PlanGrid

Security 101: 5 Best Practices in Construction Software

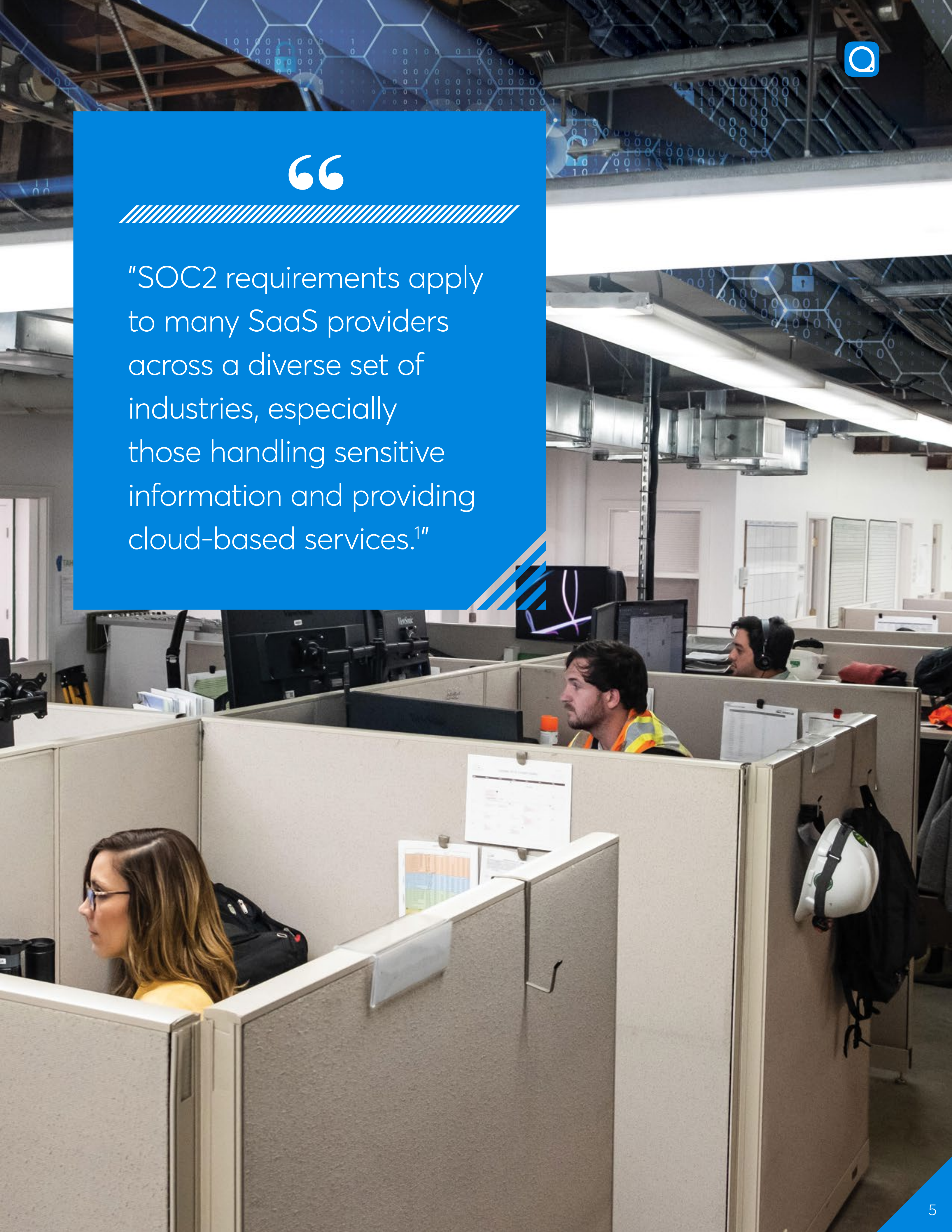
Why SOC2 and other security best practices are essential for construction professionals

What's Inside

MAX CAPACITY 1 TON

SOC2 and Your Team

Although the construction industry has historically resisted some forms of technology, construction software is now essential for construction professionals. The productivity losses stemming from many of the "old school" processes in construction are well documented, but forward-thinking teams are now adopting new tools to get their work done more efficiently and effectively. Additionally, many bid or proposal requests require information to be submitted digitally in specific file formats and a robust construction software suite is the easiest way to manage and produce that. However, committing your company to new software presents new security risks such as compliance issues, fraud, theft and data loss.

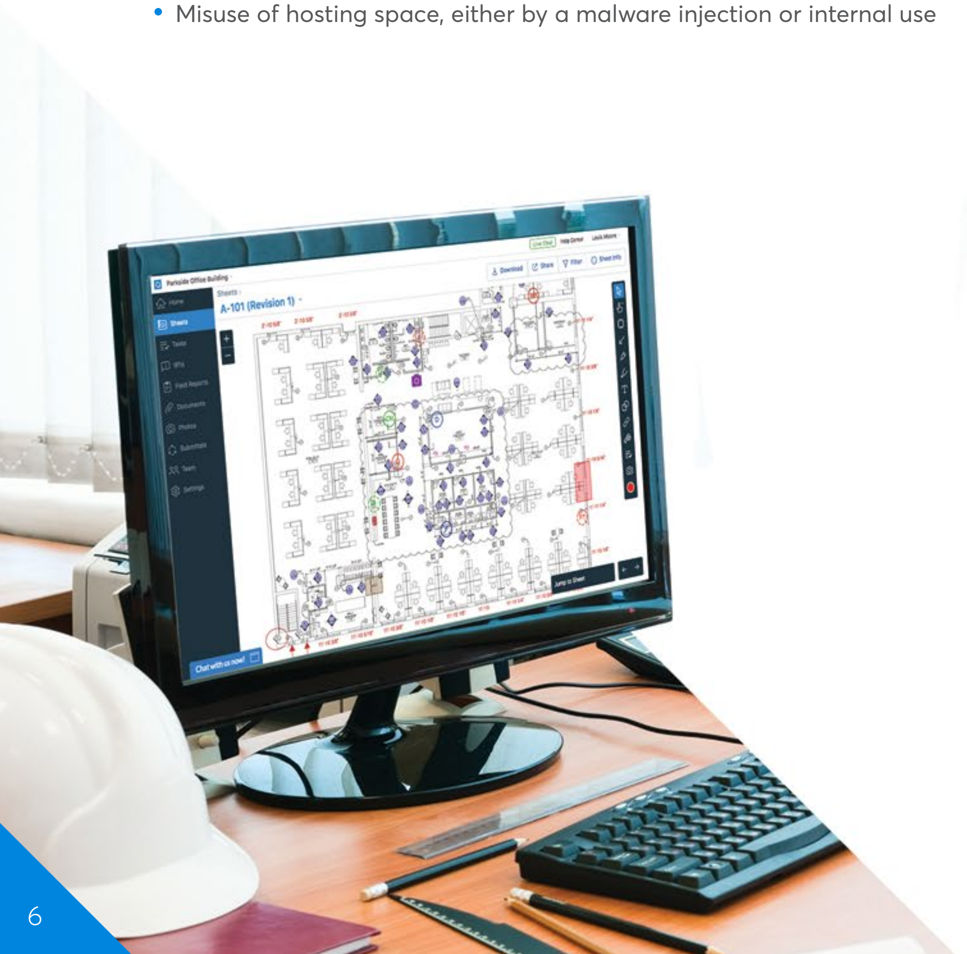


"SOC2 requirements apply to many SaaS providers across a diverse set of industries, especially those handling sensitive information and providing cloud-based services.[1]"

The Risks of Insufficient Software Security

Any software your company uses for tracking construction work and managing client data must conform to specific security requirements. Failing a compliance check from a governing body could result in steep fines and loss of clients. While many construction firms go years between checks, you can expect a compliance inspection if you experience any of the following common security breaches:

- Denial of Service (DoS) attacks on the software itself or the servers storing your information
- Direct data loss, either by theft, malware infection, or accidental destruction
- Unapproved access from inside the organization, leading to lost or stolen data
- Account theft through remote access and keyloggers, leaking client data
- Application programming interface (API) weaknesses, which are software options for customizing access to a platform that can come with their own vulnerabilities
- Misuse of hosting space, either by a malware injection or internal use



Losing access to your database of client information during a data breach or DoS can result in a compliance inspection. In order to prevent these problems, Service Organization Control (SOC) 2 audits can help you set standards for cloud-based services. Whether you need to find a SOC2 SaaS vendor due to a client's requirements or just for the additional security, there are only a limited number of construction management software firms currently achieving this standard. SOC2 requirements apply to many SaaS providers across a diverse set of industries, especially those handling sensitive information and providing cloud-based services.[1] If you're storing your construction planning and organization services in the cloud, you need to know the SOC2 requirements and how to meet them. You should also work with a SOC2 certified vendor to protect your company's reputation even if it's not required by any of your current contracts.

Voluntarily undergoing the SOC2 audit can also help you qualify for more government and healthcare construction bids. Since sensitive data is often transmitted through the construction security software you choose, look for a data management SaaS solution that has already achieved the SOC2 certification to help you protect your assets.

Choosing a vendor for your company's SaaS installation goes beyond simply finding a good deal. The software should handle as many different organizational and bid building tasks as possible. Prioritize vendors that have complete construction security software solutions, such as PlanGrid, to prevent these risks from interrupting your business and costing you contracts.
To give our customers confidence that their data is secure and private, PlanGrid maintains SOC Type 2 compliance.

Understand the Main Differences Between SOC1, SOC2 and SOC3

All three forms of SOC compliance are based on standard security practices and technology requirements. Since hosting data in the cloud presents more opportunities for hacking, data theft and illegal access, these software services must meet a higher standard of security. As an end-user of the software who is voluntarily handling sensitive information from potential and existing clients, you are also likely to be held to the current security standards.

SOC1

These standards of compliance were all designed by the American Institute of CPAs (AICPA). Prior to 2014, vendors selling cloud SaaS services only needed to meet the SOC1 standard[1]. Also referred to as the SSAE 16 standard, this set of compliance requirements was relatively basic compared to SOC2. The companies and vendors seeking this kind of report were fewer as well, limited mainly to payment processors and SaaS services processing financial data. With most construction management software packages offering plenty of payroll and financial reporting features, SOC1 certification was often required.

SOC2

Introduced in 2014 by AICPA2, the SOC2 protocol was a noteworthy advancement over the standardized reporting of SOC1[1]. The compliance report is based on five Trust Service Principles. The data provider or vendor can meet the requirements in any way they see fit, as long as their solutions satisfy the security standards[2]. This allows each vendor to add the security features that make sense for the specific industry serviced by the SaaS. Construction security software needs a different approach from what a payment vendor or open data storage vendor might use, so SOC2 compliance is the best fit for flexibility in security certification. Along with the new protocol, the requirements for meeting SOC2 standards were also expanded. As of 2018, all cloud-based SaaS vendors storing customer data must meet this compliance level, regardless of whether or not they store and process financial data. PlanGrid has undergone a security audit and as a result, maintains SOC2 compliance to best serve our customers and keep their data secure.

SOC3

SOC3 reports remain optional for most data centers and SaaS vendors for now, but some companies are voluntarily undergoing the audit process. These reports are published publicly to demonstrate how a particular cloud-based service is performing in the security- and data-handling field[4]. Most construction companies won't need this kind of report; it is used primarily by government agencies, non-profits and similar databases that serve these kinds of customers.

SOC2 and Construction Software

By choosing SOC2-compliant software (like PlanGrid), you can assure your clients and customers that you're protecting their data. Even if you don't seek separate certification for your company's practices, you can list your use of a SOC2 database service on bid proposals, marketing materials and your company's website.

Healthcare Clients

SOC2 compliance is often the minimum of security auditing required by a healthcare client before they'll accept your proposal for a hospital or clinic construction process. Since your software could put their systems at risk and potentially violate the data rules established by the Health Insurance Portability and Accountability Act (HIPAA), you need to choose a software vendor that can handle protected health information (PHI). The SOC2 audit qualifies you to do that, so sharing a copy of a Type 1 or Type 2 report from an auditor could help you attract new healthcare clients for major construction projects.

Engage Your Team with the Five Trust Service Principles

Even if your construction team chooses a SOC2-certified software vendor, you'll still need to understand the trust service principles to fully grasp the audit report provided[2]. Sharing the principles that form the basis of a SOC2 audit will also prepare your construction team for a compliance check in the future.

1. Privacy

The privacy principle refers to the way each user's personal data is handled and protected during and after their use of the system. This includes login credentials, personal identification details, IP addresses and more. Particular attention is paid to personal identifiable information, or PII[5]. This includes a full or partial name, Social Security number, a user's religion or race and other sensitive health-related information. While you might think this category is limited in application to a construction software suite, you'd be surprised at what qualifies as PII data when you include security questions about a user's history and background for retrieving a lost password. The software needs to properly dispose of any data that doesn't need long-term storage, so it can't be accessed later by the wrong party.

2. Security

Security trust service principles include all the methods a software vendor uses to protect the cloud-based service from unauthorized access and brute force attack. This includes measures against alteration of the software, malware intrusions, network interruptions and outright theft of data. In particular, the vendor's use of two-factor authentication and web application firewalls is examined. Intrusion detection to notify the vendor of a system breach is also required to pass this category in an audit.

3. Availability

The privacy principle refers to the way each user's personal data is handled and protected during and after their use of the system. This includes login credentials, personal identification details, IP addresses and more. Particular attention is paid to personal identifiable information, or PII. This includes a full or partial name, Social Security number, a user's religion or race and other sensitive health-related information. While you might think this category is limited in application to a construction software suite, you'd be surprised at what qualifies as PII data when you include security questions about a user's history and background for retrieving a lost password. The software needs to properly dispose of any data that doesn't need long-term storage, so it can't be accessed later by the wrong party.

4. Processing Integrity

Processing integrity determines whether data arrives at the right place at the right time. Without processing integrity, software can fail to update properly and display outdated blueprints or purchasing records to a contractor in the field. Even one small data-processing error can result in exposure of sensitive information to the wrong parties or a bid thousands of dollars under or over the actual budget.

5. Confidentiality

The confidentiality portion of the audit addresses how access to data is controlled by the software. An RFP response for a client should be accessible only by team members working on that project, not by everyone in the office. Proper authentication, encryption and internal firewalls are required to satisfy the confidentiality trust service principle.

Evaluate Your Software Vendors

When evaluating a software vendor, don't just take the word of auditors and certifying organizations. Personally research the background of the SaaS company and ask your own questions[3]. Any construction security software vendor worth a contract will happily supply the information you need to decide if they're secure enough to trust.

Data Breach History

Start by checking online and offline news sources for stories about data breaches and leaks linked to the vendor or software. Look beyond the construction software you're currently considering because most SaaS providers sell more than one service. If there have been breaches or security issues with one service, more are likely to come from the vendor's other offerings.

Local Security

Ask the software provider what measures they take to secure their offices, servers and equipment from local issues. All the online security in the world can't help if a fire destroys the server hosting your data and there are no backups. Locked doors and employee identification cards are just as important in data security as firewalls and encryption methods. If your software vendor is relying on a remote hosting arrangement, which is common in SaaS arrangements, ask about the security measures used by the data hosts.

Cloud and Online Security

Wrap up your investigation of a software vendor with a few questions about their security features for cloud storage and online access. How much control can they offer over access to individual files and data? What kind of encryption and authentication processes do they use? How will they notify you if there is a data breach and what will they do to remedy it? Asking these questions before you sign a contract can prevent a lot of headaches later, even if all the vendors claim to have undergone a SOC2 audit.

> "PlanGrid has undergone a security audit and as a result, maintains SOC2 compliance to best serve our customers and keep their data secure."

Improve Your Team's Approach to Software Security

Each individual use of a software service still plays a large role in the total security of the system. If users are writing their passwords on their desks, finding ways to circumvent bothersome authentication features, or accessing their accounts from the wrong equipment, data breaches are all but inevitable even with the most secure software.

Improve your construction company's approach to software and IT security with a few basic approaches. Check how patches are being applied to employee hardware used for accessing the software. If there's a Java or Windows OS vulnerability on a laptop used on the jobsite, the entire system can be breached through that one weak point.

Follow up with a training audit of all IT professionals with the company. Since IT is a relatively minor focus of the construction company, it's often overlooked. Managers responsible for keeping the company's data assets safe can go years without new security training. Invest in annual education seminars and courses for your software team, so they can keep everyone else working instead of dealing with software and security issues.

References

[1] 4 Things You Need to Know About SOC 2 Compliance. Threat Stack

[2] SOC 2 Compliance. Incapsula

[3] How and Why to Request a SOC Report from Your Vendors. Smith & Howard Certified Public Accountants

[4] SOC 1, SOC 2 & SOC 3 Report Comparison. Online Tech

[5] Rules and Policies – Protecting PII – Privacy Act. U.S. General Services Administration

See a Live Demo

or give us a call at +1 (415) 429-1227

PlanGrid's Construction Productivity Software is the easiest and most cost-effective way to get substantial return on your investment in construction mobile apps. By using PlanGrid you will:

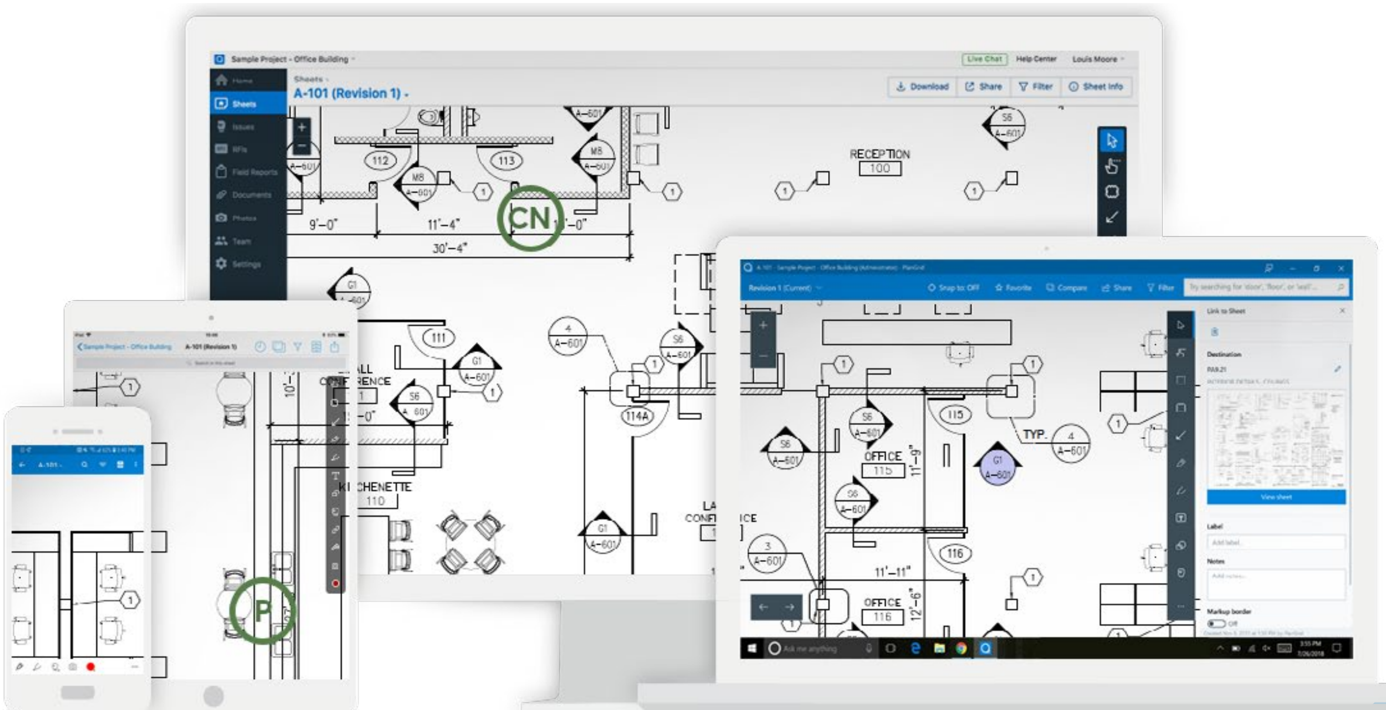
- **Complete projects faster:** 90% of project costs occur in the field and not in the office. This includes wasted time and project delays. With PlanGrid, you can reduce wasteful trips to the trailer and time delays, while eliminating costly rework. PlanGrid also allows for faster collaboration and communication.
- **Reduce costs:** PlanGrid allows you to optimize productivity in the field, which eliminates time waste that causes project overruns. By completing projects early or on time with PlanGrid, contractors will benefit from reduced costs.
- **Win more bids:** The best way to bid more competitively is not just to track costs so you can provide more accurate estimates — it's to improve your overall productivity. PlanGrid's Construction Productivity Software will allow you to increase productivity so you can reduce costs and win more bids.

PlanGrid is construction productivity software used on more than 1 million projects across 90 countries. Our software helps teams collaborate more efficiently with access to an intelligent record set on any device.

Available on the App Store ★★★★★ (3,904)

Get it on Google Play ★★★★½ (2,080)

Available on Windows



PlanGrid

Used on more than 1,000,000 projects around the world, PlanGrid is the first construction productivity software that allows contractors and owners in commercial, heavy civil, and other industries to collaborate, collect, and share project information from any desktop or mobile device through the entire project lifecycle.

PlanGrid increases project efficiency by streamlining document management, providing construction teams with easy access to all project information from any device, and enabling seamless collaboration within teams.

Connect with PlanGrid

© 2018 PlanGrid, Inc. All Rights Reserved.

United States
+1 (415) 963-4088
www.plangrid.com

Australia
AUS 1800 316 406
www.plangrid.com/au
apac@plangrid.com

United Kingdom
+44 (0) 20 3695 0292
www.plangrid.com/gb
emea@plangrid.com

Canada
(800) 646-0796
www.plangrid.com/ca-en
www.plangrid.com/ca-fr

Hong Kong
+852 5808 3598
apac@plangrid.com