Absolute for K-12 Education

Manage Devices Remotely and Maintain Security Controls

The web usage feature allowed us to track what programs our students were using during their time on and off campus. We couldl correlate that with the expense of the program and whether it was worth renewing for further school years. We enjoyed the fact that it share the opoerating system and version so that we can ensure all of our devices are up to date.

ERIC RAMOS
CHIEF TECHNOLOGY OFFICER
DUARTE USD (3,400 STUDENTS)

Recently, school districts around the world have adopted 1:1 device programs to keep students learning while unforeseen events force school closures. But many of these initiatives were created under tight deadlines, leaving educators and IT leaders without much visibility or control over students' devices. Our research found that missing devices are a major challenge for 41% of schools. 20% of endpoints have gone dark[1]. And audits loom, where visibility is necessary to prove the impact of IT investments on learning outcomes.

The challenge of managing and securing multiple device types and operating systems — remotely — has made schools easy targets, with outdated OS versions and inconsistent patching resulting in ever-widening security gaps. Use of online collaboration tools and remote desktop protocols has skyrocketed — increasing the risks of a ransomware attack[2].

Absolute Software, embedded in the BIOS by all major PC manufactures, enables K12 IT leaders to remotely monitor and manage their entire fleet, ensuring the effectiveness and safety of remote learning programs. Districts rely on Absolute to track devices, flag risks, and automate endpoint security — controls, apps, and agents — to safeguard learning.

Problem: An Increasingly Complex IT Environment

With limited resources and budget, IT and security teams are faced with obstacles that must be managed remotely.

IT Asset Management

- Unable to locate, track and manage all devices — regardless of platform — from a single, cloud-based console
- No way to recover missing devices
- No way to measure student device usage

Security

- Failing security controls like encryption, outdated anti-malware, and vulnerable OS versions create a risk of cyberattacks
- No way to enforce updates and configurations on off-network devices
- Unknown personal data on endpoints creates the risk of non-compliance with CIPA & HIPAA

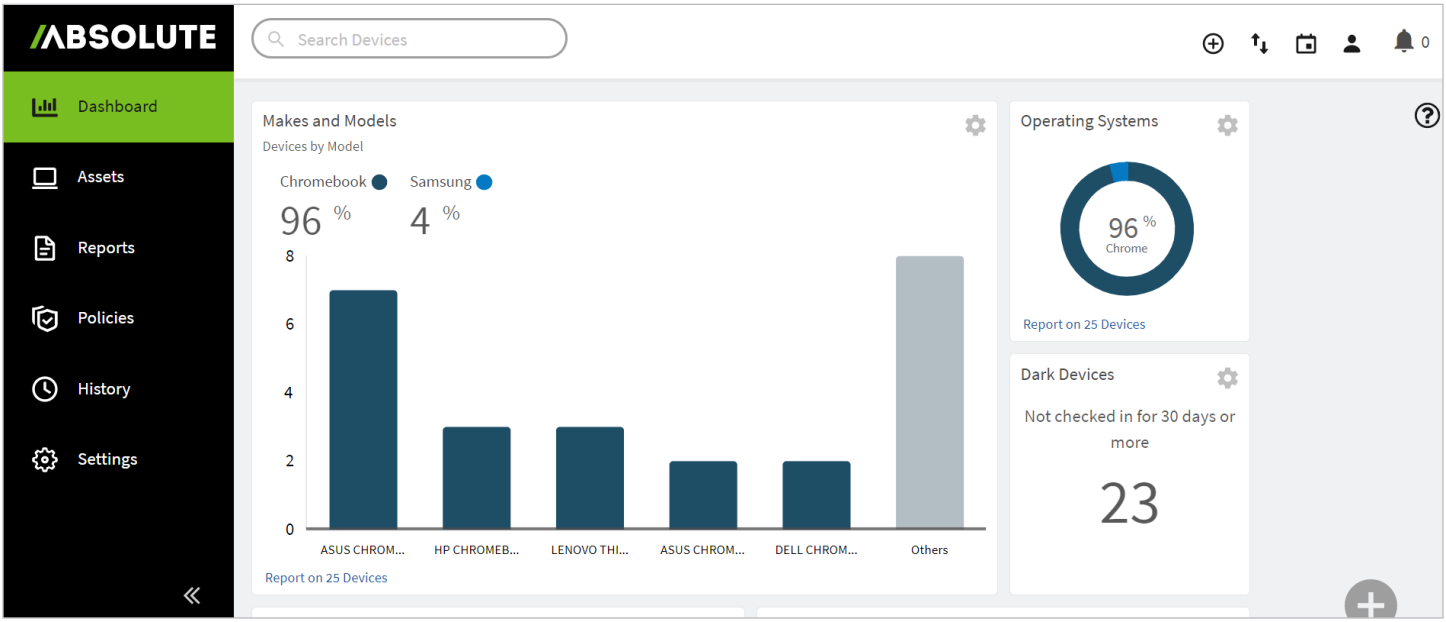
[1] Gallagher, S. Rash of ransomware continues with 13 new victims — most of them schools, ARS Technica, Aug 30, 2019

[2] Absolute's *Distance Learning's Impact on Education IT, 2020*

Lenovo

ABSOLUTE®

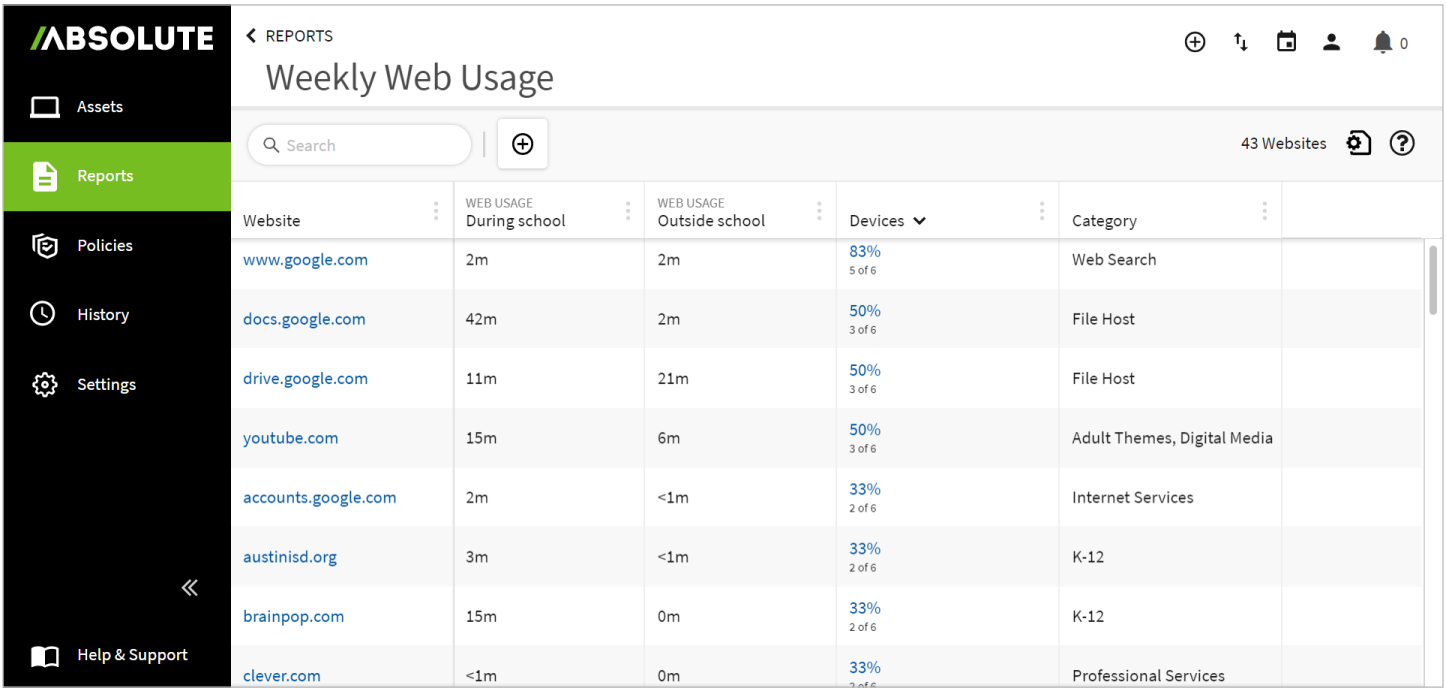
Solution: Maintain Security Controls, Manage Your Fleet, and Safeguard All Your Devices and Students



Absolute gives you an unbreakable connection to student, teacher, and staff devices, wherever they happen to be. From a unified cloud-based console, you can remotely track, manage, control, and monitor your entire device population — whether they're Chromebook, Windows, or Mac devices.

Absolute syncs with the Google Admin Console (GAC) for greater visibility and control. Manage all devices from one single cloud-based console: automate hardware, detect suspicious activity, reduce device loss or theft, and maintain compliance.

Web & Device Usage Reports let you know what websites students are spending their time on, monitor the adoption of EdTech tools and identify potentially harmful or unsafe web usage so you can take action.



Lenovo ABSOLUTE®

Reduce Device Theft and Loss Throughout the School Year

Flag a device when it's missing, and you will be notified via email the next time it connects to the internet. If stolen, **Absolute's Investigations** team helps you reduce the resources you invest in security incident management, by collaborating with law enforcement to track and recover the location of stolen devices — even off the school network.

Track and Secure your Assets

Activate a persistent connection to all your endpoints, giving you unrivaled visibility and control — including the ability to geolocate, freeze, and wipe remote devices. Absolute's end of year Device Collection Guide enables customers to plan, execute, collect, control and monitor remote devices.

Unified, Cloud-Based Console

Dramatically improve your IT operational efficiency by seeing, managing, controlling, and securing your entire device population from one place. Integrate Absolute with your existing Google Admin Console structures to seamlessly manage student devices.

Measure Student Engagement

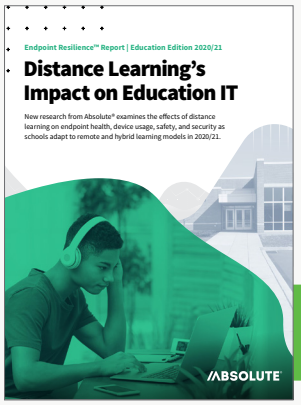
Web and Device Usage Reports let you know what websites students are spending their time on and monitor the adoption of EdTech tools. Drive better learning outcomes by identifying valuable or underused learning resources.

Maintain your district's security controls

Absolute Persistence's self-healing capability can be extended to AV, encryption, VPN, or any other application that you depend on — so they're always installed, up-to-date, and working correctly.

Fix vulnerabilities remotely

With **Absolute Reach**, your IT team can remotely execute scripts to repair, patch, and remediate devices. Get alerted to suspicious activity, inappropriate use, and early precursors of security issues — so you can take remote action to prevent incidents and ensure compliance.



Distance Learning's Impact on Education IT is the landmark report on key trends and new threats in the 20/21 school year, providing a strategic blueprint for IT teams tasked with supporting modern learning environments. Know the risks. Adapt your approach.

GET IT NOW

ABOUT ABSOLUTE

Absolute empowers more than 12,000 customers worldwide to protect devices, data, applications and users against theft or attack — both on and off the corporate network. With the industry's only tamper-proof endpoint visibility and control solution, Absolute allows IT to enforce asset management, security hygiene, and data compliance for today's remote digital workforces. Patented Absolute Persistence™ is embedded in the firmware of Dell, HP, Lenovo, and 26 other manufacturers' devices for vendor-agnostic coverage, tamper-proof resilience, and ease of deployment. See how it works at **absolute.com** and follow us at **@absolutecorp**.

For more information about Absolute for Lenovo devices, contact your sales representative or Lenovo partner.

Lenovo

ABSOLUTE®