CADY

Data Security Overview

Purpose

CADY fully understands the security implications of the cloud model. Our cloud service is designed to deliver better security than many traditional on-premises solutions. Furthermore, we acknowledge the confidentiality of circuit schematics and the importance of keeping it guarded and safe. This paper outlines CADY's approach to data security and compliance of CADY's platform. It focuses on security including details on technical and organizational controls regarding how CADY protects your data.

Background

CADY is a cloud-based SaaS platform providing a service for users to upload their circuit schematics design files for integrity design analysis. The output is a report containing circuit errors, warnings, and recommendations.

Each platform user is provided with a unique username and account. Once authenticated, users can upload the design's Netlist and BOM files for analysis. The sole information item saved for further use is a metadata file relating to the analysis results, which does not enable any user-data reconstruction.

CADY does not permanently store any of the user uploaded files.

The analysis report can be viewed in the system or downloaded as HTML/.xlsx file.

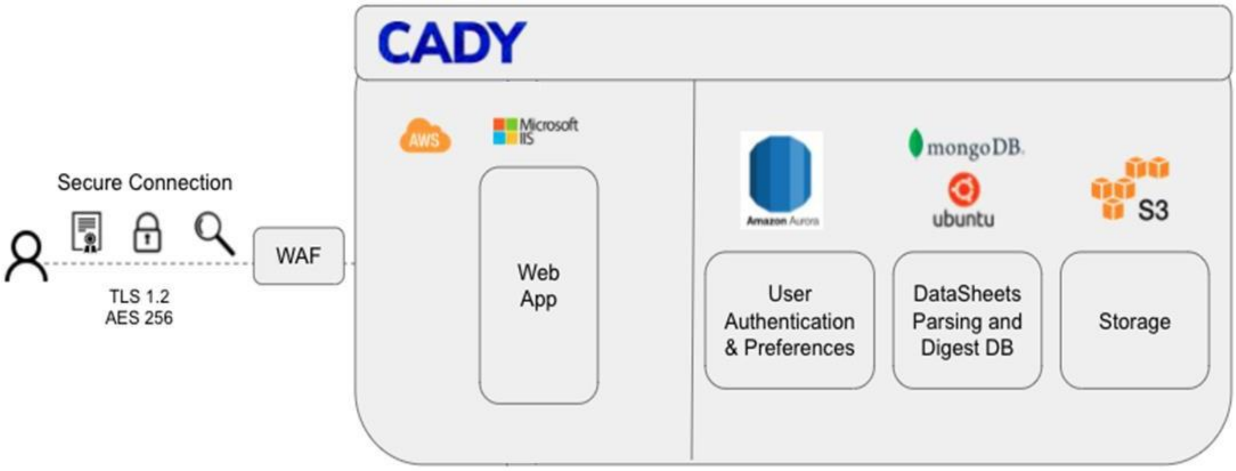
Architecture

CADY's platform operates on a Virtual Private Cloud (VPC) within Amazon Web Services (AWS) in EU-WEST-1 (Ireland). This is where data processing and metadata storage take place. To satisfy stringent security requirements, CADY implements multiple AWS built-in security functions, services, and tools. Among them are CloudTrail and GuardDuty.

Files uploaded to CADY's platform over public networks are encrypted using TLS 1.2 and above with strong cipher suites and settings. Incoming traffic is monitored and filtered by multiple layers of protection including Web Application Firewall (WAF). Only validated requests are allowed to pass through for processing.

This document is for informational purposes only. CADY Solutions Ltd. PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. No part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of Cady Solutions Ltd, except as otherwise permitted by law. Prior to its publication, reasonable effort was made to validate this information. Actual savings or results achieved may be different than those outlined in the document. This document could include technical inaccuracies or typographical errors.

The web-application reside on Microsoft Windows Server 2019 Datacenter EC2 instances. User Authentication and Preferences service is based on an AWS Aurora managed RDS/MySQL service.



Access Control

Access to CADY's application is restricted to authorized users based on unique username and password, in accordance with authentication best practices. Each user is provided with user account that can be managed from within the web console.

Data Classification & Retention

CADY does not permanently store any of the user uploaded files, hence data retention is at minimum possible and no segregation is needed.

Information Security Policy and Framework

CADY's Information Security framework and policies are designed by security experts and based on ISO 27001. Policies are reviewed and approved by management annually. Security policies are communicated to all employees periodically, as part of the ongoing data security awareness and training program.

Multi Tenancy Precautions

CADY's platform is designed, built, and maintained under the multi-tenancy assumption. Thus, user-data is constantly segregated thus preventing cross user data-access or exposure.

This document is for informational purposes only. CADY Solutions Ltd. PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. No part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of Cady Solutions Ltd, except as otherwise permitted by law. Prior to its publication, reasonable effort was made to validate this information. Actual savings or results achieved may be different than those outlined in the document. This document could include technical inaccuracies or typographical errors.

Encryption

Data in transit is encrypted using TLS 1.2 protocol or higher, in alignment with industry best practices; Furthermore, confidential non-user related data is stored on AES 256bit encrypted disks and storage volumes within the CADY Cloud environment.

Penetration Test & Vulnerability Assessment

CADY performs periodical penetration tests to seek and identify potential security vulnerabilities. Tests include (but not limited to):

1. Weekly application-level vulnerability scanning performed by a 3rd party SaaS scanner.
2. Weekly Infrastructure level vulnerability scanning performed by a 3rd party SaaS scanner.
3. Annual application security penetration test by a 3rd party “White-hat“ vendor

Incident Monitoring & Response

CADY closely monitors all data-security related events. Incident response procedure ensure that corrective and preventive actions are taken immediately in any case of suspected data security breach.

Availability, Backup and Restoration

CADY’s platform is hosted on the highly trusted Amazon Web Services infrastructure, ensuring high-availability and uptime. Data and system components are regularly backed up using the infrastructure’s built-in capabilities. Restoration tests are performed periodically to ensure full and rapid recovery in case of an emergency.

HR Security

CADY’s Human Resources performs personal interview and reference check all hiring candidates and employees. In addition, where applicable and in accordance with local laws, background checks and identity validation checks are performed as part of the HR security protocols.

Physical Security

Access to CADY facilities is restricted and allowed only to authorized personnel, using a physical access control system. Data center security is fully controlled by Amazon, CADY’s hosting provider. All Datacenters include multiple, top-tier security controls such as biometric identification, cameras, vehicle barriers, and advanced intrusion detection systems.

For more details, see: https://aws.amazon.com/compliance/data-center/controls/

This document is for informational purposes only. CADY Solutions Ltd. PROVIDES THIS DOCUMENT “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. No part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of Cady Solutions Ltd, except as otherwise permitted by law. Prior to its publication, reasonable effort was made to validate this information. Actual savings or results achieved may be different than those outlined in the document. This document could include technical inaccuracies or typographical errors.