

A man with short dark hair and a goatee, wearing a grey t-shirt and a gold watch, is in a server room. He is looking at a laptop on a desk in the foreground and reaching up with his right hand towards a server rack. The server racks are filled with equipment and have some lights on. The background is a perforated metal wall with some light reflecting through it.

A new school of thought for K-12 IT backbones

APC[™]

Innovative approaches to
fortify IT networks in the era
of online learning

apc.com/us

Life Is On

Schneider
Electric

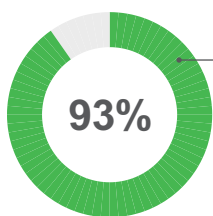


Student outcomes have never depended more on IT infrastructure.

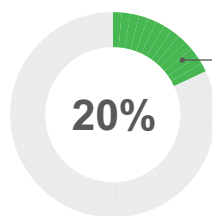
The world of K–12 education is changing. The slow evolution toward online and digital learning accelerated into a sprint in the wake of the pandemic.

Now that the future is here, it's time to assess whether your IT backbone — all the infrastructure that keeps your network running — is ready. This guide explores the technology IT administrators will need to fortify their networks.

Old school, new school: K–12 at the crossroads



households with students who participated in online learning in 2020¹



surveyed school districts that plan to continue virtual school programs after the pandemic²

¹ U.S. Census Bureau, "[Schooling during the COVID-19 Pandemic](#)," August 2020.

² RAND Corporation, "[Remote learning is here to stay](#)," 2020.

Does this situation look familiar?

A case study from a school district in New York represents the current challenges facing many IT administrators.




-  **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 lacking 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 online learning, coupled with tight budgets, strained many schools' 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, school 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 online learning, that's all 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



MDF UPS experiences fault due to bad battery



Power glitch causes MDF system to drop



School IT systems offline



MDF UPS battery nearing end of life



IT staff receives alert, schedules replacement



Battery replaced; downtime averted



Securing the network

As criticality has increased, so has the number of cyber-attacks on public schools.

408

Disclosed cyber-attacks on public schools in 2020

18%

Increase in cyber-attacks from 2019

1,180

Incidents counted since 2016³



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

³ All statistics in this section sourced from K-12 Cybersecurity Resource Center and the K12 Security Information Exchange, [The State of K-12 Cybersecurity: 2020 Year in Review](#), 2021.



Investing in IoT connectivity

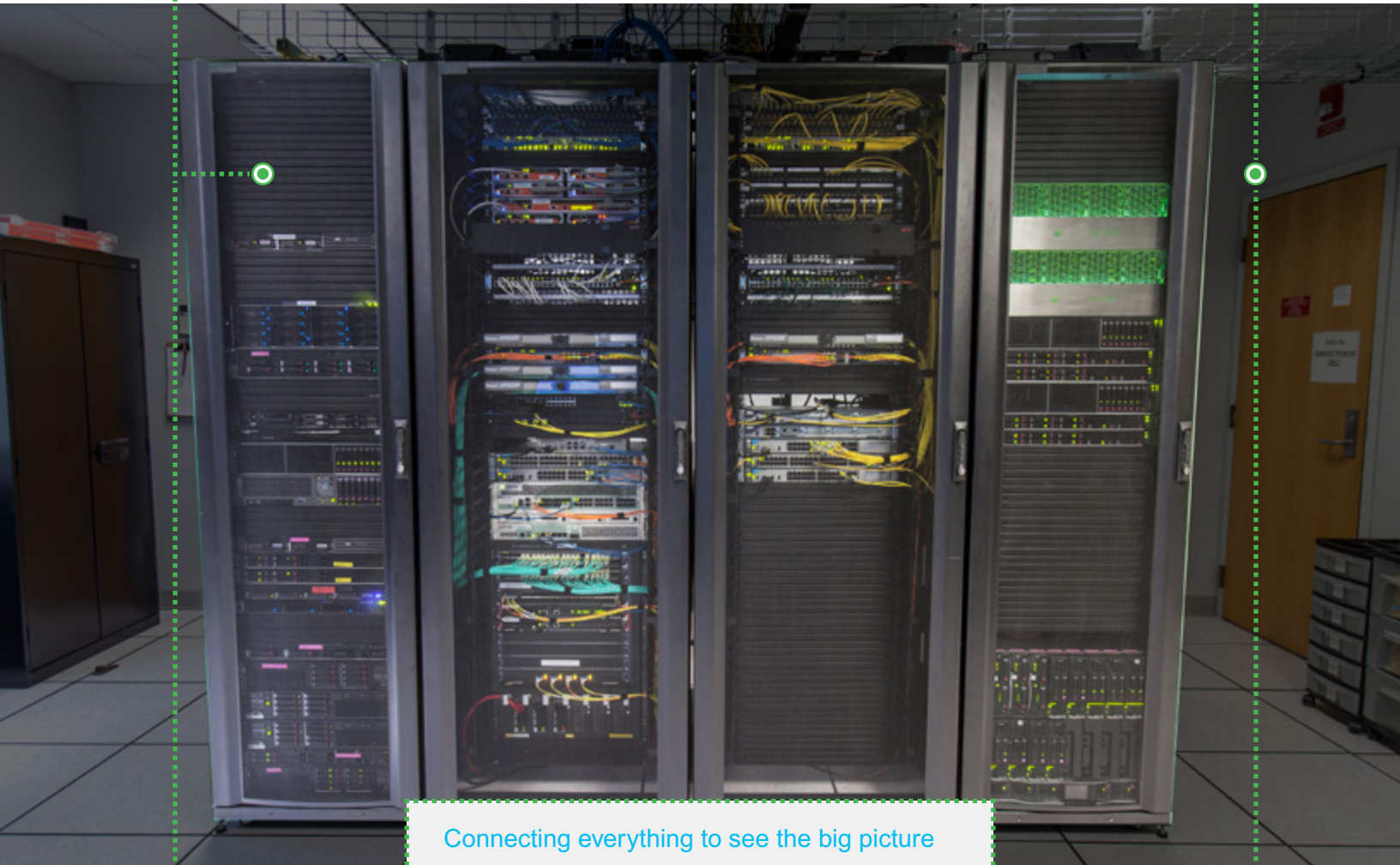
With new federal funding available, many schools are connecting their IT backbones. Here are some of the top areas getting attention.

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 every other piece of the IT backbone.

Monitoring external conditions where the asset operates

You can't just monitor the inside of the assets. The exterior environment is just as important. 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

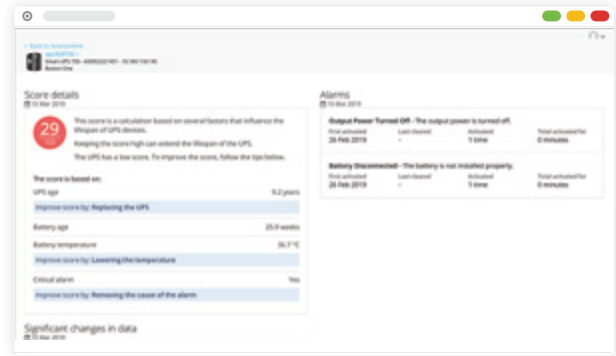
EcoStruxure™ IT Expert software

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 storage⁴



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 fits your budget and qualifies for federal funding

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

⁴ Camera pod is only available on the NetBotz 750 and 755 series models.