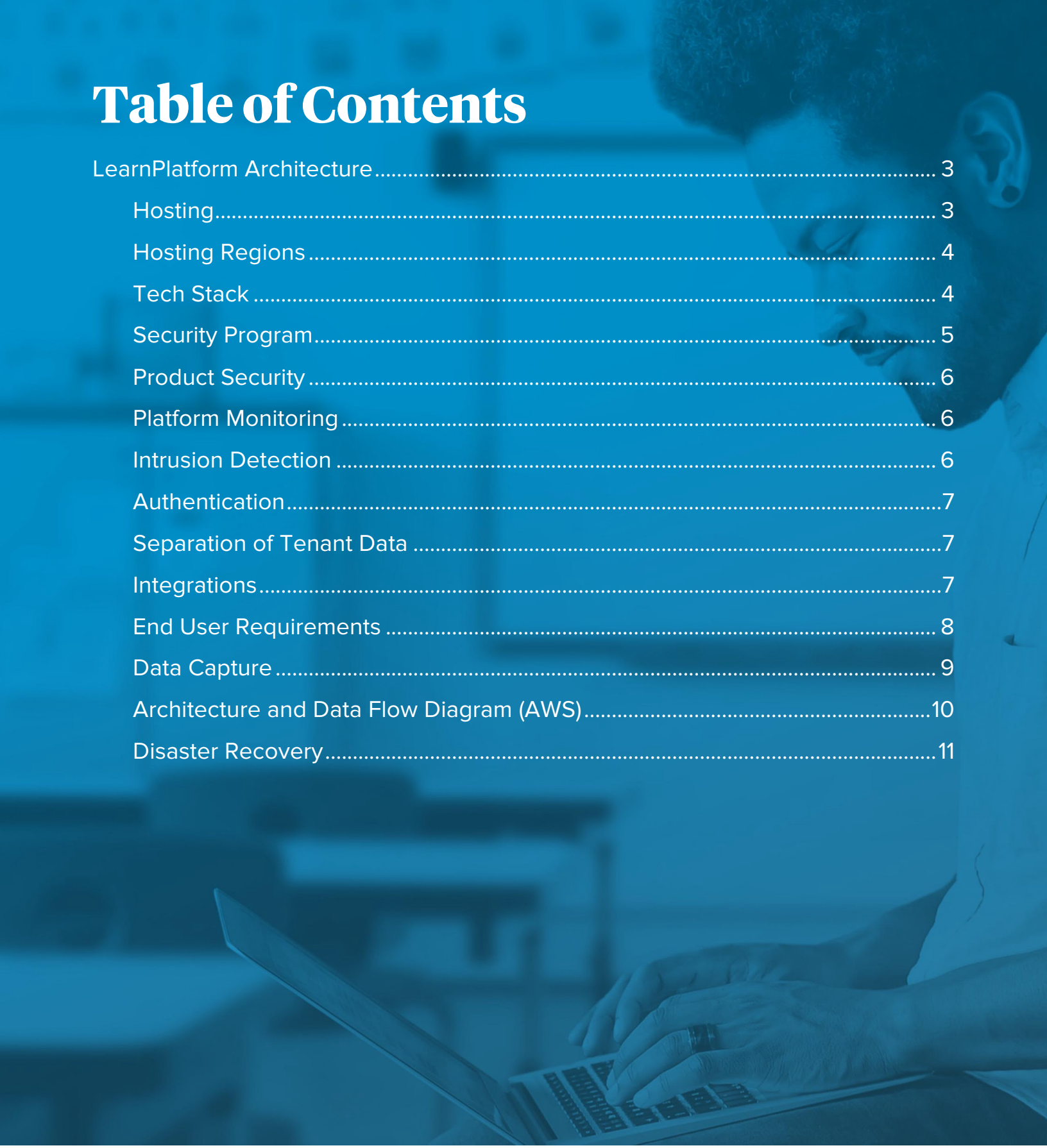
LEARN PLATFORM BY INSTRUCTURE

LEARNPLATFORM ARCHITECTURE OVERVIEW

Engineering, Security, and Operations

April 2024

Table of Contents



PLATFORM LEARN BY INSTRUCTURE

LearnPlatform Architecture

They say "May you live in interesting times..." and nothing could be more apt than today's technology driven world where we witness daily the complexity and intricacies of navigating periods of change and transformation.

In today's learning environment, K-12 organizations are deploying more technology and tools than ever before and need efficient, evidence-based approaches for gaining insight into the selection and ongoing management of these platforms. Shareable spreadsheets, homegrown efforts, and disconnected systems can limit scalability, inhibiting achievement of equitable outcomes, plus open organizations up to cyber risk and non-compliance with federal/state data privacy regulations. LearnPlatform offers a better solution for instructional, operational, and budget decision support.

LearnPlatform provides central office automation and data-rich insights that empower K-12 organizations to make informed decisions about their edtech investments to ensure safety, efficacy, equity, compliance, and cost-effectiveness. Customizable libraries and workflows allow leaders to streamline and centralize edtech vetting and communication, while unique research-driven technology and services give districts the tools to evaluate product effectiveness in context.

The following supplemental document describes the LearnPlatform architecture for those curious technical types who love getting into the detail of just how we make this beautiful partnership work.

Hosting

Instructure's product family, including LearnPlatform, is hosted in the cloud by Instructure and delivered over the internet through the world's most trusted public cloud provider, Amazon Web Services (AWS). The basic building blocks of AWS include services such as Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Auto Scaling Groups (ASG), Simple Storage Service (S3), Elastic Block Store (EBS), Virtual Private Cloud (VPC), Simple Email Service (SES), and Identity and Access Management (IAM).

We also use advanced AWS platform capabilities including AWS Redshift which powers the Inventory Dashboard. Amazon Kinesis, AWS Lambda, AWS Fargate, AWS Elastic Kubernetes Service ("EKS"), and Amazon Relational Database Services ("RDS") are additional services utilized. Instructure's products are designed to make full use of the real-time redundancy and capacity capabilities offered by AWS, running across multiple availability zones in regions throughout the world. Primary storage is provided by Amazon S3, which is designed for durability exceeding 99.99999999%.

LearnPlatform is hosted on a horizontally and vertically scaling virtual private cloud (VPC) using various instance types including m5.large, m5.xlarge, db.m6g.xlarge, db.m6g.4xlarge. Instance types are examples and may change as sizing needs change.

Hosting Regions

For US customers, LearnPlatform uses one Amazon Web Services (AWS) region, ensuring that client data is not stored outside of the United States:

- AWS US-East-1 (Virginia) with the following availability zones: us-east-1a, us-east-1b, us-east-1c, us-east-1d, and us-east-1f.

Tech Stack

LearnPlatform is made up of several components, with the core services as follows:

- LearnPlatform is run on Debian
- Platform services are written in Ruby on Rails, Elixir, and Node.js
- Node is utilized for Data Collection and Data Aggregation

- Our front-end framework for the LearnPlatform website application is React
- Platform extensions leverage Javascript (Chrome Extension) and Swift (iOS extension)

Security Program

LearnPlatform is included as part of Instructure's robust information security program that runs on a continuous, PDCA-cycle. It was created based on guidance provided by ISO/IEC 27000:2018 and controls described in ISO/IEC 27001:2013, and is managed by Instructure's Chief Information Security and Privacy Officer. The security program is attested to by a number of current security certifications including ISO 27001, SOC 2, SOC 3, UK Cyber Essentials Plus, PCI DSS SAQ D and Attestation of Compliance.

LearnPlatform has a software development lifecycle (SDLC) that incorporates secure coding practices and controls. All code goes through a developer peer-review process before it is merged into the code base repository. The code review includes security auditing based on the Open Web Application Security Project (OWASP) secure coding and code review documents (including the OWASP Top Ten) and other community sources on best security practices.

Instructure's Security Team regularly performs vulnerability scans on the Instructure Learning Ecosystem using a number of internal and external tools and techniques and we make available to customers the results of our annual third-party penetration tests because we believe that being open about all things - security included - enables us to build the best possible product for our customers.

In addition to these measures, the Amazon Web Services infrastructure on which LearnPlatform is hosted has a variety of formal accreditations. Some of the many certifications include:

DoD SRG • FedRAMP • FIPS • IRAP • ISO 9001 • ISO 27001 • ISO 27017 • ISO 27018 • MLPS Level 3 • MTCS • PCI DSS Level 1 • SEC Rule 17-a-4(f) • SOC 1 • SOC 2 • SOC 3 • UK Cyber Essentials Plus

For additional information about AWS security certifications and standards compliance, please refer to http://aws.amazon.com/security and http://aws.amazon.com/compliance/.

Product Security

The AWS shared-responsibility model provides a number of resources out-of-the-box for anti-hacking measures including private-by-default services (least privileged access), DDoS protect, Web Application firewall, and others. Built on top of that, the LearnPlatform VPC includes further anti-hacking measures such as using authorization then authentication and RBAC schemes, disabling unnecessary services/users, encrypting data in transit and at rest, and physical and logical separation of source code from production sites. In addition, Instructure practices secure coding principles and performs manual, static, and dynamic assessment of code against the OWASP Top 10.

The following is an overview of LearnPlatform's product security measures:

- All data is encrypted in transit with TLS v1.2 or higher.
- All data is stored at rest within AES-256-bit-encrypted volumes.
- All environments are deployed into an AWS Virtual Private Cloud (VPC) within secure private networks. Each component is protected by a security group with an appropriate, restrictive rule set.
- Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

Platform Monitoring

System performance, availability, and capacity are monitored with New Relic, AWS CloudWatch, and Rollbar. Internal performance dashboards and alerts monitor critical metrics such as data event types and volume, CPU, memory, latency, IOPS, and error rates across the Platform’s services. Rollbar monitors specific error types (both backend and frontend) to detect potential user experience issues.

Intrusion Detection

LearnPlatform leverages AWS's GuardDuty service (including Threat Intelligence) to continuously monitor for malicious or unauthorized behavior. It monitors for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. GuardDuty also

detects potentially compromised instances or reconnaissance by attackers. Any alerts generated by GuardDuty are forwarded to Instructure's Security Team. GuardDuty includes the ability to set up automated preventative actions such as automatically modifying security group rules and restricting access on ports based on triggered security findings.

Authentication

LearnPlatform acts as a Service Provider and will integrate with any Identity Provider implementing SSO with SAML 2.0 (e.g. Google SSO, Azure, Active Directory (ADFS)). In addition to SAML 2.0, LearnPlatform can also support some OAuth 2.0 authorization flows.

Separation of Tenant Data

Tenants within LearnPlatform are logically separated through roles and organizational memberships. Pre-execution hooks validate that an authenticated user has the expected roles and memberships to the organization in order to view or modify data.

Integrations

LearnPlatform can incorporate data from a range of other online sources and agency data:

- **JAMF**: Organizations can use the JAMF data connection to build a list of EdTech products deployed to an organization’s fleet of iOS devices managed by the same JAMF instance. Integration with JAMF is accomplished over HTTPS using JAMF’s publicly available API.
- **1EdTech**: The system enhances Product Library metadata by obtaining product certification data via 1EdTech’s TrustEd Apps API. All data is retrieved over HTTPS using 1EdTech’s publicly available API. No client data is sent to 1EdTech beyond the tool name.
- **OneRoster**: Organizations roster their membership by uploading OneRoster v1.1 compliant files to the system via SFTP.
- **Clever**: The system can auto-generate launch links for applications within Clever. This integration can be accomplished by organizational Administrator's through configuration screens in the application.

End User Requirements

Users can interact with and use LearnPlatform via:

- the platform website;
- the teacher or the student Chrome extension;
- IMPACT (module that integrates data from multiple sources for evidence-based reports and dashboards)

LearnPlatform's cloud hosted EdTech Effectiveness System is accessible through any operating system using standard web browsers including:

- Chrome
- Firefox
- Edge
- Safari

A component of LearnPlatform's EdTech Effectiveness System - Inventory Dashboard - is able to collect usage data from Windows, Chrome, and iOS devices.

Browser Extensions

For monitoring high-level usage of tools, LearnPlatform employs a browser extension. For districts managing devices with Google Admin Console or Microsoft InTune, the extension is pushed out by the district through InTune for use with Edge browsers so LearnPlatform can identify visits to browser-based educational technology. Districts can provision LearnPlatform's functionality to identify page visits [*events*] and time on application [*minutes*] at a browser level via the extension for all logged-in users accessing educational technology tools via Chrome or Edge browsers. Personal student and teacher devices will continue to track usage as long as the user is logged into the browser with their school credentials and has syncing turned on. LearnPlatform will also be able to identify iOS events through a LearnPlatform application that can be installed via the district MDM; iOS events tracking is specific to school-issued devices managed by the MDM.

Data Capture

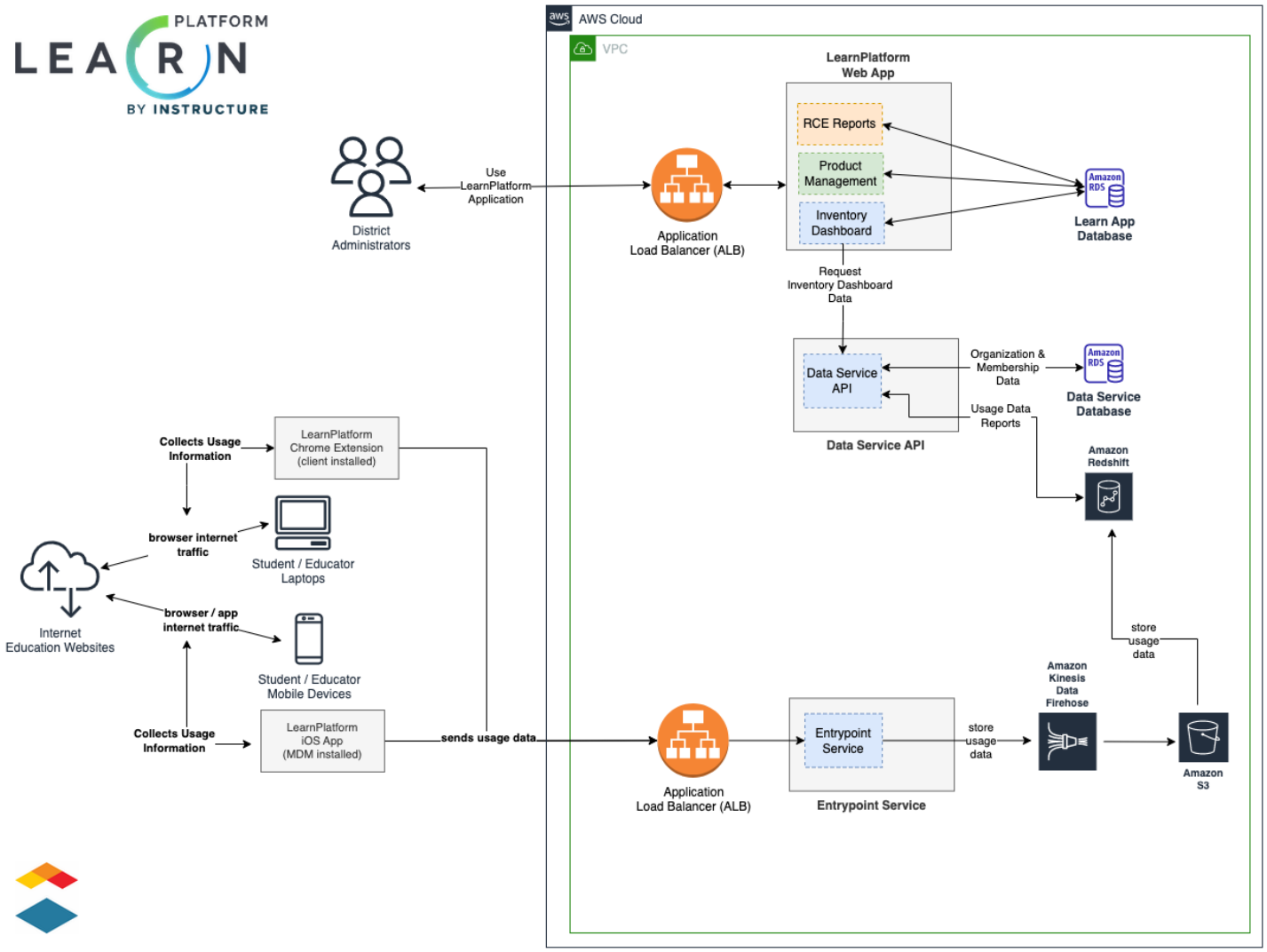
Extensions are deployed to student and teacher laptops/tablets. These extensions capture data on ed tech product usage and transmit this data to the system. Data is sent in batches. The typical data payload size per minute for each device is less than 1KB.

Data captured by the entry point service is pushed into a data warehouse through Amazon's Kinesis Firehouse.

A data service aggregates data from the data warehouse and stores the results in a database for reporting purposes. The app.learnplatform.com web interface accesses aggregated data through an internal API.

District administrators can access reporting and other aggregated views of data through the app.learnplatform.com web interface, and if granted a privileged role, can also configure their instance of the platform through this web interface.

Architecture and Data Flow Diagram (AWS)



Disaster Recovery

Instructure maintains Business Continuity and Disaster Recovery policies which are updated at least annually. Annually, we also conduct full disaster recovery tabletop testing and make any policy changes required.

Learn Platform is backed up daily and DR/retention is as follows:

- The recovery point objective (RPO) for all data is 24 hours.
- The recovery time objective (RTO) for all services is 1 hour.
- Last 7 days of backups are retained.
- Data can be restored to a point in time within the 7 days retention period