COMPARISON: BRIGHTSPACE VS. BUILD

FEATURES

FEATURES	BRIGHTSPACE	BUILD
Assignment, Quiz, Grades	Available	Available
Open Source	No	Yes
Native Learning Repository	Available	Available
Offline and Online Tablet Grader	Available	Not Available
Native Webcasting and Online Capture	Available	Not available Must integrate to 3rd party with additional cost
Pathways Based on Learning Outcomes / Competencies	Available	Not Available
Predictive Analytics	Available	Not Available
Machine Learning	Available	Not Available
Adaptive Learning	Available	Not Available
Accessibility	Available	Not Available
Learning Outcome	Available	Not Available
Gamification (badges & certificates)	Available	Not Available
User Experience Design / UX	Simple user interface. 100% mobile friendly.	Complicated - depends on the programmer
Data Export	Available – 70 presets data	Need to be built
Roles and Permissions	Available – without coding	Need to be build
Integration	Available – open API	Need to be built

SCALABILITY & SUPPORT

SCALABILITY	BRIGHTSPACE	BUILD
Servers	Cloud based – no investment	On premise – large capex
Troubleshooting Servers	Included	Not included - manual
Server Bandwidth	Included	Not Included
Community	Included	Not Available
Guaranteed SLA	Available (99.97%)	Not Available
Integration to 3rd party	Open API, integrated to more than 500 add-on applications	Manually Integrate
Security level (see appendix for detail)	ISO 27001:2013 Certification	Not Available
Local support	Available	Not Available
Training	Available	Not Available
Track Record	20M+ users worldwide	Not Available

TIME – OPPORTUNITY COST

TIMELINE	BRIGHTSPACE	BUILD
Platform Development	Immediately	Minimum 9 months
Platform Integration	Immediately (use open API)	Minimum 3 months
Infrastructure Development	Immediately	Minimum 1 month
Content Design	1 month full support on course builder	1 month without support
Setting up Roles and Organization Structure	1 week	> 1 month

COST

COST	BRIGHTSPACE	BUILD
Implementation fee	One-time fee	One-time fee
Monthly fee	- Subcription based per user - No hidden fees - All is included	- Monthly bandwidth - Electricity - Genset backup - Programmer fees (salary) - Maintenance fee - Support fee
Support team	- Administrators & Helpdesk (IT) - Instructors (Managers or HR)	- Administrators & Helpdesk (IT) - Instructor (Managers or HRl) - Infrastructure Team (additional cost) - Programming Team (additional cost)
Customization fee	- Theme, logo, design customization: drag and drop with no coding, **FREE** - Settings: configurable, **FREE** - Integration: full documentation, use existing resources - **FREE** - Community: **FREE**	- Customization fee occur every customization (man days / project based) - New code needed for every customization - Role settings: need to be defined from the start, change it might add additional fee - Integration: might cost a lot, no documentation - Yearly maintenance fee (recurring)

APPENDIX 1 – SECURITY & COMPLIANCE

APPLICATION SECURITY

Brightspace owned by "D2L", in which Sejahtera Group under PT. Kreasi Sejahtera Teknologi is their sole representative in Indonesia, have high-standard security in their application. This appendix is to give more information about our security and best practices that we have implemented into our company and into our system. More info can be found on https://www.d2l.com/security/certifications/

DATA CENTER

D2L hosted services are provided on Amazon Web Services (AWS). Physical and operational security processes are described for network and infrastructure under AWS' management, as well as service-specific security implementations documented in Amazon Web Services: Overview of Security Processes, which outlines AWS' data center controls such as:

- Physical and Environmental Security
- Fire Detection and Suppression
- Power
- Climate and Temperature
- Management
- Storage Device Decommissioning: AWS uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process.
- Amazon's infrastructure fault tolerant design: Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.
- Certification: AWS holds numerous security certifications, which can be reviewed at https://aws.amazon.com/compliance/

BEST PRACTICES

1. NETWORK PROTECTION
   - D2L takes a layered approach to protecting its network infrastructure and resources.
   - Perimeter stateful packet inspection firewalls and edge routers block unused protocols and help protect against malicious network traffic, viruses and malware.
   - **Intrusion Detection Systems (IDS)** and **Intrusion Prevention Systems (IPS)** detect and remediate potentially malicious network traffic. Signature sets are reviewed and updated on a regular cadence for typical releases and point in time for high priority releases.
   - Deep packet inspection technology is deployed to allow for forensics if required.
   - VLAN segmentation helps keep traffic segmented and internal firewalls segregate traffic between network boundaries.
   - **Security Information and Event Management (SIEM)** technology is deployed throughout D2L infrastructure. This technology collects and aggregates events from end points and stores it centrally for event correlation, security alerting and analysis.

2. SECURE TRANSMISSION
   - Connection to the Brightspace environment is via **TLS cryptographic protocols** with **RSA® encryption**, ensuring that customers have a secure connection from their browsers to our service.

- Individual user sessions are identified and re-verified with each transaction, using a unique token created at login.

3. DENIAL OF SERVICE MONITORING

- D2L uses internal network technology such as firewalls, WAF's and IDS/IPS to protect against denial of service (DoS) attacks.
- D2L uses a 3rd party service provider to protect against distributed denial of service (DDoS) attacks. This service provides detection and mitigation for volumetric DDoS attacks.

4. VULNERABILITY MANAGEMENT AND PATCHING

- **System hardening**
  - Before a server image is certified, unnecessary services are disabled and ports closed. Templates (such as those from National Institute for Standards & Technology (NIST), Center for Internet Security (CIS), as well as Microsoft's Baseline Security Analyzer (MBSA) are used in order to validate that the image has been hardened to industry standard best practices.
- **Vulnerabilities and Patching**
  - D2L tests all code for security vulnerabilities before release, and regularly scans its network and systems for vulnerabilities.
  - Each month following "patch Tuesday", a group representing Brightspace Cloud, QA, Product Development, and Implementation meets to review all Microsoft® patches in order to assess the critical nature, risk and potential effect to D2L services. Patches may go through a QA process prior to being scheduled for implementation during the next available maintenance period.
- **Annual Third-Party Assessments**
  - D2L uses a third party to conduct penetration and vulnerability scans against the Brightspace platform annually.

5. ENDPOINT THREAT AND PROTECTION

- Anti-virus software is deployed on all personnel laptops and desktops and is centrally managed to ensure all DAT files are up to date. Centralized reporting ensures malware infections are properly quarantined and escalated for further actions where needed.

6. APPLICATION SECURITY

- The application is developed using the **OWASP Top Ten framework** and various security components are integrated into the application architecture. Security analysts regularly look for vulnerabilities through code reviews, application scans, and internally-run penetration tests. Third parties validate the technical controls by conducting regularly-scheduled network penetration and application vulnerability tests.

7. INCIDENT MANAGEMENT

- D2L has a defined Security and Privacy Incident Management process to handle security and privacy incidents. This process can be initiated by a D2L customer,

internal D2L employee or the public. If a security incident is identified the following high-level process is followed.

- **Monitoring and Awareness**: A security and/or privacy incident is identified, communicated to the Security Incident Response Team (SIRT).
- **Detection and Analysis (triage):** The incident is assessed to determine the severity, priority, scope and impact. This step can include evidence preservation and containment activities.
- **Mitigation:** Recommendations are created and executed that will to contain, eradicate and/or recover from the incident in question.
- **Recovery:** Containment is complete. Where applicable, scanning of environments occurs to ensure mitigation is complete.
- **Communications:** This can include communications with internal resource teams, stakeholders and D2L customers. Based on the findings of triage and analysis, the appropriate communications are drafted, approved and shared.
- **Post Incident Activity:** In this stage, lessons learned are completed to gather feedback and evolve incident response process and procedures. Where applicable, root cause is identified and logged.

8. VENDORS AND SUBCONTRACTORS

- D2L vets all applicable vendors and subcontractors to ensure they too provide an appropriate level of security.

9. SECURITY AWARENESS

- D2L has a security awareness program that serves to ensure employees understand the importance of security and its intersection with their workday.
- New employees are required to take security training and training completion is audited throughout the year.
- The Information Security team leverages several security threat intelligence sources to keep up to speed on the latest and emerging security threats. This information is disseminated through regular security awareness campaigns to help ensure that D2L staff are aware of these threats and what to do if they encounter them.

COMPLIANCE

We take our responsibility to protect the confidentiality, availability and integrity of your data seriously, which is why we have the following certifications:

ISO 27001:2013

ISO® 27001 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance. This is a widely-recognized international security standard. Certification in the standard requires us to:

- Systematically evaluate our information security risks, considering the impact of company threats and vulnerabilities
- Design and implement a comprehensive suite of information security controls and other forms of risk management to address company and architecture security risks
- Adopt an overarching management process to ensure that the information security controls meet our information security needs on an ongoing basis

The key to the ongoing certification under this standard is the effective management of a rigorous security program. The **Information Security Management System (ISMS)** required under this standard defines how we perpetually manage security in a holistic, comprehensive way. The ISO 27001 certification is specifically focused on the D2L ISMS and measures how our internal processes follow the ISO standard. Certification means a third party accredited independent auditor has performed an assessment of our processes and controls and confirms they are operating in alignment with the comprehensive ISO 27001 certification standard. **Request Certification**

ISO 27018:2014

ISO/IEC 27018 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect **Personally Identifiable Information (PII)** in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. In particular, ISO/IEC 27018:2014 specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which might be applicable within the context of the information security risk environment(s) of a provider of public cloud services.

SSAE 18 (SOC 1 TYPE 2 AND SOC 2 TYPE 2)

Service Organization Control (SOC) Reports are independent third-party examination reports that demonstrate how D2L achieves key compliance controls and objectives. The purpose of these reports is to help you and your auditors understand the D2L controls established to support operations and compliance. The D2L SOC Reports include four of the Trusted Services Principles: Security, Confidentiality, Processing Integrity and Availability with no exceptions in related controls.

CLOUD SECURITY ALLIANCE (CSA) SECURITY, TRUST AND ASSURANCE REGISTRY (STAR)

As part of the Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR) Self-Assessment program, D2L submitted a self-assessment report, the Consensus Assessments

Initiative Questionnaire (CAIQ), that documents our compliance to CSA published best practices.
The STAR program includes a complimentary registry that documents the security controls provided by D2L to manage our cloud instances. This publicly accessible registry is designed for users of our cloud services to assess our specific security practices and assist our current and perspective customers in responding to their security questions.

The Consensus Assessments Initiative Questionnaire (CAIQ), which provides industry-accepted ways to document what security controls exist in our Software as a Service (SaaS) offering. The questionnaire (CAIQ) provides a set of over 140 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider.

Copy of D2L's CAIQ is located at: https://cloudsecurityalliance.org/star-registrant/desire2learn