ABSOLUTE®

KEY INSIGHTS

Cybersecurity and Education: The State of the Digital District in 2020

Threats to student and school safety exposed in study of 3.2 million devices

Modern learning platforms enrich the lives of students, but technology must be managed with care. Understanding the threats uncovered in this research provides a blueprint for protecting your schools from data breaches and ransomware attacks and keeping your students safe.

Complexity makes schools easy targets

700+
cybersecurity incidents since 2016[1]

49
school districts hit by ransomware attacks this year[2]

#2
schools are the second highest targets of ransomware[3]

No digital district is immune. Absolute studied:

3.2M
devices

1,200
K-12 organizations

1.2B
change events

11
analyst reports and peer research

K-12 has gone digital. According to public research:

94%
have high-speed internet[4]

62%
increase in tech spend from 2016 to 2019[6]

82%
provide student devices in one-to-one or similar programs[5]

Digital creates complexity. Our research detected:

137,000
unique application versions

93%
K-12 organizations managing up to 5 versions of common apps

11
device types

6,409
Chrome OS extensions

250+
unique versions of Windows, Mac, Chrome & Linux

[1] The K-12 Cybersecurity Resource Center, Accessed 24 Sept, 2019

[2] Sheridan, K. Ransomware Strikes 49 School Districts & Colleges in 2019. *Information Week*, Sept 20, 2019

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

[4] IT Leadership Survey Report. *Consortium of School Networking*, 2019

[5] Fulfilling Our Promise to America's Students. *Education Superhighway*, 2017

[6] The State of EdTech 2019-2020. *EdTech Digest*, 2019

Savvy students open the door to threats. Our research detected:

42%
of schools have students or staff that circumvent security

319
unique web proxy/rogue VPN apps

10.6
devices with web proxy/rogue VPN apps per school

And while 68% of K-12 IT leaders list cybersecurity as their top priority[7], we found:

Client/patch controls fail

53%
rely on native client/patch management tools

56%
failure rate for client/patch management agents

9%
client/patch management failures never recovered

Critical security controls fail

12%
failure rate for encryption controls and agents

44%
of agent failures never recovered

Justifying tech spend in the digital district

Devices are underused

21%
devices used <1 hour/day

60%
of students don't use devices at home

Devices disappear

17,000
crime-related device losses in two years

34%
of users don't return devices

Students & districts are exposed when security controls fail

38%
of agents require at least one repair monthly

28%
of encryption agents fail monthly

50%
of failing encryption agents fail over 25 times/month

50%
client/patch management tools requiring over 9 repairs/month

[7] IT Leadership Survey Report, *Consortium of School Networking*, 2019

Download the full report for deeper insight into the threats facing IT leaders in K-12, gained from analyzing more than 3 million student devices across 1,200 K-12 organizations over one year

GET THE REPORT