Microsoft

Securing Student Data: Microsoft vs. Google

Last updated: November 2020

SECURITY RISKS FOR SCHOOLS

Student Data is at risk
The number of cyber-attacks on US public schools is increasing with 348 incidents reported in 2018.[1]

Threats continue to rise
2019 saw a 300% increase in identity-related attacks[2]

Schools are the main targets
13% of education institutions have experienced ransomware attacks, the most of any sector[3]

TOP DIFFERENTIATORS

Microsoft has a more robust security portfolio

- Microsoft Teams supports **more Security and Compliance regulations** than Google G Suite Comprehensive compliance offerings (Google has 37 as of Aug. 2019; Microsoft has over 90[7]
- **Microsoft secures data at multiple levels** from the device, at the server and in the cloud via technologies such as Windows Information Protection, multi-factor authentication, and Windows Defender

Microsoft is a recognized leader in security

- Microsoft remains a **leader in a number of Gartner Magic Quadrants**[7-8]
- **Microsoft takes a more comprehensive approach**, bringing top level security to devices, servers, and end points of the solution.

Microsoft does not mine or sell student data

- Google has admitted to **"scanning and indexing" student** emails in April 2018[5]
- Google was sued in February 2020 for allegedly **"spying" on children as early as kindergarten**[6]
- Google was **fined $57 million** by the CNIL in January 2019, for **failing to comply with the General Data Protection Regulation** by not properly disclosing how they collect data to present personalized ads[4]

SECURITY AND PRIVACY CAPABILITY COMPARISON

	Comparison item	Microsoft	Where Google's gaps exist
Student Safety	Identity	✓	Google does not protect beyond Google Cloud, Chromebooks, or 3rd-party SaaS apps
	Access Management	✓	Google does not protect beyond Google Cloud, Chromebooks, or 3rd-party SaaS apps
	Communication Policies	✓	Google provides limited communication compliance functionality that only scans message in their G Suite environment
	Advanced Thread Protection (ATP)	✓	Google lacks intelligent, ML-backed recommendations for advanced threats
Information Protection and Governance	Data Loss Prevention (DLP)	✓	Google Limited to Gmail and Google Drive with no automated data classification or retention policies
	Encryption	✓	G Suite encrypts data at rest but does not allow customers to provide and control their own encryption keys
	Data Policies	✓	Google data policies only apply to Gmail messages and sensitive data (credit cards, social security)
	Malicious URLs	✓	Google protects across malicious attachments but not URLs
	Auditing	✓	Google has limited auditing capabilities, and can only audit activity that happens in the G Suite
	Reporting	✓	Google has limited reporting capabilities and can only report on Gmail or Google Drive data
Campus Security	Device Management	✓	Google does not have complete device management across breadth of devices
	Risk Management	✓	Google does not have a single location (single pane of glass) for accessing and managing risk – and compliance – across campus
	Advanced Analytics and insights	✓	Google does not have a single location (single pane of glass) for accessing and managing risk – and compliance – across campus
	Automatically identify Suspicious Behaviors	✓	Google can not automatically identify suspicious behaviors and people of interest through real-time video analysis

IMPORTANT CONSIDERATIONS

- Which IT partner would you trust more, one who sells software and hardware, or one whose main revenue generator is selling data to advertisers? (70.9% or $134Billion of Google's revenue in 2019[9])
- How many security vendors do you have? How many would you like to have?
- How important is student privacy to you, your board of directors, parents and students?
- How do you secure your organization against advanced threats?
- How do you view of all the cloud apps your students and teachers use today?
- How do you control where your institution's information is stored and accessed?

REFERENCES

1. EdTech Magazine, 2020
2. Digital Shadows; 2020
3. Bitsight; 2020
4. The New York Times; 2019
5. National Review; 2018
6. CBS News; 2020
7. Gartner "Magic Quadrant for Cloud Access Security Brokers," 2019
8. . Gartner "Magic Quadrant for Unified Endpoint Management Tools," 2019
9. Statista, 2020