Endpoint Resilience™ Report | Education Edition 2020/21

Distance Learning's Impact on Education IT

New research from Absolute® examines the effects of distance learning on endpoint health, device usage, safety, and security as schools adapt to remote and hybrid learning models in 2020/21.

Executive Summary

The COVID-19 pandemic caused an acceleration of K-12 education's digital roadmap in several key areas.

The rapid shift to remote or distance learning in spring 2020 revealed that access to Wi-Fi and digital devices at home was inadequate for millions of U.S. households.[1] The so-called "homework gap" moved from being an issue of digital inequity in the home to becoming a major roadblock to learning for millions of students.

Schools responded by accelerating or creating programs that ensured students could learn online, regardless of the technical infrastructure. Before the COVID-19 outbreak, 82% of schools in the U.S. provided student devices in one-to-one or similar programs[2], though not all of those devices left the school grounds. Today, schools are getting closer to a device for every student — with few restrictions on device movement.[3]

The rapid response rates across both public and private sectors complicated planning for the school year, as contradictory policy recommendations circulated. Federal stimulus packages for public education are rolled out, while, simultaneously, state and local education budgets are tightened.

The additional COVID-19-related expenses for an average U.S. school district are estimated to be in the range of $1.7 million, or about $500 per student.[4]

In summary, large and small schools and districts find themselves in an unprecedented situation — they are educating broad and diverse student populations with distance learning for the first time; navigating new learning platforms; finding new ways to engage students with unfamiliar technology; and investing in professional development to support teachers. And they're doing this on tighter budgets with fewer resources.

Further, the cybersecurity challenges highlighted in Absolute's K-12 report last year have grown.[5] With many teachers and IT staff working from home and many students learning remotely — outside the safe perimeter of the school network and web filters — cybersecurity incidents are increasing and, even more concerning, they're happening off the school network where IT has no visibility. As a result, education is still the most vulnerable sector, accounting for 60% of all malware attacks.[6]

As a standard platform deployed in over 1,200 schools and districts in North America, Absolute embarked on its second annual education technology research project to better understand and address the challenges facing K-12 education in this unique 2020/21 school year. We looked at anonymized, de-identified data from millions of education endpoints to find the answer to key questions such as:

- **How can school districts stay connected to — and manage — a more mobile device inventory?**
- **How are devices being used by K-12 students?**
- **What technology is required to enable the remote classroom?**
- **How are students engaging with online learning tools?**
- **Does distance learning technology put students and schools at greater risk?**
- **What can schools do to make their devices more resilient in the 2020/21 school year?**

This report includes a summary and analysis of our findings.

[1] Digital Divide Persists Even as Lower-Income Americans Make Gains in Tech Adoption. *Pew Research,* 2019.
[2] CoSN's 2019 K-12 IT Leadership Survey Report Consortium of School Networking. *CoSN*, 2019.
[3] Coronavirus Pushes Schools Closer to a Computer for Every Student. *EdWeek,* 2020.
[4] With Budget Cuts Looming, Here's How Districts Will Decide What to Keep or Cut. *EdSurge,* 2020.
[5] Verizon's 2020 Data Breach Investigations Report. *Verizon,* 2020.
[6] Global Threat Activity. *Microsoft,* 2020.

Key Insights

Distance Learning's Impact on Education IT

New research by Absolute examines the effects of distance learning on endpoint health, device usage, safety, and security as schools adapt to remote and hybrid learning models in the 2020/21 school year.

COVID-19 caused an acceleration of K-12 education's digital roadmap in three key areas:

1. **Closing the "homework gap" to enable digital learning.** Mobile hotspots are increasingly going home, with students, creating an "always-connected" online learning dynamic[1]
2. **Enabling remote and hybrid learning models.** 75% of schools intend to operate remote or hybrid models[2]
3. **Protecting students, staff, and schools from cyberattacks.** 60% of all malware attacks (particularly ransomware) occur in education[3]

To better understand what is happening on the ground, Absolute studied:

- millions of devices
- 10,000 Schools and Districts
- 12 analyst reports and peer research

This is what we discovered…

Reliance on devices to drive learning outcomes has increased.

61% increase in devices used heavily

28% rise in daily active hours used

8% increase in the number of older devices in school fleets

80% of schools have or plan to purchase more devices to enable remote learning[4]

IT teams are doing more with less.

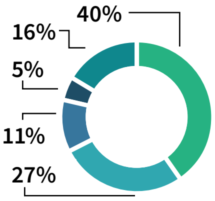
While federal stimulus packages may help in the short term, long-term budgets are uncertain:

$750B predicted decrease in state and local government budgets[5]

$3.7B additional COVID-19 costs[6]

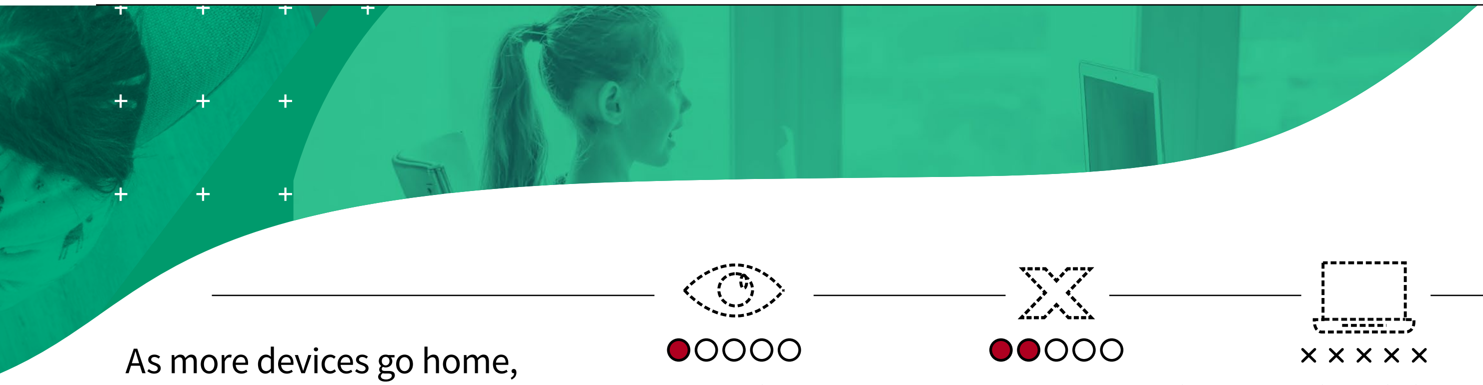
$500 incremental per student distance-learning costs[7]

School devices are mainly being used for learning.



YouTube, Edgenuity®, Google Docs™, and Google Classrooms are where most students are spending their time.

● Education and Online Learning
● Entertainment and Videos
● Cloud-Sharing Services
● Web Search
● Other



As more devices go home, IT teams are challenged to manage them:

●○○○○

20% of all devices have gone dark or have not been online so far in the first five months of 2020

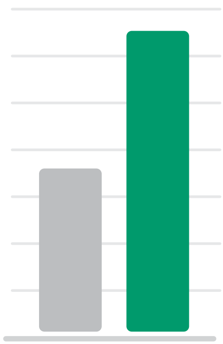
●●○○○

41% of school IT teams said tracking lost or missing devices is a big challenge.[8]

× × × × ×

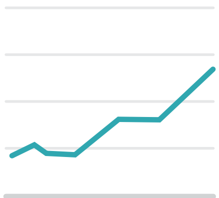
30 devices missing on average at each school in the past nine months.

To support and manage remotely, IT teams are rolling out Remote Desktop Protocol (RDP) and collaboration applications.



141% ▲
increase in collaboration software.

WebEx® | Zoom | Skype™ | Microsoft Teams™ | Slack® | Blue Jeans | Pidgin | Flock™ | GoToMeeting® | Microsoft Lync™ | Join.Me



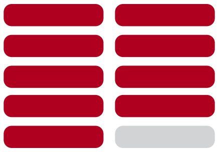
87% ▲
increase in remote desktop protocol (RDP) usage.

RemotePC™ | Zoho Assist | LogMeIn Pro® | GoToMyPC® | Connectwise Control® | Parallels® Access | TeamViewer | Splashtop® | Chrome Remote Desktop | Remote Desktop Manager | RemoteUtilities® for Windows

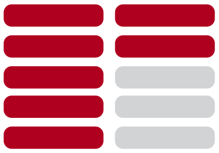
⚠

But the FBI warned schools of the increased risk of RDP as a vector for ransomware![11]

Remote learning is creating tech support challenges that are taking away valuable time from teachers to "teach".

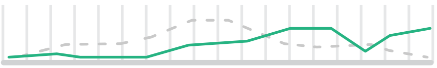


9 out of 10 teachers reported spending more time troubleshooting technology problems[9]



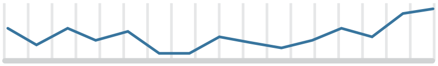
7 out of 10 teachers reported spending less time on student instruction during COVID-19 than when they were they were in their physical classroom[10]

With increasing complexity, device security is more challenging than ever.



72% of devices have out-of-date OS versions (two or more versions old)

454 unique patch versions across Windows 10 devices alone



81% spike in outdated Chrome OS versions, due to new versions released in early April 2020

183 days average patch age for Windows 10 devices

31 days average patch age for MacOS devices

46% of schools have at least one device that uses rogue or non-authorized VPN or web proxy applications (up 4 percentage points from 2019)

[1] Coronavirus Pushes Schools Closer to a Computer for Every Student. *EdWeek, 2020.*

[2] School Districts' Reopening Plans: A Snapshot (2020, July 28). *EdWeek, 2020.*

[3] Global Threat Activity. *Microsoft, 2020.*

[4] Distance Learning Study. *Hanover Research, 2020.*

[5] Projected State Shortfalls Grow as Economic Forecasts Worsen. *Center on Budget and Policy Priorities, 2020.*

[6] What Will It Take to Stabilize Schools in the Time of COVID-19? *Learning Policy Institute, 2020.*

[7] What Will It Take to Stabilize Schools in the Time of COVID-19? *Learning Policy Institute, 2020.*

[8] Distance Learning Study. *Hanover Research, 2020.*

[9] How COVID-19 Is Shaping Tech Use. What That Means When Schools Reopen. *EdWeek, 2020.*

[10] How COVID-19 Is Shaping Tech Use. What That Means When Schools Reopen. *EdWeek, 2020.*

[11] FBI Warns K12 Schools of Ransomware Attacks via RDP. *ZDNet, 2020.*

New Challenges Facing Schools in 2020/21

There are extensive changes taking place in the K-12 education technology landscape as a result of COVID-19 school closures and other distancing requirements. These changes are accelerating digital transformation efforts and reducing digital inequity in education. The rapid speed of change is creating new challenges for the education IT teams that must support the near tectonic shift that has taken place. Some of the main challenges highlighted in Absolute's current education report include:

1. Requirement for Seamless Transitions Between Distance, In-Person, and Hybrid Learning

Few schools will get through the 2020/21 academic year without some form of distance or hybrid learning model. It is expected that health officials' ongoing recommendations for social distancing in classrooms will limit the number of students attending school in-person.

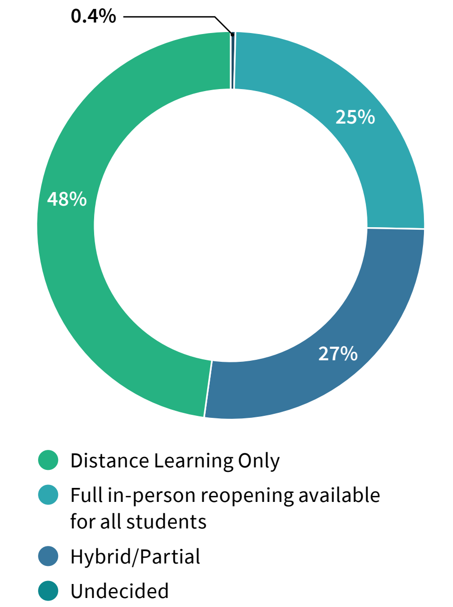
According to a recent report, 48% of the sampled school districts from across the U.S. plan to operate via distance learning only and 75% plan to operate via distance learning or a hybrid instructional model.[7]

For schools adopting a hybrid or in-person model, IT teams must be prepared to switch to distance learning on short notice. Since periodic outbreaks are to be expected in the coming years, operational agility is now a critical capability for IT teams.

Following any distance learning periods, devices that have been connected to insecure home or public Wi-Fi networks will connect back to the school network. IT teams will have to ensure these devices are malware-free and don't contain sensitive data that could result in a security incident. Learning about problems after they happen is too late. IT teams need advanced visibility into what is happening on school devices to remain proactive and mitigate risk.

Figure 1

% School Districts with Various Learning Models



2. Expansion of 1:1 and Other Student Device Programs Placing Stress on Over-Stretched IT Teams

In 2020, there was an excessive and hurried demand for new devices from education ministries, school districts, and schools across the world in response to impending school closures and the shift to distant learning.[8]

Many schools pulled retired devices back into commission to fill temporary gaps. As a result, many education IT teams are now managing a much larger inventory of devices and applications — with the same or fewer IT staff resources than in previous years. Since these devices are now in students' homes, rather than in the classroom or computer labs, the complexity of endpoint management has increased. This complexity is exacerbated since IT teams themselves are working remotely and cannot physically access devices to assist students, administrators, or teachers.

U.S. state revenues are expected to decrease $750 billion (or 20%) over the next two years.[9] At the same time, school systems face many new pandemic-related costs including food services, personal protective equipment (PPE), and student technology. The U.S. School Superintendents Association (AASA) estimates the new health and safety

[7] School Districts' Reopening Plans: A Snapshot (2020, Aug 28). *EdWeek,* 2020.
[8] The Impact of COVID-19 on the K-12 Education Mobile PC Market. *FutureSource,* 2020.
[9] Projected State Shortfalls Grow as Economic Forecasts Worsen. *Center on Budget and Policy Priorities,* 2020.

expenses alone could cost each district an extra $1.7 million.[10] The Learning Policy Institute estimates the cost of distance learning at about $500 per student.[11] While Federal stimulus packages may help in the short term, continued uncertainty and its impact on longer-term budgets remains.

IT teams will be tasked with accounting for every tech dollar spent to ensure their school budgets are justified.

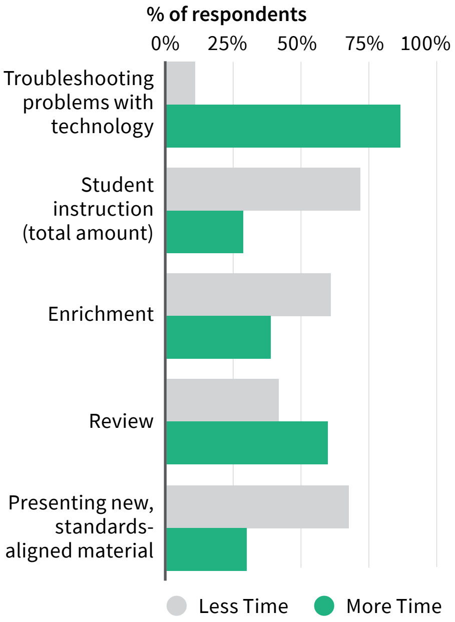
3. Accelerated Adoption of Digital Learning and Collaboration Tools Causing Teacher Frustration

According to a report from October 2019, 93% of U.S. school districts were already using digital learning in at least half of their classrooms every week and 85% of teachers and principals supported the increased use of digital learning in their schools.[12]

Despite this, teachers and students faced some issues when forced to rely solely on digital learning suddenly in the Spring. Nearly nine out of ten teachers reported spending more time troubleshooting technology problems and seven in ten reported spending less time on student instruction during COVID-19 than they did when they were in their physical classrooms.[13]

Figure 2

Recent Changes in Classroom Usage due to COVID-19



**Results show responses from teachers*
SOURCE: EdWeek Research Center survey, 2020

This means that valuable instructional time is being spent tackling technology challenges — either learning the intricacies of a new learning management system or fixing access problems.[14]

Teachers' problems are compounded by the fact that many schools are now operating a remote IT helpdesk. Since IT doesn't always have physical access to devices, troubleshooting and remediating issues is more difficult. After all, tools like Microsoft® System Center Configuration Manager (SCCM) don't always work effectively when devices are off the school network.

4. Keeping Students and Staff Safe and Productive While Off the School Network

With many devices outside the perimeter of the school network, web filtering and other security tools that depend on appliances or the network may become obsolete. As a result, cybercrime in education may continue to increase as bad actors exploit new holes in security measures.[15]

IT teams are tasked with ensuring that students are using devices to learn, while also minimizing the risk of a student accessing inappropriate content on a school-issued device.

These challenges are significant — but not insurmountable.

The following chapters offer insights that can help teams take a more proactive approach to enabling positive learning outcomes for remote students and staff, while protecting them from inappropriate content and malicious threats.

[10] With Budget Cuts Looming, Here's How Districts Will Decide What to Keep or Cut. *EdSurge,* 2020.
[11] What Will It Take to Stabilize Schools in the Time of COVID-19? *Learning Policy Institute,* 2020.
[12] Mission Accomplished: EducationSuperHighway Announces Closure of the K-12 Connectivity Gap. *EducationSuperhighway*, 2019.
[13] How COVID-19 Is Shaping Tech Use. What That Means When Schools Reopen. *EdWeek*, 2020.
[14] How COVID-19 Is Shaping Tech Use. What That Means When Schools Reopen. *EdWeek*, 2020.
[15] Verizon's 2020 Data Breach Investigations Report. *Verizon,* 2020.

Management of School Devices in Distance and Hybrid Environments

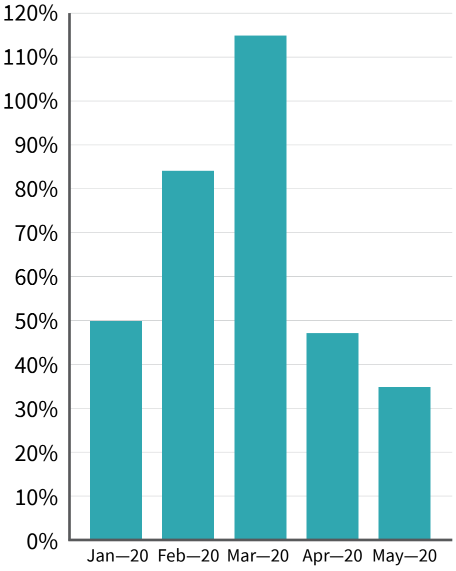
Reliance on endpoint devices to drive learning outcomes has increased. As more devices go home for longer periods of time, IT teams are struggling to manage those devices and ensure their safe return.

Increase in Number of Devices
Over 80% of schools have purchased or plan to purchase more devices to enable distance learning.[16]

In March 2020, Absolute's data uncovered a spike in the number of devices first connecting to the internet as students took home devices that previously remained in the classroom or activated new home-based devices.

Figure 3

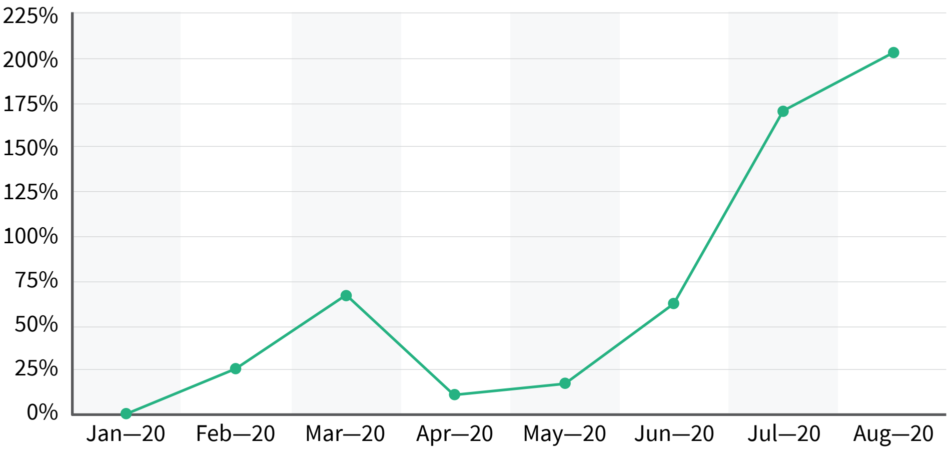
Devices Connecting for the 1st Time



Since January, there has been a 205% increase in the number of new devices first connecting to the internet as schools ramp up inventory to support distance learning in the new school year.

Figure 4

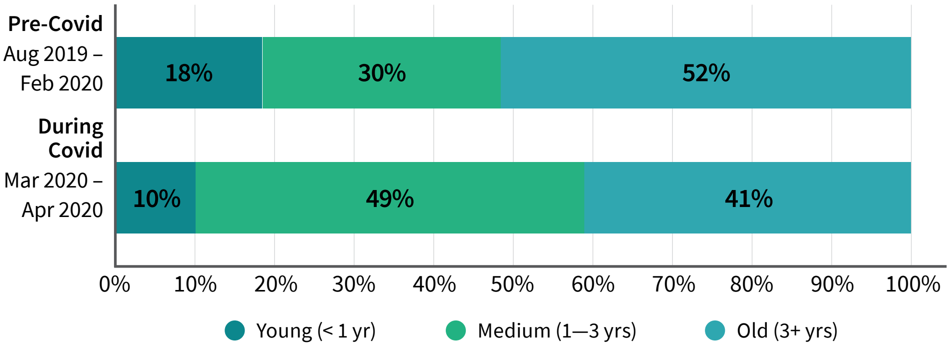
% Increase in Number of Devices 1st Time Connecting vs. Jan 2020



However, the use of older, more vulnerable devices being redeployed to fill the gap is evident in Absolute's data. After February 2020, the number of older devices in school fleets increased by 8%. In an effort to equip every student, teacher, and administrator, we saw IT recommissioning retired devices from storage to meet the demand. It is unlikely that these older devices have the most recent patches, security updates, and application versions installed — increasing the risk factors of an already expanded fleet.

Figure 5

Average Age of Devices Deployed for Remote Learning



[16] Distance Learning Study. *Hanover Research,* 2020.

Decrease in IT Visibility

According to Absolute's data, 20% of all education devices have gone dark or were not online between January and May 2020. Of all new devices deployed in the first half of the school year (July to December 2019), it appears that 14% have not been used at all in the second half of the school year (January to May 2020).

This lack of connectivity could, in part, be a result of the "homework gap," whereby 21.3 million people lack access to broadband in the US[17], including 35% of school-age children[18]. It could also be attributed to stolen, missing, or unused devices.

Increase in Device Drift

According to recent research, 41% of school IT teams said tracking lost or missing devices was a big challenge.[19]

On average, schools had 30 devices go missing at some point in the last nine months. Within two weeks of them being flagged as missing, Absolute played a pivotal role in locating 20% of them. Of stolen devices, 42% of stolen devices were kept by the user despite the school's attempt to retrieve it, 11% were taken from cars, and 8% were taken from homes.

Absolute data shows that, between 2017 and 2020, 65% of stolen devices running Absolute were recovered and returned to schools. When using Absolute's solutions, schools had stolen devices returned to them in an average of 47 days.

While these are high numbers, the acceleration of devices going into education, coupled with the fact that most of these devices are going home, means that this problem will increase exponentially.

> *"We started using Absolute when we had a rash of laptop thefts. Absolute stemmed the thefts and because it was so effective, we now use it on all our endpoint devices."*
>
> **Erik Greenwood**, CTO
> Anaheim Union High School District
> (30,000 devices)

Figure 6

Percent of Active vs. Dark Devices in 2020

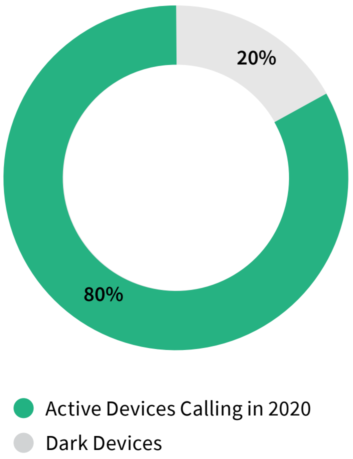


Figure 7

Percent of Stolen Devices Recovered

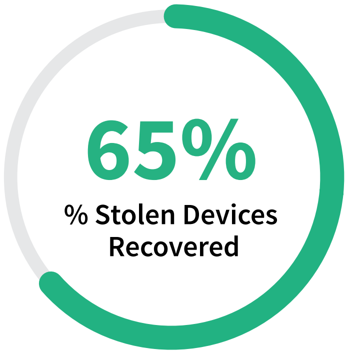


Figure 8

Number of Days to Device Recovery

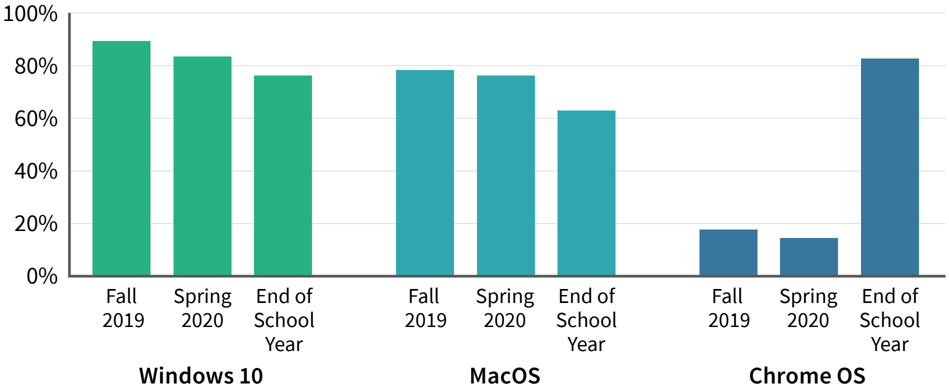
[17] 2019 Broadband Deployment Report. *Federal Communications Commission,* 2019.
[18] Digital Divide Persists Even as Lower-Income Americans Make Gains in Tech Adoption. *Pew Research,* 2019.
[19] Distance Learning Study. *Hanover Research,* 2020.

Preventing Endpoint Vulnerabilities is Challenging

Due to the wide range of device types, operating systems, and applications used in education, managing and patching devices is more challenging than ever. Absolute found that 72% of school endpoints in our sampled data are running operating systems two or more versions old. For example, there was a spike in outdated Google Chrome OS™ versions due to a new version released in early April 2020.

Figure 9

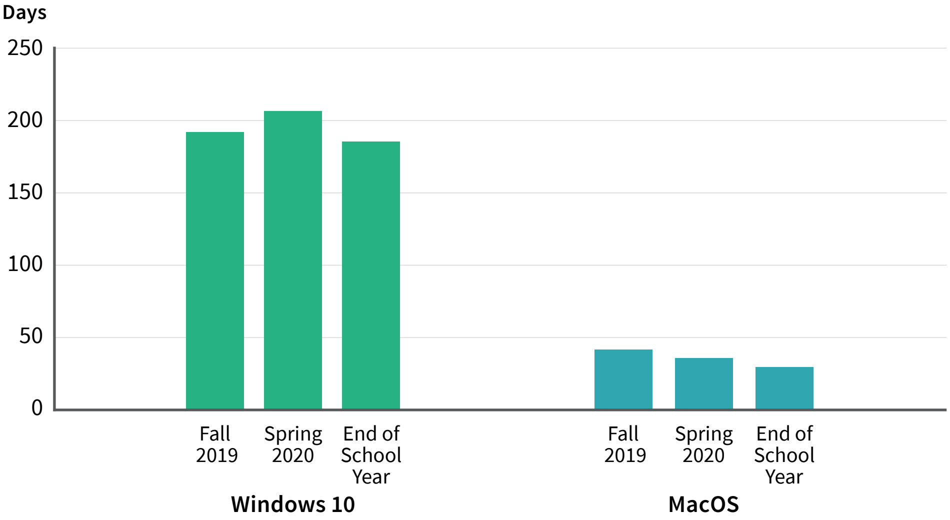
Devices with OS 2+ Versions Behind, by Operating System



According to Absolute's data, the average patch age is 183 days for Microsoft Windows® 10 devices and 31 days for Apple® MacOS. Worryingly, Absolute's data also noted 454 unique patch versions present across Windows 10 devices alone. Outdated operating systems present an opportunity for hackers to access school devices with ransomware.

Figure 10

Average Patch Age by Operating System



Visibility into the Remote Classroom

In addition to managing devices and ensuring students and staff are protected online, IT teams require visibility into device usage so they can prove their technology spend is being used to drive effective learning outcomes.

Device Usage is Increasing
As device usage has increased to support the new education model, Absolute noted a 61% increase in heavily used devices and a 28% rise in active daily hours since fall 2019.

Figure 11

Percentage of Devices Used Heavily (4 – 8 Hours / Day, over 30 day period)

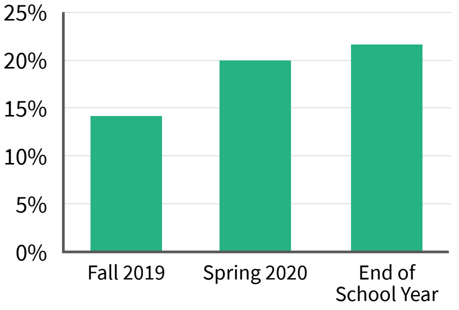
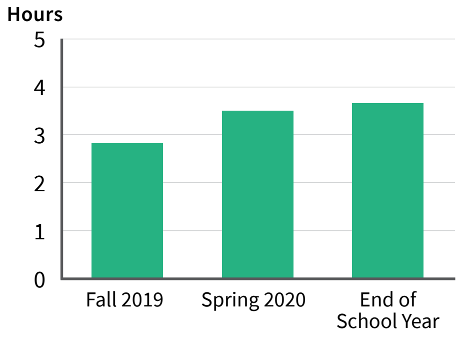


Figure 12

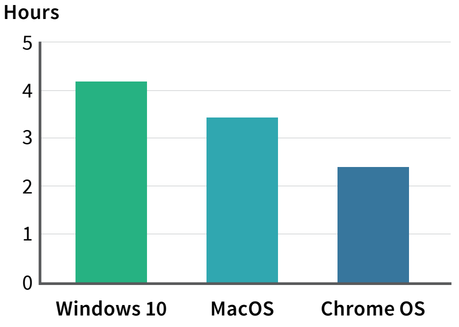
Average Active Daily Hours of Use (over 30 day period)



Absolute's data indicates that devices running Microsoft Windows 10 and Apple MacOS see heavier daily usage than devices running Chrome OS. This is likely due to these devices being used by higher grades (grade six and upwards). Students in higher grades are typically assigned more online classroom instruction and spend more time on their devices, given the nature of their studies. There is also an increased acceptance of older students spending more time on devices.

Figure 13

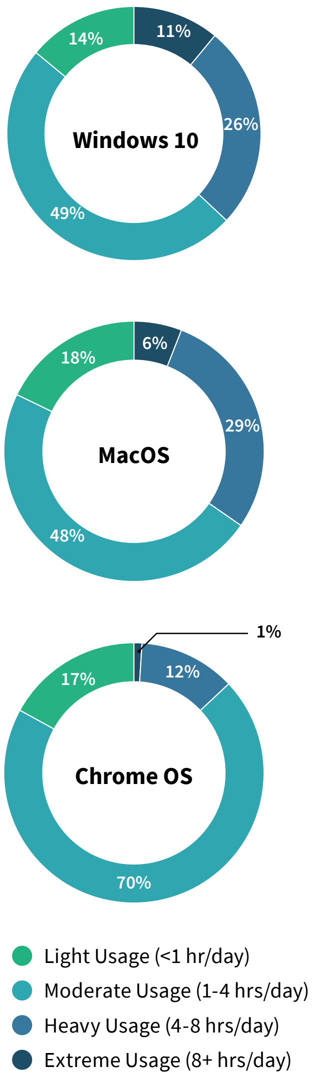
Average Active Daily Hours of Use (during April 2020)

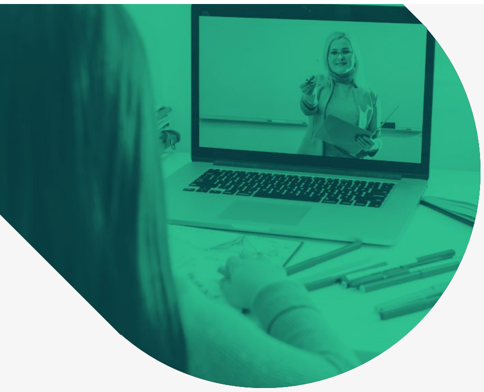


Absolute's data indicates that the majority (70%) of devices running Google Chrome OS are used between one and four hours per day. Comparatively, devices running Windows 10 and Apple MacOS are more likely to be used more than four hours per day.

Figure 14

Hours of Device Usage by OS





Customer Insight

> *"Absolute Web Usage has provided us with much needed insight into how our district utilizes both paid and free applications within our system. The weekly snapshots allow me to dive deeper and investigate websites that have high traffic as well as those websites that seem to have bypassed our web filter."*

Eric Ramos
Chief Technology Officer
Duarte USD

Duarte Unified School District protects students while facilitating student engagement

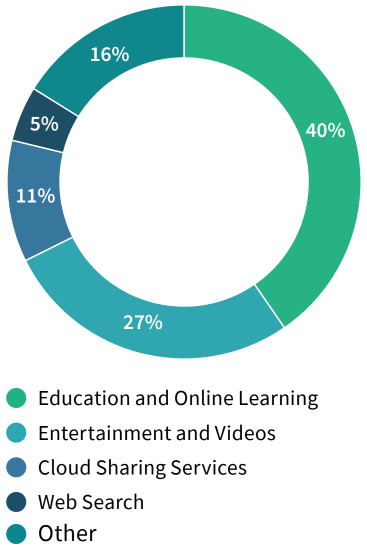
Duarte Unified School District (USD) needed to ensure their students had access to devices and online curriculum, and that their teachers had visibility into student engagement and where gaps in connectivity may exist. They are leveraging Absolute Web Usage, which allows administrators to measure how engaged their students are with online curriculum and gain detailed insights into which learning resources are underused.

Devices are Mainly Used for Learning

As of May 1, 2020, Absolute's data indicates that 40% of time online was spent on, though this time was spent on education and learning applications. Entertainment and videos accounted for 27%, including YouTube, which is often used for learning.

Figure 15

% Average Daily Time Spent Online by Category (week ending May 1, 2020)

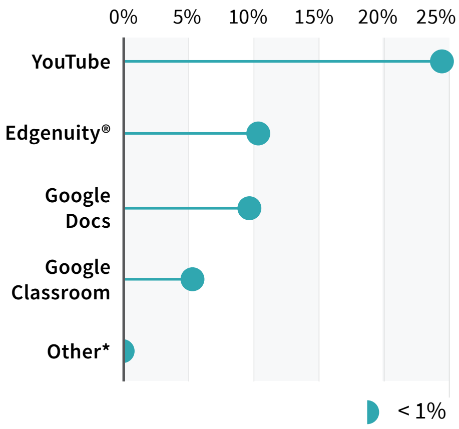


More time is spent on YouTube than on any other education-orientated website. However, YouTube content includes both educational and non-educational material, so it's unclear how much time is actually spent learning on YouTube. After YouTube, Edgenuity®, Google Docs™, and Google Classrooms are where students are spending most of their time.

Absolute's data indicates that an average of one hour per day was spent on sites with inappropriate content. Despite web filters, harmful and inappropriate online content is still being consumed on school-issued endpoints.

Figure 16

% Average Daily Time Spent by Platform (week ending May 15, 2020)



*Other includes these platforms, each at less than 1%: Cool Math Games, Schoology®, Class Link, Khan Academy, Quizlet, Seesaw, Achieve 3000®, I-ready™, Flip Grid, Class Dojo.

Keeping Student and Staff Devices and Data Safe

Despite being among the top three priorities for IT leaders in education[20], cybersecurity remains a challenge in schools, exposing staff and students to threats. As described in chapter two, the threat is amplified by the complexity of device and application management as schools reacted to the COVID-19 pandemic.

Today, ransomware accounts for approximately 80% of malware infections in education, up from 48% in 2019, and unwitting insiders are responsible for 33% of incidents[21]. Interestingly, education is the only sector where malware distribution to victims was more common via websites than email[22].

This year, Absolute noted a spike in the number of devices with remote management applications installed, which may also be responsible for the rise in ransomware in schools[23]. It should be noted that schools are particularly vulnerable to ransomware attacks because malicious actors find them to be easy and unwitting targets.

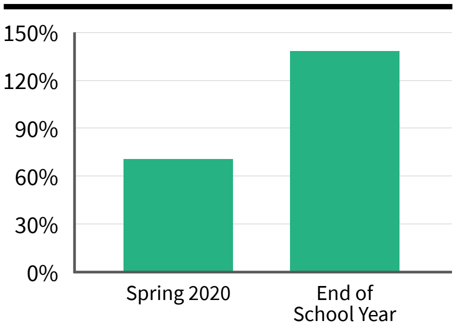
The circumvention of security controls on school devices (which continues to get more popular) may also be to blame. VPN or web proxy applications with names like ‘IP Vanish,’ ‘NordVPN,’ ‘CroxyProxy,’ and ‘Hide My Ass’ are purposely designed to evade web filtering and other content controls. Absolute’s data indicates that 46% of schools have at least one device that uses rogue or non-authorized VPN or web proxy applications — but it only takes one vulnerable device to create a security incident. This is up four percentage points from last year (42%).

New EdTech Creates More Device Complexity

Absolute’s data noted a 141% increase in the number of devices with collaboration software installed from fall 2019 to May 2020 including popular applications like Cisco Webex®, Zoom, Skype™, Microsoft Teams™, Slack®, Blue Jeans, Pidgin, Flock™, GoToMeeting®, Microsoft Lync™, and Join.Me.

Figure 17

% Increase in Devices with Collaboration Apps Installed (compared to Fall 2019)



With these new applications being rolled out so quickly, it has been a challenge for IT teams to ensure they are secure, patched, and that sensitive student data is protected.

Remote Management Poses Ransomware Threat

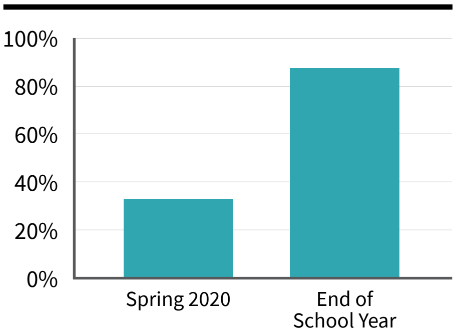
In an attempt to manage the increased number of devices and applications off the school network, IT is deploying remote management solutions. Last year, Absolute found that over half of K-12 schools and districts (53%) rely on native client/patch management tools. This year, we noted that between early in the 2019/2020 school year and the school year ending, there was an 87% increase in the number of devices with remote management applications.

These include tools like RemotePC™, Zoho Assist, LogMeIn® Pro, Connectwise® Control, Parallels® Access, TeamViewer, Chrome Remote Desktop, Remote Desktop Manager, Splashtop®, RemoteUtilities® for Windows, and GoToMyPC®.

However, schools must be wary of remote desktop applications. In June, the U.S. Federal Bureau of Investigation sent a private industry notification (PIN) alert to schools about increasing attacks from ransomware gangs that abuse RDP connections to break into school systems[24].

Figure 18

% Increase in Devices with Remote Management Apps Installed (compared to Fall 2019)



[20] CoSN K-12 2020 Hurdles and Accelerators. *Consortium for School Networking,* 2020.
[21] Verizon’s 2020 Data Breach Investigations Report. *Verizon,* 2020.
[22] Verizon’s 2020 Data Breach Investigations Report. *Verizon,* 2020.
[23] How to Protect your Organization and Remote Workers Against Ransomware. *TechRepublic,* 2020.
[24] FBI Warns K12 Schools of Ransomware Attacks via RDP. *ZDNet,* 2020.

Application Persistence™ Improves Anti-Virus Security Compliance Rates
Absolute's data found that education customers with Application Persistence for anti-virus (AV) enabled on their devices had AV compliance rates 28 percentage points higher than those seen on the average device (without App Persistence running). These customers also saw an increase of eight percentage points in the number of devices with an AV app properly installed.

Figure 19

% of Total Devices with AV App in Compliance

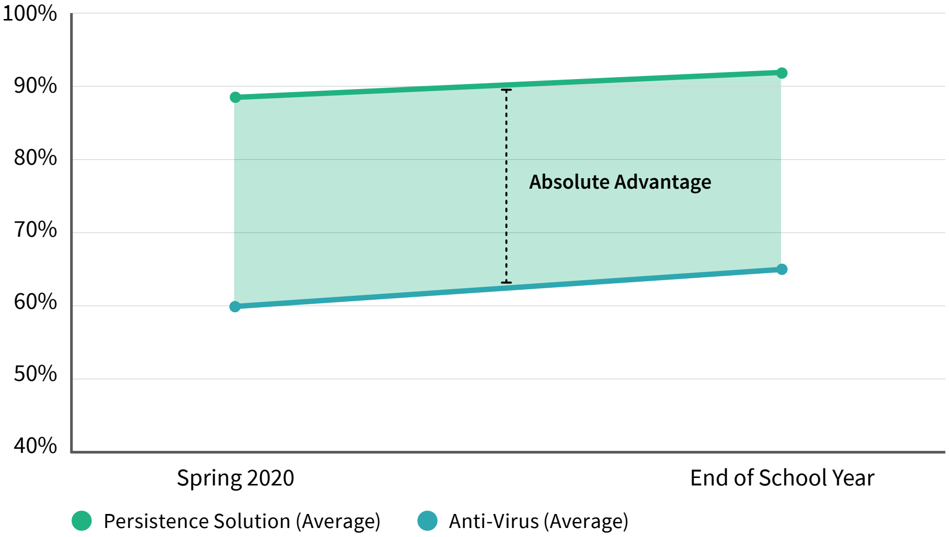
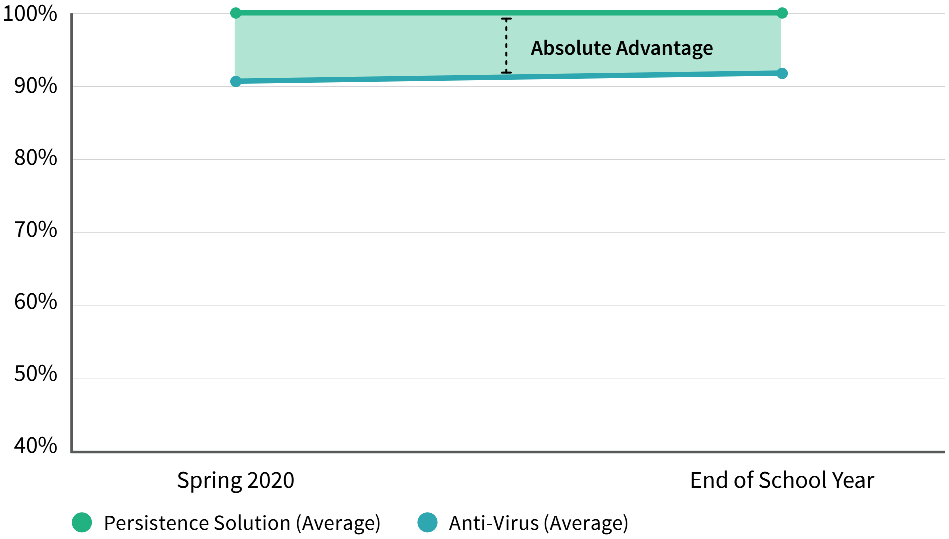


Figure 20

% of Total Devices with AV App Installed



Customer Insight

> *"With the right technology resources in place, including Absolute, we can ensure an exceptional, seamless remote learning experience."*

Dean Phillips
Director of Technology
PA Cyber Charter School

PA Cyber Protects Mission-Critical Apps with Absolute's Endpoint Resilience

PA Cyber Charter School, a pioneer in online learning, selected Absolute for control over their fleet of 15,000 devices. They also use Absolute's Application Persistence™ service to ensure an always-on, two-way connection to their IT management solution, which they use to remotely push out security patches, new applications and scripts.

Enabling the "New Normal" in Education

Since March 2020, IT teams have been tasked with enabling a new, more agile education model. With the situation still changing constantly, IT teams may liken their strategies to "building a plane as it's flying." The summer offered many teams a reprieve to reset and plan for the "new normal" in education, a normal that must be secure, agile, and efficient.

With the new school year already in full swing, IT teams can now focus on measuring the success of their efforts and optimizing their strategies as they go. Here are some metrics that we expect will be top of mind for IT:

Goals	What IT Should Report on	Capabilities Required
Mitigating Device Drift	1. Are devices still in the district? 2. Are devices lost or stolen? 3. Can I take action on missing devices? 4. Can I improve my device recovery rate?	• Geolocation • Geofencing • Missing Devices Report • Freeze • Call-In History Reports • Investigations and Recovery • Persistence® technology embedded in firmware[25]
Security	1. When devices connect back to the school network after being on home networks, will they be safe — or introduce risk? 2. Will devices contain sensitive family data?	• AV Compliance/Install Rate Reporting • Scan for Sensitive Data
Facilitating Distance Learning	1. Are online learning tools being used as expected? 2. Which ones have the greatest adoption?	• Web Usage Reporting
Ensuring Endpoint Resilience	1. Can IT manage, repair, and remediate IT issues when devices are off network and IT staff is working from home?	• Reach Scripting (push applications, change device settings, etc.) • Application Persistence[25] • Detailed Device Data Reporting (troubleshooting and investigation)

Absolute's complete Endpoint Resilience platform supports safer, smarter, and more secure learning environments — whether in-person, remote, or hybrid — by providing IT teams with the critical controls and valuable data they need to make important decisions about asset management and security.

[25] https://www.absolute.com/platform/persistence/

2020 signals a new chapter in education. The challenges we are seeing are not a minor blip — there will be no return to the pre-virus status quo. As distance learning becomes a valuable part of a long-term strategy for student education, digital resiliency will become a key performance indicator (KPI) for schools.

Before the COVID-19 pandemic, school IT teams were already overwhelmed with the complexity of managing and securing student devices and one-to-one programs, not to mention the need to justify every dollar spent.

The “new normal” has amplified these challenges, as IT teams are faced with complex and varied device and application environments, a lack of visibility into device usage and student safety, insufficient or reduced budgets and resources, and incredibly tech-savvy students.

Today, IT teams must address these challenges while supporting the seamless operation of distance and hybrid learning models. As such, IT leaders should aim to:

Gain Visibility and Control of Devices

When devices are not property secured, visibility and control becomes even more important. The imperative for IT to remotely reach devices to ensure proper usage, secure student and staff devices, and the protect the school network become preeminent. Moreover, these critical capabilities are needed to allow schools to remain accountable for technology spending.

Use Device Intelligence to Inform Decisions

Powerful device and application health and usage analytics can drive decision-making in areas like professional development training and software and hardware technology purchasing decisions.

For example, teams may find that the money they spend on web filtering tools is wasted since these tools are insufficient off the school network. Perhaps they can redirect those funds to a tool that will better address the new reality.

Leverage Endpoint Resilience to Support Student Safety and Privacy

School IT teams need to ensure that their schools can run effectively and securely, regardless of the learning model they choose to adopt. To do this, they need to ensure their approaches are built on Endpoint Resilience — an emerging and critical KPI for school security strategy.

Endpoint Resilience requires a digital tether that provides an unbreakable connection between the device and the school that manages it. Its purpose is to be the lifeline and single source of truth: to know where devices are, what which applications are installed and healthy, and where there are vulnerabilities. Absolute’s Endpoint Resilience solutions deliver the ability to persist and self-heal the mission-critical applications and controls on that device, should it be necessary, whether the device is at home or at school.

For real-time data on the state of the digital district, keep an eye on **Absolute’s Coronavirus Response Dashboard**.

Customer Insight

> *"Absolute will help us on the software side and the hardware side, frankly. We're discovering new ways to use Absolute to help us manage our various systems."*

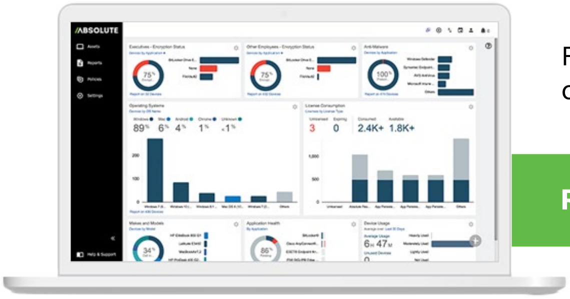
Erik Greenwood
CTO
Anaheim Union High School District
(30,000 devices)

With Absolute, Anaheim Union High School District ensures complete visibility and control of 30,000 devices.

Because the future of learning remains somewhat in flux, Anaheim Union has focused on honing the mechanics of a few different learning models: in person, fully virtual or a hybrid approach. With the capabilities Absolute is delivering, the district is much more prepared to roll out whatever model makes the most sense at the time.

Absolute is the industry's only undeletable defense platform, embedded in the firmware of more than a half billion devices and deployed across more than 12,000 customer organizations. This unique position enables our customers to look at endpoint protection holistically – to see the complete picture and create a feedback loop that enables IT and security teams to eliminate blind spots. We're defining the next generation of endpoint security — true Endpoint Resilience.

To learn more about how your organization can achieve Endpoint Resilience with Absolute, contact an Absolute sales representative at **sales@absolute.com** or 1-877-600-2295, or request a demo **here**.



Find out how our solutions can benefit your organization.

REQUEST DEMO

Report Research Methods

This report leverages anonymized data from millions of Absolute-enabled devices active across approximately 10,000 schools and districts.

Types of anonymized endpoint device data that was analyzed include:

- Device operating system and latest version installed
- Number of security applications installed
- Names and types of security applications installed
- Compliance rates of security applications, based on Absolute-defined parameters

Pre-COVID-19 insights use data points collected November to December, 2019. Insights that reflect trends or changes seen in post COVID-19 outbreak time frame use data points collected from late March through late May, 2020.

This report also includes certain data and information from trusted public third-party sources, which are cited accordingly.

About Absolute

Absolute serves as the industry benchmark for Endpoint Resilience, visibility and control. Embedded in over a half-billion devices, the company enables more than 13,000 customers with Self-Healing Endpoint® security, always-connected visibility into their devices, data, users and applications — whether endpoints are on or off the corporate network — and the ultimate level of control and confidence required to support the modern enterprise. For the latest information, visit **www.absolute.com** and follow us on **LinkedIn** or **Twitter**.

EMAIL:
sales@absolute.com

SALES:
absolute.com/request-a-demo

PHONE:
North America: 1-877-660-2289
EMEA: +44-118-902-2000

WEBSITE:
absolute.com