# Strategic Briefing
## Security at FUJITSU

Fujitsu underpins clients and social innovation by continuous efforts to realize safe and secure Information and Communications Technology (ICT). This strategic briefing describes that high security is an inherent part of products, services and solutions.

**Contents**



# How Fujitsu makes sure information is secure

## Information security is growing in importance

People, organizations and businesses around the world communicate with each other through the Internet – 24 hours a day. Some two billion people and 50 billion devices were already involved in the "digital world" in 2012. And the globalization of this world continues at a rapid pace. Thanks to cloud computing and smarter devices, Information and Communication Technology (ICT) now impacts all aspects of our daily lives. However, the digital world also has a dark side – cyber crime – which continues to pose a serious threat. Theft, fraud, criminal activities and intrusions of all kinds are on the rise. Personal data in particular, such as bank and credit card information, is often the target of cyber criminals. All of us are affected – people, business enterprises, organizations and society in general. In the worst case scenario, the repercussions can be devastating, even posing an existential threat.

That is why businesses need to effectively protect their intellectual property, know-how and information against criminal activities, loss and inconsistency of data. What's more, enterprises are responsible for protecting their own data as well as that of their customers and partners. They can only meet this obligation by providing security at three levels: data access authorization, data availability and data consistency (integrity). Providing enterprises with solutions that enable them to maintain comprehensive security that is easy and reliable to realize is one of the most important challenges facing the ICT industry today.

FUJITSU as a business, manufacturer and IT service provider complies with all security standards and has ISO 27001 certification. Furthermore, security is a central aspect in the development of products and solutions. The ongoing development of customers and society is also bolstered by the FUJITSU Security Initiative. Fujitsu cooperates with security providers to offer its customers and society high-tech security products and services. Fujitsu is thus in a position to serve as a trusted partner for its customers as they realize safe and secure IT. The following examples illustrate just some of the comprehensive security solutions included in the Fujitsu portfolio.

# Workplace systems

Long before information security gained widespread media attention, Fujitsu was already equipping its workplace systems with effective security technologies and solutions. Ever since customers have come to prefer Fujitsu workplace systems, especially for two reasons: their outstanding functionality and their comprehensive security features. These features include:

## Authentication with Workplace Protect

Workplace Protect is a set of authentication modules for various work environments and security levels. The modules can be used individually or in various combinations. The set includes:

- User authentication for Microsoft Windows
- Preboot authentication based on fingerprint, palm vein or smart card
- Single sign on to Microsoft Windows
- Password safe – stores your secret login details needed to log on to protected websites
- Encrypted container – virtual disk encryption to protect user data

## Data deletion with EraseDisk

Inadequate hard disk cleaning is often the cause of data leaks and data loss. Fujitsu's unique EraseDisk technology solves this problem: EraseDisk permanently deletes data on hard disks before a workplace system is taken out of service, refurbished or sold – and helps business enterprises meet compliance regulations governing data deletion.

## Secure preboot authentication with SystemLock3

Pre-boot Authentication with smart card and PIN combination is the strictest form of access control and basically shuts out adversaries before they can even start the system. Fujitsu offers this access control function at BIOS level known as SystemLock 3. In conjunction with single-sign on SystemLock 3 provides the highest level of comfort, because the user credentials are handed over to the operating system.

## Advanced Theft Protection

Advanced Theft Protection is based on an incremental security concept. Systems can be locked and deactivated remotely. Remote and automatic deletion of sensitive data is also possible in order to satisfy compliance requirements. Stolen devices can be located thanks to a GPS- and Wi-Fi-based tracking function. Furthermore, changes made to the software and hardware can also be tracked to support law enforcement agencies – this is important for investigative and legal purposes.

# Servers

**FUJITSU PRIMERGY servers** are equipped with effective and field-tested security features that prevent unauthorized access to server hardware, to a broad range of management functions and related sensitive data on the systems.

Lockable racks protect PRIMERGY servers installed in data centers, whereas individual locks safeguard standalone systems in office environments from being opened by unauthorized personnel or intruders. In addition, PRIMERGY servers are fitted with alarm switches which enable the ServerView® Management Software to detect whenever the server housing cover and the HDD/SSD module cover are removed – this information is then recorded in a log.

However, these measures are just one aspect of security – safeguarding the software products installed on servers is also very important. Operating systems, applications and server management software like FUJITSU ServerView offer a wide range of security features to protect software. For example, access to ServerView functions is governed by comprehensive, configurable role-based user management. Administration data is also transmitted via secure, state-of-the-art protocols. Furthermore, it is possible to separate the administration data from productive data in a management network – the server design guarantees this strict isolation in two networks.

Another aspect to consider is the availability of data and thus the availability of the systems. This is where FUJITSU PRIMERGY servers are especially effective – customers benefit from outstanding performance as well as excellent availability with the lowest Annualized Failure Rate (AFR).

Effective protection against unauthorized access through advanced hardware and software security features, plus excellent system availability: That is the concept behind PRIMERGY servers that enables them to deliver reliable 24x7 performance.

# Storage

The **ETERNUS** brand is known for its high levels of security – both in terms of data access as well as availability and data consistency. The FUJITSU Storage ETERNUS portfolio comprises the ETERNUS DX disk storage family for online storage purposes and the ETERNUS CS data protection appliances for backup and archiving. "Business-centric Storage" was the underlying philosophy when developing this new generation storage systems. Applying ETERNUS enables allocation of storage resources according to business priorities – this also includes security demands:

- Extremely robust, disaster-resilient system design
- Comprehensive functions to prevent data loss and corruption
- Role-based administration
- Advanced data encryption
- Secure data communication
- Flexible support for disaster-recovery concepts
- Stringent quality assurance processes

Data encryption with ETERNUS protects confidential data against unauthorized access – effectively and at low cost. The data encryption method is controller-based and/or disk-based. Fujitsu offers 128-bit AES encryption and – alternatively – its own brand of encryption technology. Self-Encrypting Drives (SEDs) are used for disk-based encryption; the data is automatically encrypted before it is written to the hard disk or read from the disk. This also means that data on SEDs is fully protected even when these hard disks are removed from the system for disposal.

Various technologies are available with ETERNUS DX and ETERNUS CS, e.g. Data Block Guard to ensure data integrity, or Database Data Guard and self-healing functionalities which contribute to data consistency.

For many business enterprises it is essential to have data availability concepts that can be easily applied across several sites at relatively low cost. ETERNUS DX online storage systems and ETERNUS CS data protection appliances have many options for achieving this. For example: In a so-called split-site configuration with cache mirror, one logical ETERNUS CS8000 system is available for two geographically separate sites. The backup software treats this configuration as one logical setup so that data can be read and written across both sites. The result is a system without a single point of failure that is available even during an outage at one of the sites. By the way, ETERNUS CS8000 is the only system having this feature worldwide.

# Cloud

FUJITSU Cloud Services are based on the Tier 3 data centers operated by Fujitsu in various parts of the world. The data centers have a „defense in depth" approach when it comes to security – starting with the infrastructure of the building and including the virtualized workloads – so that all physical and virtual levels are covered. Examples of security measures at specific levels include:

- Physical Security Protection – Entrance and Exit Management, Server Rack Protection
- Network Perimeter Protection – Firewall, IDS, Network Access Protection
- Internal Network Protection – Network Segmentation, Secured Communications (IPSEC)
- Core Infrastructure Protection – Virus Check on Servers, Security Patches on Servers, Secured Communications (IPSEC), Federation Services, OS Fortressing, Encryption
- Hypervisor Protection – Secured Communications, Port Filtering, Security Patches for Hosts
- Workload Protection – Network Segmentation (VLANs), Virtual OS, Virtual Firewalls, Encryption

Furthermore, the data centers are also certified according to ISO/IEC 27001 Information Security Management. This means that information security is assured through comprehensive security mechanisms that apply to the entire infrastructure, all processes and human resources.

The security concept is bolstered with specific portfolio offerings. For example, with Infrastructure as a Service (IaaS), enterprises having IaaS Trusted Public S5 can take advantage of a service giving them on-demand access to a pool of virtual, completely configured server, storage and network resources. IaaS Trusted Public S5 also features enterprise-class security controls and advanced platform monitoring. IaaS Trusted Public S5 is strictly role-based and precisely defines which components remain under customer control and which are controlled by Fujitsu. Such powerful security mechanisms, tailored for regional needs, are also available for IaaS Private Hosted offerings. Outsourcing and Managed Services customers also have the authority to conduct compliance audits. To determine which cloud service is suited for a specific scenario, customers can turn to FUJITSU Security Consulting Services for complete advice and support.

# Security solutions

## FUJITSU SURIENT

**Transparent and user-friendly end-to-end security - from the terminal to the data**

The FUJITSU Security Solution SURIENT is a family concept of innovative patented end-to-end IT security offerings. It provides secure application environments based on existing infrastructures and enables – dependent on the specific customer requirements - up to highest degree of security, especially for sensitive data and processes. High user-friendliness, easy and smooth integration in existing data center and high performance levels are characteristics of this security concept covering data centers, data transfer and terminals as well as the sensors which play a central role in the "Internet of Things". The concept comprises various modules. It is possible to adjust the protection levels to the various requirements. The modules can be used individually or in combination. FUJITSU SURIENT family includes following components:

- **SURIENT MRS (Managed Rack Solution)**
  The Managed Rack Solution module protects data center infrastructures from non-authorized access. The Managed Rack Solution is designed for average security requirements. Authentication can be via infra-red palm vein scan using PalmSecure but also other biometric authentication systems can be used as well. The rack can thus only be accessed by authorized administrators. Depending on the protection requirements access can also be combined with a "double-check" (4 or more eyes). The door of a security rack can thus only be opened jointly via a defined group of persons.
- **SURIENT SRS (Sealed Rack Solution)**
  The Sealed Rack Solution module protects data center infrastructures from non-authorized access. The Sealed Rack Solution offers even greater protection levels as well as monitoring and audit features according to ISO 27000. Authentication can be via infra-red palm vein scan using PalmSecure but other biometric authentication systems can be used. The rack can thus only be accessed by authorized administrators. Depending on the protection requirements access can also be combined with a "double-check" (4 or more eyes). The door of a security rack can thus only be opened jointly via a defined group of persons.

# Security solutions

- **SURIENT EBS (Encrypted Boot Solution)**
  The new Encrypted Boot Solution (EBS) is based on technology patented by Fujitsu. The module is used to start IT systems in the data center with encrypted system partitions and without having to enter a password manually. The passwords are created and transferred by the system decentrally and are not even known to the administrators. This provides effective protection against non-authorized access by employees.
- **SURIENT SCS (Stealth Connect Solution)**
  The Stealth Connect Solution (SCS) ensures that today's external attack methods against servers and services will be unsuccessful. Authorized users can log in via a secure Virtual Private Network (VPN) in the data center. The solution disables the server process VPN port and an attacker does not receive any response to his port scans and is thus not provided with any information about the location of possible attack points. A Zero Day Exploit and Man-in-the-Middle attacks are made extremely difficult as a result of this "digital stealth" function.
- **SURIENT SAS (Sealed Application Solution)**
  The Sealed Application Solution (SAS) module ensures effective protection for applications on terminals, such as PCs, tablets, workstations and notebooks. It is a highly-secure runtime environment which is started parallel to the operating system. The applications and data processing run completely separated from the hardware and operating system in this encapsulated environment . Applications and data can thus be protected against attacks in a very effective manner. The solution is not dependent on any manufacturer and can be used on all standard-based terminal systems; it is suitable for processing sensitive company data and for applications, such as online banking.

## FUJITSU PalmSecure

### Authentication management

Today passwords, personal identification numbers (four-digit PIN numbers), and ID cards are used for personal authentication. However, cards can be stolen, and passwords as well as numbers can be guessed or forgotten. Another issue is how to handle growing numbers of passwords. To solve these problems, biometric authentication technology, which identifies people by their unique biological information, is attracting attention.

**FUJITSU PalmSecure** technology relies on the very complex vein pattern inside the palm of the human hand. The position of the veins remains the same for a lifetime and is different for each and every individual. Dirt or superficial skin injuries have no impact on the palm vein pattern. And being beneath the surface of the skin, it is fully protected against any misuse or manipulation. Palm vein recognition with PalmSecure is practically impervious to environmental influences, and it is a very hygienic solution because it is touch-free. It works with living tissue and, in view of the present state of technology, is free from manipulation. PalmSecure also provides significantly higher precision and security than the biometric recognition of a fingerprint or an iris. PalmSecure authentication is a convenient and fast process that keeps administration and costs low.

PalmSecure technology has been deployed worldwide in a wide range of vertical markets, including security, financial/banking, healthcare, commercial enterprises and educational facilities.

SUMMARY

Fujitsu has a vision of "A Human Centric Intelligent Society." And we are sure that this is possible through the power of ICT. Information security is a central prerequisite for making this vision a reality. Effective security measures, clearly defined and verifiable governance, and protection of the private sphere will enable business enterprises and society as a whole to use information with peace of mind, knowing that everything is safe and secure. Fujitsu and its own products and solutions completely support information security and thus promote business innovation and society innovation.

Published by
Fujitsu Limited