VERTIV.™

SmartCabinet™

Micro data center for edge computing

VERTIV™ SMART CABINET

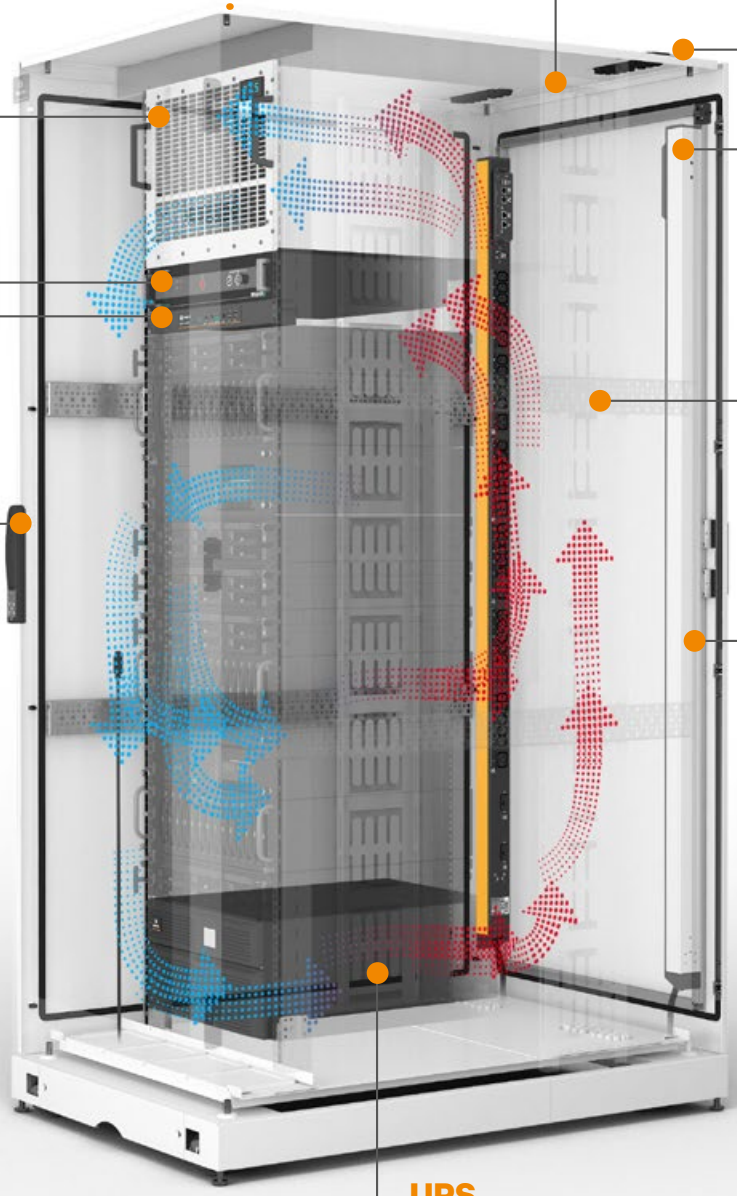
Remote monitoring
Control, alarm management, and reports.

Cooling system
Highly efficient split cooling, redundancy due to backup fan.

Optional fire suppression
Highly sensitive smoke detection and automatic, reliable fire extinguishing.

Remote monitoring/ control
You can securely and remotely manage every device, every site, from every supplier, at any time.

Access control
Convenient management and secure physical access.



Smoke detector
Highly sensitive detection and alarms.

Monitoring
(Temperature, humidity, and door contacts) with alarm function.

Cable management
For simple and safe component use.

PDU
Maximum availability, inherent security architecture, quick & easy installation, sustainable long-term solution.

UPS
Real online UPS for critical applications, 1.5 to 10 kVA.

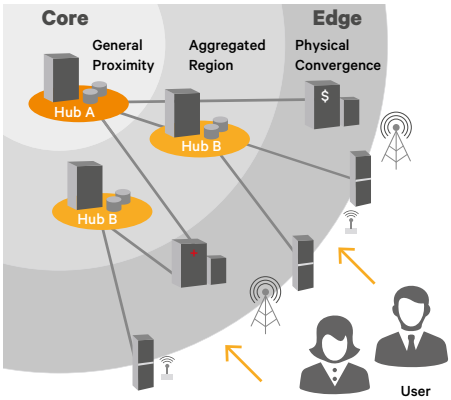
IT Mega Trends

The next-generation data center will exist beyond walls, seamlessly integrating core facilities with a more intelligent, mission-critical edge of network. These **Gen 4 data centers are emerging and will become the model for IT networks of the 2020s.** The advent of this edge-dependent data center is one of five 2018 data center trends identified by a global panel of experts from Vertiv, formerly Emerson Network Power.

Other trends presented by Vertiv which are expected to impact the data center ecosystem in 2018 are:

- Closer collaboration between cloud providers and colocation providers
- Reimagining and reconfiguration of the data center middle class
- High density will become an increasingly important topic
- Edge computing installations are facing new challenges, including concerning the security and ownership of data

The IT "Edge Computing" Trend



Edge computing in the communication network

Companies and authorities today are increasingly transferring their applications to their own large, central data centers, colocation, and the public cloud. There are many good reasons, however, to keep or expand data storage and processing close to the users (people, sensors, devices, machines, vehicles etc.). Nowadays, the digitalization of all processes and things has resulted in a rapidly growing need to process and store data right at the edge of the network, not simply transfer it into remote large-scale data centers. Edge computing is the answer to this problem.

Edge computing

Edge computing refers to the processing and storage of information near to where the data is created or used, i.e. at the edge of a network.

Essentially, there are 4 reasons to do this:

- The ability to protect sensitive data and/or critical processes at the site
- Local operations are independent of the network connection
- Avoidance of network latency – short response times, real-time processing
- Insufficient bandwidth, costs of transferring large amounts of data

There are many examples of edges – here are a few

Enterprise edge

Companies take a multi-pronged approach nowadays when it comes to IT. Even if a lot of things have moved to “the cloud”, the critical data and processes in particular remain in-house. It’s exactly for this reason that the capacity, availability, efficiency, and security of the infrastructure must be just right so that the requirements that come with increasing digitalization of all processes can be met. This forces large companies with several branches, as well as smaller businesses and institutions, to ask themselves how they will prepare their data centers and server rooms for the demands the future will place on them.

Cloud edge

To make large amounts of data available, the cloud has to be closer to the users. Applications like HD or UHD video require huge amounts of bandwidth, especially if several users want to stream content at the same time. As well as this, applications like virtual reality require extremely short latency periods. That’s why the large providers are moving ever closer to their users with their data centers.

Edge of things

In the IoT (Internet of Things), sensors and actuators, devices, machines, and vehicles exchange huge amounts of data in real time. Most of the data is only used for a short time and locally. The transfer to a large, central data center would take far too long, and there is no reason to constantly store it centrally. For this reason, the data is processed near to the place in question, e.g. to make cities, power networks, factories, and cars “smart”.

Can I prepare my small IT rooms for the digital future...

- Efficient, fast, and secure
- Little planning effort required
- Low total costs
- Reliable operation – without expert members of staff on site

... with an expert partner?

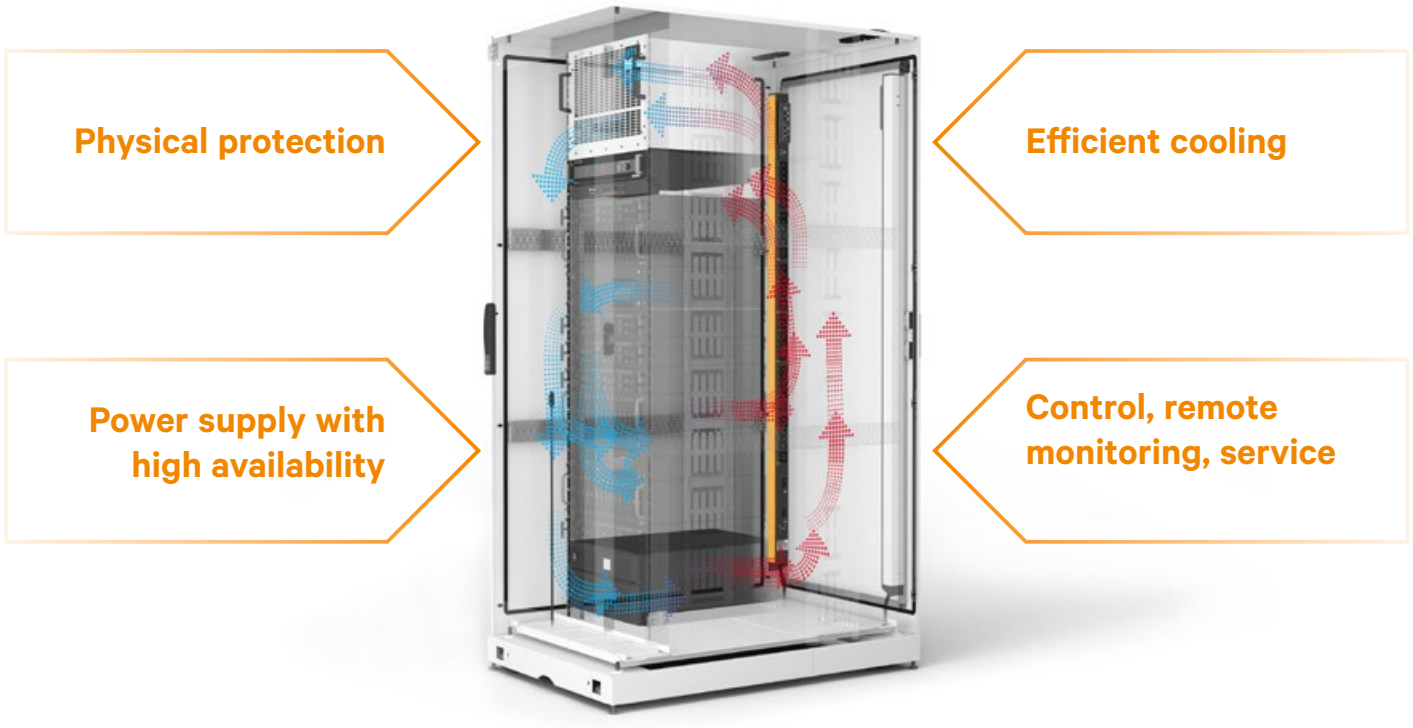
Micro data centers for edge computing

SmartCabinet™ – the intelligent, integrated infrastructure solution in one housing

Edge computing does not require a special type of data center; there is no typical edge data center. In many cases, a very small data center is sufficient – one or just a few racks with a connected load of just a few kVA. A micro data center, in which all infrastructure systems required for IT operations are integrated.

SmartCabinet™ is the recent iteration of such a micro data center – the complete infrastructure of a data center together in one cabinet. It includes an uninterruptible power supply, power distribution, cooling, monitoring, and infrastructure management – consistently integrated, optimized, and developed from tried-and-tested components. The IT components can be started up after it has been set up, the cooling system has been installed, and the building power supply has been connected.

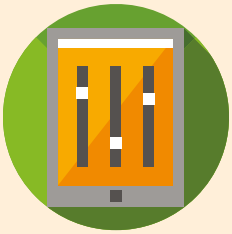
SmartCabinet saves you planning and building effort and simplifies the operation of complex network and server rooms made up of individual components. This saves a considerable amount of the time it takes to start up compared with conventional methods of construction. SmartCabinet is preconfigured, largely preinstalled in the factory, and tested. This ensures that the entire system, along with its coordinated components, is ready for operation from the get go.



Features and advantages

Fully integrated

- No special IT room is needed
- Complete data center infrastructure housed in one cabinet with high-quality protection against environmental hazards
- Cooling, uninterruptible power supply, monitoring, and security for all IT applications



Sophisticated system

- Reliable compliance with all requirements concerning capacity, availability, security, and efficiency thanks to the comprehensive, fully developed, and tried-and-tested system
- Constructed from coordinated components

A complete solution from one source

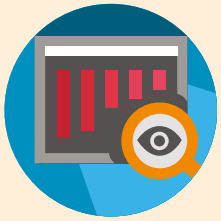
- Highest quality
- Installed and tested in a factory with a certified QA system
- Highly efficient, secure, and reliable

Quick and easy set-up and start-up

- Quick and easy set-up on site
- Eliminates the time and effort required to build and equip an entire server or network room
- Can be quickly and easily transported to other sites if needed

Save on costs

- Total costs are greatly reduced compared with the conventional method of construction
- Lower investments, quicker start-up, and better efficiency



Unmanned operation

- Central monitoring, management, and IT administration over various sites across the network as well as out-of-band GSM connection

Service from one source

- Start-up, maintenance, and repair for all components
- Remote monitoring as a service

Technologies & components:
Physical protection

Physical protection

Data-center-tested network/server cabinet offers secure installation of 19" equipment, flexible use of accessories for power and data cabling, integrated cooling air routing, and high-quality protection against internal and external hazards.

The castor base enables easy transportation of the empty cabinet to the installation site and room for cabling from below. 800 kg load bearing capacity with castor base.

Protection against the ingress of foreign objects and water

- IP 20 protection against foreign objects > 12.5 mm diameter for network cabinet and server cabinet with perforated doors
- IP 54 protection against dust and splash water from all sides, largely airtight for active cooling and gaseous fire suppression

Access protection

- Mechanical lock with profile half cylinder
- Electronic lock, operated via local keyboard

Smoke detection/fire extinguishing

- Optical smoke switch
- Preparation for early fire detection and extinguisher

For the best protection against fire, smoke, water, break-ins: SmartCabinet™ XP

The micro data center in a safe

- Fire resistance class F90 – system tested
- Protection against combustion gases
- Protection against water jets and dust IP56
- WK2 break-in protection

Technologies & components:
Power supply/distribution with high availability

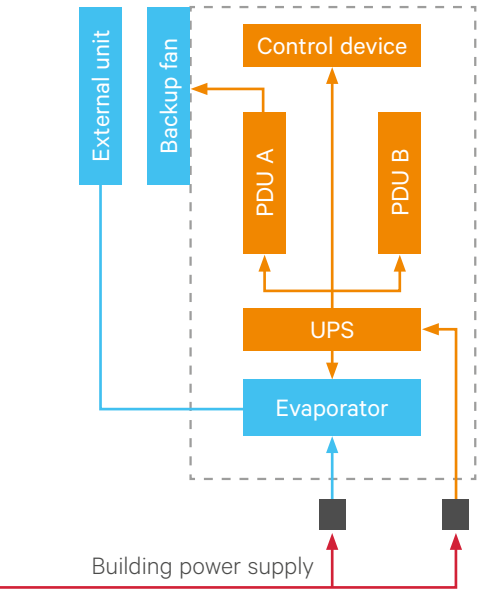
Power supply with high availability

Double conversion UPS for applications with high availability

- Ensures constant voltage and frequency
- Protects in the case of a short-term power failure and enables the IT devices to shut down safely during longer failures
- A second, optional (redundant) UPS unit for a secure power supply, even when the main UPS is being serviced

Intelligent rack PDU

- High-quality rack PDUs ensure the distribution of power to the IT components. To meet higher availability requirements, two rack PDUs are installed to provide largely independent power supply pathways for IT equipment with redundant power supplies.
- Integrated residual current monitor/alarm.
- Depending on the equipment, comprehensive measurement, alarm, and switching options are available.



Cooling power supply

- The external unit is controlled and supplied with power via the evaporator.
- In the case of a power failure, the control and fan are supported in the evaporator by the UPS, but not the compressor in the external unit.
- If the cooling unit fails, the UPS-supported backup fan takes over the cooling.
- We recommend connecting the UPS and cooling units to different sub-distributors in the building as far as possible (separate fusing, separate residual-current circuit breakers if necessary).

Supply limitations

A SmartCabinet cannot ensure a power supply beyond the capabilities of the building. Often, buildings do not have an emergency power system and have only one connection to the power grid. This means that a power failure directly affects the power connection to the SmartCabinet. Only the temporary bridging via the built-in UPS remains.

Technologies & components:
Efficient cooling

Passive cooling – IP20 cabinet

Free cooling using ambient air through the base/raised cover (network cabinet) or large perforated doors (server cabinet), heat is released into the room.

Suitable for operation in clean, well ventilated or air conditioned side rooms. Only suitable for office spaces to a limited extent as there is no sound insulation for the IT components.

Active cooling/compact cooling unit – IP54 cabinet

Cooling for the interior of the cabinet with the door closed with heat released into the surrounding room.

Suitable for well ventilated rooms with exposure to dust, dirt, splash water, and increased temperatures. Typical areas of usage are large rooms or corridors in the warehouse or in production.

Active cooling/split cooling unit – IP54 cabinet

Cooling for the interior of the cabinet with the door closed with heat released outside of the building.

Suitable for use in all types of rooms, also in office spaces due to the sound insulation for the IT devices.

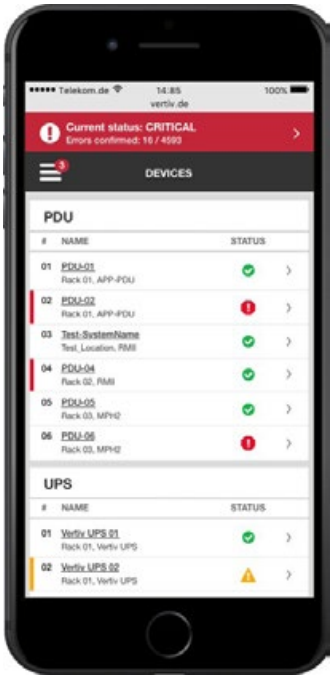
Availability of cooling

The cooling is designed to keep the intake temperature of the IT components constantly under 27°C, and only allow it to rise to a maximum of 32°C for a limited time (ASHRAE Standard TC9.9).

A failure of the active cooling is far less critical than one of the power supply; the thermal inertia of the system prevents a rapid increase in temperature. In this case, the UPS-supported backup fan in the rear door automatically turns on and draws the cooling air in from the room through a filter at the bottom towards the front of the cabinet.

Technologies & components:
Control, remote monitoring, service

Control, remote monitoring, service



Central control device

- Remote access to all installed components via an IP address via the network using a browser and SNMP protocol
- Can also be accessed via mobile network as an option
- Secure network interface with configurable access rights, secured internal network
- Central monitoring/control of all components and sensors via user-configurable dashboard
- Configurable alarm management, reporting of alarms via SNMP, SMS, or e-mail
- Programmable process logic for automated operation and handling of faults up to a secure IT shut-down, even if the network connection is lost
- Configurable local log file for operating data and alarms
- Possibility to connect optional IP camera

Sensors

The built-in sensors enable seamless remote monitoring of

- Temperature
- Humidity
- Door status (open/closed)

Software

We recommend Trellis™ Critical Insight

- Simultaneous monitoring of up to several thousand sites
- Management of all components installed in the SmartCabinet
- Alarms via network, SMS, or e-mail
- Easy to configure to specific requirements

Remote monitoring/administration of IT devices

- Optional console server, KVM switches, and LCD consoles

Services

The SmartCabinet comes with comprehensive services to ensure streamlined implementation and operation:

- Installation and start-up
- Warranty, maintenance, and repair
- Remote monitoring/maintenance services

My company has found a reliable, expert partner for the future, and its name is SmartCabinet!

VertivCo.com | **Vertiv Infrastructure Limited**, George Curl Way, Southampton, SO18 2RY, VAT Number: GB188146827