

# Three key trends impacting K-12 IT and security

What was accomplished and what's next for the teams transforming education



# Executive summary

While the global pandemic certainly affected every industry, some sectors and professions experienced the impact more than others—and face a higher degree of uncertainty about the future as a result.

While healthcare, hospitality, and travel may immediately spring to mind, the challenges faced by another group cannot be overstated—the IT teams empowering our nation's schools.

Under the watchful eyes of government regulators—and parents across the nation suddenly home each day with their school-age children—their immediate priority was to keep students learning and in social—albeit virtual—contact with their peers.

Even organizations with sophisticated IT infrastructures found meeting the unanticipated demands brought about by the pandemic to be a daunting task. For IT teams in K-12, tasked with “building the plane while it was flying,” it was downright Herculean.

And yet the result of their efforts was profound: not only maintaining continuity of education within individual schools and districts, but simultaneously effecting the digital transformation of an entire industry.

This edition of the Endpoint Risk Report for K-12 uncovers the solutions and challenges brought about by this massive undertaking. Featuring anonymized data collected from over 10,000 schools and districts, it explores both what was accomplished—and where IT teams in education should prioritize their efforts for the next school year and beyond.

Throughout 2020 and 2021, school districts expanded their device fleets by hundreds or thousands, in many cases introducing new operating systems or aging machines to the mix.

The scramble to stand up 1:1 programs meant that standard procedures were sometimes overlooked, with the resulting lack of visibility placing new management and security challenges on already-taxed IT teams.

Digital learning was embraced, with devices used more frequently—and from more locations—than ever before, but introduced new requirements to monitor adoption, justify expenditures, and ensure the safety of students online.

New applications, delays in patching, and failing security controls added complexity and vulnerabilities to environments where security had often been an afterthought—making education the number one target for ransomware and placing student and school safety at risk.

**Three notable trends highlight the work that remains:**

- › 1:1 acceleration leaves a logistical nightmare in its wake
- › The rise of digital learning introduces demands and risks
- › Complexity takes security from afterthought to imperative

TREND 1

1-to-1 acceleration leaves a  
logistical nightmare in its wake

### Technology roll-out on hyperdrive

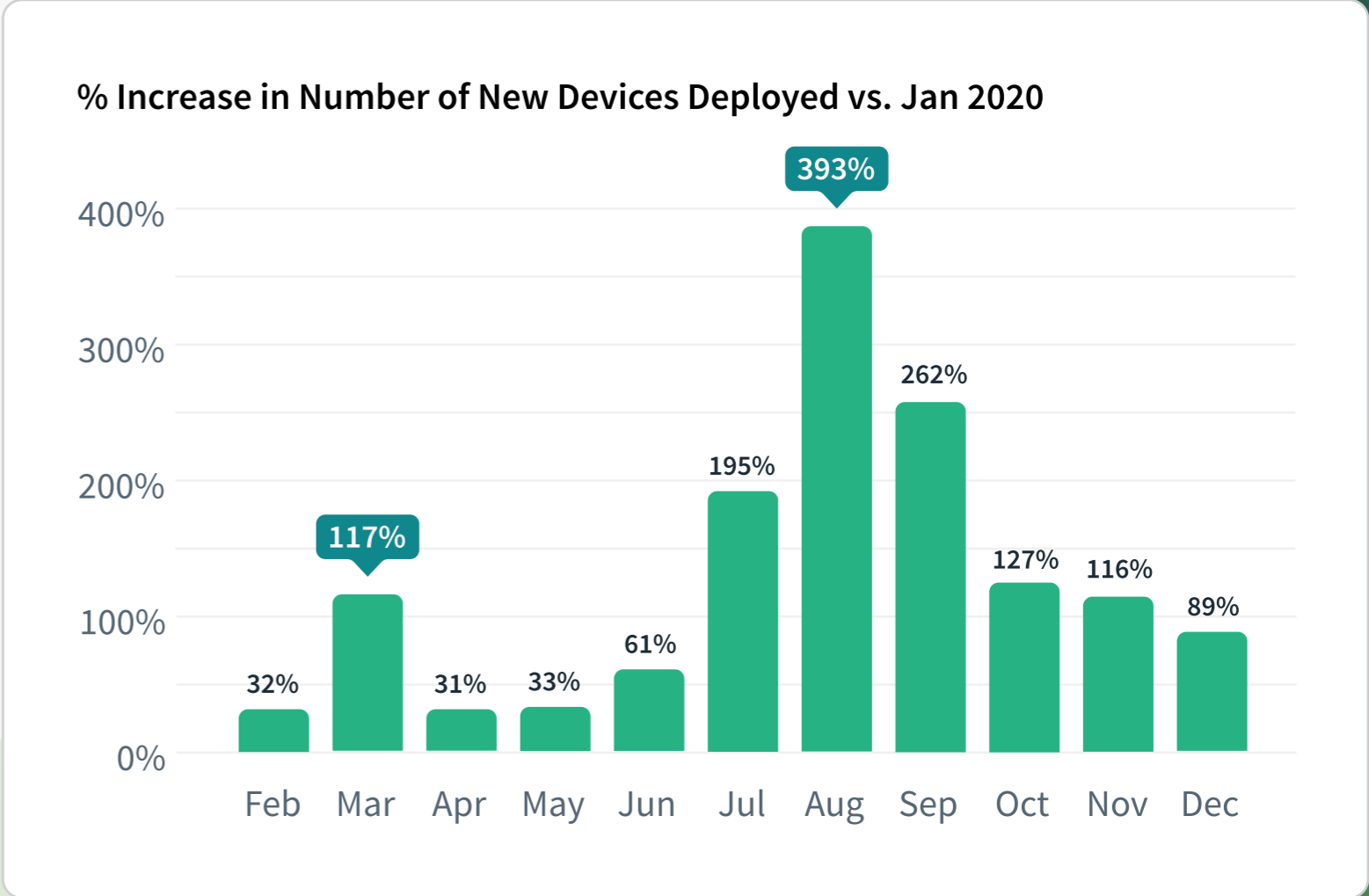
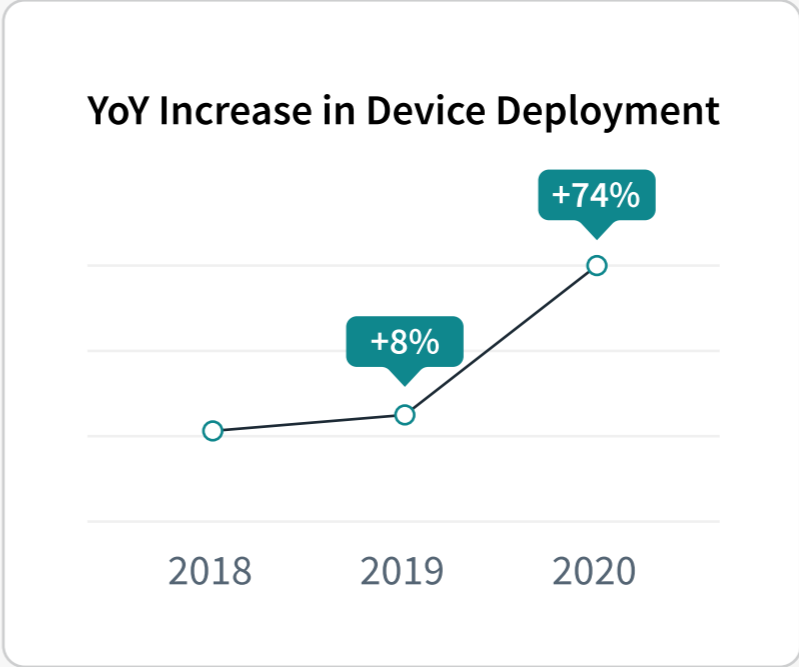
Fueled by multibillion-dollar emergency funds such as the CARES Act, CRRSA, and the American Rescue Plan, 20/21 was the school year 1:1 programs went mainstream.

In a 2021 study by EdWeek Research Center, 42% of districts reported purchasing devices for every student, with 55% purchasing them for at least some.<sup>1</sup>

In the same survey, district leaders reported that true 1:1 programs (one student per device) were now in place for 90% of middle and high schoolers and 84% of elementary students, up from 66% and 42% respectively, prior to the pandemic.

Within K-12 environments using Absolute, the number of devices deployed spiked several times during the pandemic—often correlating with new funding disbursements or school terms—increasing 74% in total from 2019 to 2020.

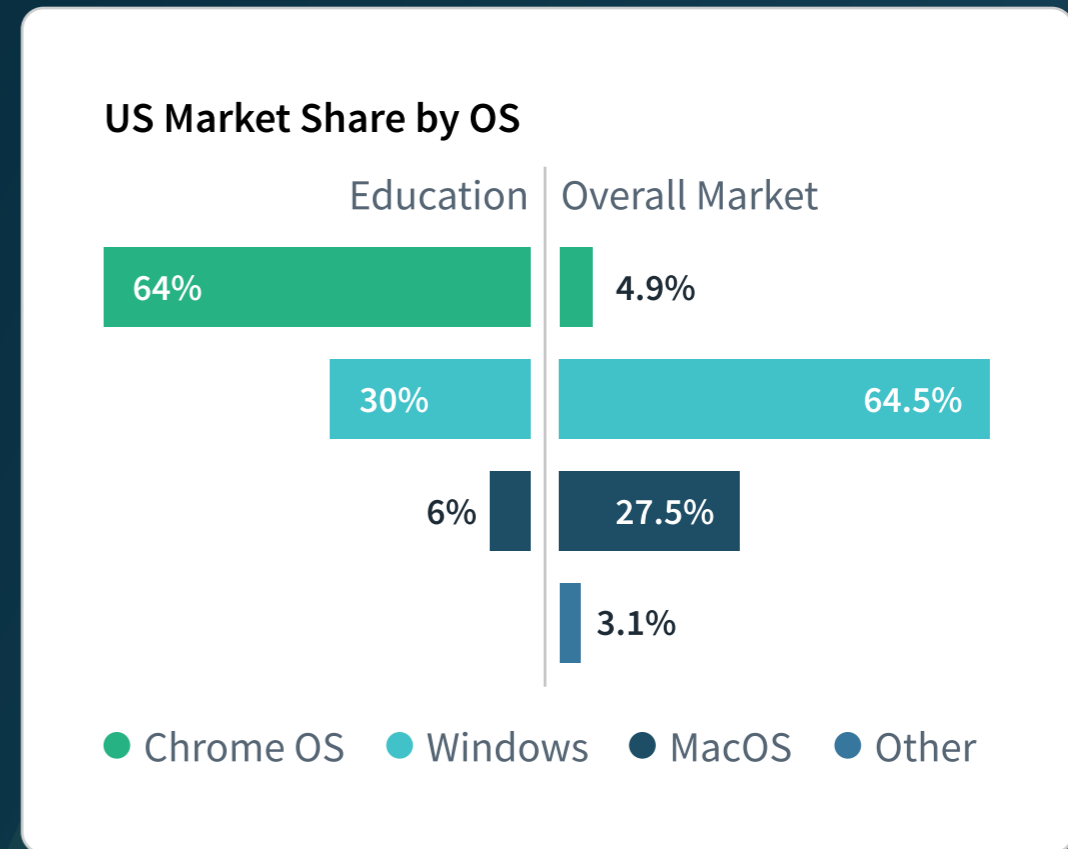
<sup>1</sup> [EdWeek Research Center survey, 2021](#)



Chromebooks strengthened their leadership position, as schools scrambled for budget-friendly, easily managed devices. It's estimated that 64% of devices in education are now Chromebooks<sup>2</sup>, particularly notable as they represent only 4.9% of the market overall.<sup>3</sup>

New deployments began to level out at the beginning of 2021—a result of both the rush to secure devices at the start of the pandemic, and the subsequent supply shortages it entailed. As of March 2021, 31% of districts were still waiting for at least some of their purchased devices to arrive.<sup>4</sup>

For many, that meant keeping older devices in circulation longer than intended or introducing new manufacturers and operating systems into their environment.



<sup>2</sup> [IDC PCD Tracker 2020, U.S. K-12 and Higher Education \(excluding tablet sales\)](#)

<sup>3</sup> [StatCounter Desktop Operating System US Market Share, 2020](#)


<sup>4</sup> [EdWeek Research Center survey, 2021](#)

### Really remote learning environments

While we may think of 20/21 as “the year the world went home,” the reality in education was somewhat more far-reaching—as evidenced by Absolute’s aggregated geolocation data.


In spring 2021, 47% of devices were located more than 25 miles from their school or district, compared to 27% in spring 2020. Many wandered further afield, with 21% over 500 miles away, up from 13% the previous year.

Year-over-year movement increased by 48%, contributing to a 45% increase in devices reported as missing or stolen in spring 2021 versus spring 2020.

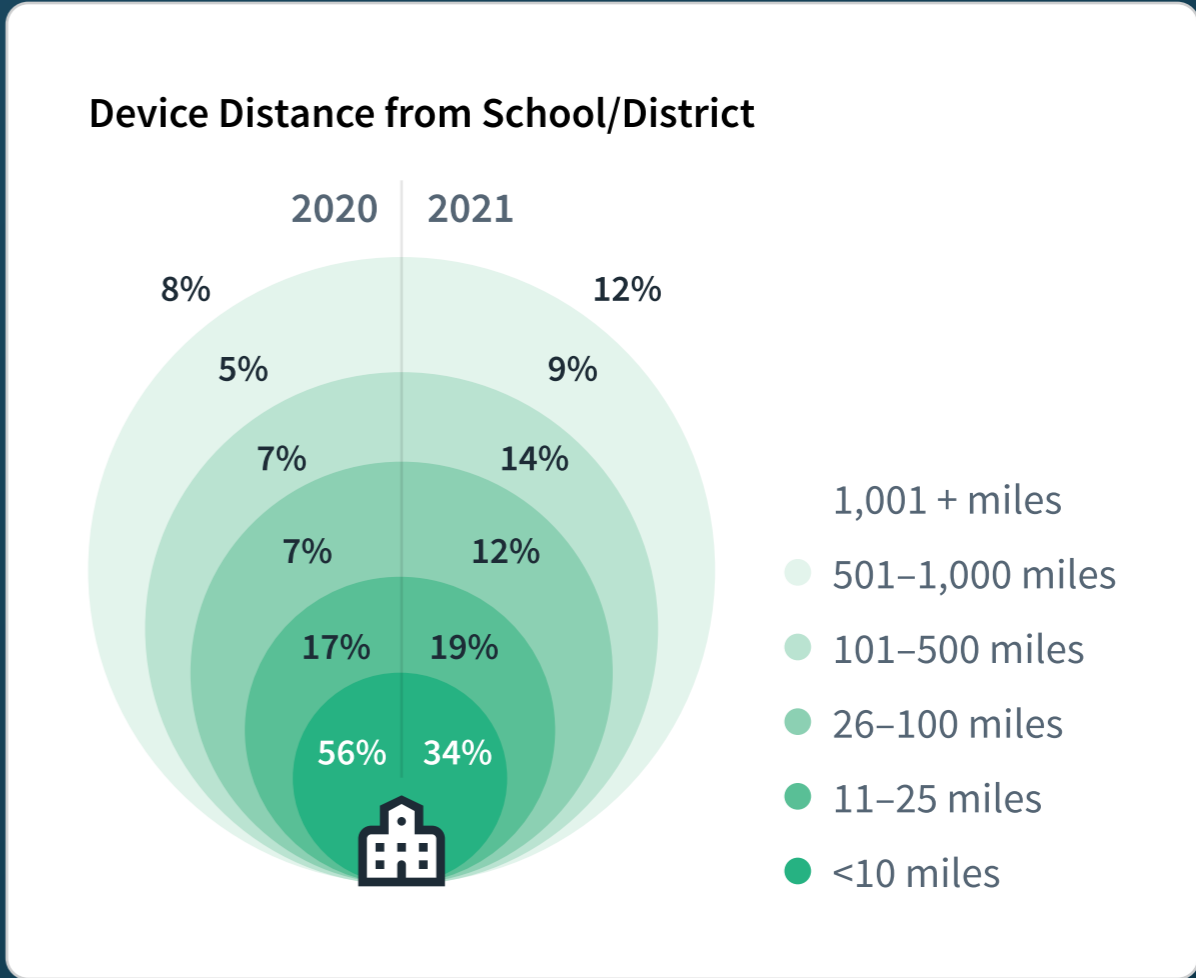


**48%** increase in device movement YoY

---



**45%** increase in lost or stolen devices



Inevitably, the pace and scale of the roll-out has heightened existing challenges for IT teams, and the long-term impact is only now being considered.

With asset accountability and lifecycle management both more important—and more arduous—than ever, IT teams should prioritize achieving visibility and control of every device, regardless of type or location.

Supporting an expanded user base and operating environment—often without additional IT resources—will require efficiencies in platforms and processes, and automation should be applied wherever possible.

And, with funding audits looming, measures to justify budgets and correlate allocation to learning outcomes cannot be overlooked.

**“We started using Absolute reporting as a sanity check against our physical inventory. Now, the Absolute report is our inventory.”**

Kurt Madden, CTO,  
Fresno School District  
**100,000+ devices**





A young girl with long dark hair is wearing large white headphones and holding a tablet computer. She is sitting at a desk with a laptop and several books. The background is a soft-focus office or study environment. The entire image has a teal overlay.

TREND 2

The rise of digital learning  
introduces demands and risks

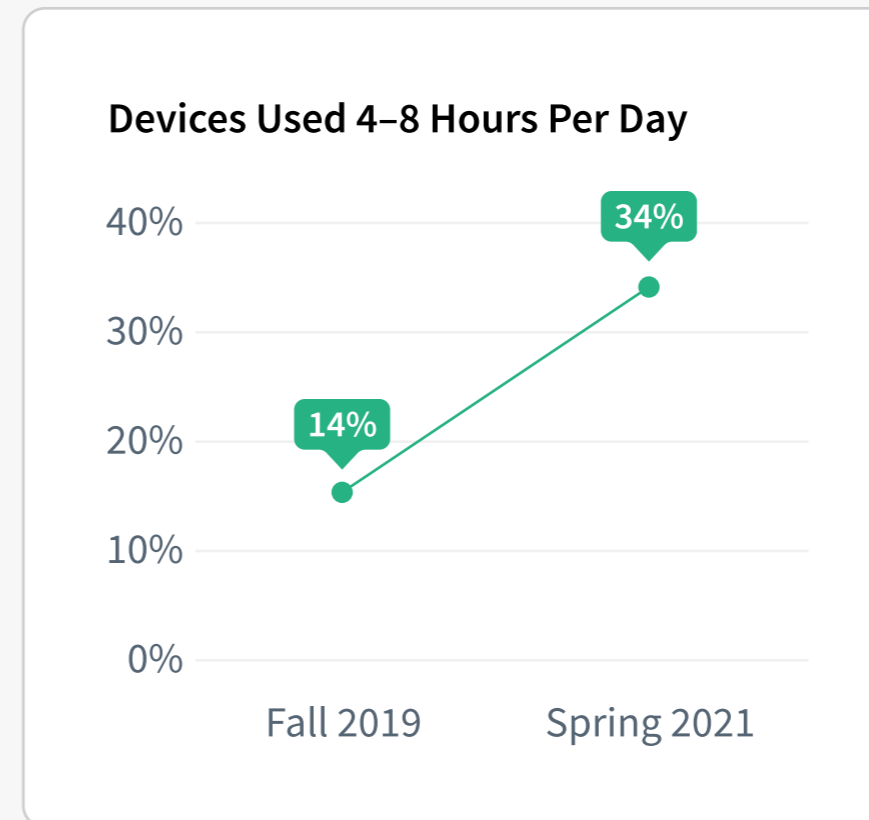
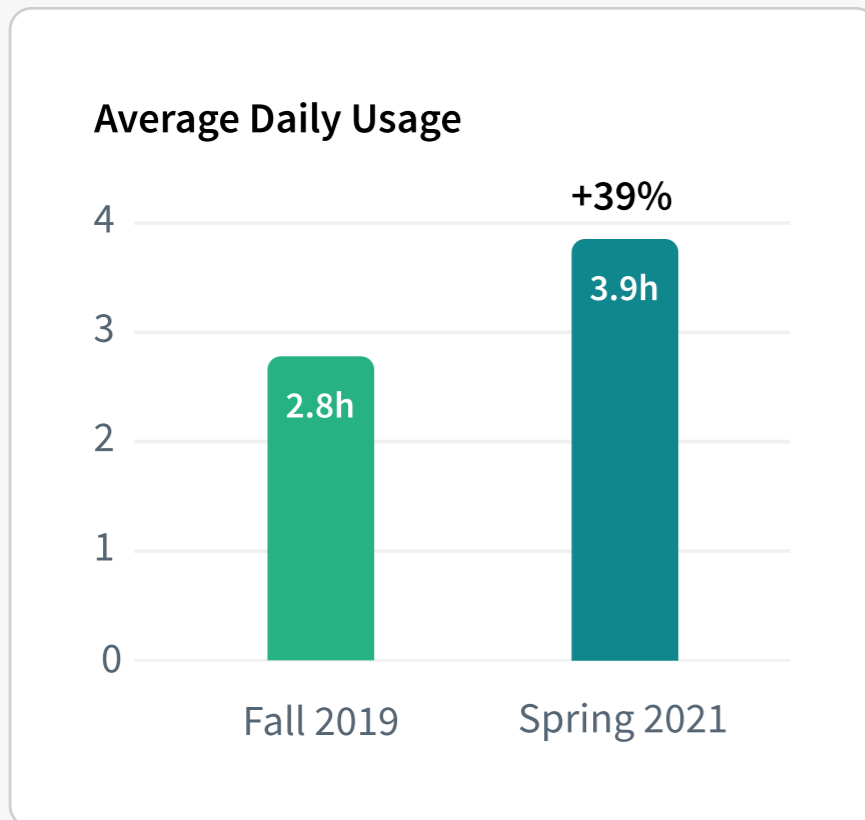
### Less Roblox, more learning

Maintaining productivity and performance were universal concerns during the pandemic—but perhaps felt nowhere so acutely as in our school system.

Beyond the challenge of getting appropriate technology into the hands of every student and faculty member, the ability to remotely engage a young audience prone to digital distraction was a great unknown.

The result? Like the rest of the world, teachers—and students—rose to the occasion.

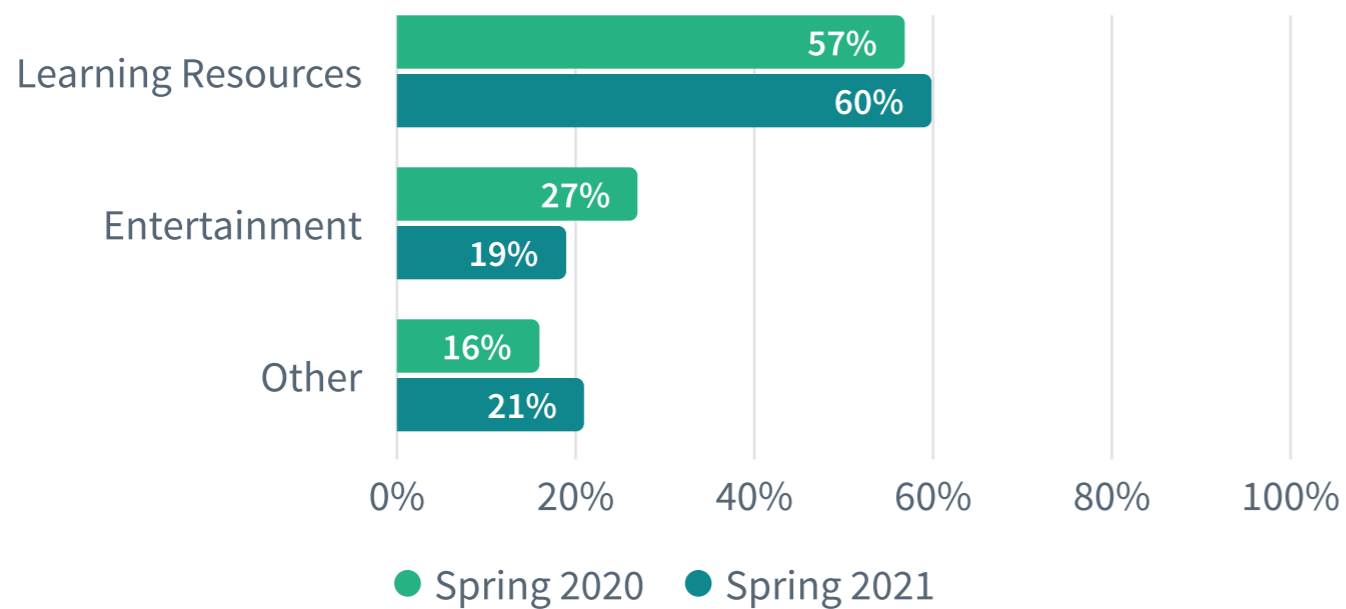
From fall 2019 to spring 2021, online activity increased by 39% overall—consistent across both student and faculty devices—with the number of those used heavily (four to eight hours per day) more than doubling.



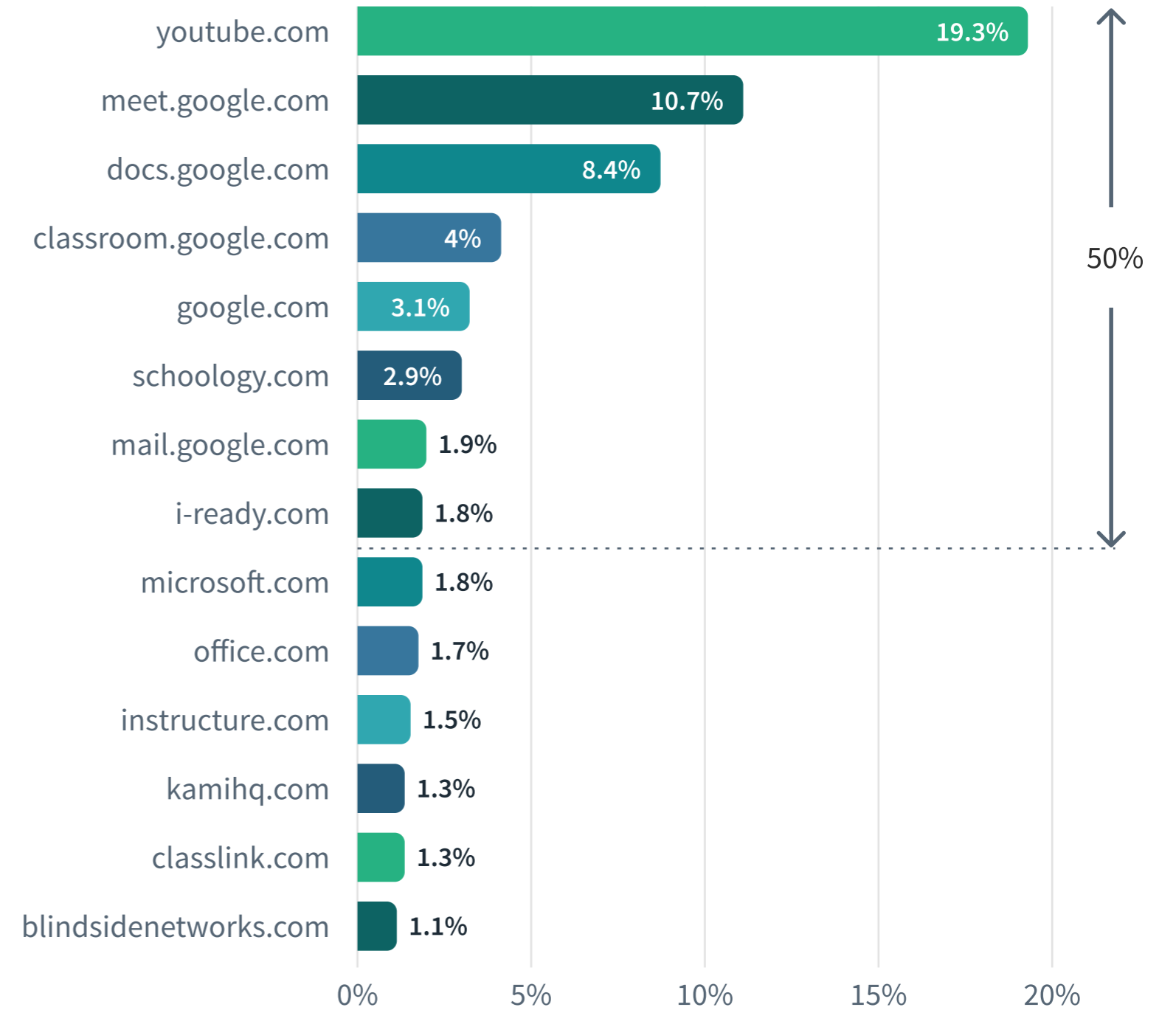
More importantly, the percentage of time online actively utilizing educational resources across students and faculty increased from 57% in 2020 to 60% in 2021, accompanied by an even greater decrease in time spent on entertainment sites, from 27% to 19%.

Google dominated in both education and entertainment, with almost half of all time online spent on their collaboration and education platforms or YouTube.

**Time Online by Category**



**Most Used Sites by Time Spent Online**





### Lurking in the shadows

Beyond these positive trends, 21% of activity in 2021 took place outside established education or entertainment resources—potentially by other household members.

Even appropriate learning activities increasingly occur on unauthorized sites, as teachers and parents seek to supplement digital curricula still in their infancy that have left many students unchallenged. Driven by the pandemic, the global market for private tutoring, or “shadow education,” is expected to reach \$218B by 2027.<sup>5</sup>

5 [Global Private Tutoring Industry](#), Reportlinker, 2020

Given the importance of technology's role in the modern classroom—wherever that may be—understanding online activity and device usage is now necessary to optimize the educational experience and justify current and future expenditures.

With learning outcomes, student safety, and budgets on the line, K-12 systems should incorporate tools that provide the ability to monitor and measure when and how devices are used and take action when necessary.

**“We were able to provide the board with quantitative information about device utilization that drives consensus so the budget could be approved. Also, peace of mind with security, privacy and theft recovery.”**

Dr. Rich Contrartesi, CIO, Loudoun County Public Schools  
78,000 students



TREND 3

Complexity takes security  
from afterthought to imperative

## Education's fourth "R"

In education, cybersecurity is rarely top-of-mind—until a major incident occurs. Yet, according to the FBI, schools are now the top targets for cybercriminals, resulting in ransomware attacks, data theft, and the disruption of online learning.<sup>6</sup>

57% of all reported ransomware attacks in August and September 2020 were targeted at K-12, up from 28% for the period from January through July.<sup>7</sup>

New attack vectors introduced by the complexity of evolving learning environments illustrate why, for those seeking illicit financial gain, schools are an attractive target.

<sup>6</sup> [Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data](#), Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC), 2020

<sup>7</sup> Ibid



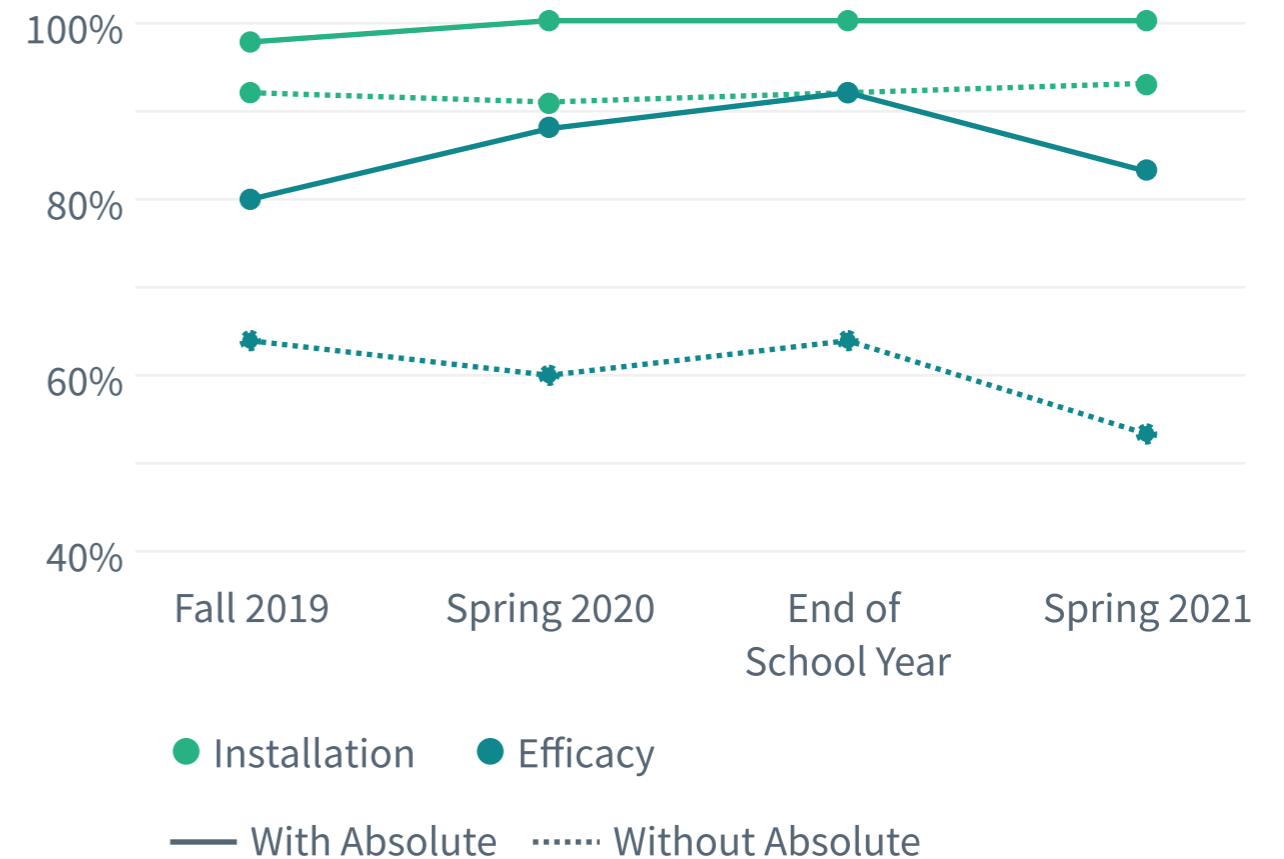
### Complexity is a vulnerability

There is now an average of 6.7 applications to facilitate online learning, including 5.4 security controls such as VPN, anti-virus and anti-malware, per device— a notable difference from the 11.7 security apps per device average in corporate environments, despite K-12 school systems now facing enterprise-level threats.

Even still, every app adds friction to the operating environment, increasing the likelihood of their collision or decay.

Underscoring this point, only 53% of anti-virus applications studied were operating effectively. When Absolute was enabled to allow applications to autonomously maintain effectiveness, that number rose to 83%.

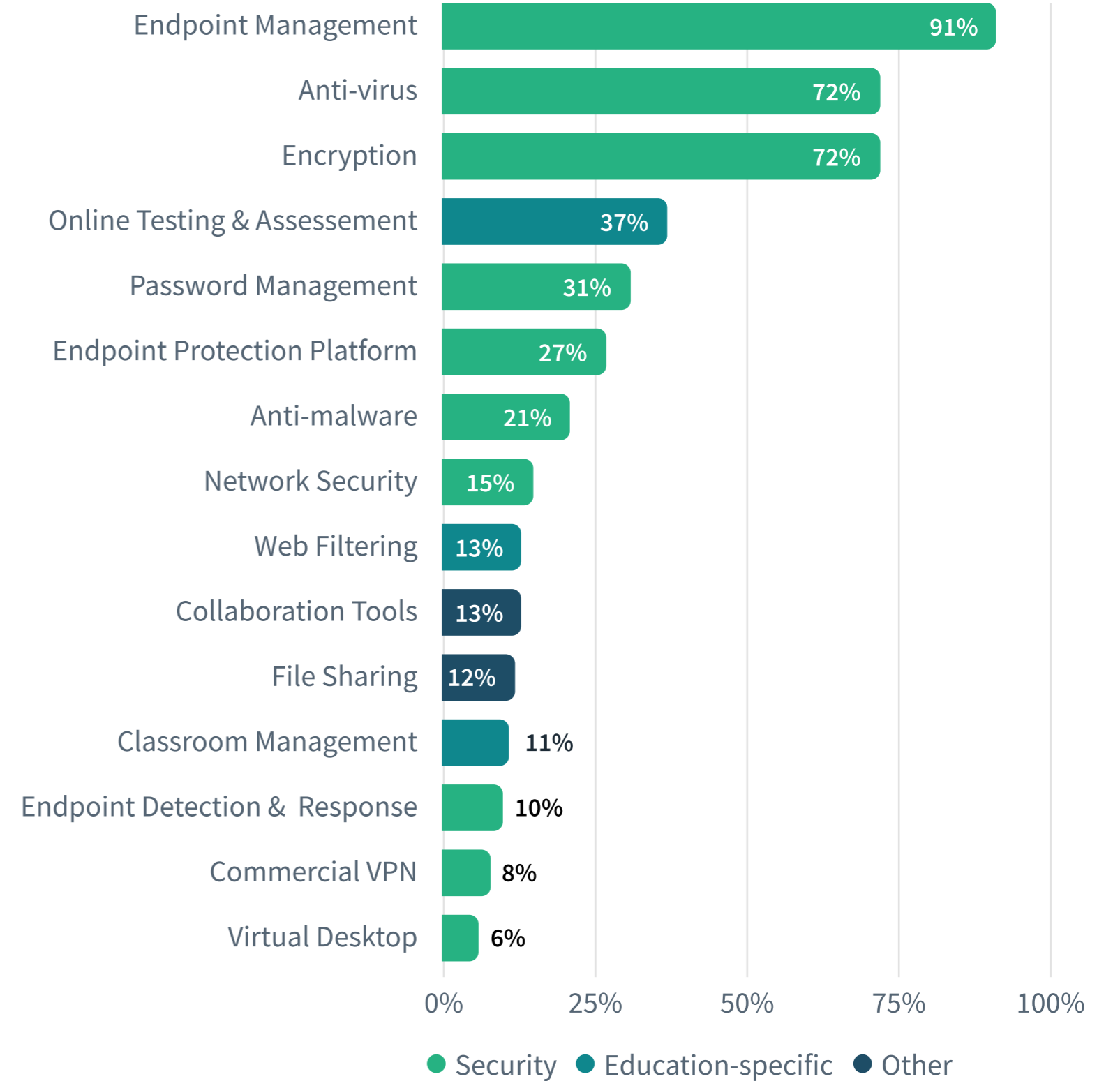
**Anti-virus Install and Efficacy Rates**



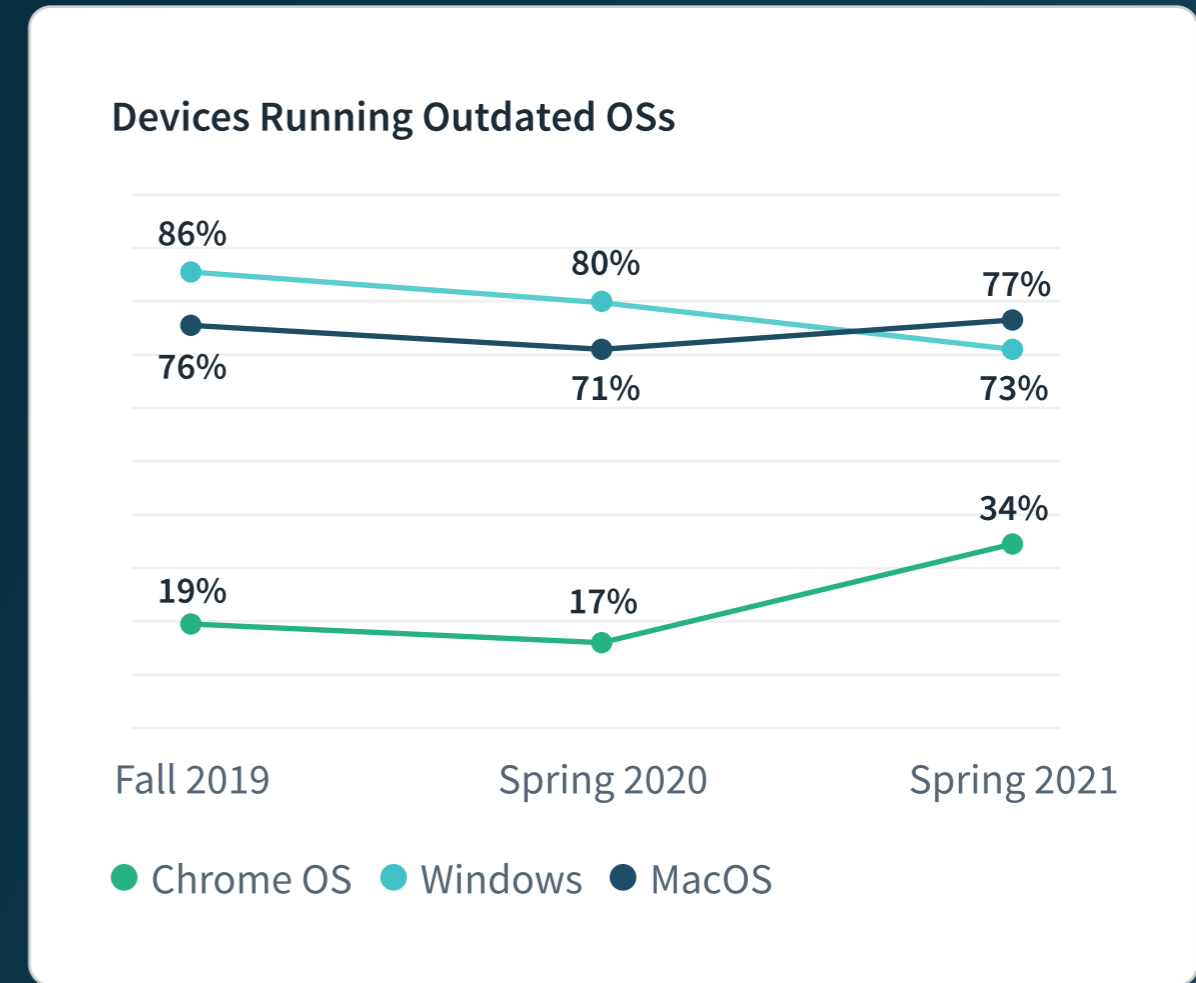


Further, this year saw the adoption of new endpoint applications to extend the digital learning environment, including web filtering, found on 13% of devices, and classroom management tools on 11%. In addition, nearly 40% of devices had at least one online testing and assessment application installed.

**Application Install Rates**



Potential vulnerabilities are also evident in the prevalence of outdated operating systems (OSs) and software, with the majority of devices running OSs that are more than two versions behind, including over one-third of devices running Chrome OS.

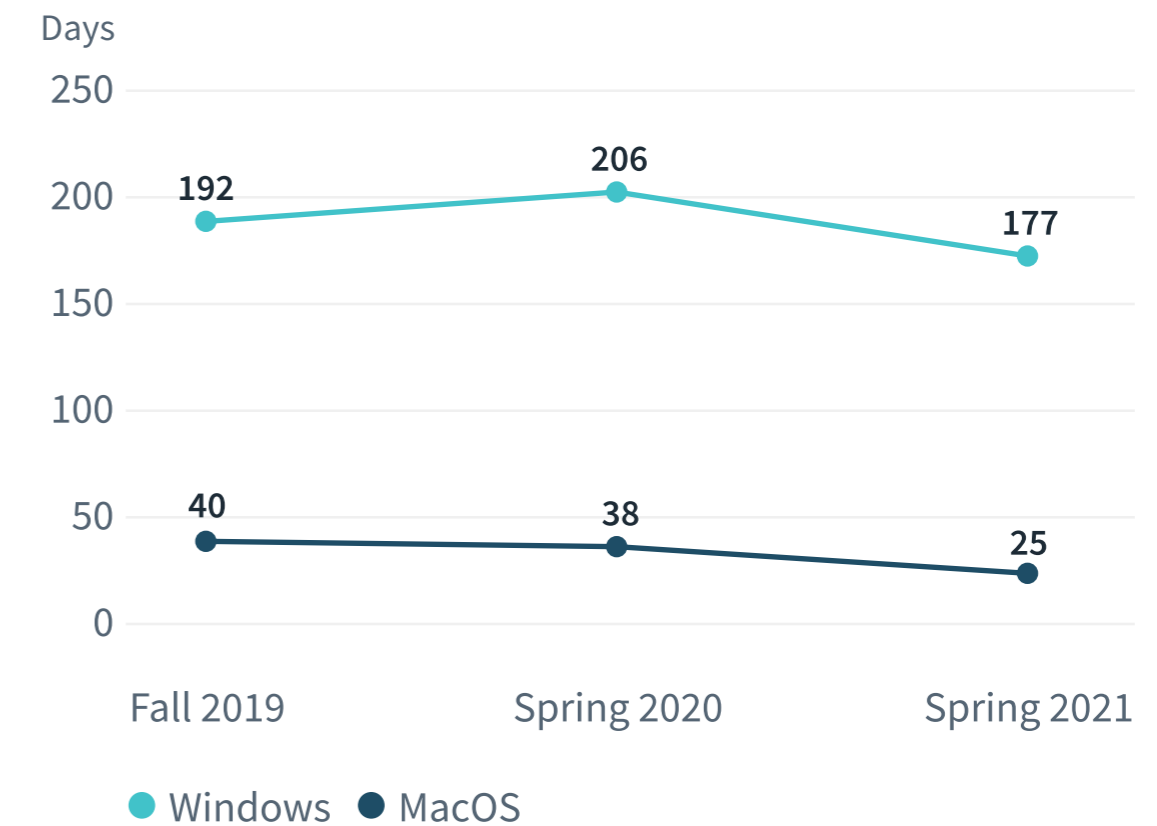


Even with some schools intentionally delaying updates and patches to minimize potential interruption, 2021 saw an improvement over 2020’s 206-day lag, with Windows 10 devices averaging 177 days behind current releases.

However, with any delay leaving schools and students vulnerable to attack, the FBI, CISA, and MS-ISAC advise that K-12 institutions patch operating systems and software as soon as updates are available.<sup>8</sup>

Should these vulnerabilities be exploited, the risk is significant.

Average Patch Age by OS\*



8 [Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data](#), Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC), 2020

\*Chrome OS omitted due to nature of updates: new versions are released instead of patches.

Almost one-third of education devices studied contained sensitive data—nearly half of which was social security data and 39% of which was protected health information.

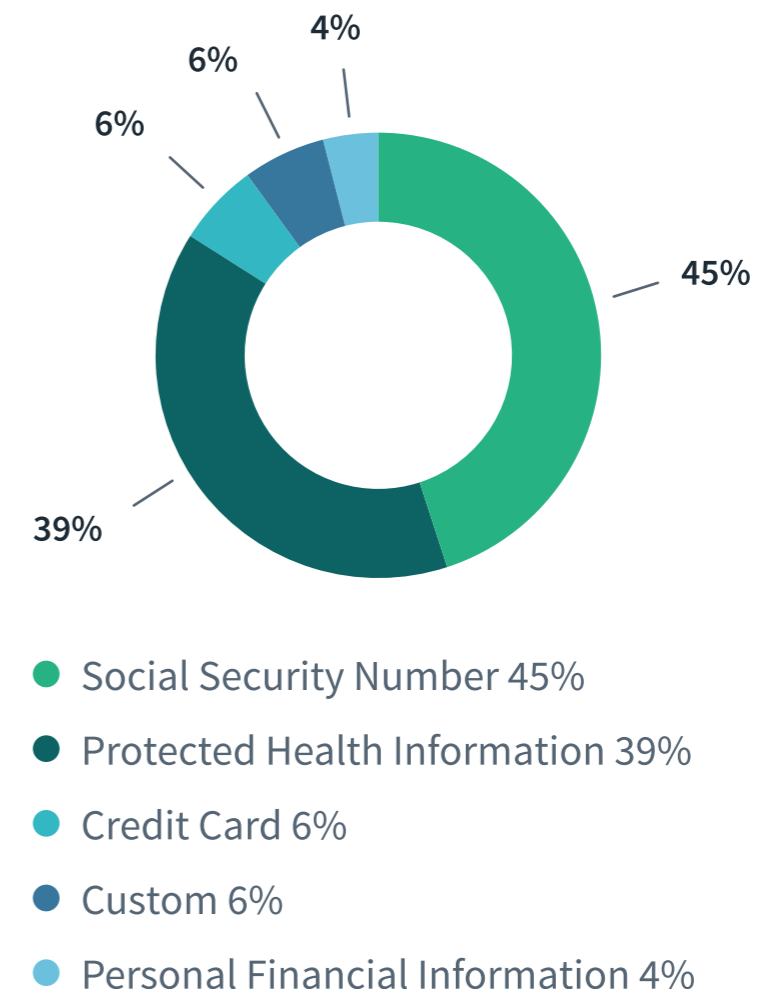
Although long underfunded and under-resourced, cybersecurity in education must now step to the forefront, with schools adopting the strategies of their counterparts in the corporate world.

**“We worried about the risk of sensitive data and information on teachers’ laptops getting into the wrong hands. Absolute gave our IT department peace of mind.”**

Mike Pitroff, CTO, Baltimore School District

85,000 students

**Prevalence of Sensitive Data, by Type**



# The Road Ahead

The K-12 technology landscape has irrevocably changed. Teachers and students alike have adapted to and embraced the new digital reality, and regardless of where physical learning takes place, devices are the new classroom.

For IT teams tasked with capitalizing on this opportunity to redefine education for the modern era, the work has just begun.

Managing and securing vastly increased device fleets needs to be incorporated into daily operations. Investments have been made and must be accounted for. Measures must be taken to ensure student safety and productivity online—as well as providing the ability to measure student engagement and performance. And, with school networks and devices an increasingly attractive target, cybersecurity must now come to the forefront of every EdTech strategy.

Together, these requirements highlight the critical need for visibility—and control—of the entire endpoint environment.

Over 10,000 schools and districts rely on Absolute to manage and secure their endpoint environments from a single, cloud-based console.

Firmware-embedded in almost every Windows device—and easily extended to Chromebooks and Macs—Absolute can be activated remotely for instant access to a continuous stream of data from every device and a powerful suite of tools for asset and data management, as well as threat remediation.

Absolute meets ESSA criteria as an evidence-based intervention, qualifying it for federal and state grant programs.

## Managing 1:1 devices

The new dynamic of learn-from-anywhere underscores the need for IT teams to scale systems and processes for device management—from deployment to collection, configuration to end-of-life.

With hundreds or thousands of new devices to contend with, platforms offering automation, efficiency, and insights can ease the administrative burden while protecting assets, data, and productivity.

## The Absolute Platform for K-12

IT teams rely on Absolute to streamline operations, automate device management, and minimize loss in their 1:1 programs.



Prebuilt commands and tools for remote lifecycle management—from configuration to decommissioning—ease the administrative burden on IT staff.



A continuous stream of analytics further simplifies device management with insights on geolocation, hardware and software inventory, usage, and hundreds of other data points.



Asset loss and data risk are minimized with the ability to locate, freeze, or wipe any device—even off-network, and Absolute's dedicated Investigation Services team is always on-hand to aid in recovery.



Policy management and audit preparation features include the ability to separately manage and report on devices purchased with state or federal disbursements such as CARES or the American Rescue Plan Act.

# Empowering the digital classroom

Web-based learning and collaboration solutions have played a critical role in enabling digital learning programs. The need to measure and monitor the impact of technology in the classroom—wherever that may be—is now necessary to optimize the learning experience and justify current and future expenditures.

The American Rescue Plan Act has four times the level of funding that the CARES Act provided—but schools must provide evidence that their investments have a measurable impact on learning outcomes.

With program success, student safety, and budgets on the line, K-12 systems should incorporate tools that provide the ability to monitor and measure activity and usage and take action when necessary.

## The Absolute Platform for K-12



Absolute enables IT teams with granular insights and customizable reports to understand device usage, web usage, and application adoption, including how much active time is spent on approved educational resources and whether web filters and controls are being bypassed.

Detailed analytics make it easy to compare usage and performance within schools or across the district, prove the value of technology investments, and help cut waste from IT budgets.

Integration with Google Admin Console extends its output with Absolute's asset and user metrics and consolidates device management from a single pane of glass.

# Navigating the threat landscape

No longer secured behind district firewalls, the endpoint is the new network edge, and the primary attack surface is literally in the hands of children.

Schools should take measures to identify and secure sensitive data, keep devices up-to-date, and, critically, ensure that their endpoint security controls are working at all times. They should invest in platforms that make devices and applications resilient—that is, self-aware and capable of automatically monitoring and maintaining their effectiveness.

Endpoint resilience is critical to managing and securing modern K-12 technology environments.

## The Absolute Platform for K-12

- Many security applications such as anti-virus, anti-malware, VPN, and disk encryption are autonomously monitored and maintained to ensure they are always installed, active, and up-to-date on all devices.
- Vulnerabilities are surfaced automatically and can be addressed remotely at-scale.
- Sensitive data discovery highlights location and type, with the ability to secure or delete individual files, or wipe the device entirely.

[Learn More](#)



## Report methodology

We analyzed anonymized data from Absolute-enabled devices across over 10,000 schools as well as public data and information from trusted third-party sources.

## About Absolute Software

The Absolute Platform for Endpoint Resilience® helps educational institutions ensure that their devices and security controls maintain a secure operational state automatically, without user intervention. Embedded in the firmware of over half a billion Windows devices and extendable to Chrome OS and iOS, Absolute provides continuous visibility, control, and intelligence of the entire endpoint environment—data, devices, and applications. More than 10,000 schools rely on Absolute for instant access to geolocation data and the ability to lock, freeze, or wipe any device—on or off-network. With a self-healing connection and granular endpoint telemetry, IT and security teams are able to streamline device management, secure data, remediate cyber threats, and help ensure that security controls are always installed and delivering ROI.

 [ABSOLUTE.COM](https://www.absolute.com)

 [SALES@ABSOLUTE.COM](mailto:SALES@ABSOLUTE.COM)

 [NORTH AMERICA](#) | [EMEA](#)



# Secure Your Devices with the Self-Healing Power of Endpoint Resilience

Contact us by [email](#) or call [1-877-600-2295](tel:1-877-600-2295) for a custom demo.

[Book a demo](#)

