Life Is On | Schneider Electric

Attributes of Effective DCIM Systems for Distributed, Hybrid IT Environments

White Paper 281

Version 2

by Patrick Donovan

Executive summary

Enterprise data center owners are embracing hybrid IT architectures with physical infrastructure assets widely distributed on premise, at colocation providers, and increasingly at the edge of the network. This creates management challenges, particularly since these geographically-dispersed sites are often unmanned and operated in a “lights out” fashion. In addition, the criticality of small IT installations at the edge is increasing. This makes the use of data center infrastructure management (DCIM) tools critical. In this paper we describe the essential functions and attributes of a DCIM platform optimized for hybrid IT that is best able to solve today’s challenges. Such a platform is also well positioned to take advantage of newer, emerging technology trends. This paper will assist readers who are in the process of selecting a DCIM platform for hybrid IT environments with multiple edge computing sites.

RATE THIS PAPER ★★★★★

Introduction

Data Center Infrastructure Management (DCIM) software tools have been fundamentally used to maximize the efficient use of power, cooling, and space resources. Well-implemented, DCIM improves the availability and resiliency of physical infrastructure systems and the IT workloads they support. However, much has changed since DCIM suites became commonly used toolsets. Data center owners and managers face new challenges and requirements such as an acceleration of small, unstaffed IT deployments at the edge, meeting corporate sustainability goals, and defending against cybersecurity threats. At the same time, recent technology developments offer new possibilities. In this paper we describe the essential functions of a DCIM platform deployed for hybrid IT environments. Next, we explain five attributes that make a DCIM software suite more effective at providing those functions in a way that takes advantage of emerging technology trends. **Modern DCIM systems will simplify deployment and management regardless of the number of assets and sites, optimize operations and maintenance through analytics and new digital services, and will provide the data and tools necessary to support integration with existing management apps and services such as 3rd party monitoring and management services, building management systems (BMS), and electrical power monitoring systems (EPMS)**. **Figure 1** shows a high-level modern, cloud-based DCIM system architecture optimized for hybrid IT environments that will be described in this paper.

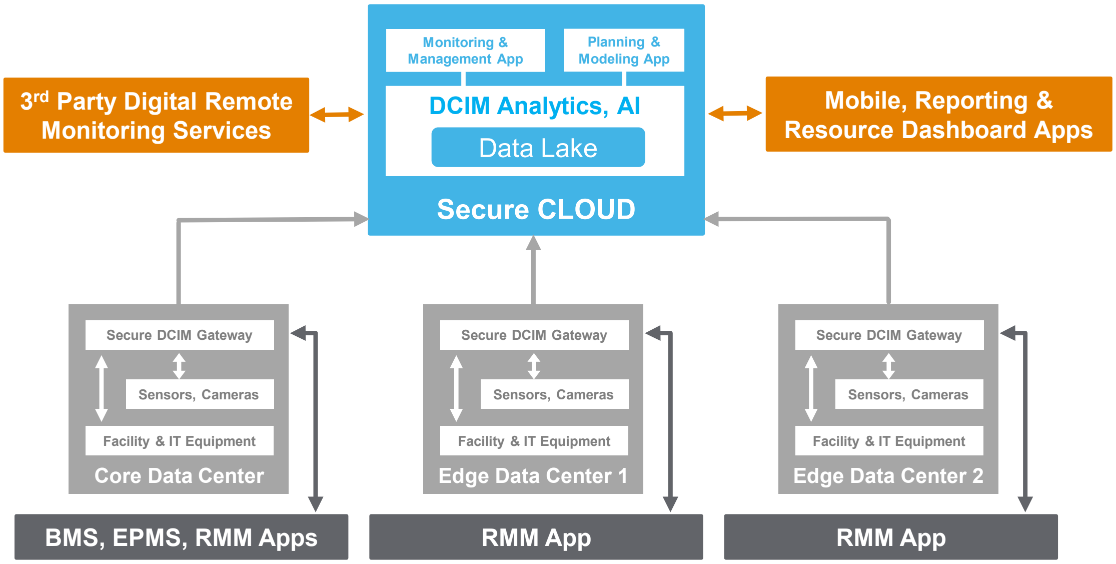

Figure 1
Example high-level architecture of a DCIM system optimized for hybrid IT environments where IT assets are distributed geographically. Note, the arrows indicate data flow.

Note, the cloud-based DCIM system functions and attributes in this paper are not theoretical or future-looking concepts. Solutions capable of providing the essential functions and that embody the five attributes are available in the market today. The next section briefly explains the technology trends and management drivers that have led some DCIM vendors to implement these types of architectures.

3 drivers of DCIM software evolution

The data center industry has gone through significant change and evolution since infrastructure management tools first became common years ago. Originally designed for larger single sites, DCIM and its user requirements have evolved as the industry and technologies have changed. Driven by IT and networking advancements, enterprise data center portfolios are changing. This, in turn, has led to new management challenges (discussed below). Management priorities are also shifting. At the same time, newer technologies have emerged that DCIM software can now take advantage of to better address these new challenges and priorities. Each of these three drivers of DCIM software evolution are explained below.

Enterprise data center portfolios are changing

In the early days of DCIM software tools, for a given organization, data centers tended to be centralized and few in number. This began to change when cloud computing and data center colocation providers emerged. Enterprises increasingly have both owned and leased IT physical and virtual assets spread across more locations. This is referred to as "hybrid IT" or "hybrid computing environments". This growing sophistication complicates operations and maintenance by making it more difficult to maintain visibility and control over all assets.

This management difficulty is also intensifying due to the growth of critical IT deployments at the edge of networks. Trends like digitalization, the growth of IoT devices, the need to reduce network latency, and the desire to reduce network bandwidth costs, are all working together to drive more IT compute and storage capacity deployments at the ends of the network, closer to users. White Paper 226, *The Drivers and Benefits of Edge Computing*, delves further into this. These edge computing deployments are being done by cloud and colocation providers, as well as by enterprises themselves. One study determined that while only 10% of enterprise data was created outside of core centralized data centers in 2018, estimates for 2025 suggest up to 75% will be generated and handled by edge computing sites[1]. **This means the typical enterprise now exists in a very complex hybrid IT environment with assets highly distributed across an increasing number of sites, many of which are small, unstaffed, and operated in a "lights out" fashion.**

This complex environment creates unique management challenges. **Table 1** lists some of the more common difficulties that arise.

Table 1
Common management challenges that result from complex hybrid IT environments that include multiple local edge sites

Challenge	Description & impact
Managing multiple, geographically dispersed sites	Inability to see all assets in aggregate, maintain equipment and software cost-effectively, and remain situationally-aware of what is happening particularly with adds, moves, changes, and security patch/firmware updates.
Lacking on-site staff	Lack of visibility and ability to respond to problems; Being unaware of who might be accessing equipment. Increased likelihood of unplanned downtime, cost to maintain, and time to resolve issues.
Procuring multiple servers and IP addresses	With traditional on-premise DCIM, each site would require going through the procurement process for a virtual or physical server and IP address for installation of the DCIM software.
Receiving large numbers of alarms and status change notifications	The need for "eyes and ears" at all locations means potentially thousands of environmental and device sensors are reporting status and alarm notifications. The alarm "storms" can overwhelm users and result in missed critical notifications and wasted effort.
Maintaining a large fleet of dispersed equipment and software	The distributed, "lights out" nature of the smaller sites makes cost-effective maintenance a challenge as it is not practical to have trained staff at every site with replacement parts.

[1] Rob van der Meulen, *What Edge Computing Means for Infrastructure and Operations Leaders*, 2018

These challenges can present themselves in many ways. Here are some examples we have heard…

- Trying to troubleshoot a problem with a store clerk or security guard
- Making sense of a storm of “UPS on battery” – “UPS online” alarms
- Getting a call that “something” is beeping or flashing its lights
- Having to deal with multiple vendors when problems arise
- Figuring out how to deploy security patch updates to dozens or hundreds of sites
- Servers unexpectedly rebooting at a site while service personnel perform maintenance, but no way to know for sure if they caused it
- Trying to forecast power capacity needs during budget cycle time

Management priorities and concerns are changing

This changing environment and the emergence of the challenges described above has led to a shift in management priorities that places new requirements on DCIM software tools today. As an enterprise’s portfolio of sites and IT assets expand, new priorities and needs emerge, including:

- Need for simple remote management capabilities showing all assets and sites in aggregate.
- Growing focus on energy efficiency and sustainability (resource management) driven by need to control expenses, to address customer and investor expectations, and to meet government regulations.
- Increasing concern over cybersecurity-related issues; e.g. how do you ensure apps and devices are secure?
- Need for service provider/3rd party integration with DCIM monitoring system to enable more cost-effective maintenance options.
- Increasing desire for simplicity and ease of use in deploying, operating, and maintaining DCIM software as sites and assets increase in number and distribution.
- Need for DCIM integration with existing management platforms and reporting tools to ensure DCIM functions fit with existing operations processes.

Technology evolution leads to new management capabilities

While data center architectures were changing and management priorities evolving, technologies have also been developing that make data center infrastructure management simpler and more capable than it had been before. The emergence and maturation of these technologies is fundamentally what is making DCIM solutions today more optimized for complex hybrid IT environments. **Table 2** lists three technologies and their impact on DCIM systems.

Technology	DCIM impact
Cloud computing	Can move from CAPEX to OPEX (upfront license expense to on-going subscription) model; increased scalability, provides basis for big data analytics and AI, enables visibility across all sites via mobile technologies, as well as simpler software maintenance.
Internet of things (IoT)	This trend has made the cost to add sensors and network connectivity to devices and systems relatively low. This makes it more practical to fully instrument "lights out" facilities to ensure good monitoring coverage and the ability to accurately plan and model sites digitally from afar.
Analytics and artificial intelligence (AI)	The tools and necessary volume of data exist to begin to build and train models that optimize mechanical system operations, for example, or predict wear out of components in infrastructure equipment.

Table 2
Technology evolution are enabling DCIM systems to do more

By selecting DCIM solutions that take advantage of these maturing technologies, you will be better positioned to handle the management challenges of complex hybrid IT environments. The last section of this paper will explain in more detail the key attributes of DCIM to look for. These attributes build off these key technologies. But first, we describe the essential functions of DCIM software deployed in hybrid IT environments with distributed sites and assets.

Essential DCIM functions for distributed IT sites

While DCIM suites offer a wide variety of functions and capabilities, a smaller subset of essential functions is needed for hybrid IT environments where there are smaller IT installations distributed geographically at the edge of the network (i.e., local edge). **When you are in the process of selecting a DCIM solution for a hybrid, distributed environment, focus on these functions first and compare each vendor's approach and performance in delivering them.** Most, if not all, vendors will offer these functions in some form. But they will differ in terms of the platform architecture used to deliver the functions. As the next section will show, **the platform's architecture drives the effectiveness of DCIM tools in hybrid IT environments.**

Fundamentally, most DCIM suites offer 2 core functions:

- Monitoring & management
- Planning & modeling – simulating adds, moves, changes

Functions essential to solving the hybrid IT management challenges discussed earlier are explained in the following two sub-sections.

Monitoring & management

Operation of IT equipment – either in a core data center or a remote edge IT site - depends on stable electrical power, sufficient ventilation (or active cooling), as well as a secure location that is safe from unauthorized access or exposure to other physical and environmental threats. These dependencies mean that a highly resilient IT installation requires monitoring and management of the infrastructure equipment with DCIM software tools. Afterall, you cannot effectively manage something that cannot be seen. **DCIM software provides that remote visibility in conjunction with device and environmental sensors and cameras**. These are summarized in **Table 3** below. White Paper 280, *Practical Guide to Ensuring Availability at Edge Computing Sites*, goes beyond the DCIM system and describes specific actions to take to improve availability of the power and cooling systems that support small, remote IT installations.

Table 3
Functions to focus on when selecting a DCIM monitoring and management tool

Function	Description	Why function is important
Device & environmental monitoring	Provides a "read only" connection to all critical infrastructure devices (e.g. UPS, rack PDU, cooling, etc.) – regardless of vendor – to monitor status, access & alarms in real time.	Awareness of status changes, trends, and alarms prevents issues from becoming critical incidents that could lead to IT service interruptions. Monitoring for unauthorized access to equipment reduce physical security risks.
Device management	Provides a means by which infrastructure devices can be configured and their firmware updated.	Configuration & updates ensures equipment performs as expected and helps secure the overall system from cyber security threats.
Asset tracking	Provides a holistic view of all assets, including their location, name, status, etc.	IT resiliency requires having an asset inventory and understanding their attributes.
Data analytics & visualization	Presents useful and actionable information on device status, alarms, and the health of the infrastructure systems and their environment through simple dashboards and reports.	Raw device data, frequent status change notifications, and "alarm storms" can overwhelm users; analytics and clear visualization of data makes DCIM use simpler and more effective.
3rd party platform integration	Allows DCIM data to be shared with a remote monitoring and management (RMM) tool or building management system (BMS) using application programming interfaces (APIs) or an SNMP management information base (MIB).	Managed service providers (MSPs) commonly manage edge computing IT and use their own management platforms; sharing DCIM data with these tools solves "lack of staff" challenge by enabling trusted partners to manage it for you.

Planning & modeling

Managing and operating a portfolio of mission critical sites is very different from managing commercial office buildings, for example. For most data centers and critical IT installations, failure is not an option. Some liken it to "maintaining an airplane while flying it". Today, businesses are often either wholly dependent on their data centers or their data centers ARE the business. Complexity is much higher, and the pace of change is much greater than in most other types of facilities. Increasingly software defined (i.e. virtual machines, virtual storage, and virtual networks) with moving workloads combined with short IT refresh cycles, these hybrid IT environments make for a challenging operations environment. These challenges require careful coordination and planning with the facilities and IT teams when it comes to adds, moves, and changes. The potential impact on system availability can be so severe that each operational task must be carefully evaluated in terms of its net effect on availability.

This not only makes device monitoring and management important but makes planning and modeling a critical function of DCIM as well. This function begins with creating and maintaining an accurate map of all infrastructure assets and IT equipment along with their interdependencies with each other. Note, this requires on-going, disciplined use of the DCIM tool. If the asset information in the software does not reflect reality, then planning and modeling functions will produce flawed results. White Paper 170, *Avoiding Common Pitfalls of Evaluating and Implementing DCIM Solutions*, provides tips on how to ensure the map of assets is maintained over time.

By creating, in effect, a "digital twin" (in both 2D and 3D, typically) of your portfolio of data centers and edge IT sites, this DCIM function can simulate adds, moves, and changes so that operators can understand the potential impacts before real action is taken. By first performing actions virtually, the risk of an unplanned interruption in IT service as maintenance is performed is minimized. Particularly when there's no onsite IT staff, having this digital visualization of all assets and their interdependencies is important. Note, with all assets fully documented (type, serial number, rack location, network port, power path, etc.) and mapped to each other, this information could serve as a basis for a disaster recovery (DR) plan.

Imagine needing to “swap and replace” all of your remotely-located UPSs. With DCIM planning and modeling functionality, you would understand – without being on site - which physical servers, virtual workloads, and applications were dependent on each of the UPSs. Turning the UPS off and switching to a redundant power path could be simulated to understand what the impact would be on connected workloads and applications. Affected critical workloads could be identified and safely migrated to another server or site before the UPS replacement takes place. This information and the ability to run simulations makes it easier to plan and execute the actual transition while reducing the chances of an unexpected outage.

Table 4 summarizes the key modeling and planning fucntions that are key to solving management challenges in distributed, hybrid environments.

Table 4
Functions to focus on when selecting a DCIM planning and modeling tool

Function	Description	Why function is important
Visualization of assets in each site	2D and typically 3D views of each data center and IT installation showing rack locations, installed IT equipment and front/back rack views along with supporting infrastructure such as UPSs, rack power distribution units (PDUs), cooling units, etc.	Provides location-based inventory of IT assets (physical and virtual) along with their network, power, and cooling dependencies; provides a basis for DR planning and running simulations to understand business impact of adds, moves and changes.
Adds, moves, and changes planning & simulation	Map of assets enables the software to recommend optimal placement of new servers based on user-defined policies and availability of resources; Allows for simulation of changes to understand impact before actually doing the work.	Good planning reduces risk of causing business interruptions and makes work orders proceed more efficiently. Gives the ability to simulate equipment failures to understand their impact for proactive incident management. Ability to do this planning remotely reduces the need to be on site.
Remote analytics & reporting	Typically provides standardized reports to analyze rack capacities, inventory, available rack U-spaces, server utilization, energy use, work orders, and so on.	Can share with management team a common view and understanding of portfolio of data centers and edge sites; Can be used to identify opportunities to be more efficient operationally and energy-wise. This can be done without having to be onsite everywhere to collect the information.

Modern, cloud-based DCIM systems are most capable of delivering these essential functions for a hybrid IT environment. The next section describes 5 attributes that largely define these modern platforms.

5 attributes of effective DCIM for hybrid IT

A modern DCIM platform optimized for hybrid IT environments is defined by 5 key attributes. These attributes are what differentiate them from standard, on-premise DCIM systems that were designed for a single or small number of larger data centers. Adopting a platform based on these attributes will put you on the path of benefiting from newer, evolving technologies such as machine learning and predictive analytics. Note, cloud computing technologies (attribute #1) enables the other attributes and is fundamentally what makes these suites most effective at achieving the functions described above, and thereby, solving today's hybrid IT management challenges.

1. Uses **cloud technologies** for ease of implementation, scalability, analytics, and maintenance
2. Connects to a **data lake** enabling insight and event prediction with **artificial intelligence (AI)**
3. Uses **mobile and web technologies** and integrates with 3rd party platforms
4. Prioritizes **simplicity** and **intuitive** user experiences in its design
5. Serves as a security **compliance tool** to identify and eliminate potential cybersecurity risks

Uses cloud technologies for ease of implementation, scalability, analytics, and maintenance

By hosting the DCIM server in the cloud, **deployment is simpler and faster** by eliminating the need to go through the procurement process for a new server for every site. Next-generation DCIM typically installs as a simple gateway app on an existing server (physical or virtual). This avoids the often-lengthy security and validation reviews that can take weeks or months. Since each site would have required a DCIM server, this time savings can be significant when there are dozens or hundreds of small remote sites. This also makes the tool **highly scalable** in that it can handle an unlimited number of monitored devices across any number of sites. Cloud technologies also facilitate further value as described in the attributes below.

Connects to a data lake that enables insights and event prediction with AI

The cloud-based architecture of next-generation DCIM also provides the opportunity for vendors to offer a "data lake", or a secure repository of massive amounts of anonymized device data. **"Big data" analytics and machine learning algorithms** can be developed and trained on this data to **yield insights and make predictions** that improve reliability, improve efficiency, and/or reduce operating expenses. Early examples of "big data" analytics and artificial intelligence applied to data center physical infrastructure include:

- Predicting when UPS batteries will fail – allows for early planning and budgeting for service replacements
- Real-time optimization of cooling system controls based on changing climate and load conditions – reduces operating expenses
- UPS health scorecard sorting the inventory of UPSs based on a determination of the device's age and health – simplifies management by first focusing user on what needs attention most

While this functionality is still in its infancy (at the time of this writing), data center and hybrid IT **owners and operators considering DCIM solutions today can put themselves on the right future path by adopting a modern cloud-based DCIM architecture that includes a data lake.**

Uses mobile and web technologies and integrates with 3rd party platforms

With this attribute, end users, trusted service partners, and vendors can **all access the same data at the same time from any browser** or mobile device. **Open APIs** enable DCIM data to be shared with any trusted vendor or partner. Being browser based and encrypted, the need for VPN and unique login credentials for every single site is eliminated. This gives **real-time visibility to all assets and sites from one login**. These attributes serve to mitigate the challenge of having many, unmanned sites. For example, mobile access could help remote IT staff guide untrained, on-site personnel to troubleshoot and resolve issues without dispatching service. And integration into your **MSPs** RMM tool means that they **can now manage and service your physical infrastructure equipment for you**, just as they might be doing for your IT applications.

Prioritizes simplicity and intuitive user experiences in its design

Modern, cloud-based DCIM tools tend to perform better in terms of ease of installing, configuring, and using the software. Some of the common improvements include things like:

- Installations that use easy-to-follow wizard-based routines
- Device alarm thresholds that come with useful default settings
- Device health scorecards that sort devices in need of attention or action first
- Performance benchmarking that provides context on how you are performing relative to peers
- Alarms and status changes, grouped based on common causes to eliminate alarm “storms”
- Device setting and policy changes that can be mass applied to many devices at once
- DCIM app gateway and device firmware that can be set to auto-update to roll out bug fixes, feature enhancements, and security patches as soon as they are available; no longer a vendor-provided server that must be maintained by the end user

Serves as a compliance tool to identify and eliminate potential cyber security risks

Given that DCIM systems are made up of software apps, servers, gateways, and critical infrastructure devices, all inter-connected over mobile and IT networks, it is important to ensure cyber security best practices are continuously followed by both the vendor and end user. Next-generation DCIM should simplify this for the end user by **automating the detection and reporting of DCIM gateway and device vulnerabilities**. Some DCIM solutions do this using a threat assessment tool. Users are notified if device configurations (e.g., set to use SSH or Telnet) put the device at risk of attack. Devices with outdated firmware are also identified. This greatly simplifies management and automates a critical function of the DCIM system.

Digital services for leveraging partners and vendors

As stated in White Paper 277, *Solving Edge Computing Infrastructure Challenges*, it is the challenge of having many sites and too few staff, combined with increasing criticality, that makes operating hybrid IT deployments in a traditional way difficult. An improved model is emerging that addresses these problems. This paradigm is based, in part, on embracing cloud-based DCIM tools and cooperative partnerships with managed service providers and equipment vendors. DCIM suites based on the attributes above, better enable you to leverage the assistance and expertise of trusted partners and vendors to monitor and service your data center infrastructure. DCIM service apps that provide this outside assistance are what we call, “digital services”.

Cloud-based DCIM tools not only provide a means for the data center owner and operator to monitor their equipment for themselves, it can also be designed to facilitate having a trusted service provider or the equipment vendor monitor it as well. And this is done without having to provide these 3rd parties with access to your local networks since secure access to data is through the DCIM cloud. Your partner, equipment vendor, and your operations team can all have access to the same data at the same time.

That being said, of course, for the DCIM suites that embody the five attributes described earlier, it is easier for owners to securely manage their own sites and assets. But for those who lack the bandwidth, expertise, or staffing, digital services such as digital remote monitoring and field service dispatch can be an effective alternative.

Linking field service dispatch with DCIM monitoring-as-a-service is an offer some vendors are providing. The aim is to further reduce downtime and improve maintenance response times by enabling MSPs and equipment vendors to immediately send out parts and service personnel upon discovering a problem while monitoring your equipment. This type of “monitoring and service dispatch” digital service reduces the burden on your operations and maintenance staff.

White Paper 283, *A Quantitative Comparison of UPS Monitoring and Servicing Approaches Across Edge Environments*, describes key considerations when deciding between monitoring and managing a fleet of uninterruptable power supplies (UPSs) yourself vs. outsourcing that responsibility to a third-party vendor or partner using DCIM digital services. Although specific to UPSs, the considerations discussed could well be applied to other infrastructure device types as well. Additionally, the TradeOff Tool, *Edge UPS Fleet Management Comparison Calculator*, allows you to compare the cost of managing a fleet of single-phase UPSs yourself versus paying a 3rd party to do it for you.

Conclusion

For those who own and operate a portfolio of data centers and/or edge sites (distributed, often unstaffed, small IT sites at the edges of the network), the use of data center infrastructure management (DCIM) software tools is imperative. Without DCIM, you are essentially flying blind unable to see and keep track of an increasingly complex and sprawling universe of IT, networking, and infrastructure assets. Without DCIM, the risk of downtime increases and operational efficiency is lower. Furthermore, the distributed, often “lights out”, nature of data centers today creates unique management challenges. When evaluating DCIM architectures to meet the needs of a hybrid environment, these five attributes address the unique needs of this environment:

1. Relies on **cloud technologies** for ease of implementation, scalability, analytics, and maintenance
2. Connects to a **data lake** enabling insight and event prediction with **artificial intelligence (AI)**
3. Uses **mobile and web technologies** and integrates with 3rd party platforms
4. Prioritizes **simplicity** and **intuitive** user experiences in its design
5. Serves as a security **compliance tool** to identify and eliminate potential cyber security

About the author

Patrick Donovan is a Senior Research Analyst for the Energy Management Research Center at Schneider Electric. He has over 20 years of experience developing and supporting critical power and cooling systems for Schneider Electric’s IT Business unit including several award-winning power protection, efficiency, and availability solutions. An author of numerous white papers, industry articles, and technology assessments, Patrick's research on data center physical infrastructure technologies and markets offers guidance and advice on best practices for planning, designing, and operation of data center facilities.

RATE THIS PAPER ★★★★★

Resources

The Drivers and Benefits of Edge Computing
White Paper 226

Practical Guide to Ensuring Availability at Edge Computing Sites
White Paper 280

Avoiding Common Pitfalls of Evaluating and Implementing DCIM Solutions
White Paper 170

Solving Edge Computing Infrastructure Challenges
White Paper 277

A Quantitative Comparison of UPS Monitoring and Servicing Approaches Across Edge Environments
White Paper 283

Browse all white papers
whitepapers.apc.com

Edge UPS Fleet Management Comparison Calculator
TradeOff Tool 27

Browse all TradeOff Tools™
tools.apc.com

Note: Internet links can become obsolete over time. The referenced links were available at the time this paper was written but may no longer be available now.

Contact us

For feedback and comments about the content of this white paper:

Data Center Science Center
dcsc@schneider-electric.com

If you are a customer and have questions specific to your data center project:

Contact your Schneider Electric representative at
www.apc.com/support/contact/index.cfm