

A photograph of two men in a server room. The man on the left, with a beard and glasses, is pointing at a laptop held by the man on the right. They are both wearing lanyards with ID badges. The background shows rows of server racks with blue lighting.

How to take the edge on

APC[™]

Fortifying distributed IT infrastructure
for the growing network edge

apc.com/us

Life Is On

Schneider
Electric



The great data migration is here.

The network edge, distributed or on-premise IT, is in an explosive growth period. In 2018, just 10 percent of enterprise-created data was processed at the edge. By 2025, it will rise to 75 percent, [according to Gartner](#).

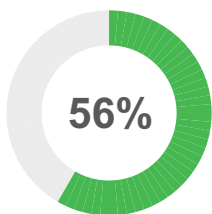
Today the edge is where the action is. It's key to high bandwidth and low latency. It's key to 5G. And it's increasingly key to your customers' operations, no matter the industry.

Here is the challenge: Moving toward the edge will require you to monitor much more than before. Not only are there more IT deployments, they're also running at higher densities, with greater energy use and criticality.

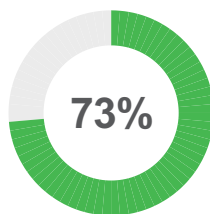
Amid increased complexity, how do you elevate resilience, efficiency, and security?

This guide has answers.

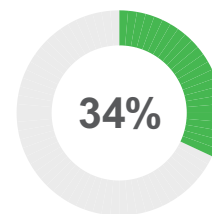
A new [IDG survey](#) of IT leaders reveals optimism and concerns about the edge.



See reduced network latency as a key benefit



Associate edge computing with security concerns



Prioritize upgrading IT and data security to boost resilience

Does this situation sound familiar?

This case study from an end-user in New York reveals the common challenges IT administrators face.



Old equipment

100% of Cisco network switches and 75% of wireless access points past end-of-life date.



Security vulnerabilities

All closet locations deemed insecure due to ease of public access.



Limited power redundancy

While MDF closet has a UPS for power redundancy and management, none of the 5 IDF closets have UPSs.



Heating and ventilation issues

Closets often lack adequate environmental climate control, ventilation, and conditioning.



What does that mean if there is a downtime event?

Did your IT network pass the test?

Throughout the pandemic, the rapid shift to remote operations, coupled with tight budgets, strained many organizations' IT backbones. Now that IT administrators have had time to assess how their network performs under higher capacity demands, it's time to turn that assessment into action.

Here are three approaches that are becoming increasingly popular:



1
Pivoting to proactive maintenance



2
Elevating physical and cyber security



3
Investing in connectivity





From reactive to proactive maintenance

In the past, IT networks weren't nearly as mission-critical as they are today. IT administrators could respond to each alarm as it happened. In the era of remote work and IoT, that has changed.

Now, IT teams need to stay one step ahead of downtime — and proactive maintenance is how they do it. Here's a comparison of what reactive versus proactive maintenance looks like.

Common scenario: MDF room — UPS with bad battery

← REACTIVE



MDF UPS experiences fault due to bad battery



Power glitch causes MDF system to drop



Organization's IT systems offline

→ PROACTIVE



MDF UPS battery nearing end of life



IT staff receives alert, schedules replacement



Battery replaced; downtime averted



Securing the network

The cost of a breach continues to climb, per a [2021 IBM study](#).

\$4.24M

average cost of a data breach in 2020 globally, the highest ever measured

\$9.05M

average cost of a U.S. data breach in 2020

\$5.54M

average cost of breach for organizations with 81 – 100% of employees working remotely



Cybersecurity starts with physical security — preventing unregulated access to servers. Too often, IT closets double as janitorial or storage closets. **Going forward, IT teams need to secure IT spaces via:**



High-definition video monitoring



Badged access control



Instant, user-defined alerts



Investing in IoT connectivity

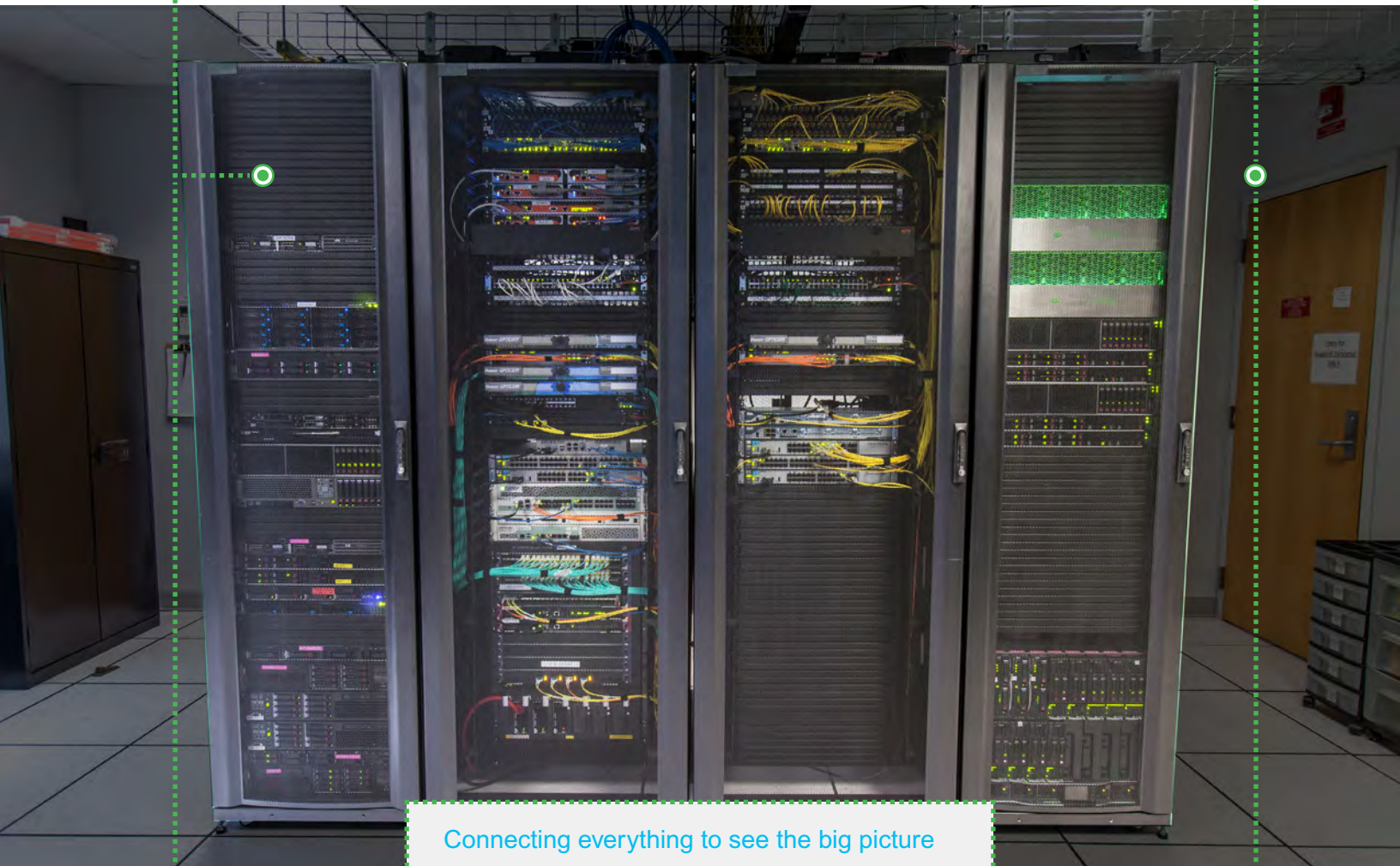
As the migration to the edge accelerates, many organizations are harnessing IoT connectivity to elevate resilience, efficiency, and security.

Monitoring internal asset conditions

Data center infrastructure management software enables you to track battery levels in uninterruptible power supplies, power consumption in cooling units, and other components of the IT backbone.

Monitoring external conditions where the asset operates

The exterior environment is just as important as the inside assets. IoT-connected sensors can monitor temperature, humidity, physical access, vibration, smoke, fluid leaks, and many other variables that impact performance.



Connecting everything to see the big picture

To tap the full potential of IoT connectivity, use software tools to monitor internal asset conditions and external environmental conditions together. When everything is connected, everything can be optimized.

Meet the technology that's fortifying IT backbones from the cloud to the edge.

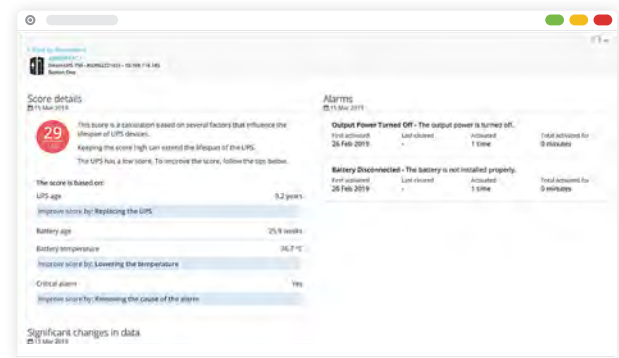
EcoStruxure™ IT Expert software

Our cloud-based, vendor-agnostic, secure solution enables wherever-you-go monitoring and visibility into your IT backbone. Achieve continuous performance gains via health assessments and benchmarking, while maintaining reliable operating conditions for your network.



Instant visibility through centralized and vendor neutral device monitoring

Monitors an extensive range of Schneider Electric™ and third-party devices



Device health assessments of your critical assets, including UPS health checks and lifetime alarms

Generates a health score attributed to each UPS and provides recommendations on how to improve it



Benchmarking data from UPSs, cooling systems, and other data center infrastructure equipment is stored in the EcoStruxure data lake, anonymized and analyzed.

Enables data-driven decisions on the performance, efficiency, and health of your equipment



Device security assessments reduce the risk of a security breach by running a security vulnerability assessment on your devices.

Helps you identify and report on current security vulnerabilities, comply with security policies and regulations, and understand industry best practices

APC NetBotz™ Series

The NetBotz series is a set of hardware sensors that can be placed throughout your IT spaces. NetBotz mitigates downtime and elevates security via integrated sensing, video surveillance, and badged rack-access control. Designed for an IT administrator that needs to be everywhere at once, NetBotz gives you an extra pair of eyes and ears across your distributed IT network.



NetBotz 250



NetBotz 750



NetBotz 755



HD camera support
with video storage¹



Badged access
control



Wide array of
intelligent sensors



Instant, highly
customizable
user-defined alerts



Highly scalable with
expansion pods



Remote management
with built-in network
management



Seamless third-party
IT infrastructure
integration



Enhanced cyber
security



Easy to deploy
and configure

Strengthen your IT backbone

We're ready to help you design a custom solution that takes your customers to the edge — resiliently, efficiently, and securely.

apc.com/us

One Boston Place, Suite 2700
Boston, MA 02108
United States
Tel: (617) 904-9422
apc.com/us

Life Is On

Schneider
Electric

¹ Camera pod is only available on the NetBotz 750 and 755 series models.