How to take the edge on

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.

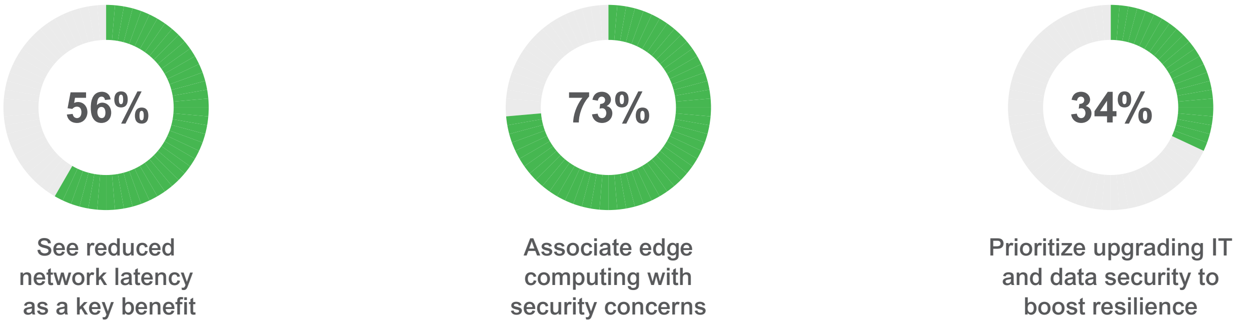
Today the edge is where the action is. It's key to high bandwidth and low latency. It's key to 5G. And it's increasingly key to your customers' operations, no matter the industry.

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.



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

1

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 experieces 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

2

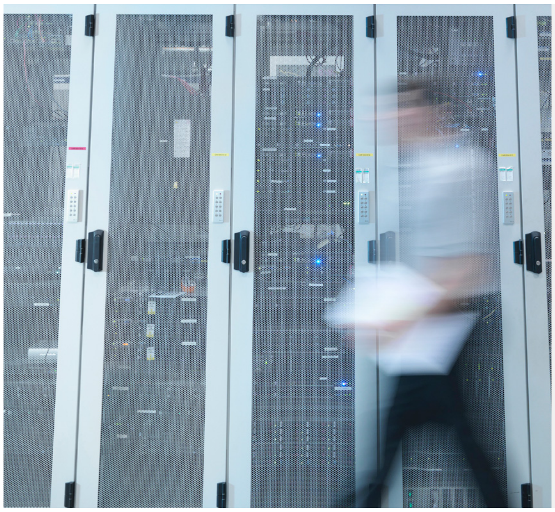
Securing the network

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

3

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.

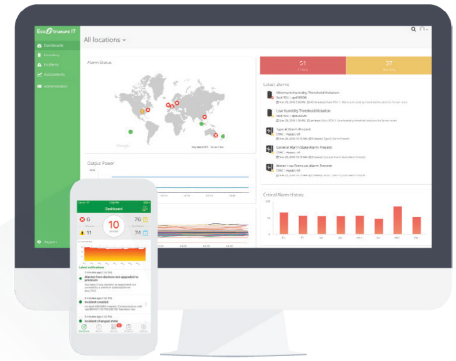
Connecting everything to see the big picture

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.

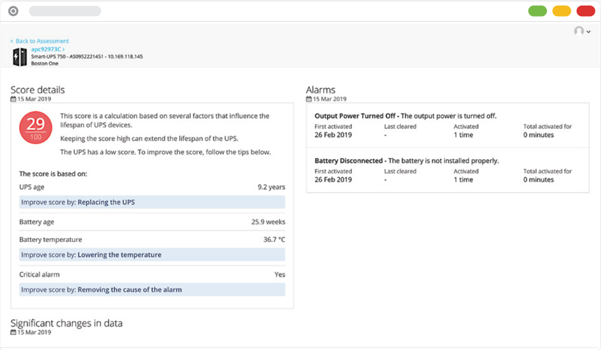
EcoStruxure™ IT Expert software

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



‹ Back to Assessment

apc92973C ›

Smart-UPS 750 - AS0952221451 - 10.169.118.145

Boston One

Score details

15 Mar 2019

29 / 100

This score is a calculation based on several factors that influence the lifespan of UPS devices.

Keeping the score high can extend the lifespan of the UPS.

The UPS has a low score. To improve the score, follow the tips below.

The score is based on:

UPS age	9.2 years
Improve score by: Replacing the UPS	
Battery age	25.9 weeks
Battery temperature	36.7 °C
Improve score by: Lowering the temperature	
Critical alarm	Yes
Improve score by: Removing the cause of the alarm	

Alarms

15 Mar 2019

Output Power Turned Off - The output power is turned off.

First activated	Last cleared	Activated	Total activated for
26 Feb 2019	-	1 time	0 minutes

Battery Disconnected - The battery is not installed properly.

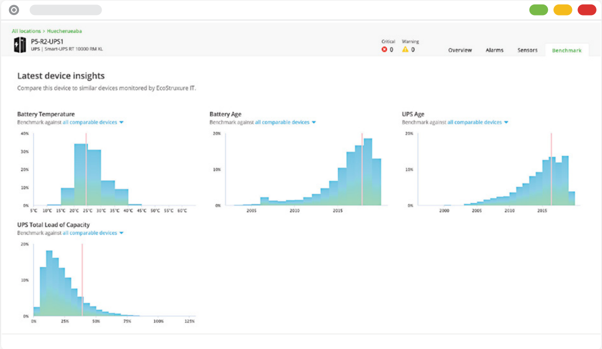
First activated	Last cleared	Activated	Total activated for
26 Feb 2019	-	1 time	0 minutes

Significant changes in data

15 Mar 2019

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



All locations › Huecherueaba

P5-R2-UPS1

UPS | Smart-UPS RT 10000 RM XL

Critical 0 Warning 0

Latest device insights

Compare this device to similar devices monitored by EcoStruxure IT.

Battery Temperature

Benchmark against all comparable devices

Battery Age

Benchmark against all comparable devices

UPS Age

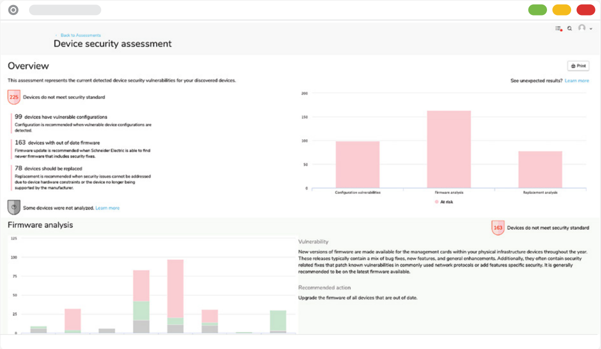
Benchmark against all comparable devices

UPS Total Load of Capacity

Benchmark against all comparable devices

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



‹ Back to Assessments

Device security assessment

Overview

This assessment represents the current detected device security vulnerabilities for your discovered devices.

See unexpected results? Learn more

225 Devices do not meet security standard

99 devices have vulnerable configurations

Configuration is recommended when vulnerable device configurations are detected.

163 devices with out of date firmware

Firmware update is recommended when Schneider Electric is able to find newer firmware that includes security fixes.

78 devices should be replaced

Replacement is recommended when security issues cannot be addressed due to device hardware constraints or the device no longer being supported by the manufacturer.

Some devices were not analyzed. Learn more

Firmware analysis

163 Devices do not meet security standard

Vulnerability

New versions of firmware are made available for the management cards within your physical infrastructure devices throughout the year. These releases typically contain a mix of bug fixes, new features, and general enhancements. Additionally, they often contain security related fixes that patch known vulnerabilities in commonly used network protocols or add features specific security. It is generally recommended to be on the latest firmware available.

Recommended action

Upgrade the firmware of all devices that are out of date.

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 storage[1]

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.