White Paper

The Self-Aware Datacenter: How Condition-Based Maintenance Turns Fragmented Multivendor Datacenters into Predictable Infrastructure and System Intelligence

Sponsored by: Schneider Electric

Luis Fernandes Mary Johnston Turner

June 2026

IN THIS WHITE PAPER

Demand for datacenter capacity is shifting to gigawatt scale. Hyperscaler CAPEX is on track to exceed $600 billion by the end of 2026. Rack densities in AI zones have jumped from 15kW to 300–600kW.

Operators are absorbing this growth through mergers and acquisitions (M&A) and brownfield expansion, inheriting multivendor assets with no operational history — all while the skilled-technician supply gap has reached unsustainable ratios.

In this environment, calendar-based maintenance is no longer fit for purpose. Fixed intervals miss emerging failures and trigger unnecessary interventions, and root-cause analysis across vendors remains largely unsolved, with 70% of datacenter failures still tracing back to human error during maintenance windows. At the gigawatt scale, manual execution of traditional maintenance is physically impossible.

Condition-based maintenance delivered as a managed service that combines vendor-agnostic remote monitoring, 24 x 7 expert-in-the-loop health checks, and predictive fault analysis is emerging as the de facto operating model for AI-era infrastructure.

Early adopters report fewer manual interventions, OPEX reduction, less unplanned downtime, extended asset lifetimes, and overall better efficiency. This paper outlines the condition-based maintenance capability stack, the tangible outcomes operators are achieving today, and what to look for when evaluating a condition-based maintenance partner.

June 2026, IDC #META54611526

CLOUD SERVICE PROVIDERS MARKET OVERVIEW

Unprecedented growth in datacenter footprint

Demand for datacenter capacity is shifting to gigawatt scale. Hyperscaler campuses of 300–500MW are now quite common, and individual customers are requesting capacities over 1GW.

Total global datacenter capacity is forecast to grow to in excess of 100GW from 2026 to 2030. As VP of Global Operations Sudhir Kalra, Compass Datacenters, notes, "Nobody wants to talk about capacity in less than gigawatt terms. That just sounds unreal. That unreality has come in a few short years. The driver for that demand is really the AI expansion. The hyperscalers are in a race, an AI race with each other."

Governments around the world are in that same race to gain AI superiority. This creates an environment where demand is rapidly outpacing supply.

Some of the largest cloud and technology companies in the world are scrambling to acquire land, resources, and preexisting connections to the electricity grid — so much so that hyperscaler CAPEX for datacenters is forecast to exceed $600 billion by the end of 2026.

The construction of AI factories has only added to the complexity of an already vast problem. Aside from other requirements, AI factories are architecturally distinct from traditional datacenters, creating new operational challenges.

Rack power densities have shifted from 15kW per rack in standard datacenters to 300–600kW in AI-heavy compute zones. These facilities are built, cooled, and powered differently and have no historical maintenance baseline, since many designs have never been operated before.

Power availability has become a hot topic because it is the top constraint during the selection and construction phases. Grid interconnection timelines from initial request to activation in established markets (e.g., Northern Virginia) now extend to 7–10 years, driving operators to distributed campuses, onsite generation, and brownfield strategies through the M&A of existing local service providers. A big part of capacity coming online is in the existing installed base, not new builds.

This M&A strategy is accelerating heterogeneity in the asset base. When operators acquire existing facilities rather than build from scratch, they introduce unknown equipment configurations from multiple vendors with no operational history, requiring immediate integration with asset performance management systems.

Challenges in talent recruitment

The structural gap is widening between demand for skilled datacenter technicians and the supply the market can provide.

In the United States, the gap is stark: For every new skilled worker entering the workforce, seven new datacenter vacancies open. Multiple surveys show datacenter executives citing skilled labor shortage as a top operational concern.

These roles are highly specific, such as datacenter technicians, controls engineers, electrical engineers, mechanical/cooling engineers, and commissioning engineers, which require specialized certification and experience with high-voltage systems.

The geographic decentralization of new builds compounds this problem. The most power-available and land-available sites are often in secondary and tertiary markets or, at the very least, remote locations, where qualified workers are scarce.

Remote monitoring and AI-assisted diagnostics become essential operational tools when onsite expertise cannot be guaranteed.

One way to work around this is through standardization. This enables workforce resilience. Compass Datacenters, for example, deploys identical equipment across all its global campuses.

This allows staff to move between sites and vendor partners to hold deep technical expertise in their own equipment, rather than requiring expert engineers at every site. The vendor's approach is designed so that onsite staff need to recognize anomalies and escalate, not diagnose and fix. As Sudhir Kalra observed, "My onsite team has to know relatively little about the equipment. What they do have to know is that the equipment is misbehaving, and they have to know who to call. They have to know what number to dial."

Suppliers are also doing their share by codifying expert knowledge in AI to scale scarce expertise. By leveraging field technicians' years of experience, vendors are turning their AI systems into subject matter experts by embedding institutional knowledge, including asset-specific alarm histories, troubleshooting guides, and safety procedures, into AI-powered tools accessible to technicians on mobile devices in the field.

The increased complexity of asset performance management

Very few companies can afford the luxury of a homogeneous environment when it comes to their datacenter facilities. Fragmented multivendor environments are the norm, not the exception.

All large datacenter and industrial operators manage non-IT assets: power, cooling, and backup generation from multiple OEMs across multiple generations of equipment.

The practice of using three to six primary vendors for critical infrastructure categories is common, with further variation introduced by the acceleration of mergers and acquisitions.

In describing the vendor analysis process, a datacenter operations manager in Europe, working for a global online retail company that standardizes suppliers across all

geographies, said, "For any of our areas, we have at least three different suppliers. In some situations, three can increase to five. This is the range that we use to be more competitive in price, a plan B, in case some of our suppliers cannot deliver."

Calendar-based (time-based) maintenance remains the prevailing approach, although it is becoming increasingly inadequate. Fixed maintenance intervals developed for generic operating conditions do not account for actual asset stress, utilization, or environmental factors.

This results, paradoxically, in both unnecessary interventions (increased cost) and missed emerging failures (increased risk). Production-loss events are tolerated as a normal part of doing business, not as exceptions to be minimized or outright eliminated.

Root cause analysis across multivendor environments remains the biggest unsolved challenge. The lack of integration between different vendors, equipment, and generations leads to poor diagnostics.

Even sophisticated operators with high computerized maintenance management system (CMMS) adoption struggle to correlate upstream failures with downstream alarms when data resides on separate vendor platforms or across generations.

Cross-vendor condition-based maintenance (CBM) integration has not yet been achieved in the market. As one senior manager, who is based in the United States but a part of a worldwide operations team and directly responsible for North America and Europe in an aerospace company, commented, "Do we do integration across vendors? We do it, but do we do it for every single thing? No, not really. That's one of our goals for this year and the next year: figure out how we can better capture these and keep track. At the moment, it's not very trackable."

Asset performance management software fragmentation multiplies the management burden. Operators are already running multiple dashboards for their CMMS tools, datacenter infrastructure management (DCIM) platforms, and supervisory control and data acquisition (SCADA) systems simultaneously and separately; layering in further disjoint tools only deepens the complexity, as most do not speak to each other natively.

Integration projects require high levels of standardization across products, are resource and cost intensive, and entail system changes that risk operational discontinuity. Different systems speak different languages, compounding each of these challenges.

The scale of assets under management is expanding faster than human capacity can manage those assets. At gigawatt-scale campuses, traditional calendar-based maintenance is physically impossible to execute without automation.

CONDITION-BASED MAINTENANCE CAPABILITIES

Remote monitoring

Some vendors in the datacenter space have started to introduce condition-based maintenance. Ideally, it would be delivered as a comprehensively managed service, not simply a software product.

This enables a risk-sharing model in which the OEM owns both the monitoring infrastructure and the expert interpretation layer. This way, accountability for asset health is clearly assigned and response SLAs can be guaranteed.

This is the main difference between condition-based maintenance and standalone monitoring or DCIM platforms. This remote monitoring must be strictly outbound to ensure network integrity, with data flows not allowed to enter the customer networks.

The methodology of collecting and sending out the information can vary. Some systems handle their own telemetry and push outbound data via an API. In other cases, the customer hardware allows a software agent to send out that information remotely. In other instances, the use of specialized equipment can be retrofitted onto legacy assets to enable them to have modern functionalities.

The monitoring platform needs to be vendor agnostic by design. We have already seen that most datacenters have assets from multiple vendors. The monitoring needs to ingest data from SCADA, DCIM, building management systems, third-party sensors, and customer data lakes, constructing a system-level view across mixed-OEM environments.

"One vendor is monitoring the condition of its cooling units on its own platform; the other is monitoring on its own platform," Sudhir Kalra commented. "Vendor number 1 does not supply any type of health data on its cooling units to vendor number 2 or vice versa. That is something we need to evaluate when looking for a more advanced solution to get a holistic view [of our cooling infrastructure]."

Existing data sources are leveraged before introducing new sensors, beginning by mapping existing data, such as polling rates, data types, and coverage gaps, and then providing low-cost solutions, like wireless sensors (e.g., thermal, temperature, and humidity sensors or gas detectors), where necessary to address gaps. This minimizes integration costs and time to value.

Data ownership and customer rights need to be contractually protected. All monitored data must be owned by the customer and governed by formal data rights agreements embedded in CBM service contracts.

To achieve this, customers should work with vendors that support cybersecurity natively in their solutions or with qualified cybersecurity consulting partners that can help them validate their architectures to suit their security needs.

Continuous health check

Given its criticality and its around-the-clock asset monitoring, this service should be staffed 24 x 7 by remote domain experts who continuously monitor the health of connected electrical assets, with AI-powered anomaly triage and escalation for human expert review — all before alarms or field dispatch.

Performing a continuous health check means the system's overall health is updated in real time from sensors that measure stress, wear, thermal behavior, and aging.

Every connected asset continuously compares expected versus actual behavior. Deviations from learned baselines, adjusted for seasonality, load cycles, and environmental conditions, trigger automatic updates to health and risk indexes, thereby accelerating root cause analysis at the asset and system levels.

An OEM vendor with a large installed base and several years of experience collecting and analyzing cross-industry data is an advantage, as it enables the training and model development that underpin prediction accuracy.

This rich history enables capturing seasonal patterns, aging trajectories, and rare failure types across asset populations that would not be statistically significant in any single operator's data set. This is then fed to a single dashboard, which can be accessed 24 x 7 via web or mobile and provides a broad view of the current state, along with any alarms that need attention.

These alarm notifications are pushed whenever an asset's health status changes, allowing operations teams to prioritize responses without reviewing raw sensor data. The alarms themselves differ not only by the type of anomaly detected but also by the criticality of the assets that present them.

A human expert review must then be layered on top of AI outputs before any recommendation reaches the customer. Institutional knowledge and experience remain essential to this process. As expressed by a senior manager and head of North America and Europe operations at an aerospace provider, "We use a lot of lessons learned from the past and from how we keep up with our equipment to capture these and build them into our maintenance plan, where we can predict or be proactive about some of these inspections and capture any issues beforehand."

The tools extend expert capability access to asset-specific alarm history, maintenance procedures, safety documentation, and real-time sensor readings. And this is valid for both the teams working remotely and the technician who is eventually sent to the field in case of need.

The field technicians have access to all this information, all of it contextualized to the specific serial number of the asset they are physically working on. This translates institutional knowledge into actionable guidance at the point of intervention. This optimizes scheduling by shifting from calendar-based to risk-driven intervention triggers.

Predictive fault analysis

Condition-based maintenance is fundamentally distinct from alarm-based monitoring. Alarms are reactive, happening after the fact (a threshold crossed, a gate breached), which essentially means something has already gone wrong.

Condition-based maintenance tracks trends against operating boundaries and intervenes before limits are reached, using predictive models to identify trajectories toward failure months in advance.

A fault-detection layer underpins this trend tracking. It can be enabled by three sensor types, depending on the type of asset we are referring to:

- **Wireless temperature and humidity sensors** provide continuous environmental monitoring of assets, such as medium-voltage/low-voltage switchgear enclosures or uninterruptible power supplies (UPSs), by detecting moisture and pollution-driven deterioration.
- **Wireless thermal sensors** continuously monitor critical connection points in several assets, such as cables, circuit breakers, and busbar connections, with a particular focus on cooling solutions, detecting thermal anomalies before connection damage occurs.
- **Gas and particle sensors** detect overheating indicators in assets such as switchboards before smoke or visual browning occurs, catching deterioration from vibration, corrosion, pressure, and thermal cycling.

System-level analysis enables cascade failure prevention. By ingesting data from across the datacenter powertrain, condition-based maintenance can distinguish downstream alarms caused by upstream faults, preventing unnecessary equipment replacement or misdiagnosed failures.

"Maintenance management has been an evolution for quite a while." Sudhir Kalra said. "We went from purely calendar based to usage based, and now we're moving to condition based, where the engine is outfitted with real-time sensors that can assess the condition on a real-time basis and give you a warning before things break down."

A single cross-system correlation can avoid the most expensive and disruptive types of outages.

These models should necessarily be extensible to other vendors' equipment. Vendors with a long history across multiple industries are better able to generate health assessments for other vendors' assets of the same class, making their platforms viable for the mixed-OEM environments that characterize most operators.

Customers that have implemented condition-based maintenance recognize it as much more than just monitoring. Those that adopted it early describe the solution as predicting remaining useful life and proactively avoiding failures. The trajectory is toward AI

systems that not only assess current condition but also forecast future asset behavior under anticipated operating conditions.

PREDICTIVE ANALYTICS APPLIED TO SYSTEM INTELLIGENCE

By applying condition-based maintenance, the environment is set up to retrieve powerful insights from assets and transform them into system-level decisions that can be validated for scope and breadth of impact and documented for governance and accountability.

These can be expanded from insights into single assets to system-level intelligence that examines how assets behave within a system or ecosystem, rather than in isolation.

System-level intelligence examines a multivendor environment with real operational constraints and defines solutions to potential issues, while keeping humans fully accountable and in control.

System-level intelligence sees not at the single-asset level but across a broader system context, enabling it to correlate seemingly separate issues and answer questions beyond those related to any single asset. It can evaluate the medium- and long-term impact of an issue, determine the most efficient solution to it, or identify actions to prevent its spread or minimize exposure.

By using digital twin technology, system-level intelligence can simulate the existing infrastructure and its behavior under real operating conditions. This system intelligence is vital, especially in multivendor and brownfield environments, where one tool per device and a shortage of expert resources make consistent, sustainable management almost impossible.

Humans must remain in the loop. Although system-level intelligence assists in automation and orchestration, expert validation is still required for experience, governance, and accountability.

For organizations managing large portfolios expanding through brownfield modernization and high-density deployments, predictive analytics yields system-level intelligence, which, in turn, enables predictable infrastructure operations.

TANGIBLE OUTCOMES OF CONDITION-BASED MAINTENANCE

Reduced planned downtime

By basing maintenance on actual asset health rather than rigid intervals, planned maintenance activities and associated planned downtime can be reduced by deferring interventions when assets are healthy and accelerating them when an emergency issue is detected, as in the case of Compass Datacenters.

"Because of the condition-based maintenance that we're doing, we've been able to reduce manual interventions on the equipment by 40%," Sudhir Kalra noted, "and we think we've been able to minimize our OPEX by some 20% [compared with what it would have been] had we not been doing condition-based maintenance."

This, in turn, extends asset life cycles, nearly doubling their expected lifespan in some cases.

In addition, unplanned downtime can be decreased by up to 75%. By detecting fault trajectories weeks before asset failure, condition-based maintenance converts what would have been emergency shutdowns into planned, controlled interventions, leading to shorter outage windows by pre-positioning spare parts and expert teams.

Outage planning cycles can be significantly shortened. For large operators, that is crucial, given that planning a single maintenance outage today can require months of coordination.

Preemptive health confirmation either clears assets that do not require intervention or optimizes scheduling by combining multiple interventions in a single visit, directly compressing the planning burden.

In an aerospace and manufacturing context, as the same senior manager explained, "If we are able to effectively incorporate predictive maintenance, and be ahead of any issues that may arise, it will, in the long run, make us more efficient and allow us to reduce the turnaround time and any downtime on the product lines."

Reduced total cost of ownership

The value proposition of condition-based maintenance is reduced maintenance costs, driven by fewer interventions, optimized spare parts consumption, and minimized risk and costs associated with emergency services.

Asset life-cycle extension is also achievable. By maintaining assets at their optimal operating point rather than on fixed schedules, condition-based maintenance reduces cumulative wear.

In turn, this extends the usable life of capital-intensive equipment, delaying capital expenditure, postponing retirement of existing assets, and reducing environmental impact by avoiding premature replacement.

As Sudhir Kalra commented, "A UPS, for example, will typically last 15 years or so, but we think, because we're doing optimized maintenance on our UPS systems, we can extend the life to 20 years, maybe even 25 years. That means delaying our refresh investments by a decade."

Spare parts alone, especially in decentralized regions, can account for up to half of total maintenance costs. Condition-based maintenance eliminates premature parts

replacement and replaces reactive, premium-priced emergency field dispatches with planned, lower-cost interventions.

Cost analysis of condition-based maintenance supports its case:

- Improved condition monitoring reduces maintenance costs.
- Preventive versus reactive maintenance delivers savings versus corrective/break-fix approaches.
- Maintenance and unplanned downtime together account for 25–30% of total life-cycle cost in equipment-intensive industries.

Energy efficiency, along with sustainability and reduced carbon emissions, becomes an ancillary total-cost-of-ownership benefit. Equipment maintained near optimal operating specifications performs more efficiently. Unmaintained electrical assets operate under increased stress, degrading efficiency and increasing energy consumption, costs that accumulate silently over multiyear periods.

Asset history documentation has valuation and financing benefits. A complete, auditable history of condition-based maintenance data increases facility valuation in M&A transactions, enables more accurate insurance pricing, and can improve financing terms by demonstrating stable, well-managed OPEX, particularly relevant in the active merger-and-acquisition environment for datacenter infrastructure.

Risk mitigation

By intervening before failures occur, condition-based maintenance reduces unplanned outages, replacing them with controlled maintenance windows.

The financial exposure from unplanned downtime justifies investing in risk mitigation. For companies and government agencies whose operations are critical, the prospect of unplanned downtime can take a heavy financial toll and incur an even higher reputational cost throughout the ecosystem.

For datacenter providers at all scales, from global hyperscalers and colocations to regional and local operators, this risk is exacerbated by contractual penalties from their top customers. In addition, outages impact reputation, undermining credibility among existing and potential customers.

According to Uptime Institute data, around 70% of all datacenter failures are due to human error. And most datacenter incidents occur during state-change events: the moments when humans intervene to perform maintenance. By reducing the frequency of necessary interventions, condition-based maintenance reduces the likelihood of human-error-induced failures. "Our ultimate vision is to keep the humans out of the machines as much as possible," Sudhir Kalra observed.

Condition-based maintenance shifts business conversation from emergency response to strategic risk management. Operators at the leading edge of condition-based maintenance adoption are making board-level commitments to the approach, recognizing

that the pace of AI infrastructure growth will outstrip their ability to maintain operational reliability without proactive asset management.

Equipment breakdowns can be minimized through formalized data-driven maintenance planning. Condition-based maintenance provides the systematic framework to capture, act on, and continuously improve the institutional knowledge that would otherwise reside only in experienced technicians. This ensures continuity of protection regardless of workforce turnover.

As for cybersecurity risk, it should be addressed through an architecture that does not expose entry points. With strictly unidirectional data flows, the network exposure vectors are eliminated. For datacenter operators with hyperscaler tenants and contractual SLAs, this architectural decision is not a feature; it is a prerequisite. Vendors with a clear, proven cybersecurity practice are ultimately the players that can truly support datacenter operators seeking peace of mind in their day-to-day operations.

Datacenter operators should also seek vendors with market-verified expertise in end-to-end datacenter solutions and the global coverage to act quickly when business disruptions arise.

ABOUT THE IDC ANALYSTS

Mary Johnston Turner, global lead, Digital and Datacenter Infrastructure and Services

Mary Johnston Turner is group lead for Worldwide Digital and Datacenter Infrastructure Strategies at IDC — a group responsible for the coverage of datacenter facilities, service providers, and owner operators, as well as tracking enterprise tech buyer sentiment and strategies related to using digital infrastructure to drive business outcomes. Mary and her team collaborate closely with IDC's Cloud Infrastructure and Services, Network Infrastructure and Services, Semiconductors and Enabling Technologies, and Core Infrastructure research teams to produce a comprehensive view of the dynamics, competitive positions, and market opportunities created by these technologies delivered across syndicated analysis and custom engagements.

Luis Fernandes, senior research manager, Datacenter Facilities Services Markets and Strategies

Luis Fernandes is a senior research manager for IDC's Datacenter Facilities Services Markets and Strategies practice within the Digital and Datacenter Infrastructure and Services domain.

Luis develops research that spans from edge to core to cloud, looking at trends and strategy shifts on how companies buy, build, and run their digital infrastructure.

He specializes in Datacenter Facilities Software Management solutions that enable companies to effectively monitor, manage, and ultimately optimize their IT environments.

In addition, Luis serves as a go-to resource in EMEA for Digital Infrastructure Trends and Strategies.

MESSAGE FROM THE SPONSOR

Schneider Electric is a global energy technology leader, driving efficiency and sustainability by electrifying, automating, and digitalizing industries, businesses, and homes. Its technologies enable buildings, datacenters, factories, infrastructure, and grids to operate as open, interconnected ecosystems, enhancing performance, resilience, and sustainability. The portfolio includes intelligent devices, software-defined architectures, AI-powered systems, digital services, and expert advisory. With 160,000 employees and 1 million partners in over 100 countries, Schneider Electric is consistently ranked among the world's most sustainable companies.

Through its services business, Schneider Electric applies its energytech expertise across the full life cycle of critical assets and systems. Powered by Energy Intelligence, an AI-enabled layer, Schneider Services is shifting from asset-centric operations to a system-level, outcomes-driven approach. By combining consulting, software, and expert-led digital and field services, Schneider Electric helps customers enhance reliability, improve energy and operational performance, advance sustainability, and increase flexibility as a trusted partner.

Discover EcoCare for your datacenter and achieve predictable system-level performance here.

ABOUT IDC

International Data Corporation (IDC) is the premier global market intelligence, data, and events provider for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community make fact-based technology decisions and achieve their key business objectives.

IDC U.K.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
X: @IDC
blogs.idc.com
www.idc.com

Copyright notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2026 IDC. Reproduction without written permission is completely forbidden.