INFORMATION SECURITY UNDERPINNING "CONNECTED SERVICES"

As the use of digital technologies rapidly spreads, threats in the cyber domain pose a much greater risk to society from a variety of perspectives. Through its security-related services, Fujitsu is tackling these threats head on as a business partner to its customers, thereby supporting "Connected Services."

Security Threats in the Connected Era

By 2022, digital products and services are expected to account for over 60% of the world's GDP.*[1] In line with this is an expansion in the digital economy that is spurring the emergence of unprecedented risks. In 2017 alone, cybercrimes caused nearly US$600 billion (¥61 trillion) worth of damage to the global economy.*[2] In addition, in the IoT world, where everything is connected to a network, a single cyberattack has the potential to spark a chain reaction of damage. Accordingly, the establishment of measures to address cyberattacks and information leaks is an important task for top management around the globe. In light of this, global corporate investment in cybersecurity is expected to reach US$96 billion (over ¥10 trillion) in 2018.*[3]

*1 IDC, "IDC FutureScape: Worldwide IT Industry 2019 Predictions"
https://www.idc.com/getdoc.jsp?containerId=US44403818

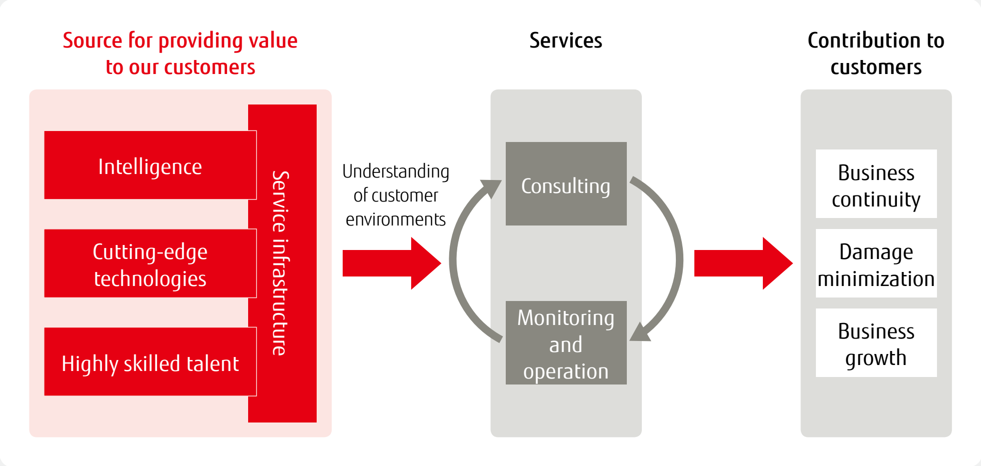
*2 McAfee, "The Economic Impact of Cybercrime–No Slowing Down"
https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf

*3 IDC, "New IDC Spending Guide Forecasts Worldwide Spending on Security Solutions Will Reach $133.7 Billion in 2022"
https://www.idc.com/getdoc.jsp?containerId=prUS44370418

Fujitsu's Strengths in the Security Domain

The security business at Fujitsu consists of a wide range of services, such as consulting and operation, and it also fosters talented personnel—we believe that security is one of the domains where Fujitsu is most able to demonstrate its superior integration capabilities. Linked to Fujitsu's ability to maintain a high level of global competitiveness in this area are a number of elements, including intelligence with regard to the collection and analysis of information on the latest security threats, regulations, and standards; research on cutting-edge technologies; experts with sophisticated analytical capabilities, know-how related to encryption technologies, insights on various industries; and a deep understanding of customers' IT systems.

We are also strengthening our service delivery infrastructure. Our Security Operations Centers (SOCs) monitor and analyze threats to the IT systems of our customers on a 24/7 basis, while our Advanced Artifact Analysis Laboratory (A3L), a specialist institution, also carries out sophisticated security analysis. Through these institutions, we provide services to over 1,400 customers around the world. Overseas, we provide high-quality security operations services in Europe, mainly in the United Kingdom. Going forward, we will work to further reinforce our service structure led by our dual security business headquarters in Tokyo and London.

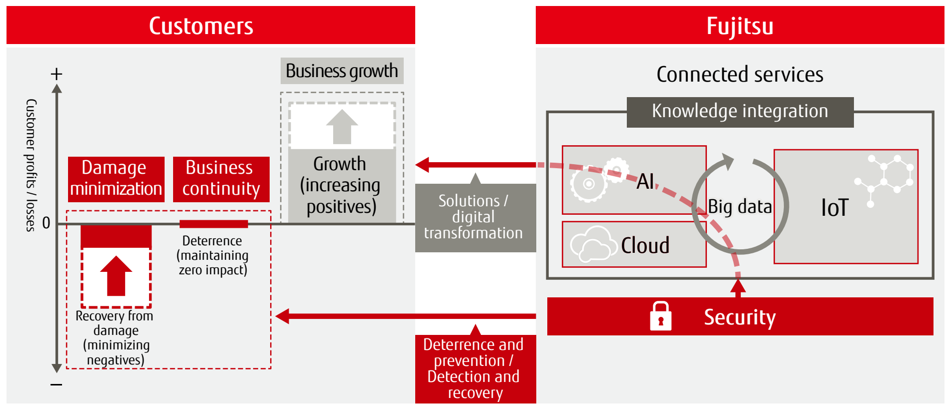


Security Underpinning Connected Services

We view security as comprehensively protecting our customers' IT systems, which enable them to create value. Through the provision of Connected Services that are underpinned by sophisticated security systems, we help our customers grow their core businesses and expand their profits. At the same time, we offer highly specialized security services that reduce risks for our customers and that minimize damage should risk occur. This in turn helps us earn customer trust.

Specifically, we support the safety and security of our customers' businesses through security-related consulting and a broad range of security products and operations services. We additionally hold workshops at the Security Initiative Center and other locations, letting our customers experience cyberattacks firsthand. Other opportunities are also offered to help our customers understand the importance of cybersecurity.

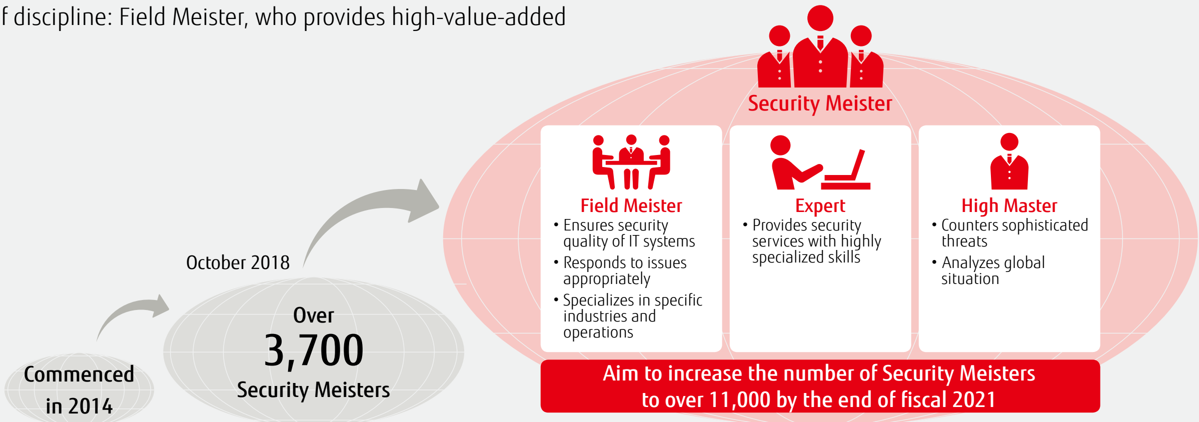
Fujitsu's Security Business Contributing to Our Customers' Value Creation


Customers
Fujitsu
Customer profits / losses
+
0
–
Business growth
Growth (increasing positives)
Damage minimization
Business continuity
Recovery from damage (minimizing negatives)
Deterrence (maintaining zero impact)
Solutions / digital transformation
Deterrence and prevention / Detection and recovery
Connected services
Knowledge integration
AI
Big data
IoT
Cloud
Security

Cultivating Security Meisters

As cybersecurity grows in importance, organizations continue to face critical gaps in skills, as well as the overall number of cybersecurity technicians. In light of these circumstances, the Fujitsu Group created the Security Meister Certification in 2014, and has since been leveraging this certification to cultivate human resources with specialized abilities pertaining to cybersecurity (over 3,700 certified Security Meisters as of October 2018).

The Security Meister Certification consists of three areas of discipline: Field Meister, who provides high-value-added SI services that incorporate security requirements; Expert, who has sophisticated and specialized cybersecurity skills; and High Master, who boasts industry-leading capabilities. Going forward, we plan on increasing the number of Security Meisters to over 11,000 by the end of fiscal 2021 with a view to further expansion of digital business such as IoT and operation technologies.


Commenced in 2014
October 2018
Over 3,700 Security Meisters
Security Meister
Field Meister
• Ensures security quality of IT systems
• Responds to issues appropriately
• Specializes in specific industries and operations
Expert
• Provides security services with highly specialized skills
High Master
• Counters sophisticated threats
• Analyzes global situation
Aim to increase the number of Security Meisters to over 11,000 by the end of fiscal 2021