White paper
FUJITSU Server PRIMERGY Security Overview

During the last few years server security has become a key building block for end to end security. We see strongly increasing cyber-attacks on server infrastructure, which results in an intense need for server security. This whitepaper presents an overview of the security features which are available for PRIMERGY server.

Inhalt

Importance of Server Security

During the last years the attack vectors for server have been changing significantly and server become more and more a target for different types of hackers. The old school approach only to protect endpoints, network communication and applications does not fulfil today's needs. In the past it was sufficient to protect server infrastructure physically and down to the hypervisor. Today we see the need to establish a complete E2E chain of trust starting with the hardware, including development processes, supply chain and manufacturing.
Fujitsu has a long history in providing best in class security for PRIMERGY server and will help to guard you against cyber security threats. This whitepaper will summarize some important aspects on server security, give you a guideline for improving your server security and show you, where to find more detailed information.

Security Goals and Certification

Server security is about confidentiality, availability and integrity. That means a server has to be nearly invisible, should work 365 x 24 hours a year in a well-defined state and keep its integrity. For data residing or processing on the server this means: Access to the data only to authorized people, whenever they need access they can access and nobody unauthorized could modify or delete the data. PRIMERGY servers provide you with key functionality, so you can keep your server secure. We show our commitment to IT security with ISO 27001 certification.

Security for the whole Lifecycle

It is very hard or even impossible to fix a security leak in the lower hardware near levels with measures in the higher application near levels. It is also very hard to fix vulnerabilities in the early life cycle later. Security has to start in the early beginning of a server's life and ends after its disposal and not before. It is a permanent process. PRIMERGY server are designed for a long lifetime and we are committed to provide security updates and patches for all our components for at least 5 years. The next sections will highlight some lifecycle security aspects.

Security through the Supply Chain

PRIMERGY servers are well specified to reduce the risk of weak points to a minimum. This starts with the selection of our partners. Before becoming a Fujitsu supplier every vendor has proof that he is trustworthy and has stable quality processes in place. Therefore, he must pass an intense assessment to prove that he can meet Fujitsu standards and required processes which we recheck through defined audits.

Security out of the Factory

Naturally we run secure factory processes with regular audits. But furthermore, we allow you to preconfigure our servers and freeze hardware and firmware configuration to ensure that security settings are set right in the factory and wherever we deliver your server everybody who switches on the server has the desired security settings on a well-defined state with no changes - for years if you like. This is an optional configuration service called made4you and ensures security out of the box for your PRIMERGY server.

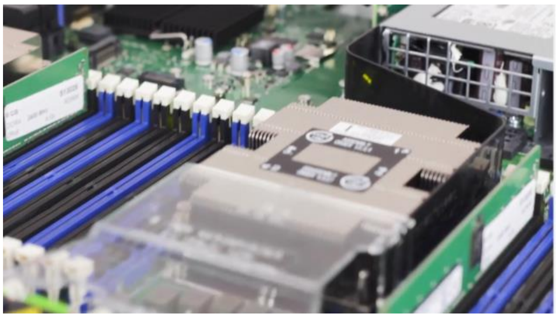
Server Security Capabilities

Secure Boot

After production and delivery now it is up to you to keep the server secure. This starts when you boot the system for the first time. In the PRIMERGY UEFI Bios you can restrict the boot options for your server systems and secure the boot process. A center piece is the Secure Boot method. Secure Boot ensures the code integrity during the boot process of the server. For every boot phase the code must be verified by the previous phase. If the code does not pass the integrity check the system could stop the boot process and send out a notification.
To ensure the integrity every software and firmware component has to be signed properly. Fujitsu ensures this through its development and QA. Secure Boot ensures that tampered systems can be detected, and you can initiate measures before malware is active.

Trusted Platform Module (TPM) Version 2.0

All Fujitsu PRIMERGY server support Trusted Platform Module (TPM) Version 2.0 as an option. The TPM is a computer chip which securely stores information, such as passwords, certificates or encryption keys, and is used to authenticate your server. A TPM enables you to determine the identity of your server in a very secure way and keeps "secret" information secret.



Intel® Trusted Execution Technology

Most malware prevention tools execute only after the system has booted into the runtime environment. In an age of ever-growing threats from hypervisor attacks, BIOS and other firmware attacks, malicious root kit installations, and more, Intel TXT helps to close an important security gap by providing evaluation of the launch environment and enforcing "known good" code execution. Complementing runtime security protection solutions, Intel TXT adds a foundational (hardware-based) protection capability to server systems by allowing greater control of the launch stack and isolation in boot process. For more information see https://www.intel.com/txt.

Secure Communication

Our customer can completely control and secure the communication. We support secure protocols like TLS1.2, HTTPSboot, SNMP v3 and DMTF Redfish. He is able to protect his system by disabling unsecure protocols like SNMP 1.x/2.x. For sure he could add his specific certificates to secure the communication channel. All communication uses TLS 1.2 or higher. HTTP-requests will automatically be changed to HTTPS.
We reduce used ports to a minimum. All ports are well described and could be changed according to customer policies. For detailed information see Secure PRIMERGY Server Management Enterprise Security http://manuals.ts.fujitsu.com/file/4289/sm-security-en.pdf.

Secure Authorization and Authentication

Authorization and Authentication could be comfortably handled in your environment and you can easily adopt it so it fits with your security policies. User management and security architecture of FUJITSU Software ServerView Suite and the out of band management with Fujitsu iRMC or eLCM (embedded Life Cycle Management) are based on three fundamental user security concepts:

- ONE (global) user management using an LDAP directory service
- Flexible Role Based Access Control (RBAC)
- Single sign-on (SSO) based on a centralized authentication service (CAS)

For a good start we provide predefined roles: Administrator, Operator, Monitor or User. You can easily change the rights of these or add new roles according to your security rules. You can find detailed information in this manual.

Physical Protection

Tampering your systems is a huge problem. If somebody gets access on your hardware, he can steal components like storage devices or dump the RAM or copy all activity of the processor by putting additional (malicious) hardware into the system. To avoid physical intrusion, we provide our systems with

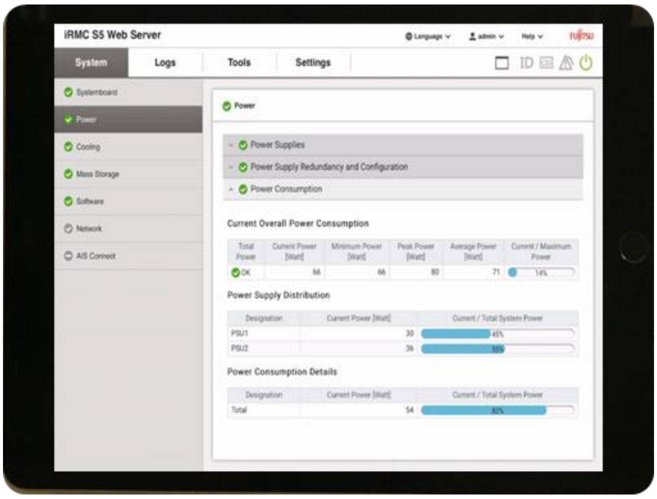
- Intrusion Detection Switch, which detects any opening of the cover (available for PRIMERGY Tower Servers)
- Lockable front bezel for our rack server and a 3 way lock for PRIMERGY Tower Server. With these you are able to control physical access to devices and interfaces.
- For our floor stand server we provide a Kensington mount and addition brackets to avoid theft of the complete Server.
- Control of USB ports. You can easily switch off external USB-ports, both, at the rear and at the front.
- In addition, we offer PalmVein protected secure racks on project base. These racks can only be opened with biometric authentication, or even better a two-way authentication (PalmVein plus RFID). If you like you can also urge a 4 eyes principle.

Secure Out of Band Management with Fujitsu iRMC

The integrated Remote Management Controller iRMC represents a BMC with a separated LAN connection and extended functions. The iRMC therefore offers comprehensive control over PRIMERGY servers, irrespective of the system status. In particular, the iRMC allows for out-of-band management (Lights Out Management, LOM) of PRIMERGY servers to monitor and manage servers via remote control, regardless of whether the server is powered on.

As an autonomous system on the system board of a Fujitsu server, the iRMC has its own protected subsystem, separated from the "productive server" with operating system, web server, user management and independent alert management. The iRMC remains powered on even when the server is powered off or in standby mode. The iRMC protects your server after power and in case of a malicious attack it helps to reset your system to a good working state.

By the way: You can set more the 1500 system attributes via iRMC. All these attributes could be monitored, so you can detect a drift in the security level compared to your reference.



Current Overall Power Consumption

Total Power	Current Power [Watt]	Minimum Power [Watt]	Peak Power [Watt]	Average Power [Watt]	Current / Maximum Power
OK	66	66	80	71	14%

Power Supply Distribution

Designation	Current Power [Watt]	Current / Total System Power
PSU1	30	45%
PSU2	36	55%

Power Consumption Details

Designation	Current Power [Watt]	Current / Total System Power
Total	54	82%

Fully Separated Management Network

As you saw Fujitsu iRMC provides a rich feature set to manage the server and its settings. To avoid unauthorized access, we recommend physical separation of management network from data network(s). Therefore, all PRIMERGY servers provide a completely separated LAN for access on iRMC.

Reliable Installation

ServerView Installation Manager ensures a secure, reliable installation of PRIMERGY server, reproducible, totally unattended for many operating systems (Microsoft, Linux, VMware ESX). You can prepare the installation in a secure way on an encapsulated sandboxed system and control the installation of the production servers.

This reduces the risk of unwanted changes during installation and avoids risk of backdoors places during installation.

If you purchased eLCM, your system installation can be stored safely on eLCM SD card for immediate use with no access on external media. This is of enormous benefit in emergency case, if you need to reset the system completely. New setup can be initiated remotely and produces a reliable original system state.

Secure Update of System Software

Fujitsu provides highly secured system software updates for all components such as drivers, firmware and BIOS. Updates for these components run through a well-defined process to ensure quality and security. After passing all process steps we sign each software with certificates. You can be sure, that this software is tested from Fujitsu, comes from Fuijtsu and was not changed during download. For PRIMERGY server we provide security updates at least for 5 years. This helps to keep your server secure for a long time.

Because software management is one of the key pillars of server security ServerView Update Management allows you to manage updates for the firmware and software components of PRIMERGY servers very flexible. You can choose whether you want to control your updates completely by yourself or use automatic updates, which we provide. Three tools support you:

- Download Manager provides a mechanism which checks for available updates and downloads only new ones for the monitored managed nodes from the Fujitsu support server to the local repository on the management station.
- Repository Manager provides a mechanism for managing your repository on premise. You can easily update your local repository on the management station and create your collections.
- Update Manager provides a mechanism for managing updates and installing them on the monitored managed nodes.

Alerting and Logging

Our servers permanently monitor health status and other attributes, configured by our customer. In case of violation we inform you at once and fire an event to your event console or to a defined email address. For sure, all important activity will be logged from our logging system. Logging and alerting could be easily managed via ServerView Operation Manager.

Secure Service with AIS Connect

During the complete live cycle Fujitsu offers product services to provide you with best in class remote services. We do that in a very secure way. Only you can initiate the remote connection. Communication will be established using TLS. The enterprise server authenticates via certificate on the service agent.

The policies for establishing the remote connection could be individually defined solely on customer side. For inbound connection the server shows no (zero) open port. The complete session could be audited via automatic creation of audit logs on both sides (event protocol) and optional complete session logs.

Summary

Digitization is opening a myriad of possibilities for businesses to create and capture value but it also creates many possibilities for those who wish to steal from them, from their customers and partners, or to disrupt the services they provide. Security needs to be thought through end to end and the technological core is the platform on which all your data is being processed and stored. Security is not an afterthought, it is an integral part of a system designed to deliver speed and safety in equal measure. Security is something that is systematically considered when designing and delivering products, solutions and services. Take your business into the digital fast lane – while making sure that security is embedded throughout your business. With a broad portfolio and more than 40 years of security experience, Fujitsu gives you the power and the confidence to excel. Build securely on FUJITSU Server PRIMERGY systems.

Contact
FUJITSU LIMITED
Mail: server-marketing@ts.fujitsu.com
Website: www.fujitsu.com
2019-06-07 WW-EN