PRIMERGY Server Security Overview

White Paper

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.

Contents

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 attackers. The old school approach only to protect endpoints, network communication and applications does not fulfil today's demands. In the past it was sufficient to protect server infrastructure physically, and from the application down to the hypervisor. Today we see the demand to establish a complete E2E chain of trust starting with the hardware, including development processes, supply chain and manufacturing.
We have a long history in providing best in class security for PRIMERGY server and will help to guard you as the customer against cyber security threats. This whitepaper will summarize some important aspects on PRIMERGY 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 also about confidentiality, availability, and integrity. That means, a server must 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 information security and quality with an ISO 27001 and ISO 9001 certification, as well as general adherence to further international norms, catalogues, and standards, such as NIST SP 800-series for hard- and firmware and OWASP ASVS for applications.

Security for the Whole Lifecycle

It is extremely hard or even impossible to fix a vulnerability or weakness within the lower hardware levels, with measures present in the higher application levels. It is also quite difficult to mitigate or fix vulnerabilities at a later stage of the product life cycle. Thus, product security has to start in the early beginning of a server's life and only ends with its decommission. It is a permanent process. PRIMERGY server are designed for a long lifetime, and thus Fujitsu is committed to provide security updates 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 must prove that he is trustworthy and has stable quality processes in place. Therefore, he must pass an intense assessment to show that he can meet Fujitsu standards and required processes which we recheck through defined audits.

Security with Support of the Fujitsu PSIRT (Europe)

PRIMERGY servers are further secured, throughout their lifecycle, by the Fujitsu PSIRT [Product Security Incident Response Team], as the Fujitsu entity responsible for product-specific IT security. The Fujitsu PSIRT (Europe) advises customers on complex product/IT security-related issues, regarding PRIMERGY server. It manages complex threats and issues in the Fujitsu product landscape and offers consulting to you as the customer on product security matters. Its daily activities on PRIMERGY server security involve especially:

- Security incident and problem handling
- Research & Diffusion, e.g., on side-channel vulnerabilities (Meltdown, Spectre, etc.)
- Advanced, regular vulnerability scanning, i.e., of ServerView Suite, ISM and iRMC
- Standardization of products (hardening standards) on iRMC, FlexFrame Orchestrator, PF4SH, etc.
- Publication of security advisories and notices

For detailed information see the PRODUCT SECURITY section of the
Fujitsu Technical Support pages from Fujitsu EMEA.

Server Security Capabilities

Platform Firmware Resilience (PFR)

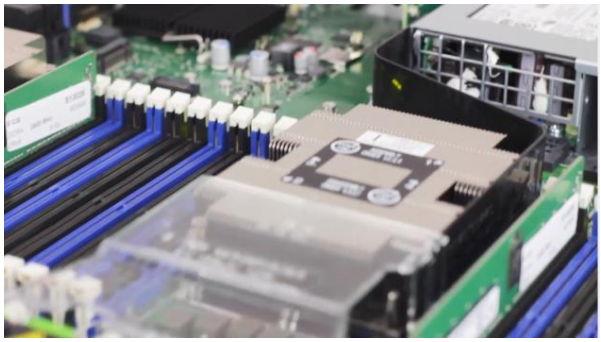
Providing security mechanisms already on silicon level by establishing a silicon root of trust is key to the overall system security which certain PRIMERGY servers provide through a feature called "Platform Firmware Resilience (PFR)".
From the press of the power button to the start of an operating system, a multitude of different firmware is executed that may act as a potential attack vector, in case this firmware was compromised and injected with malicious code.
With PFR, PRIMERGY offers a method to not only detect such tampered firmware but offers a way to prevent its execution as well as restoring a valid and secure version. PFR-enabled systems are equipped with a silicon that provides an immutable hash value, which firmware like the iRMC firmware and the UEFI firmware in the system is compared against before being started.
Only in case the comparison can prove, that the firmware about to be started is unchanged, it can be subsequently executed. Through the means of the silicon, the iRMC firmware code integrity is verified before it is started.
The iRMC firmware then proves the integrity of subsequently loaded firmware, like UEFI, which itself then secures the start and execution of an operating system. Originating from a silicon, containing an immutable hash value, these sequences of cross-checks of firmware complete and provide the Chain of Trust (CoT). In the unlikely event, that a compromised firmware was detected, the iRMC will prevent the start of it and alerts the administrator about the detected security breach. The administrator then can decide to restore the firmware to a state or version that is genuine or start a forensic analysis on the malicious code found.

Secure Boot

After production and delivery, it is up to you the customer to keep the server secure. This begins 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 centerpiece 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 can stop the boot process and send out a notification.
To ensure the integrity, every software and firmware component must 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 any malware becomes active.

Trusted Platform Module (TPM) Version 2.0

All 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.

Secure Communication

Our customers can completely control and secure the communication. We support secure protocols like TLS1.2, HTTPSboot, SNMP v3 and DMTF Redfish. Thus, customers are able protect their system by disabling insecure protocols like SNMP 1.x/2.x, and are also able to add their specific certificates to secure their communication channels. All communication uses TLS 1.2 or higher (or an equivalent protocol). HTTP-requests will automatically be changed to HTTPS.
Further, we reduce used system ports to a minimum. All ports are well described and can be changed according to customer policies. For detailed information see Secure PRIMERGY Server Management.

Secure Authorization and Authentication

Authorization and Authentication can be comfortably managed in your environment, and you can easily adopt it, so it fits with your internal security policies. User management and security architecture of ServerView Suite Software, Infrastructure Manager (ISM) and the out-of-band management with iRMC, together with 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.
With PRIMERGY server M7 generation, we have also increased ISM (default) password complexity requirements, implemented local MFA (multi-factor authentication) and additional cryptographic hash functions and KDF (key derivation function).

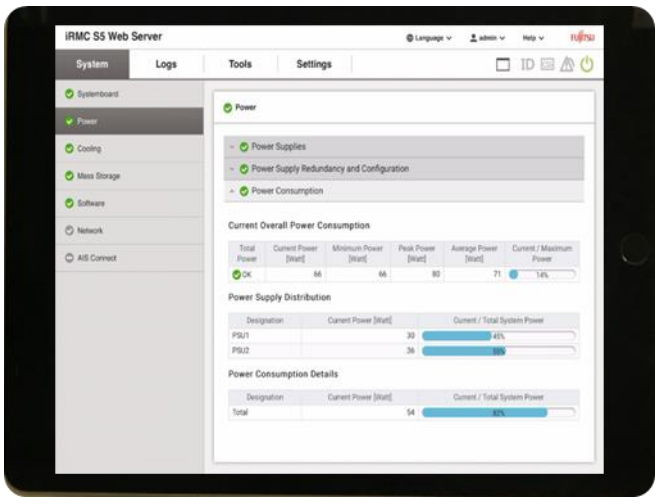
Physical Protection

Tampering your systems is a huge problem. If somebody gets access on your hardware, that individual can steal components like storage devices, or dump the RAM and 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.
- Lockable front bezel for our rack server and a 3-way lock for PRIMERGY Tower Server. With these you can 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 PalmSecure™ protected secure racks on a project basis. These racks can only be opened with biometric authentication or – even better – a two-way authentication (PalmSecure™ together with RFID). If you like you can also urge a four eyes principle.

Secure Out-of-Band Management with PRIMERGY iRMC

The integrated Remote Management Controller (iRMC) represents a BMC (Baseboard Management Controller) with a dedicated LAN interface 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, i.e., Lights Out Management (LOM), of PRIMERGY servers to monitor and manage them via remote control, regardless of whether the server is powered on. As an autonomous system on the system board of a PRIMERGY server, the iRMC has its own protected subsystem with dedicated operating system, web server, user management and independent alert management, all separated from the "productive server" and its OS. 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.
With PRIMERGY server M7 generation, we have also increased iRMC (default) password complexity requirements, implemented MFA

(multi-factor authentication) and improved account brute-force defenses.
Since iRMC S6, it also supports two modes in which systems can be configured initially in WebArchitect and then delivered to the customer:

- Standard mode (default): more secure anti-brute-force configuration, with unique, randomized, and strong initial password, mandatory password change requirement and most protocols disabled by default.
- Mass deployment mode (optional): less secure, mass-rollout configuration, well-known standardized initial default password, no password change requirement, some protocols are enabled by default (i.e., RESTful, UHL).

Fully Separated Management Network

As you saw, PRIMERGY 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 interface for the iRMC.

Reliable Installation

ServerView Installation Manager ensures a secure, reliable installation of PRIMERGY server, reproducible and completely unattended for many operating systems and hypervisors (Microsoft Windows, GNU/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 the risk of backdoors inadvertently placed during installation.
If you purchased eLCM, your system installation can be stored safely on eLCM SD card for immediate use, with no access to further external media required. This is of enormous benefit in case of an emergency, if you need to reset the system completely. A new setup can be initiated remotely and produces a reliable original system state.
In addition to that, Infrastructure Manager (ISM) is available, which simplifies IT operations and consistent management across over server, storage, and networking. ISM displays the firmware versions of all types of firmware and of all components in single view and provides one procedure to update all types of firmware in a single process. For detailed information see Infrastructure Manager Software (ISM).

Secure Update of System Software

Fujitsu provides highly secured system software updates for all components such as CPU microcode, UEFI-BIOS, CSME and SPS management engines, iRMC, hardware drivers, and other firmware or management software. 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, employing strong cryptographic primitives. You can be sure, that this software is tested by Fujitsu, comes from Fujitsu and was not in any shape or form manipulated during manufacturing, provisioning and transfer (customer download). For PRIMERGY server, we provide security updates at least for 5 years. This helps to keep your server secure for a long, predictable time.
Because software management is one of the key pillars of server security, ServerView Update Management and Infrastructure Manager allows you to manage updates for the firmware and software components of PRIMERGY servers in a very flexible way. You can choose whether you want to control your updates completely by yourself or use automatic updates, which we provide. Three tools support you with that:

- 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 premises. 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 the customer. In case of violation, we inform you at once and fire an event to your event console or to a defined e-mail address. For sure, all-important activity will be logged from our logging system. Logging and alerting can be easily managed via ServerView Operation Manager or Infrastructure 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 as a customer can initiate the remote connection. Communication will be established using strong, TLS-based cryptography. The enterprise server authenticates via certificate on the service agent.
The policies for establishing the remote connection can be individually defined solely on the customer side. For inbound connections, the server is in stealth-mode and shows no (zero) permanently open listening ports. The complete session can 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 PRIMERGY server systems.

For more information on PRIMERGY Server Security

https://www.fujitsu.com/global/products/computing/servers/primergy/server-security/

Contact
Fujitsu Technology Solutions GmbH
Mies-van-der-Rohe-Straße 8
D-80807 Munich
www.fujitsu.com