



**VERTIV WHITE PAPER**

**Tools of the Trade: Enabling  
Centralized Management of  
Distributed or Remote IT Sites**

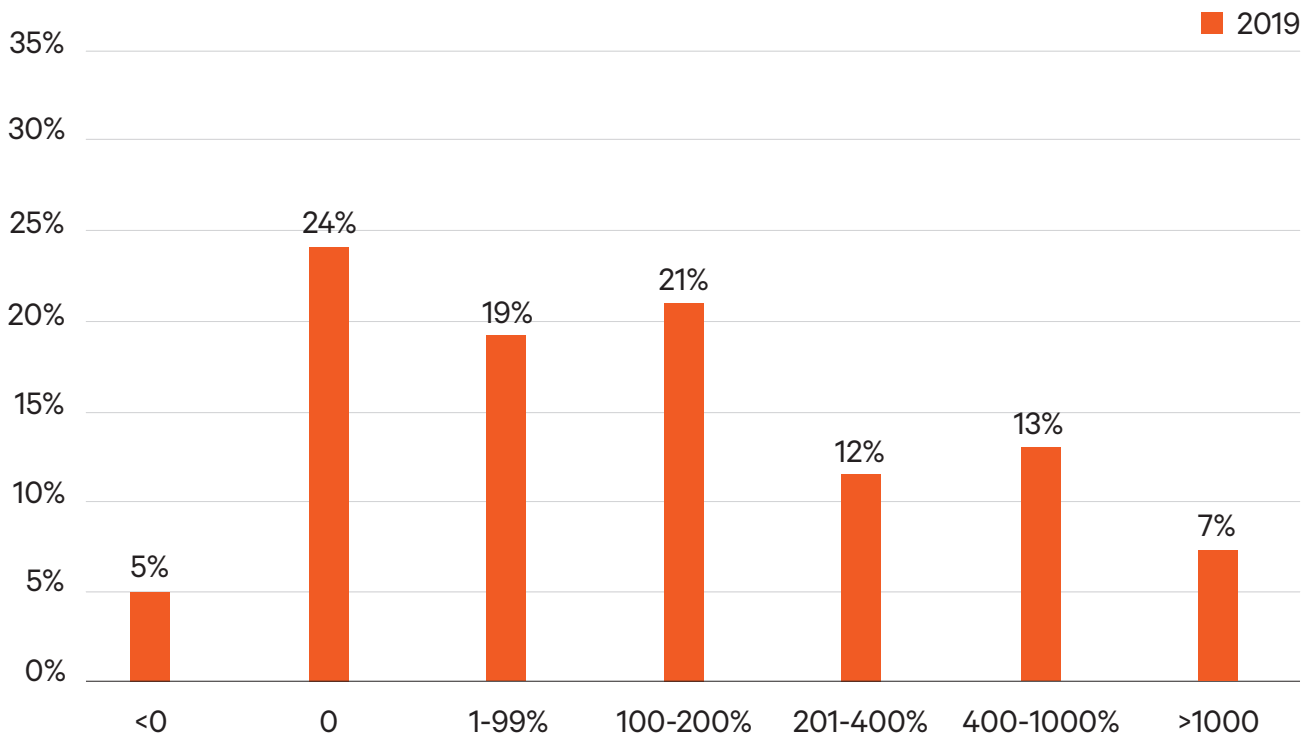
## Growing Need for Access and Control

IT networks are continuing to evolve in ways that present new challenges for managers and administrators.

One of the biggest trends facing the industry today is the growth in edge networks. Analyst firm IDC has predicted that worldwide data volume will grow 61 percent by 2025, and that growth is creating latency and bandwidth challenges for organizations that have centralized IT assets in a core data center.

To address these issues, networks are becoming more decentralized, leading to the expansion in the number and capacity of edge sites. Many organizations already support a variety of branch and remote offices in their network. These distributed or remote sites are expected to grow in the coming years as new edge-enabled applications, such as smart cities, digital healthcare, and virtual and augmented reality gain traction.

In a recent survey of more than 800 global data center specialists for the Vertiv 2019 [Data Center 2025 Report](#), participants who have edge sites today or expect to have them in 2025, projected an average 226 percent increase in the number of sites they will be required to support in the next five years.



Percentage growth in edge sites for participants with edge sites today or those who plan to have edge sites in 2025.

## Doing More with Less

While resources are becoming more distributed, expertise is not. The challenge of deploying and managing a growing number of IT sites will put a strain on many IT departments. Not only will personnel be asked to manage more sites, many of these sites will be in locations with little or no technical support, creating situations where equipment downtime takes longer to resolve.

That's where IT management tools deliver especially high value. By providing in-band and out-of-band remote access and monitoring of equipment across multiple sites, IT management tools increase the productivity of IT staff while helping maintain the availability of critical systems. Having secure and remote out-of-band connections directly to the physical KVM, USB, and serial ports complements in-band tools to create a more complete remote management solution. This unified approach enables faster diagnosis and reconfiguration or restoration of equipment to meet service level agreements and minimize downtime. Specific benefits include:

- **Faster Provisioning**

Accessing multiple devices through a single switch or console enables those devices to be provisioned from one location in much less time than it would take to provision each device separately. This practice, which is common in data centers, can save even more time when applied to remote locations.

- **Simplified Management**

Software updates and other routine maintenance tasks are also greatly simplified by enabling access to multiple devices through switches or consoles. With these tools, IT administrators can gain centralized remote access to devices across multiple locations to streamline configuration, troubleshooting and monitoring.

- **Reduced Mean Time to Repair (MTTR)**

IT management tools that provide both in-band and out-of-band access have proven their ability to reduce MTTR in the data center by enabling faster issue identification, and in some cases, remote resolution. These savings are amplified when applied to distributed locations that, without remote access, would require technician travel time just to identify the issue.

- **Enhanced Security**

Today's IT management tools minimize the need to physically access IT systems and include support for smart card/common access card (CAC) readers and other physical security systems, enabling centralized management of access to critical facilities.

- **Lower Operating Costs**

Faster provisioning, improved management, and reduced MTTR all translate directly into lower operating costs while freeing resources to focus on strategic initiatives.

## Understanding the Options

There are a variety of options available to IT professionals seeking to easily and securely manage devices through remote access. These include:

- **Secure Desktop Access**

At the basic level, desktop switches provide access to multiple computers from a single KVM (keyboard, video monitor and mouse). When equipped with advanced security features, these tools allow users to switch safely and securely between computers operating at different classification levels, providing continuous access to critical data in security-sensitive environments.



Avocent® Cybex SC845H

- **Remote Access Digital KVM**

Digital KVM-over-IP switches provide access to servers from any location. When equipped with serial capabilities, these switches can provide access to communications equipment, as well as provide a single solution to remote equipment management.



Avocent® MPU2032

- **Local Access Server Control**

A local access controller provides access to multiple servers to simplify the process of making software upgrades, troubleshooting and system monitoring. They provide an ideal solution for local management of remote sites but are not designed to support remote management.



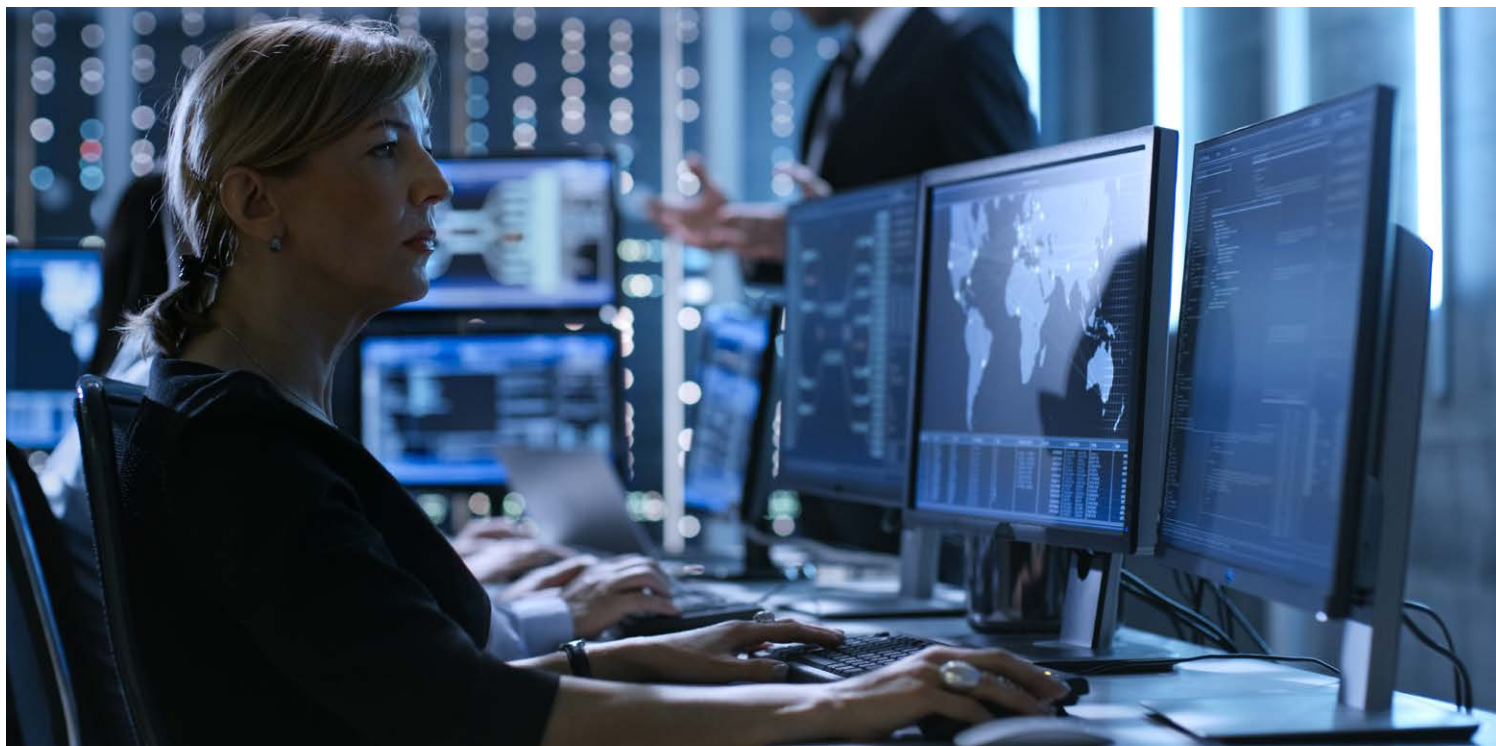
Avocent® 19" Local Rack Access Console

- **Serial Access Console**

An advanced serial console enables remote management of servers, routers and switches, in addition to supporting capabilities such as environmental monitoring and internet of things (IoT) integration. It is also an ideal foundation for centralized management of multiple remote sites. For example, a system such as the Avocent® ACS 800, which is designed for edge site management, includes sensor ports to connect temperature, humidity, differential pressure, leak, and door pin sensors in addition to remote equipment access.



Avocent® ACS 800



### Managing Data Across Systems in High Security Environments

Government agencies that rely on internal communication networks to protect against outside intrusion still face the risk of data being compromised by insiders. In these environments, a standard KVM switch represents an unacceptable security risk.

A secure KVM switch allows authorized users to switch between networks with various security levels from a single position. With a secure KVM switch, each port is isolated from the others through unidirectional optical data diodes (UODD) to prohibit data from being transferred between connected computers. Additionally, to prevent eavesdropping, the buffer is automatically cleared after any transmission of data.

### Access and Control Software

IT management tools generally feature a built-in web interface that allows them to be used without additional software. However, pairing the right software with access and control devices expands their value and enhances their capabilities.

A browser-based system such as Avocent® DSView™ can integrate access and monitoring functionality from KVM switches and serial access consoles, along with compatible intelligent power distribution units (PDUs), into a single rack view of all equipment (device state, power consumption, temperature) in real-time and as a polled device threshold event.

This enhanced solution enables control at the physical firmware level for bare metal operating system (OS) provisioning; control at the physical host OS level for application sessions; and control at the logical virtual machine instance level for virtualized OS and application sessions. It also centralizes threshold-based event notification across locations for faster response and improved management.

DSView features a hub-and-spoke architecture that enhances disaster resistance, enables fail-over management, and supports scalable deployment across complex network topologies. It also supports analog and cellular modem-based, out-of-band access to remote systems in the event of a primary network failure.

Working with a leading infrastructure provider such as Vertiv helps ensure software supports a broad range of equipment and devices and delivers information in a way that supports effective management.





### **In-Store Technology Requires New Approaches to IT Management**

Retailers are increasingly beefing up the IT infrastructure in their retail locations to support better visibility of inventory across the supply chain and enable new customer experiences through in-store applications and virtual and augmented reality. With the customer experience becoming more dependent on technology, the availability of this infrastructure becomes critical. Digital KVM-over-IP switches with serial capabilities enable centralized and standardized management of retail IT across locations to better manage configuration, updates and troubleshooting.

### **Other Key Capabilities**

Beyond software there are other features that can enhance the value of an IT management solution. Some of the features that are of particular value to our customers include:

- **Smart Card Compatibility:** Remote smart card/CAC reader support enables smart card readers across distributed sites to be mapped from a desktop computer out to a remote server to enhance security management.
- **Virtual Media Support:** Virtual media support enables remote USB connections to map CD-ROM and other USB mass storage devices directly to remote servers to transfer/copy files, load updates, or install new applications.
- **Task Automation:** Features such as automated discovery and zero-touch provisioning save valuable time during configuration.



### Managing the Growing Healthcare Network

With the proliferation of hospital networks, outpatient surgery centers, and urgent care facilities, the healthcare IT network is growing more complex and distributed. At the same time, service delivery is increasingly technology dependent. The use of console servers and intelligent PDUs supported by browser-based IT management software provides a cost-effective solution for monitoring IT and infrastructure devices across the network.

### Finding Your Solution

There are a variety of solutions available today to enable remote management of distributed IT sites. Specific management goals combined with the number and type of devices to be accessed will help guide the decision as to the type of solution that best meets requirements. Then, evaluating the availability of specific features that deliver value, including software support and compatibility with a broad range of infrastructure and IT systems, will help guide selection of the appropriate vendor.

Vertiv Avocent boasts a long history delivering access and IT management solutions around the world to companies like Dell, Gateway, Hewlett-Packard, Intel and Microsoft. With more than 200,000 users, Avocent® KVM and serial access consoles combine with renowned enterprise-class data center and edge products from Vertiv to securely and remotely manage IT devices anywhere in the world.



**Vertiv.com** | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, USA

© 2019 Vertiv Group Corp. All rights reserved. Vertiv™ and the Vertiv logo are trademarks or registered trademarks of Vertiv Group Corp. All other names and logos referred to are trade names, trademarks or registered trademarks of their respective owners. While every precaution has been taken to ensure accuracy and completeness here, Vertiv Group Corp. assumes no responsibility, and disclaims all liability, for damages resulting from use of this information or for any errors or omissions. Specifications, rebates and other promotional offers are subject to change at Vertiv's sole discretion upon notice.