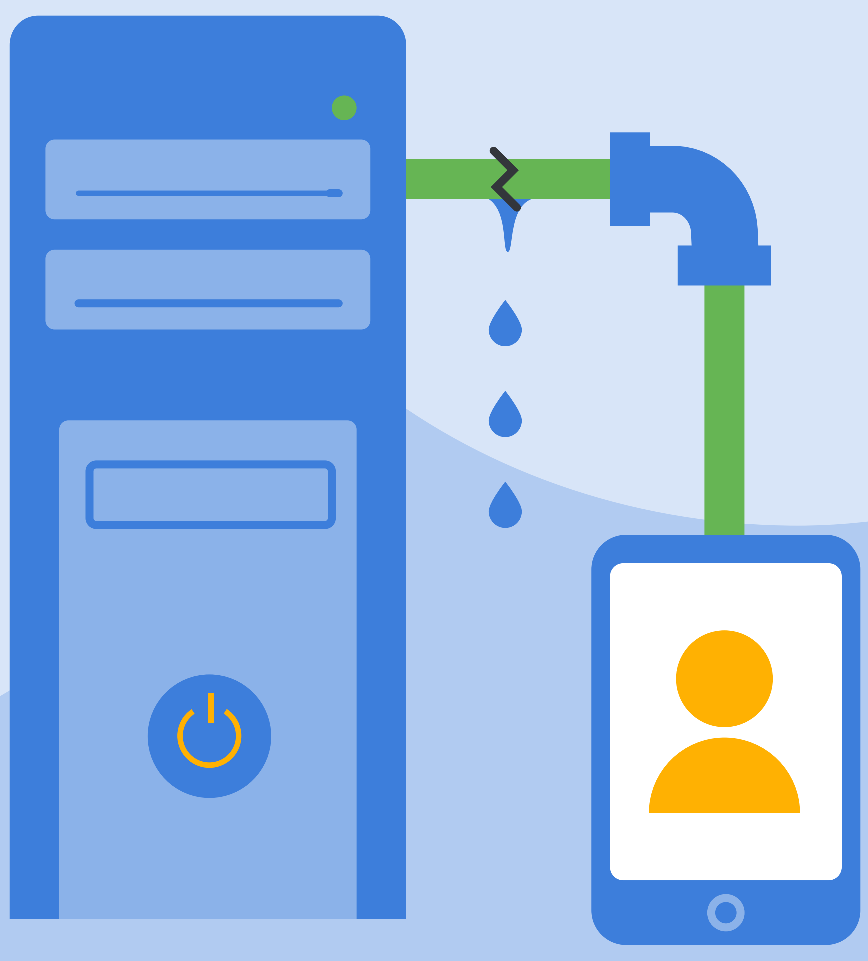
4 TRUTHS

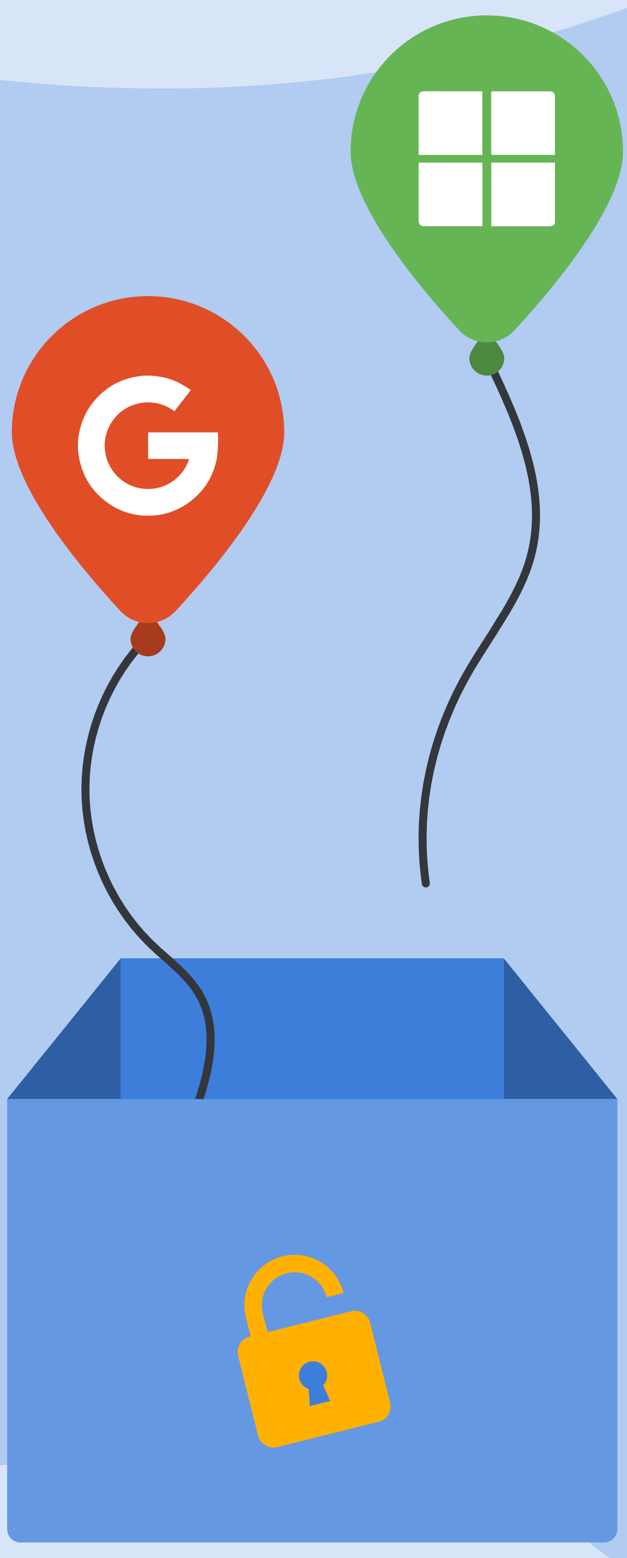
about data breaches that will help protect your district

Data breaches are on the rise, and school districts are a target. More than likely, you've already taken steps to protect your district's safety and privacy. That's all well and good – but is it enough? To answer that question, it's important to understand the truths about your district's cloud environment.

1 Insider data leaks are far more common than ransomware or cyberattack.

75% of breaches involving personal student or staff information were caused by the security practices of third-party vendors and school partners.





2 Your current cybersecurity tools are unlikely to protect Google or Microsoft domains.

60% of school districts have "quite a lot" or "a great deal" of confidence in the security of their data stored in the cloud.

Yet, **1 in 3 don't know** if their cybersecurity system monitors for risky outside file-sharing.

3 Although both are secure, Google and Microsoft aren't responsible for your service-level cybersecurity.

Despite outsourcing most of the liability, **schools districts must still protect their side of the platform** from breaches, leaks, and other threats.

4 You have gaps in your protection. The answer? Layered cloud security.

With an **additional layer of security**, your district is empowered to defend against attacks, prevent accidental data leaks, and identify student safety signals in one easy-to-use platform.

Ready to learn more? Test it out today.

Start your free trial of ManagedMethods' Google Workspace and Microsoft 365 cybersecurity, student safety, and compliance platform.

Source:

Levin, Douglas A. (2021). "The State of K-12 Cybersecurity: 2020 Year in Review." EdTech Strategies/K-12 Cybersecurity Resource Center and the K12 Security Information Exchange.

Available online at:
https://k12cybersecure.com/year-in-review/

Managed Methods