LIFE™ SERVICES
Technical Bulletin

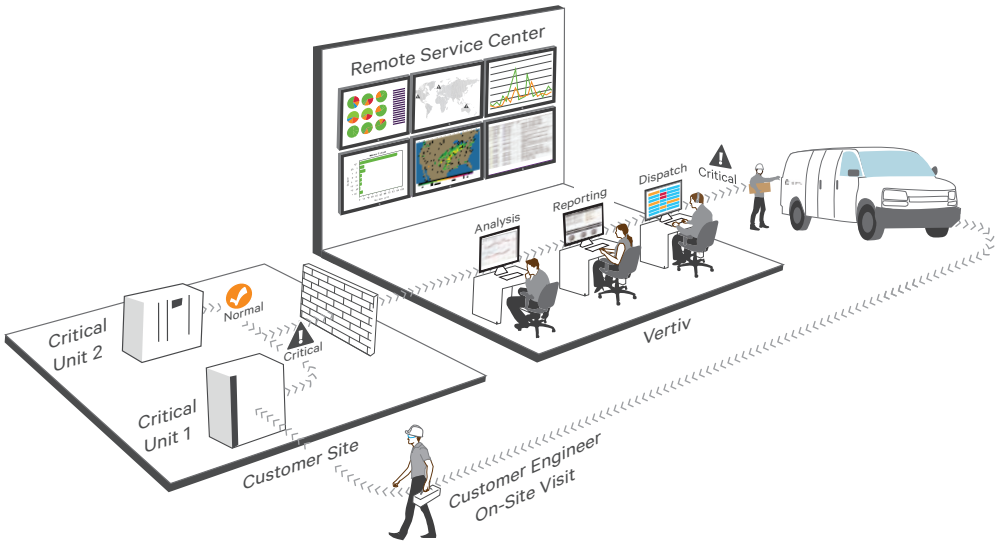
EXECUTIVE SUMMARY

LIFE™ Services, offered by Vertiv™, provides increased uptime and operational efficiency through continuous monitoring, expert analysis and proactive response.

Detailed parametric data is continuously captured with advanced technology embedded in select critical systems. At prescribed intervals, the data is transmitted safely and efficiently to an authorized remote service center staffed with remote system engineers for analysis and response.

Should an operating anomaly or alarm condition arise, the engineer performs an immediate analysis and initiates an appropriate response to have the critical system quickly, safely, and accurately restored to its proper operating condition.

This document describes the technical details of the service.



Service Overview and Benefits

BENEFIT	DELIVERED BY
Uptime assurance	• 24x7 monitoring of critical system health • Early detection of trends and operating anomalies that may lead to critical failures if not addressed • Interpretation of the critical system alarm and status messages to understand potential impact
Rapid incident response	• Critical system alarm messages and relevant data automatically transmitted for analysis, trending and diagnosis • Remote diagnosis of the equipment while customer engineer is being dispatched to the site • Shipment of parts necessary to perform corrective maintenance
Increased insight and ease of management	• Notification of operating conditions that may impact the health of the critical system • Explanation of critical system health with trend and analysis reports delivered periodically based on contract scope of work • Integration of services from remote detection of critical and anomaly conditions through on-site response to restore the critical system

Architecture

Customer Site

Critical System – The system that is designed and operated to protect a critical load.

Communication Card – The communication card is the interface between the critical system and an internet accessible network. All communication is initiated by the equipment, beginning with a request to communicate with the authorized server. Upon successful validation of the request, data is transmitted and then the connection is closed.

The following types of data transmission intervals are used:

- Emergency – Occurs in case of a condition which requires service
- Routine – Occurs on a scheduled interval (usually every 24 hours)
- Manual – Occurs when activated from the device

Vertiv™

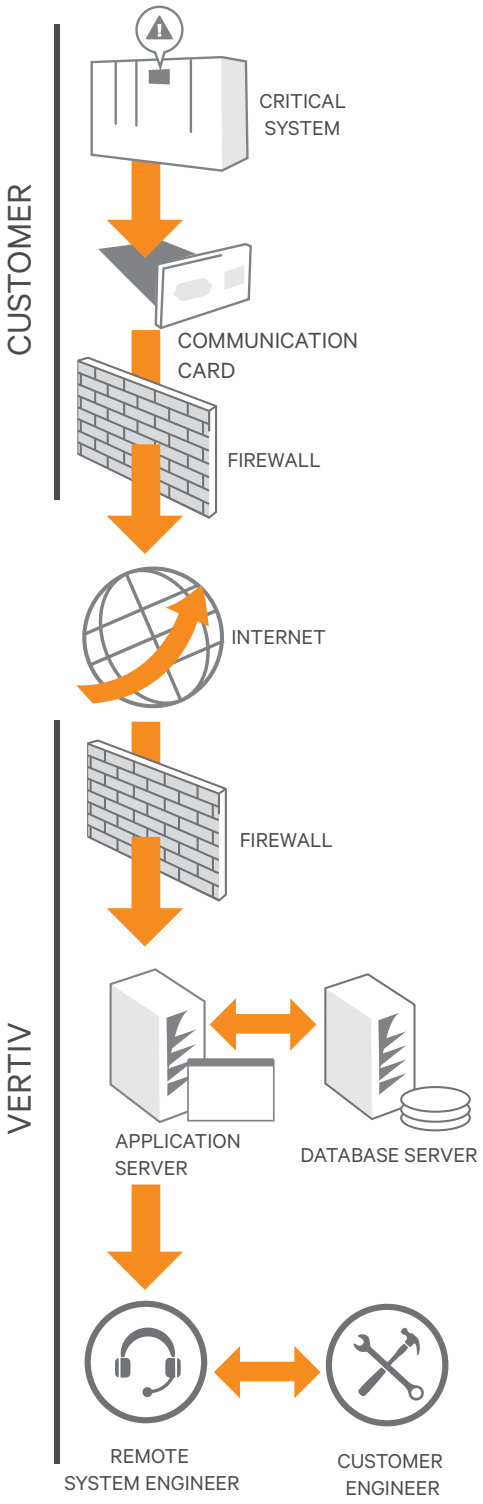
Application Server – The application server is a vital component of the service offering. It performs three primary functions:

1. Processes data transmitted by critical systems
2. Applies diagnostic algorithms to detect the severity of critical system messages
3. Provides a means for remote system engineers to analyze and report on the health of critical systems

Database Server – The database server stores the event and operating data from the critical systems for use by the application server. The server also stores customer contract and contact information pertaining to the connected critical systems.

Remote System Engineers – The remote system engineers perform monitoring, analysis, and response activities to optimize the health of the critical systems. These engineers receive specialized training to quickly and accurately identify operating anomalies and alarm conditions. In addition to using the application server to analyze systems, they also have access to detailed engineering documentation, on-site service records, and the technical knowledge system.

Customer Engineers – The customer engineers perform any required analysis and response activities at the customer site. Each is highly trained to ensure the critical systems are quickly, safely, and accurately restored to an optimum state of readiness.



Enabling Technology

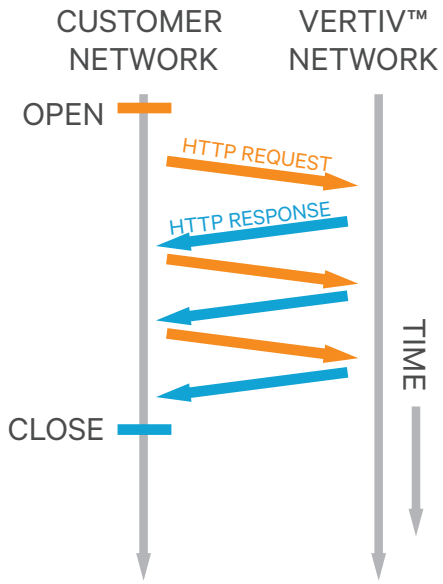
Data Collection

Detailed parametric data is continuously captured within the critical system. The data set includes select operating parameters, as well as events and alarms.

Communication

At prescribed intervals, the critical system data is transmitted safely and efficiently to the remote service center for further analysis. The transmission is performed by using a standard internet protocol, Hypertext Transfer Protocol (HTTP), to encapsulate the data. Use of HTTP eliminates transmission problems typically associated with firewalls and packet filtering. The technology has the following IT friendly features:

- Critical system initiates transmission
- Network proxy compatibility
- Network firewall compatibility
- DHCP assigned IP address compatibility
- No public IP address required
- No static IP address required
- No Virtual Private Network (VPN) required



Data Security

The technology used to enable LIFE™ Services was designed and implemented with security as a priority. This priority extends to the management of computing resources and information that is used to deliver the service. The following are expanded details related to key security topics.

Type of Data Collected

Critical system messages, operating parameters, and identification data are collected and transmitted to authorized remote service centers. The alarm and status messages contain vital information regarding the state of the critical system and are used to initiate a rapid incident response.

The select operating parameters are a source for detailed diagnosis and trending analysis to ensure an appropriate response that optimizes the health of the critical system. The unit serial number is transmitted as an identifier of the critical system. No customer contact information is transmitted.

Application and Data Access Control

Access to information and computing resources used to enable LIFE™ Services are controlled and monitored. Named accounts are used to protect access to the application server and associated critical system data. The access privileges are granted based on a need-to-know basis and segregation of duties. The accounts are managed by an authorized service center system administrator, who verifies and updates them as required.

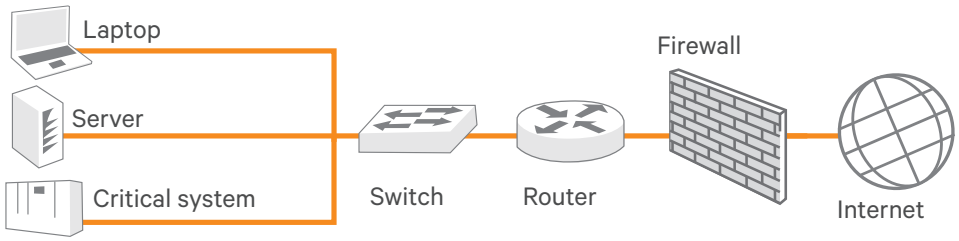
Physical and Environmental Security

Unauthorized physical access, damage and interference to the information and computing resources are restricted. An access control mechanism, including the authorization, review, and revocation process, is used to track and prevent unauthorized access to secure areas. All servers and network components are secured appropriately. Critical systems such as uninterruptible power supplies, backup generators, and air conditioners are monitored and controlled to maintain optimal levels of protection.

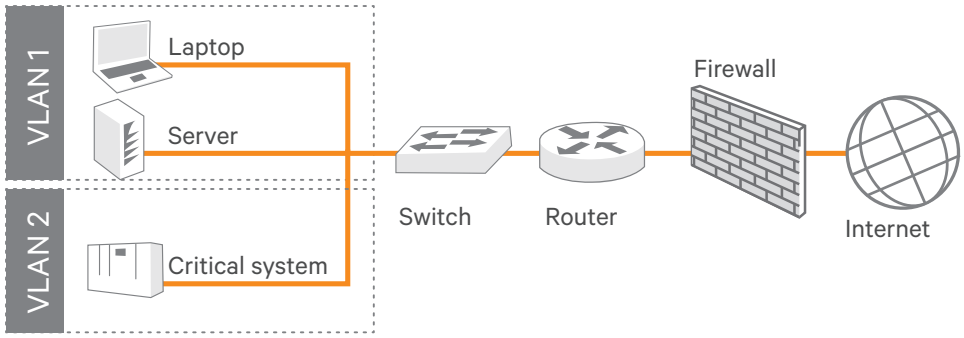
Network Configurations

LIFE™ Services can be enabled using a variety of network configurations. Three common configurations are to 1) use the existing local/wide area network (LAN/WAN), 2) create/use a separate, virtual local area network (VLAN) or 3) create/use a separate, dedicated local area network (LAN). Regardless of the configuration, the basic requirement is to ensure external connections to TCP Port 80 (HTTP) are enabled.

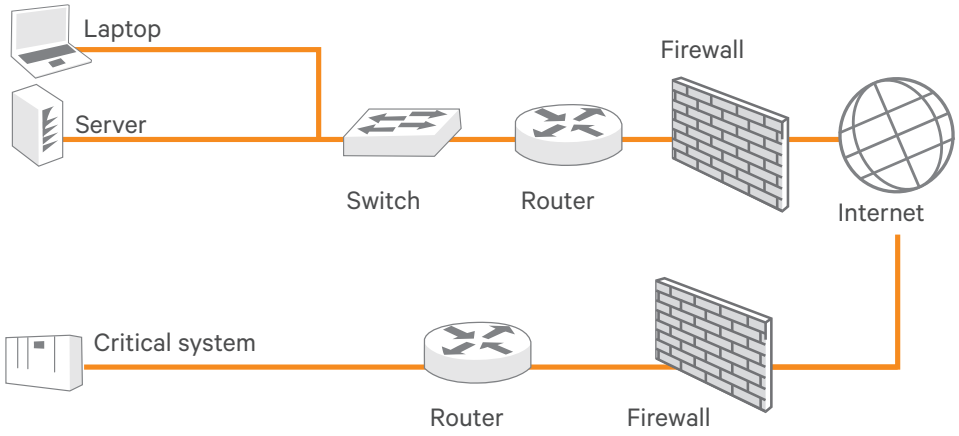
1) Existing local/wide area network (LAN/WAN)



2) Separate, virtual local area network (VLAN)

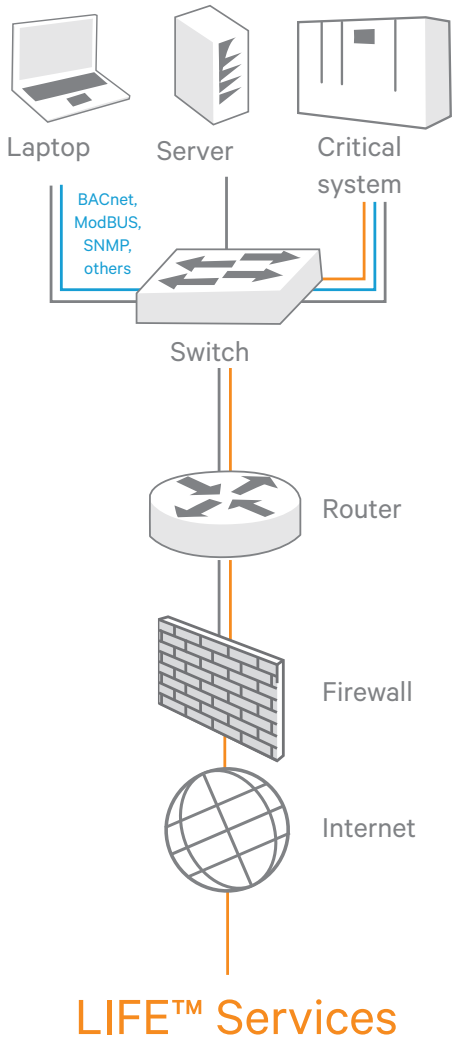


3) Separate, dedicated local area network (LAN)



Coexistence with Monitoring Systems

LIFE™ Services can be enabled for critical systems that are also monitored with a Building Management System (BMS), Data Center Infrastructure Management (DCIM) system, Network Management System (NMS), or other system. This allows complete flexibility in managing a site or multiple sites while also ensuring availability and operational efficiency of the critical systems. Below is an example with the data paths highlighted.



VertivCo.com | **Vertiv Services,** 1-800-543-2378