15

What role does zero trust principle play in REACH CAD's security?

15 What role does zero trust principle play in REACH CAD's security?

Zero trust principles are applied to enhance security in collaborative projects using REACH CAD:

1. Continuous Authentication and Authorization

REACH CAD implements zero trust principles by:

(i) Verifying user identity and device integrity for every access request

(ii) Using strong multi-factor authentication methods beyond passwords

(iii) Continuously reassessing user access privileges as context changes.

This approach ensures that only authorized users can access sensitive design data, even if they are already inside the network.

2. Least Privilege Access

Following the zero trust model, REACH CAD:

(i) Limits user access with just-in-time (JIT) and just-enough-access (JEA) policies.

(ii) Applies microsegmentation to prevent lateral movement within the system.

(iii) Enforces granular, context-based policies for data access.

These measures minimize the potential damage from compromised accounts or insider threats.

3. Assume Breach Mentality

REACH CAD's security strategy incorporates:

(i) Continuous monitoring and verification of all traffic, including encrypted data.

(ii) Advanced threat detection to track user activity and information interaction.

(iii) Real-time analytics to detect and respond to anomalies.

This proactive approach helps identify and mitigate potential security breaches quickly.

4. Secure Collaboration

To enable secure collaboration in CAD projects, REACH CAD:

(i) Implement end-to-end encryption for all data in transit and at rest.

(ii) Provide secure file sharing capabilities with external partners.

(iii) Ensure that users connect directly to required resources without exposing the entire network.

These features allow for efficient collaboration while maintaining strict security controls.

5. Compliance and Auditing

REACH CAD's implementation of zero trust principles supports:

(i) Automatic application of security controls to meet regulatory requirements.

(ii) Comprehensive logging and auditing of all access requests and user actions.

(iii) Simplified compliance with standards like PCI DSS and NIST 800-2074.

This approach helps organizations maintain compliance and simplifies the auditing process.

By incorporating these zero trust principles, REACH CAD provides a robust security framework for collaborative projects, protecting sensitive design data from both external and internal threats while enabling efficient teamwork across distributed teams.

For more information on how REACH CAD can add value to your business, please email ***info@reach-tech.com*** *and visit* ***www.reach-tech.com***

enabling agile apparel enterprises for the digital economy

www.reach-tech.com
info@reach-tech.com