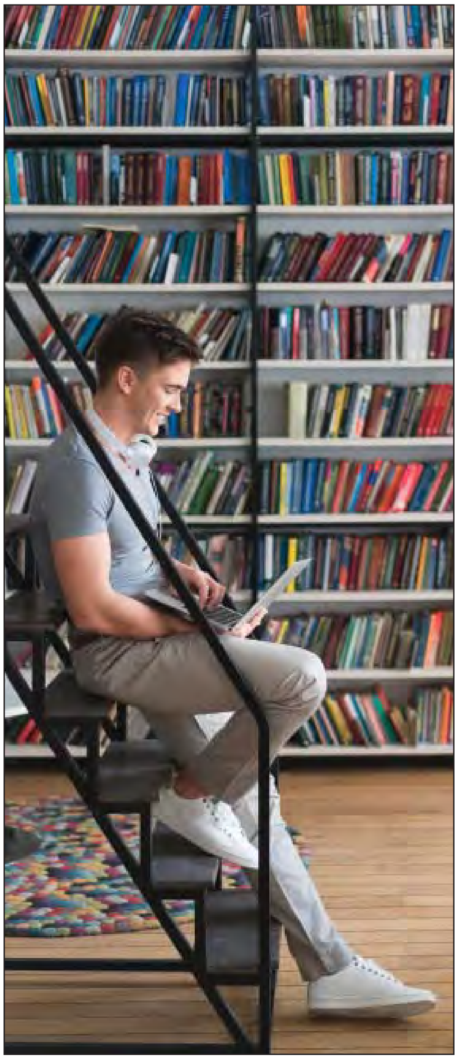
Tech Outlook

March 2017

PROSYS
A PIVOT COMPANY



# Making the Grade

## *Dell launches new line of affordable, flexible endpoint devices for the education market.*

The multiple choice exam requiring students to select the correct answer from a list of options is a time-honored test format in K-12 education. Dell EMC recently presented school districts with a multiple choice question that has no wrong answers.

The infrastructure solutions division of Dell Technologies has developed a portfolio of endpoint computing devices purpose-built for the education sector. Based on Dell's workhorse Latitude business laptop family, these new devices are affordable, flexible and built to take a beating.

The lineup includes a 13-inch laptop, an 11-inch laptop, and an 11-inch convertible with a touchscreen display and a 360-degree hinge that can be used as either a laptop or a tablet. They come with a choice of either Microsoft Windows or Google Chrome operating systems, providing flexibility for schools that have hybrid technology implementations and multiple technology needs.

The devices are also built for a full day of learning, delivering all-day battery life. Additionally, they are built to withstand classroom abuse. They have rubberized shock protection to protect against drops and sealed keyboards and touchpads to protect against spills.

### Affordable and Empowering

Best of all, they are budget-friendly — a key consideration in an age when school districts are facing increased pressure to both stretch their dollars and enhance classroom innovation.

"Dell's new devices are affordable enough that schools can move forward with one-to-one computing initiatives, where every student has access to a device," said Edna Zielmanski, National SLED Relationship Manager, ProSys. "That will allow classroom teachers to facilitate a more personalized learning environment."

continued on page 2

*continued from page 1*

Studies show that one-to-one classroom computing ratios deliver significant benefits for students. A Michigan State University study conducted over the past 15 years found that providing laptop computers to students resulted in better outcomes in English/language arts, writing, math and science. The study's authors say one-to-one programs also enhance engagement and enthusiasm among students, improve teacher-student relationships and promote "21st-century skills" such as technological proficiency and problem solving.

"Learning-model best practices have evolved and today's education environment needs to be personalized and student-led, giving students the freedom to produce their best work both inside and outside the classroom," said Jon Phillips, managing director of worldwide education strategy, Dell EMC. "With this release of our best-ever portfolio of education devices, we want to empower student-led learning by providing the tools both educators and students need to inquire, create and collaborate, wherever that may take place."

## The Details

The 3189 is the 11-inch convertible device that comes as either the Latitude (Windows OS) or Chromebook (Chrome OS) version. The device's 360-degree flexibility allows it to be used in three different modes: clamshell, tablet or tent. An outward-facing camera in tablet mode allows students to create videos and other multimedia projects.

The Windows version also offers the optional Dell Productivity Active Pen so students can improve their understanding of conceptual applications by writing notes and making diagrams with natural pen-to-paper writing motion. While there are some debates about the use of styluses, multiple studies have shown that hand-written information is committed to memory to a much greater degree when compared to typing.

The Latitude and Chromebook 3180s are 11-inch notebooks featuring a new design that reduces the overall size so they're easy to move from desk to table for group assignments. They feature an ergonomically designed keyboard for natural, comfortable student use and all-day battery life. The fully sealed keyboards and click pads provide protection against spills, and the "secure" keys are 50-percent more tamper-resistant than in previous products.

The 3180s also feature a 180-degree lay-flat, durable hinge to support collaboration, allowing students and educators to gather around a single device and view material together. The Latitude 11 is available with 7th Gen Intel Celeron and Pentium processors, while the Chromebook 11 is available with 6th Gen Intel Celeron processors.

The Latitude and Chromebook 3380 models are 13-inch notebooks that deliver a larger screen, more powerful processing performance and faster memory. These models are designed to support advanced curricula, content delivery methods and learning use cases, providing a powerful platform for students and teachers to create and explore. They are particularly useful for students running STEM (science, technology, engineering and math) applications.

Even with increased performance and reduced size, these laptops also deliver all-day battery life. Optional E-Rate mobile broadband (Windows only) allows educational institutions to support connected learning at a discounted rate wherever Wi-Fi isn't available. The Latitude 13 is available with 6th and 7th Gen Intel Celeron, Pentium, and up to Core i5 processors, while the Chromebook 13 is available with 6th Gen Intel Celeron or Core i3 processors.

## Going Digital

Dell's budget-friendly options come at a great time for school districts that are seeing more textbooks and associated learning resources go digital. A recent survey by The Learning Counsel, an education-focused research institute, finds that 86 percent of K-12 schools are looking to expand their digital curricula in 2017.

Studies show that the use of digital curricula can help schools improve on-time graduation rates, lower dropout rates and improve exam scores. Evidence suggests it is particularly helpful in creating targeted lessons for struggling students, allowing them to work at their own pace.

This shift from paper-based resources makes student access to computing devices more important than ever. In a recent survey of more than 1,300 K-12 educators conducted by Technology Horizons in Education, responding teachers ranked laptops, Chromebooks and tablets as the most valuable tools for teaching and learning.

Among those surveyed, an overwhelming 92 percent said they see laptops as either "essential" or "valuable" for teaching and learning. Tablets gained the same rating from 87 percent while Chromebooks were cited by 80 percent.

"Putting a device in front of a student doesn't automatically improve teaching or learning," said Zielmanski. "However, access to devices does create the possibility for students to become more actively involved in the learning process and for teachers to create a more enriching classroom experience.

"Dell's new portfolio of education-focused endpoint devices puts some pretty powerful tools in the hands of students and teachers. These tools can help create an environment in which students are encouraged to indulge their curiosity, collaborate with their peers and teachers, and push the boundaries of what they thought was possible."

# News Briefs

## DDoS Strikes May Hide Other Attacks

Distributed Denial of Service (DDoS) attacks are sometimes used by cybercriminals to distract businesses while hackers sneak in through the back door, Kaspersky Lab reports in its 2016 Corporate IT Security Risks survey.

The security firm says that 56 percent of businesses surveyed are confident that DDoS has been used as a smokescreen for other kinds of cybercrime. Of those, 87 percent reported that they had also been the victim of a targeted attack.

The survey found that when DDoS attacks have been used by cybercriminals as a smokescreen, businesses also faced threats such as losses and exploits through mobile devices (81 percent), the actions of other organizations (78 percent), phishing scams (75 percent) and even the malicious activity of internal staff (75 percent).

"DDoS prevents a company from carrying on its normal activities by putting either public or internal services on hold," said Kirill Ilganaev, head of DDoS protection, Kaspersky Lab. "This is obviously a real problem to businesses and it is often 'all hands on deck' in the IT team, to try and fix the problem quickly, so the business can carry on as before. DDoS can therefore be used not only as an easy way to stop the activity of a company, but also as a decoy to distract IT staff from another intrusion taking place through other channels."

## Increased Spending on Analytics Expected

IT leaders anticipate budget increases in 2017 and expect to increase investments in analytics, security and numerous other applications and platforms, according to a new survey from CIO, a leading technology content platform.

Seventy-one percent of those surveyed said they plan to increase spending on business intelligence and analytics, while 59 percent expect to spend more on securing enterprise information assets. Other top areas cited include CRM (47 percent) and mobile enterprise apps (46 percent).

Additionally, tech leaders cited several other technologies as likely growth areas for 2017. These include artificial intelligence, the Internet of Things and machine learning/cognitive systems. Topics that have been adopted and are likely to see upgrades in the coming months include business continuity/disaster recovery, data management/storage and co-location services.

"Organizations continue to explore ways to conduct business smarter and protect assets and processes," said Adam Dennison, senior vice president and publisher of CIO. "The Tech Poll results confirm that we are in an exciting time of technology growth, where organizations are exploring technologies that will enhance legacy systems, and new solutions and emerging vendors that will elevate their business."

## Tech Outlook

**Editorial Correspondence:**
10221 E. 61st Street
Tulsa, OK 74133
Phone (800) 726-7667
Fax (918) 270-7134

**Change of Address:** Send corrected address label to the above address.

Some parts of this publication may be reprinted or reproduced in nonprofit or internal-use publications with advance written permission. Tech Outlook is published monthly by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.

## ProSys locations

**Atlanta, GA**
**(Headquarters)**
Phone: 678-268-1300
Toll-Free: 888-337-2626
chash@prosysis.com

**Atlanta, GA**
**(Integration Center)**
Phone: 678-268-9000
Toll Free: 888-337-2626
twheless@prosysis.com

**Austin, TX**
Phone: 512-658-5847
Toll Free: 888-337-2626
jwestmoreland@prosysis.com

**Birmingham/Montgomery, AL**
Phone: 205-314-5746
Toll-Free: 800-863-9778
birminghamsales@prosysis.com

**The Carolinas**
Toll-Free: 888-337-2626
chash@prosysis.com

**Indianapolis, IN**
Phone: 317-688-1283
Bill.sanders@prosysis.com

**Knoxville, TN**
Phone: 865-310-8843
Toll-Free: 800-863-9778
info@prosysis.com

**Louisville, KY**
Phone: 502-719-2101
Toll-Free: 800-863-9778
info@prosysis.com

**Mexico City**
Phone: +52 (55) 3601 3755
info@prosysis.com

**Miami, FL**
Phone: 305-256-8382
Toll-Free: 800-891-8123
lspivack@prosysis.com

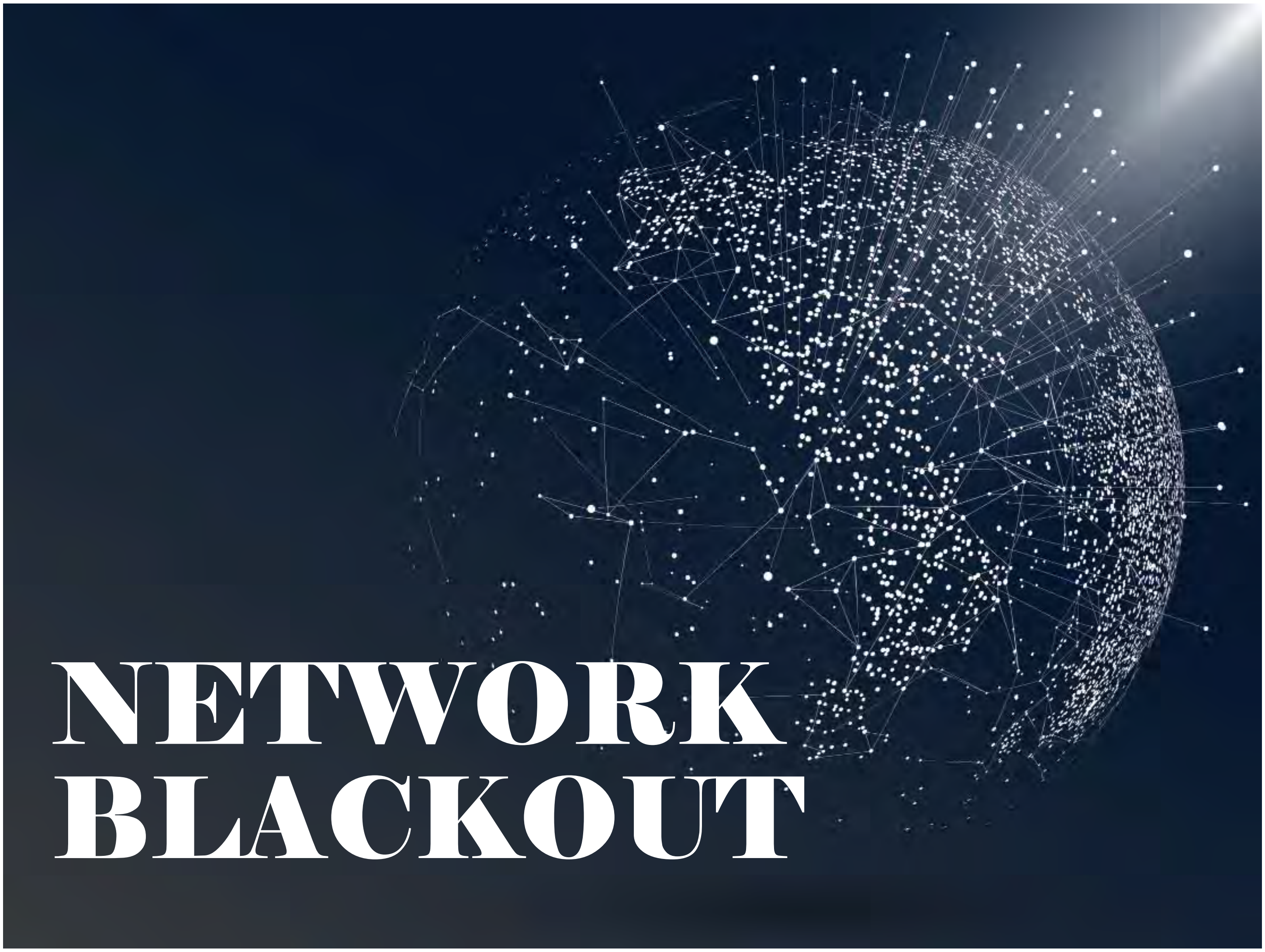
**Mid-Atlantic**
Phone: 800-634-2588 ext 2
midatlantic@prosysis.com

**Nashville, TN**
Phone: 615-301-5200
Toll-Free: 800-863-9778
info@prosysis.com

**New England**
Toll Free: 800-634-2588 ext 1
newengland@prosysis.com

**Seattle, WA**
Phone: 425-939-0342
sballantyne@prosysis.com

**Tampa, FL**
Phone: 813-440-2410
800-891-8123
lspivack@prosysis.com



# NETWORK BLACKOUT

*Software-defined perimeter aims to keep potential intruders in the dark.*

During World War II, blackout drills were nightly rituals in cities around the world. Street lights were turned out, automobile headlights were dimmed and everyone headed indoors where they covered windows with heavy curtains, blankets or blinds to minimize all outdoor lighting. The idea was that enemy bomber planes couldn't accurately target what they couldn't see.

This simple logic is at the heart of the software-defined perimeter (SDP), a new security approach in which network segments are cryptographically "blacked out" from the rest of the infrastructure. Sensitive information simply cannot be detected by unauthorized users, which dramatically diminishes the opportunities for network attacks.

"The primary objective of the SDP is to make the application infrastructure effectively invisible or 'black' by eliminating DNS (domain name system) information or IP addresses," said Juanita Koilpillai, CEO of Waverley Labs, a cyber risk management company that was selected to develop an SDP solution for the Department of Homeland Security. "SDPs establish an undetectable application infrastructure by changing the historical paradigm and establishing communications with only authorized users rather than communicating with anyone seeking access."

## Isolating Assets

The SDP approach evolved from the work done at the U.S. Defense Information Systems Agency (DISA), where network access is based on a "need-to-know" basis. Using a variety of security controls, the DISA enforces strict network segmentation once users gain network authorization in order to prevent them from seeing applications, DNS numbers, IP addresses and other sensitive network elements. This approach mitigates the most common network-based attacks, including distributed denial of service (DDoS) attacks, server scanning, SQL injection, cross-site scripting and more.

The SDP approach has been formalized as a specification published by the Cloud Security Alliance (CSA). It has recently been popularized by companies such as Google, with their BeyondCorp initiative, as well as several other enterprises active in CSA working groups. Gartner analysts say it is rapidly becoming an important element of security for today's open, multitenant cloud architectures.

“Organizations continue to struggle to properly segment and provide adequate access control over their sensitive networks, hosts and applications within their environments beyond the perimeter firewall or segmentation performed at network boundaries,” Gartner noted in its Predicts 2016: Security Solutions report. “Through the end of 2017, at least 10 percent of enterprise organizations … will leverage software-defined perimeter technology to isolate sensitive environments.”

> **“The primary objective of the SDP is to make the application infrastructure effectively invisible or ‘black’ by eliminating DNS information or IP addresses.”**

## Restricting Access

Traditional security measures have focused on creating a defensive barrier between the network and the open Internet.  The problem is that the continued decentralization of the network through cloud and mobile technologies has created too many gaps to plug.

Time-honored defenses such as firewalls and intrusion prevention systems are not entirely effective in protecting cloud and critical web applications. In a June 2016 report, cloud security firm Netskope noted that the number of enterprises finding malware in their sanctioned cloud apps nearly tripled from 4.1 percent to 11.0 percent between the Q4 2015 and Q1 2016. The majority of malware detected involved JavaScript exploits and droppers, which are increasingly used to deliver ransomware.

In traditional security models, once someone is verified at the perimeter and allowed access to a network segment — whether legitimately or through a malicious attack — they gain the ability to see and potentially access everything within the network. However, an SDP creates a virtual “air-gapped” network in which unauthorized segments are simply not visible on the network at all. If they can't be seen, they can't be compromised.

This invisible infrastructure is created by strictly controlling network access not just with user authorization, but also with session-specific controls based on contextual variables. These variables can include the user's identity, the user's location, the time of day, the type of device being used, whether the device is running security software, and many more.

## Aiding Compliance

SDP solutions go even further, providing additional security controls at the content level within a secured network segment. Even after a user is authenticated, classification and encryption tools ensure that only those with proper access can see and access sensitive data. Content-level controls can also dictate what actions a user can and cannot take with data — for example, whether data can be downloaded or attached to an email. Logging mechanisms allow tracking, alerting and analysis of any anomalies.

These functions also provide significant compliance capabilities. For instance, an SDP addresses Payment Card Industry Data Security Standards (PCI DSS) guidelines with network segmentation that isolates cardholder data from the rest of the network. It also supports current PCI DSS requirements for the use of multifactor authentication.

In addition to advanced protection and improved compliance, SDP solutions also bring new levels of simplicity and automation to the security infrastructure. By combining device authentication, identity-based access, fixed perimeter and dynamically provisioned connectivity controls, an SDP strengthens security while reducing management complexity.

The cloud computing facilitates simple, powerful and affordable solutions that resolve significant business challenges and deliver peace of mind. However, the open nature of the cloud also brings unique security risks. By blacking out sensitive network identifiers, the software-defined perimeter brings an old-fashioned sensibility to modern security requirements. Hackers can't attack what they can't find.

# Rethinking the Campus Network

## *Today's campus network represents a unified wired and wireless infrastructure that simplifies management and access control.*

Wireless networks have become imperative to support today's increasingly mobile workforce. Users need ready access to productivity-enhancing applications and services, yet many IT departments are struggling to keep pace with those demands. In many organizations, wired and wireless networks remain divided, meaning that IT must juggle multiple management platforms, security policies and access controls. Overstretched network teams lack the visibility and control they need to rapidly deploy new services and ensure a high-quality user experience.

"If managing one network is difficult, managing two is virtually impossible unless you have an army of network engineers," said Edna Zielmanski, National SLED Relationship Manager, ProSys. "Yet in many organizations networking teams are shrinking, leaving fewer engineers to handle the increasing complexities."

The solution to this conundrum is to take a campus approach to network management. The term "campus network" once referred to a set of interconnected LANs serving multiple buildings in close proximity. In this new context, the campus network was more widespread than the typical LAN but not as geographically dispersed as a WAN.

"As wireless networks have become integral parts of the IT infrastructure, the concept of the campus network has broadened to include a unified wired and wireless network environment. The 'campus' in this sense may include a single building along with any wireless access available beyond the building walls," Zielmanski said.

"The campus network has come to represent unified wired and wireless networking with single-pane-of-glass management and streamlined access control. Fully integrated management reduces the complexity of planning, implementing and operating network infrastructure. It also provides secure access to mission-critical resources and a consistent user experience across both wired and wireless networks."

### Key Components

Operational complexity is a chief reason organizations are turning to unified wired and wireless solutions. They need tightly integrated management tools that provide configuration, monitoring and fault management features that help isolate bottlenecks and speed problem resolution. The solution should have the ability to scale from hundreds to thousands of devices.

But single-pane-of-glass management is only part of the story. Organizations also need security and access controls that provide contextual policy enforcement based upon user, device, location, time of day and other criteria. The unified access layer should be based upon open standards in order to ensure compatibility with endpoints and systems and simplify application support.

Management tools should also provide multivendor capabilities in an open framework approach. This enables organizations to leverage existing investments in networking equipment while creating an interoperable, converged campus.

"Many vendors offer unified wired and wireless management, but those solutions only support that particular vendor's products," said Zielmanski. "A campus management platform should provide a clear path to convergence, integrating with current gear and evolving with the network as business requirements change."

Software-defined networking (SDN) creates a more agile campus network that can automatically adapt to application requirements and optimize the user experience. With SDN, all network policies and applications can be centrally programmed and managed through a single controller. SDN also uses automation and orchestration to provision, configure and allocate network resources, eliminating the time-consuming process of programming each network device manually according to vendor-specific protocols.

"The SDN model enables organizations to move away from hardware-focused infrastructure in order to create more customized, agile networks," Zielmanski said. "In addition to simplifying administration, SDN helps reduce capital and operational costs, centralize security, and make the network more responsive to changing demands."

## The Importance of Open Standards

Open standards have emerged in the SDN market as organizations seek to break free from vendor lock-in. In fact, some experts have predicted that open-source standards will soon become an SDN requirement. However, the dominance of proprietary operating systems, hardware and middleware in the networking and telecom sectors has made it difficult for open- source solutions to gain traction.

"Organizations should be on the lookout for 'SDN-washing' — altering the definition of SDN to suit the capabilities of a particular product," said Zielmanski. "Just because a product provides some level of programmability, virtualization, orchestration or dynamic provisioning doesn't mean it's an open-source SDN solution.

"The primary advantages of open-source networking are cost, simplicity and innovation. In an open-source environment, equipment becomes essentially interchangeable from vendor to vendor, helping to drive down prices and minimize compatibility issues. Also, ongoing collaboration within the open-source networking community has the potential to accelerate the pace of network innovation."

In a campus network environment, open standards help ensure tight integration between wired and wireless networks. One, simpler network is more reliable and agile, enabling faster service deployment, reducing total cost of ownership, and providing a high-quality user experience.

Users have come to expect wireless access that delivers the same performance and reliability as the traditional wired network. In order to meet those expectations, many organizations are looking to create a campus network environment that unifies wired and wireless under a single management and access control platform. By incorporating SDN capabilities and open standards, today's campus network provides greater visibility and control along with the agility to respond to constantly changing requirements.

# K-12 Education Solutions

DELL EMC

Dell EMC's new portfolio of education PCs is designed to help school districts transition from a one-size-fits-all instructional approach to a flexible, on-demand, student-centered model. Laptops, Chromebooks and tablets are flexible, affordable and built to survive the classroom environment with fully sealed keyboards and touchpads. Contact your ProSys representative to learn more.

PROSYS
A PIVOT COMPANY

www.prosysis.com 888-337-2626

DELL-10