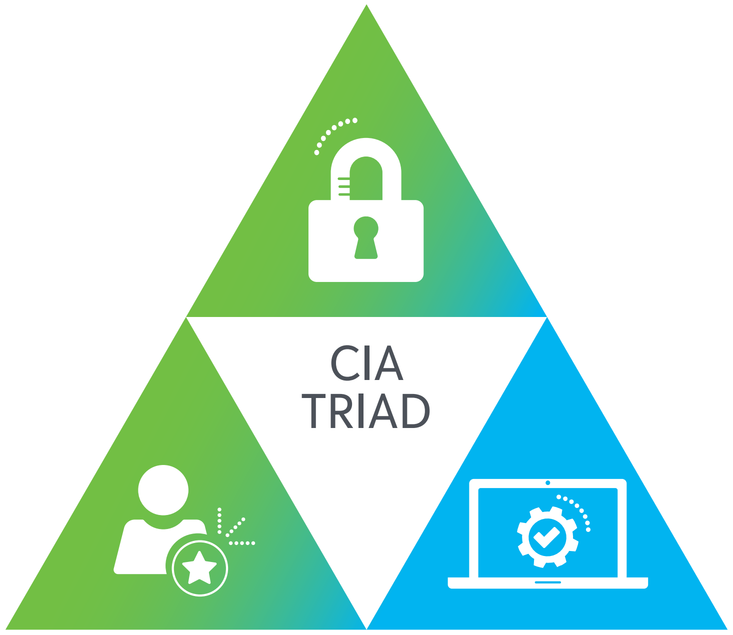
Blackbaud Luminate Online®
Security Overview

Operating in today's technology-enabled environment provides tremendous opportunity for Blackbaud and our customers to "do good" like never before. This opportunity comes with new and ever-changing risk. Internet-based adversaries can quickly disrupt a company's otherwise smooth operations. Attackers are constantly refining their tactics and developing new methods that place us all at risk.

Blackbaud strives to implement and maintain a proactive and protective information security posture focused on avoiding or mitigating attacks long before they can present a risk to our capabilities or customers.

Our Information Security team leverages the industry standard CIA Triad Model (Confidentiality, Integrity, Availability) in conjunction with various industry control frameworks, such as the NIST CSF, PCI DSS, ISO27001, SOC 1, SOC 1 type 2, and others to protect our solutions.

Blackbaud leverages these frameworks and compliance standards to ensure that the solutions we deliver to our customers are best in breed and meet the rigorous cyber security requirements outlined by various governmental and regulatory entities.



CONFIDENTIALITY
Information is not disclosed to unauthorized individuals

CIA TRIAD

INTEGRITY
Ensuring accuracy
and completeness of
data that can't be modified
in any unauthorized manners

AVAILABILITY
Information should be
readily available to authorized
users whenever it is needed

This white paper is for informational purposes only. Blackbaud makes no representations or warranties, expressed or implied, in this summary. The information contained in this document represents the current view of Blackbaud, Inc., on the items discussed as of the date of this publication.

All Blackbaud product names appearing herein are trademarks or registered trademarks of Blackbaud, Inc. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Continued on next page...

Security at Blackbaud

Our world-class security, privacy, and risk-management teams work every day to ensure the safety of your data by adhering to industry standard practices, conducting ongoing risk assessments, aggressively testing the security of our products, and continually assessing our infrastructure.

SECURITY AWARENESS

Today, so much of security is predicated upon user behavior. That's why Blackbaud employees are all engaged in ongoing Security Awareness and rigorous training campaigns to ensure they are empowered to protect both Blackbaud's and our customers' data. All employees are engaged in continual phishing simulation testing to increase their awareness of cyber security social engineering and phishing techniques. Furthermore, employees with access to customer data receive additional training to ensure they understand all of Blackbaud's data handling practices. In addition, the Blackbaud Security team partakes in global communities and conference platforms to share information and present on industry best practices to improve the community's security awareness posture.

SECURE DESIGN

Blackbaud's application security team partners with software engineers to ensure the code for your solutions is secure. This begins with training the team on secure code and threat modeling training to help our team understand how attackers decompose applications to find weak points and how to incorporate security into design principles to prevent those attacks. Our developers put those learnings to the test in gamified secure development contests throughout the year. Finally, as developers are writing software and checking in snippets of code, we have systems that scan that code and offer near real-time feedback.

MONITORING

Visibility into the activities of potential bad actors is critical to maintaining secure infrastructure. Blackbaud keeps your data secure with in-house resources that work closely with managed security services partners to monitor our environments 24 hours a day, 7 days a week, 365 days a year. Our proactive threat hunting team mines data in our environments to identify anomalous behavior that may indicate a security threat. Furthermore, we scan the dark web for risks, including potentially compromised customer credentials.

THREAT DETECTION

Finding bad actors means knowing where to look. Our team analyzes organizations that have been victims of data breaches in the past to understand what happened, how it happened, and why it happened so we can apply these key learnings to Blackbaud's program to keep data secure. Doing so also enables Blackbaud's threat risk and modeling to proactively identify potential bad actors that would want to come after us or our customers, as well as their possible motivations for doing so.

RESPONSE

Blackbaud maintains a dedicated incident response program aligned with industry standard practices to Identify, Contain, Eradicate, and Recover from security incidents. The objective of Blackbaud's Cyber Security Incident Response program is to promptly and effectively mitigate the impact and duration of a security relevant incident. In order to accomplish this, we believe much of the hard work occurs long before an incident is ever identified through proper preparation. We regularly test the incident response plan via regular tabletop exercises used to simulate potential attacks and response scenarios. This facilitates regular practice and continuously improves the incident response function. We also perform regular penetration testing to evaluate our preventative, detective, and responsive security capabilities. Additional information is available in the Blackbaud Cyber Security: Incident Management and Response Overview. More details are also available in our annual audit reports and upon customer request.

Continued on next page...

Additional Risk Management Strategies

Our world-class security, privacy, and risk-management teams work every day to ensure the safety of your data by adhering to industry standard practices, conducting ongoing risk assessments, aggressively testing the security of our products, and continually assessing our infrastructure. Our promise to you is that your Blackbaud solution is always secure, protected, and reliable through:

- Clear security requirements and reporting on data protection, encryption, and monitoring
- Routine vulnerability assessments and DDoS auto-mitigation response
- Active participation in Cyber Security thought leadership:
    - Blackbaud is a member of Cloud Security Alliance (CSA) and assesses our products and environments against the CSA Consensus Assessment Initiative Questionnaire (CAIQ).
    - Blackbaud Security is a member of the Financial Services Information Sharing and Analysis Center (FS-ISAC), a thought leadership and information sharing community for collaboration on critical security threats facing the global financial services sector.
    - Blackbaud partners with the Information Sharing and Analysis Center for Nongovernmental Organizations (NGO-ISAC) to participate in collaboration regarding US-Based nonprofit and nongovernmental organizations under attack from sophisticated threat actors.
    - Partnership with Microsoft and Azure provides us access to industry threat intelligence and early previews regarding upcoming Azure feature capabilities and security releases.
    - Partnerships with other cloud providers and independent third parties for reviews.

Blackbaud also leverages tactical Cyber Security strategies for safeguarding our environments and data by utilizing the NSA's Defense in Depth techniques and layered security, including:

- Data Protection
- Application Security
- Host Based Security
- Internal Network Security Measures
- Perimeter Security
- Physical Security
- Policies/ Procedures/ Awareness

Regulatory Compliance

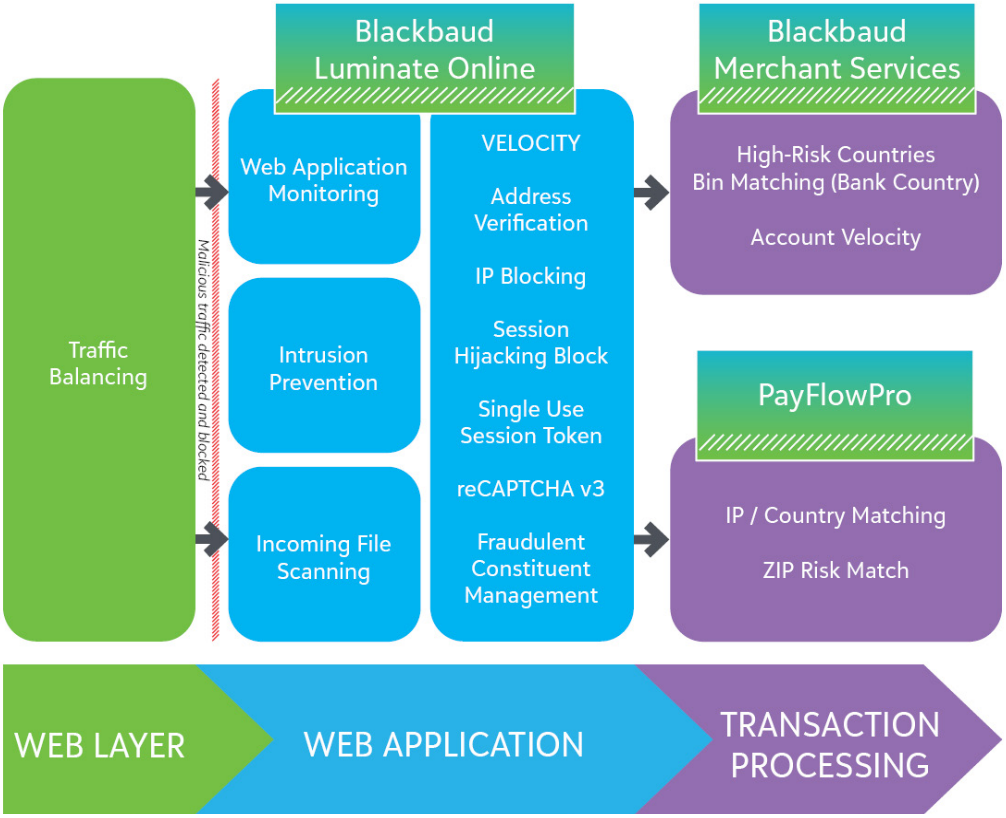
Blackbaud solutions meet industry security and data privacy standards and provides audit reports upon request to our subscription customers, their auditors, and our prospective customers. This includes SOC 2 type 2, SOC 1 type 1, and bridge letters for both SOC 1 and 2 reports, where applicable*. Blackbaud provides PA-DSS and PCI-DSS attestations of compliance to Blackbaud Internet Services and Blackbaud Payment Solutions*. Blackbaud also leverages the Cloud Security Alliance's CAIQ-Lite assessment questionnaires to provide transparency regarding the adherence of our products to the CSA Cloud Controls Matrix. These assessments are made available via the Cloud Security Alliance.*

Continued on next page...

Application Security

The Blackbaud Luminate Online platform includes several functions that prevent and mitigate fraud.

With enhanced security checkpoints and techniques applied at all stages, Blackbaud Luminate Online has you protected at every click—from the moment a visitor arrives on a website all the way through transaction processing.



- **VELOCITY fraudulent pattern detection:**
  This is a constant pattern matching algorithm that determines when transactions have high likelihood of fraud and begins to block those transactions over a period of time (Lockout period)
- **Address Verification (AVS):**
  Based on transaction bank responses, Luminate Online can decline transactions based on the correlation of the donor's physical address entered into a donation form and the address on file with their credit card.
- **IP Blocking:**
  At the application layer, specific IP addresses can be blocked from accessing any page on a Luminate Online site.
- **Session Hijacking Block:**
  For any administrator Luminate Online authentication is linked to a specific IP address. If that IP changes during use of the application, the connection is blocked from access.
- **IP Whitelisting:**
  Administrators must verify their IP address with two-factor authentication in order to access to the platform.
- **Single use token:**
  Every interaction with the site has a single-use token preventing reuse or transfer of session data to anyone but the end user.
- **reCAPTCHA v3:**
  Luminate Online form submissions are all protected by Google's reCAPTCHA v3, an invisible heuristic monitoring CAPTCHA designed to prevent bot/script submission of forms.
- **Fraudulent Constituent Management:**
  Constituent records created by interactions with the site considered fraudulent or suspect are quarantined until being accepted by authorized administrators.

About Blackbaud

Leading uniquely at the intersection point of technology and social good, Blackbaud connects and empowers organizations to increase their impact through cloud software, services, expertise, and data intelligence. We serve the entire social good community, which includes nonprofits, foundations, companies, education institutions, healthcare organizations, and the individual change agents who support them.