CADY

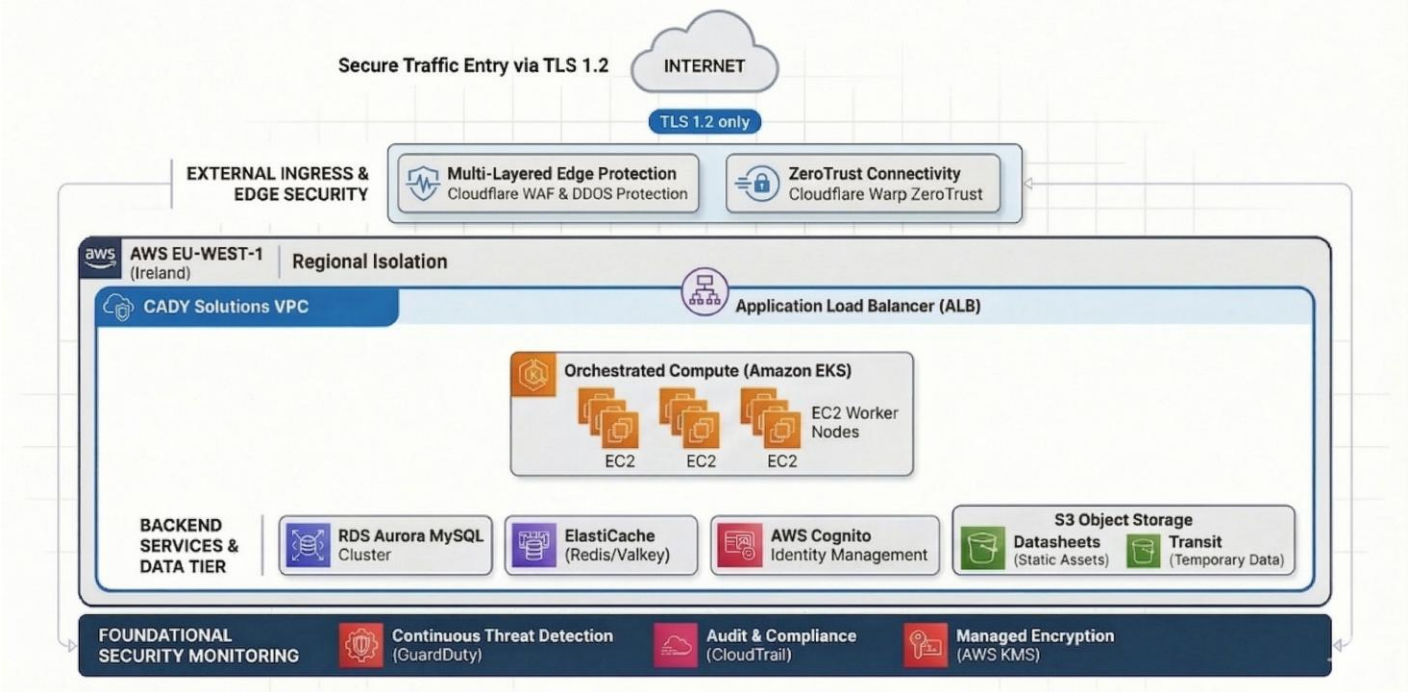
Data Security and System Architecture Overview

Introduction

CADY is a cloud-native Software-as-a-Service (SaaS) platform providing automated integrity analysis for circuit schematic designs. By parsing electrical component datasheets and validating them against design intent, CADY identifies errors, warnings, and recommendations that are critical to hardware reliability.

Our security philosophy is built on the premise that cloud-integrated analysis is inherently more secure than traditional on-premises solutions. Localized hardware environments are often plagued by physical theft risks, unpatched local servers, and fragmented audit trails. CADY mitigates these risks through a centralized, immutable audit architecture and a strict **"No Persistence"** rule.

Under this rule, user-uploaded Netlist and Bill of Materials (BOM) files are treated as highly confidential, non-persistent assets. These files are discarded immediately upon the completion of the analysis. CADY retains only the resulting metadata and analysis reports for customer retrieval and anonymous internal statistics. This metadata is insufficient to reconstruct the original proprietary design data, ensuring that client intellectual property remains protected.



CADY

Architecture and Infrastructure Segregation

CADY's infrastructure is hosted within the **AWS EU-WEST-1 (Ireland) region**. The environment is architected using a security-in-depth approach, utilizing the AWS Well-Architected Framework to ensure high availability and logical segregation.

- **VPC & Network Segregation:** The environment is isolated within a Virtual Private Cloud (VPC) divided into Public and Private subnets. Public subnets are restricted to handling incoming traffic and hosting NAT gateways. All core compute, databases, and processing nodes reside in Private subnets, effectively shielded from direct internet exposure.

- **Compute Layers:**
  - **EKS Clusters:** CADY utilizes Amazon Elastic Kubernetes Service (EKS) for container orchestration.

- **Application Servers:** The web application layer is deployed on Amazon EKS, with application workloads running in Debian-based Docker containers. The underlying cluster nodes operate on Amazon Linux, and the platform is maintained in accordance with current security hardening and infrastructure management practices.

- **Boundary Security:** All incoming traffic is filtered through the Cloudflare Web Application Firewall (WAF) to defend against OWASP Top 10 threats. Administrative access is restricted to a secured internal network accessible only via a dedicated VPN Endpoint.

Data Storage and Database Management

CADY utilizes specialized storage components tailored to specific application functions. All persistent data stores are encrypted at rest.

Storage Component	Function	Encryption at Rest (AES-256)
Aurora MySQL (RDS)	User Preferences, and Account Data	Enabled (AWS KMS)
MongoDB (Standalone)	Component formal language data	Enabled (AWS KMS)
S3 Buckets	Categorized: Transit (Landing zone), Logs, Results/Policy History	Enabled (AWS KMS)
ElastiCache (Redis/Valkey)	Caching and queuing	Enabled (AWS KMS)

Note: The "Transit" S3 bucket serves as the temporary landing zone for non-persistent Netlist/BOM files; these files are purged immediately following analysis.

Data Protection and Encryption Standards

We employ rigorous cryptographic standards to ensure the confidentiality and integrity of data across all states:

- **Data in Transit:** Public network communication is mandated to use TLS 1.2 or higher. We enforce the use of **strong cipher suites** and Cloudflare-managed certificates to prevent Man-in-the-Middle (MITM) attacks.
- **Internal Communication:** Encryption is not limited to the perimeter; all internal traffic between service components is protected via TLS.
- **Data at Rest:** All disks and storage volumes are encrypted using AES-256 bit encryption. Key management is handled through **AWS Key Management Service (KMS)**, ensuring centralized control and rotation of cryptographic keys.

CADY

Identity and Access Management

CADY implements a zero-trust approach to identity, governed by the Principle of Least Privilege.

- **User Authentication:** Access is managed via AWS Cognito, supporting Single Sign-On (SSO) through OAuth 2.0/OpenID (specifically integrated with Altair) and SAML.
- **Administrative Access:** Access to the **secured internal network** is strictly limited and requires **Multi-Factor Authentication (MFA).**
- **Logical Segregation:** We enforce a total separation of duties. Access to the production environment is restricted to dedicated admin roles. **Developers and QA staff are strictly prohibited from accessing production systems**; this is enforced through granular IAM policies and VPC-level logical segregation.

Vulnerability Management and Security Monitoring

Our proactive defence strategy includes continuous monitoring and a structured remediation lifecycle.

- **Continuous Monitoring:** We utilize AWS CloudTrail (auditing), Amazon GuardDuty (threat detection), and AWS Security Hub for centralized security posture management.
- **Scanning & Dependencies:**
    - **Snyk:** Integrated into the CI/CD pipeline to identify and remediate vulnerabilities in third-party software dependencies.
    - CADY Conducts regular infrastructure and application-level vulnerability scans.
- **Penetration Testing:** CADY undergoes an annual third-party "White-hat" penetration test. Crucially, this includes a formal **Retest phase** to verify the successful remediation of any discovered vulnerabilities.
- **Patch Management:** A definitive **monthly schedule** is maintained for applying security patches to operating systems, system software (webservers/databases), and applications.

Governance, Compliance, and Business Continuity

CADY operates under a formal Information Security Management System (ISMS), documented under policy **ISMS-POL-001**.

- **Compliance Posture:** Our framework is **ISO 27001:2022 certified**, incorporating the **93 Annex A controls** as our baseline for security operations.
- **Leadership:** Security governance is spearheaded by our CISO, **Gil Ohayon**, supported by Senior Technology Manager, **Ido Port**, and CEO, **Gilad Shapira**.
- **Resiliency & Backup:** CADY utilizes Multi-AZ (Availability Zone) deployments to ensure high availability. We employ **AWS Backup** for daily snapshots of production databases and system components.
- **RTO/RPO:** Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) are managed via AWS Backup, with restoration procedures tested at least every six months to ensure rapid recovery in emergency scenarios.

CADY

Physical and Human Resource Security

- **Physical Security**: While AWS manages data center security (biometrics, vehicle barriers, and 24/7 surveillance), CADY also restricts access to its physical facilities. All CADY offices utilize a physical access control system limited to authorized personnel.
- **HR Protocols**: All employees undergo interviews, reference checks, and identity validation.
- **Security Culture**: Personnel with network access undergo mandatory, periodic security awareness training. This program includes specialized anti-phishing and social engineering simulations to ensure our human firewall remains as robust as our technical infrastructure.

Artificial Intelligence (AI) Usage & Data Handling

Artificial Intelligence (AI) Usage & Data Handling CADY uses AI, including LLM-based services, to analyze electrical design data such as Datasheets, Schematics, Netlists, BOMs, and related documentation to identify issues, warnings, and recommendations. In some cases, relevant data may be processed by approved third-party AI providers. Customer data is analyzed using models configured such that customer data is not used to train CADY's models or third-party models, is not used for continuous learning, and is not fed back for model improvement. AI outputs are advisory only and do not automatically modify customer design files.

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

CADY