishing information management policies and encryption functions for protecting personal information and preventing information leaks.
- **Anti-Virus**
  - Provides services including protection, virus removal, monitoring, and recovery support as anti-virus measures.
- **End-point Security**
  - Creates an environment that protects customer systems from threats such as leakage of confidential information and virus damage at end-points (terminals of client-connected systems).
- **e-mail Security**
  - Provides total security assistance needed to use e-mail securely, such as anti-virus measures and preservation of audit trails.
- **Authentication ID Management**
  - Provides assistance for authentication and user information management, which are the foundations of information security, through various products and services, including biometric authentication, electronic certificates, and directories.
- **PCI DSS**
  - Provides security measure solutions for helping to ensure compliance with the PCI DSS (Payment Card Industry Data Security Standard).
- **Thin Client**
  - Provides total client virtualization using cutting-edge devices and secure networks. Also supports work style reforms by enabling mobile use of an extensive range of user devices.
- **Physical Security**
  - Provides comprehensive solutions for physical security issues in the office.

For further details on security, please visit the following website (Japanese only):
This service provides total security operation assistance to customers developing their businesses globally. It begins with a setup service, in which the customer’s existing system is audited and weak spots are identified. This is necessary before engaging in the security management service, which handles cyber-attacks by providing services that are difficult for customers to perform by themselves, such as 24-hour, year-round real-time monitoring, incident response, and long-term security-management assistance such as training.

**Global Managed Security Service**

**Service Concept**
The service provides various functions necessary to the three operation processes that are vital elements of cyber-attack response: “detect/prevent,” “analyze/respond,” and “strengthen security.”

**Service Features**
1. **Accurate malware detection using proprietary technology**
   It is essential to introduce highly accurate detection equipment to detect unknown malware. Fujitsu uses a completely new attack detection technology called Malicious Intrusion Process Scan,*1 which is capable of detecting unknown malware by focusing on the behavioral processes of the attackers rather than those of the malware.

2. **Skilled experts**
   To minimize the damage from a cyber-attack, companies need to continuously develop highly skilled human resources capable of resisting cyber-attacks, which are growing more sophisticated day by day.

Fujitsu develops human resources such as security analysts and forensic engineers through its Security Meister Certification System. These experts are deployed to operate this service.

3. **Full use of in-house experience and knowledge**
The knowledge and expertise that the Fujitsu Group has accumulated regarding security is concentrated at A3L*2 and used in developing this service.

*1 Malicious Intrusion Process Scan: A new Fujitsu proprietary technology that markedly improves the detection rate of unknown malware.

*2 A3L: FUJITSU Advanced Artifact Analysis Laboratory

**Related services**

<table>
<thead>
<tr>
<th>Service</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>FUJITSU Security Solution Hidden Malware Survey Service (PC log analysis)</td>
<td>Using technologies from Fujitsu Laboratories, this service can easily investigate malware-infected PCs and the damage status. A service engineer uses Fujitsu’s proprietary inspection tools onsite to check for the presence and spread of malware.</td>
</tr>
<tr>
<td>FUJITSU Security Solution Malware Survey Service (Network log analysis)</td>
<td>With this survey service, sensors are installed on the customer’s network to detect targeted cyber-attacks, and traffic on the customer’s network is monitored to look for malware infections or potential infections. Results are reported to the customer.</td>
</tr>
<tr>
<td>FUJITSU Security Solution Targeted E-mail Attack Drill Service</td>
<td>In line with training objectives, this service covers developing and carrying out training plans, including examinations of the contents of mock attack e-mail messages. Support includes information on issues that arise during training and suggestions for improving them.</td>
</tr>
<tr>
<td>FUJITSU Security Solution Incident Response Training Service</td>
<td>This service provides training in responding to incidents based on current trends in cyber-attacks, as well as changes in day-to-day security management, the external environment, and attack methods.</td>
</tr>
<tr>
<td>FUJITSU Security Solution Security Violation Investigation Service</td>
<td>This service provides a detailed investigation and analysis of a customer’s data (HDD images, logs, etc.). By acquiring an accurate understanding of the scope of unauthorized activity by an attacker, such as whether or not an intrusive attack has occurred, the reason for the attack and countermeasures, and the extent of the damage, the service helps customers to clarify their response policy.</td>
</tr>
</tbody>
</table>