

WE MAKE IT SAFE & EASY

Remote Multi-Vendor Platform Support Overview

Our system proactively detects equipment hardware faults across storage, server, and networking products that are maintained by us. The related alerts are then securely transmitted to our technical operations, enabling more timely and accurate failure diagnosis, part identification, and necessary repair actions.

This document is intended to proactively share the key aspects of a typical remote support service implementation, with emphasis on connectivity and data security.

Minimum requirements for implementing our remote service

The Client is responsible for providing the resources on which the remote service agent will be installed. Following are the minimum requirements:

Virtual Machine

- ▶ 2 vCPUs
- ▶ 2 GB memory
- ▶ 2 GB free hard drive space

Install as a service

- ▶ Windows Server 2008+
- ▶ 500 MB storage space

IP-enabled connection

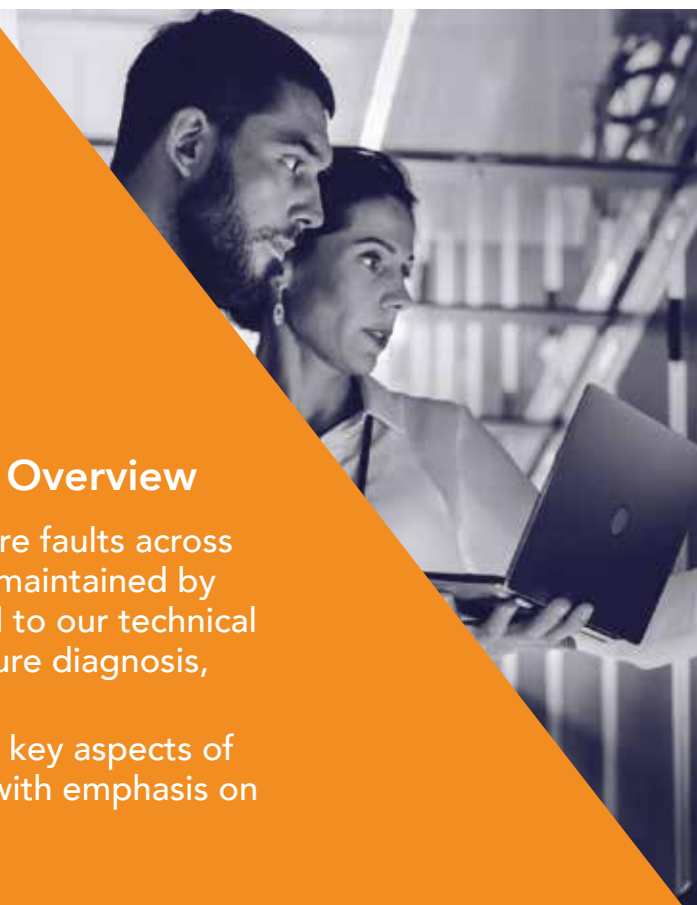
- ▶ Connection made between the client data centre agent and our service provider

Connectivity and Data Security

The Remote Multi-Vendor Platform Support Service is configured as follows. Additional options are available per the client's specific security requirements. Some clients may consider agent connectivity credentials to be sensitive information. Therefore, we have developed a process to hash the passwords or credentials, ensuring that agent to asset communications uses hashed passwords or credentials.

Connectivity

Connection between the client data centre and our technical centre is established over a secure IP connection utilising HTTPS via port 443 and 3183 (default port).



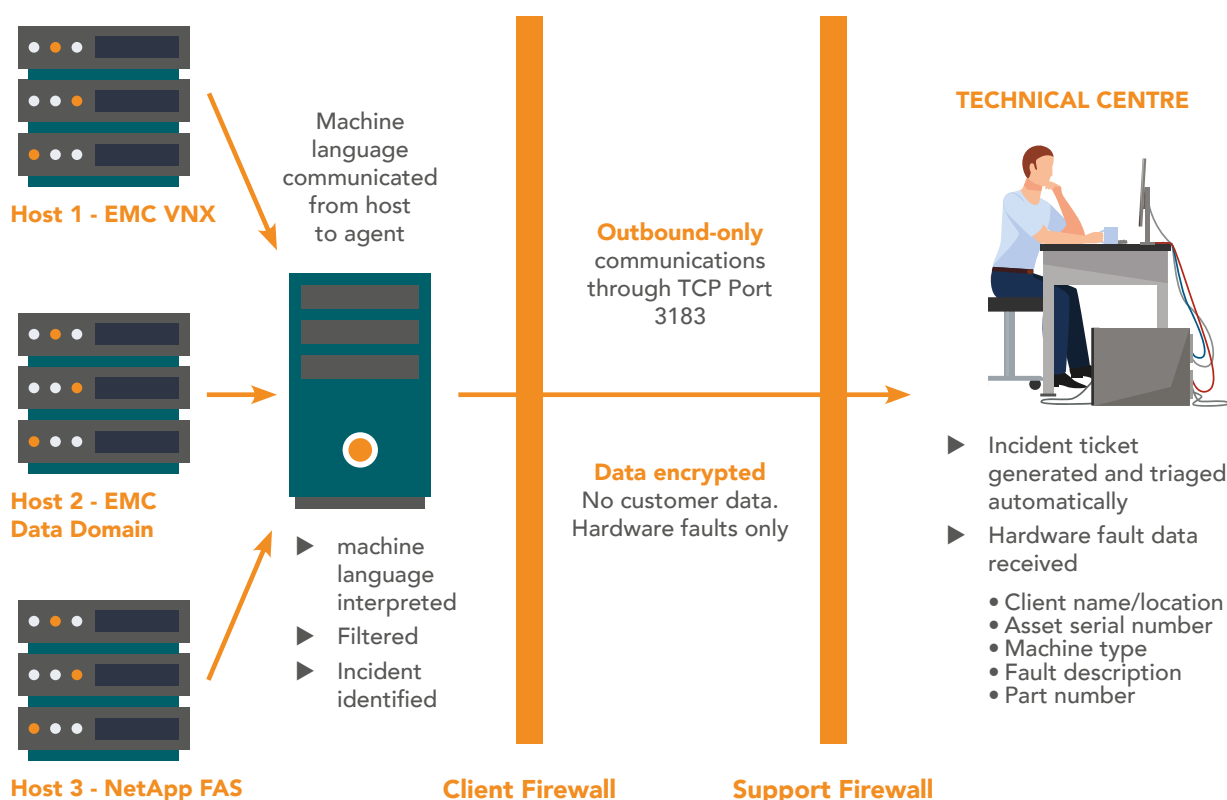
Data security

Since there is no sensitive data contained within the transmission, minimal encryption is recommended. Additional levels of security are available and may result in additional fees.

- ▶ Custom security certificates
- ▶ Dedicated VPN
- ▶ Company security keys
- ▶ Secure Transactional Authentication (BMC TEA Agent)

Data flow (reference figure 1)

When a product supported by us remotely and experiences a hardware failure, the client agent initiates communications on a one-way, outbound path, sending encrypted hardware alert information to the technical centre. Alerts that require action are visible to the Park Place Technical Centre via the Presentation Server. A support ticket is generated for all actionable alerts and remains open until the failure is resolved to the client's satisfaction.



About MaintenancePro by 7TECH

We provide organisations with post-warranty hardware maintenance and support to extend the life of their storage, server, and networking equipment while ensuring maximum uptime, reduced operational expenses, and a superior service experience. To learn more how we can provide solutions for your post-warranty hardware equipment maintenance and support, contact us on +44 (0) 1359 221038 or visit www.7tech.ltd.uk.