

Showcase Workshop Platform Security Overview



showcase
workshop

Your data is always safe with Showcase Workshop.

We work closely with our content delivery services provider, Amazon Web Services (AWS), to provide the highest levels of security, speed and uptime. All access to Showcase Workshop is secured over SSL connections, protecting your data and preventing unauthorized access.

This document will provide you with detailed platform security information. This should be everything your IT team needs to feel safe and secure with your company's use of Showcase Workshop.

If you need any further information, please don't hesitate to contact us here: securitynerds@showcaseworkshop.com



Your Data Is Safe – and Never Far Away

Data privacy and security are top concerns for every company today – including our own. If you're anxious to know what happens when your team uploads company files to Showcase Workshop, you can rest assured that your data is in good hands.



Your files are stored on the highly secure AWS cloud services platform. Our primary datacenter location is in California.



To increase the speed of your content delivery, copies of your files are stored at the closest Amazon CloudFront location to you. A current list of these locations can be found at:

<http://aws.amazon.com/cloudfront/details>



showcase
workshop



Your company content is delivered swiftly and securely to your team's devices via the Showcase Workshop app.



Users only have access to the content you grant them access to. Every content request is authorized, checked against the Showcase Workshop account and user roles, and subject to fine-grained data access rules.

Showcase Security: Specs & Features

Everything your IT team needs to know to sleep soundly at night knowing your data is secure.

Secured access

- Every user has a unique login and password.
- All access to the Showcase Workshop Platform - from your phones, tablets and desktops - is secured using SSL/TLS (HTTPS).
- Platform access is continually audited. Administrators can view logs via the Showcase Workshop website at any time.

Secure file sharing

- When files are shared, the recipient's email address is verified before access is granted. Files are then delivered via a secure website, not through potentially unsecure end-user email systems.
- Access to shared files is monitored within the Showcase Workshop platform. Administrators can view the logs at any time.



Password brute force detection

- User account access is blocked after 10 incorrect attempts to login.
- Access is automatically reenabled after one hour. No need to submit support tickets for assistance.

Remote deletion of content

Showcase Workshop content is automatically deleted from a user's devices when that user's access is revoked or showcases are deleted.

Built with the power of Amazon Web Services

The Showcase Workshop platform is built on top of Amazon Web Services (AWS) solutions. AWS is an industry leader in cloud security. For more information see: <http://aws.amazon.com/security/>

Showcase access control

User access can be granted based on a number of different criteria. Use the options within the Manage Access area of the Showcase website to grant access to individuals, determine access by user role, and define access for entire user group(s).

Compliance

The Amazon AWS Datacenters we use to host your Showcase content are compliant with government and industry rules such as PCI DSS Level 1, HIPAA, ISO 9001 — and dozens more. For more information see: <http://aws.amazon.com/compliance/>

MDM friendly

Our iPad, iPhone, Android and Windows apps work well with industry-leading mobile device management (MDM) platforms that provide encrypted app containers.



PIN Protection

Protect individual files and pages with PIN numbers. Quickly and easily require entry of a 4-digit code for access to sensitive information.

Audits

Our platform is subject to independent source-code audits, penetration testing and infrastructure audits, so you can continually rely on our platform security.

DOS Attack protection

Showcase Workshop uses the inbuilt controls of AWS CloudFront and Elastic Load Balancer to reduce the severity of denial-of-service (DOS) attacks.

For more information on data security, privacy and regulatory compliance, please refer to the following resources:

Showcase Workshop Terms of Use:

<https://showcaseworkshop.com/legal/>

AWS (Amazon Web Services) compliance regulations:

<https://aws.amazon.com/compliance/>



showcase
workshop