Hewlett Packard Enterprise

Solution brief

HPE SUPERDOME FLEX 280 MANAGEMENT AND SECURITY ECOSYSTEM

Unique embedded capabilities enable industry-leading RAS and reduce risk

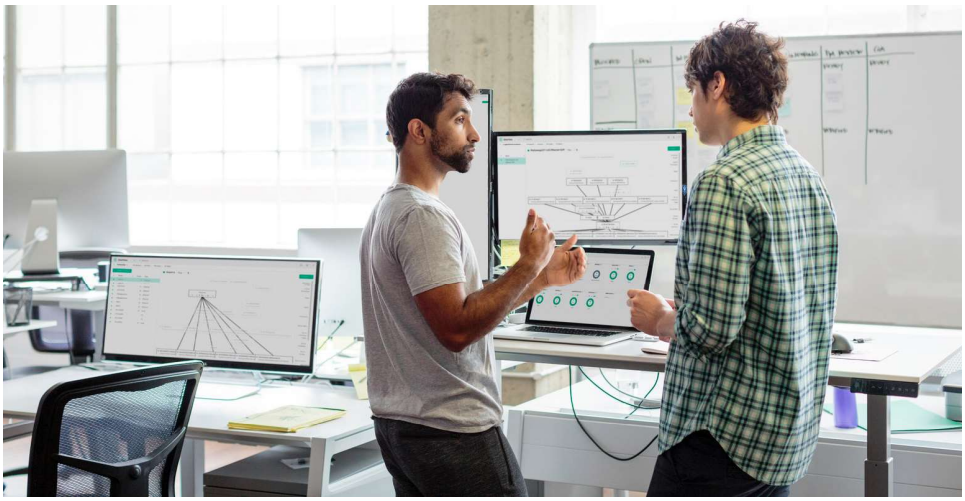
Key management and security features of HPE Superdome Flex 280

Embedded management system enables RAS and security

- Built-in fault analysis
- Fault-resilient boot
- Reduced attack surface
- Simplified management with no additional licenses required

Security capabilities help minimize threat exposures

- Reduced firmware vulnerabilities
- Silicon root of trust
- Tamper-resistant TPM 2.0
- Resilient firmware backups
- End-to-end controlled manufacturing



A NEW STANDARD FOR RAS AND SECURITY

Critical workloads demand environments that provide excellent reliability, availability, and serviceability (RAS) capabilities, with superior security to protect the business against growing threats. Running these environments can be challenging on standard servers that are:

- **Vulnerable to known attacks**—Many standard servers ship with common vulnerabilities, which weaken security of data and applications.
- **Dependent on human intervention—** Lack of automation to catch and resolve issues increases the risk of downtime.
- **Complex to manage**—More IT skills and time are needed, increasing risks to availability and security.

Designed as a building block for digital transformation, **HPE Superdome Flex 280** addresses these challenges with innovative RAS advantages that simply don't exist in other x86 server platforms. The key enablers of these RAS advantages are the system's management and security ecosystems, which combine to reduce vulnerabilities and provide peace of mind for organizations running vital workloads.

EMBEDDED MANAGEMENT INNOVATION

HPE Superdome Flex 280 features a system-level embedded rack management controller (RMC), which provides a single management interface and control point for the entire system. This control point includes:

- **A web-based GUI** for common tasks such as inventory and health reporting, configuration, vMedia, vKVM (HTML5), UEFI configuration, power controls, security, and LAN settings
- **A standards-based Redfish API** for scripting and automation
- **A command-line interface (CLI)** for power user and script access to the RMC functions

The RMC enables several industry-leading RAS and security capabilities including the following:

Built-in fault analysis
Most fault systems today rely on data collection and subsequent human analysis. In contrast, the RMC of HPE Superdome Flex 280 has an **embedded analysis engine** that constantly and automatically analyzes system information to detect and find the root cause of system faults. Based on detected errors and events, the analysis engine can predict failures and initiate automatic recovery actions. HPE OneView Remote Support or HPE Insight Remote Support has a direct connection to HPE to provide a rapid response time for diagnosis and repair.

Fault-resilient boot
Should a hardware component, such as a processor core or memory DIMM, fail, fault-resilient boot reactions in HPE Superdome Flex 280 can de-configure the component and reboot to a faultless system. The system can then return to service until a repair is made. This reduces system downtime and removes the risk of running with a faulty component. Data from the analysis engine drives continuous improvements to fault-resilient boot reactions.

Reduced attack surface
HPE Superdome Flex 280 features a custom management firmware design and requires firmware updates to be initiated by an authenticated RMC administrator. This closes off many of the entry points hackers and malware use when attempting to hijack firmware updates. This reduced attack surface means lower risk of attacks.

No additional licenses required
Because all these features are embedded at the system level, you do not need to purchase or manage separate management products or licenses.

MITIGATING THREAT EXPOSURES

HPE Superdome Flex 280 provides dedicated security features built around a strategy of reducing threat exposure to vulnerabilities, including those found in common server firmware.

Reducing firmware vulnerabilities
Today, millions of servers run signed firmware based on standard reference code and feature common components with vulnerabilities, such as legacy BIOS support and Intel® Manageability Engine, which leave organizations open to attack. HPE Superdome Flex 280 is built on a different philosophy: firmware is designed to help minimize risk by excluding vulnerable firmware components whenever possible. As part of the embedded firmware management subsystem, firmware updates are installed together as a complete set of tested and authenticated firmware components to prevent any tampering.

Silicon root of trust
If the firmware is compromised, the silicon root of trust from HPE detects the issue and prevents firmware execution by performing a series of authentication checks beginning in immutable firmware inside a dedicated security microcontroller. Silicon root of trust from HPE has received the Cyber Catalyst by Marsh designation.[1]

Tamper-resistant TPM 2.0
The Trusted Platform Module 2.0 (TPM 2.0) in HPE Superdome Flex 280 goes beyond those found in other standard solutions, being soldered to each server in a tamper-resistant package with built-in firmware resiliency. The TPM is manageable through the RMC interface, with no requirement to reboot to a BIOS menu.

Resilient firmware backups
Should any component fail its CNSA-level[2] cryptographic signature check, HPE Superdome Flex 280 automatically switches to a resilient firmware backup stored on the systems.

End-to-end controlled manufacturing
HPE Superdome Flex 280 manufacturing extends from our secure design and development processes to operations, handling, logistics, and secure lifecycle services. HPE's stringent supply chain security program prevents, detects, monitors, analyzes, and reports counterfeit and malicious taint incidents.

SUMMARY

HPE Superdome Flex 280 enables unique RAS and security features at the system and manufacturing levels to provide a highly dependable environment for critical workloads. Faults and security threats are detected and handled automatically before they can disrupt business. And where human management is required, HPE Superdome Flex 280 provides one flexible control point for the whole system, without purchasing or managing separate software, thanks to its embedded management system.

LEARN MORE AT

hpe.com/superdome

[1] Cyber Catalyst by Marsh: An industry-recognized mark of security innovation and efficacy

[2] Commercial National Security Algorithm (CNSA)

Make the right purchase decision. Contact our presales specialists.

Chat now (sales)

Call now

Get updates

Step up your digital transformation with as-a-service building blocks

Power critical applications, accelerate analytics, and tackle HPC and AI workloads holistically. Extract value from your data and grow cost-efficiently with modular, building-block architecture—HPE Superdome Flex servers. Prepare to win.

a50006278ENW

Hewlett Packard Enterprise