logdna

LOGDNA'S APPROACH TO SECURITY

Summary

LogDNA has established a security program dedicated to ensuring customers have the highest confidence in our custodianship of their data.

Contact

For more information, please contact
us at outreach@logdna.com or
visit us at www.logdna.com

Read Our Whitepaper

LOGDNA'S APPROACH TO SECURITY

INTRODUCTION

LogDNA's mission is to make engineers' working lives simpler, more pleasant, and more productive. To do that, we need to make sure your data is secure, and protecting it is one of our most important responsibilities. LogDNA is committed to being transparent about our security practices and helping customers understand our approach.

ABOUT LOGDNA

LogDNA is a highly scalable enterprise-grade log management solution serving more than 3,000 customers, from startups to Fortune 100 companies. LogDNA enables teams to effortlessly aggregate system and application logs under a single platform. It provides lightning fast Parsing, Indexing, and Live Tail, with the ability to ingest millions of events per second and petabytes of log data per day.

With LogDNA, your teams can quickly access log data to monitor operations, diagnose and troubleshoot problems, and deliver higher quality service to your customers. We believe in a world of zero downtime, and that means providing easy access to the data that matters. To learn more, visit logdna.com and start your free trial today.

> *LogDNA has established a security program dedicated to ensuring customers have the highest confidence in our custodianship of their data.*

ORGANIZATIONAL SECURITY

LogDNA has established a security program dedicated to ensuring customers have the highest confidence in our custodianship of their data. Our security program is aligned with the SOC 2 , HIPAA and PCI standards and is regularly audited and assessed by third parties.

PERSONNEL SECURITY

LogDNA's personnel practices apply to all members of the LogDNA workforce, including regular employees and contractors who have direct access to LogDNA's internal information systems. All workers are required to understand and follow internal policies and standards. Before gaining initial access to systems, all workers must agree to confidentiality terms, pass a background screening, and take security training. Upon termination of work at LogDNA, all access to LogDNA systems is removed immediately.

SECURITY AND PRIVACY TRAINING

During their tenure, all workers are required to complete privacy and security training. They are also required to acknowledge that they've read and will follow LogDNA's information security policies. Some workers, such as engineers, operators and support personnel have elevated access to systems or data.

DEDICATED TO SECURITY

The teams divide responsibilities for key aspects of LogDNA's security program, as follows:

Engineering

- Establish secure development practices and standards
- Ensure project-level security risk assessments
- Provide design review and code review security services for detection and removal of common security issues
- Train developers on secure coding practices

Security Team

- Build and operate security-critical infrastructure including LogDNA's public key infrastructure, event monitoring, and authentication services
- Maintain a secure archive of security-relevant logs
- Consult with operations personnel to ensure the secure configuration and maintenance of LogDNA's production environment
- Respond to alerts related to security events on LogDNA systems
- Manage security incidents
- Acquire and analyze threat intelligence
- Coordinate penetration testing
- Manage vulnerability scanning and remediation
- Manage the security awareness program

Compliance

- Coordinate regular risk assessments, and define and track risk treatment
- Coordinate audits and maintain security certifications
- Respond to customer inquiries
- Review and qualify vendors for compliance

POLICIES AND STANDARDS

LogDNA maintains a set of policies, standards, procedures, and guidelines ("security documents") that provide the LogDNA workforce with the "rules of the road" for operating. Our security documents help ensure that LogDNA customers can rely on our workers to behave ethically and for our service to operate securely. These policies are living documents, they are regularly reviewed and updated as needed, and made available to all workers to whom they apply.

AUDITS, COMPLIANCE, AND 3RD PARTY ASSESSMENTS

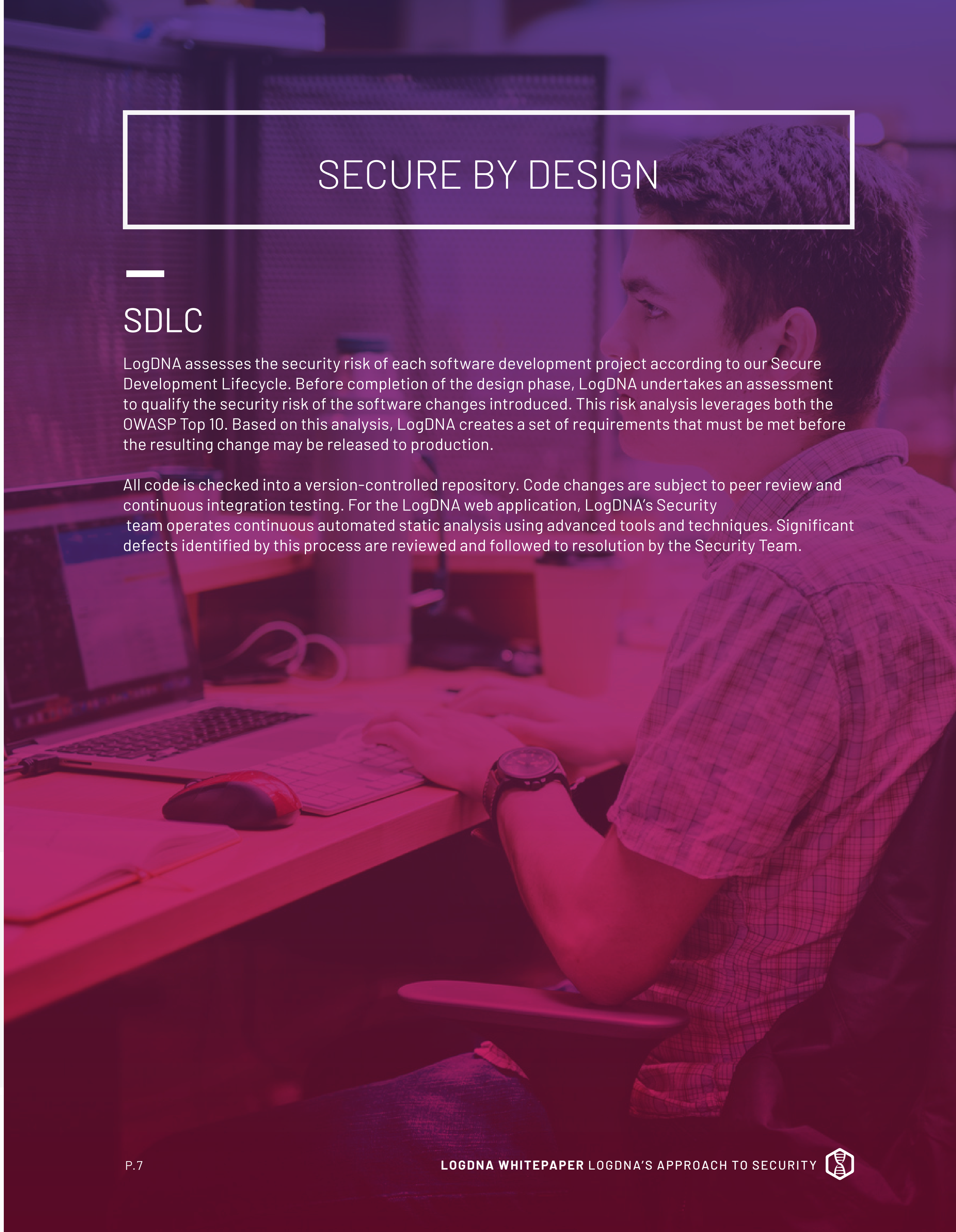
LogDNA operates a comprehensive information security program designed to address the vast majority of the requirements of common security standards. Please contact sales for more information about the security standards with which LogDNA complies and to request copies of available reports and certifications.

Audits

LogDNA evaluates the design and operation of its overall compliance with internal and external standards. LogDNA engages credentialed assessors to perform external audits at least once per year. Audit results are shared with senior management and all findings are tracked to resolution.

Penetration testing

LogDNA engages independent entities to conduct regular application-level and infrastructure-level penetration tests. Results of these tests are shared with LogDNA management. LogDNA's Security Team reviews and prioritizes the reported findings and tracks them to resolution.



SECURE BY DESIGN

SDLC

LogDNA assesses the security risk of each software development project according to our Secure Development Lifecycle. Before completion of the design phase, LogDNA undertakes an assessment to qualify the security risk of the software changes introduced. This risk analysis leverages both the OWASP Top 10. Based on this analysis, LogDNA creates a set of requirements that must be met before the resulting change may be released to production.

All code is checked into a version-controlled repository. Code changes are subject to peer review and continuous integration testing. For the LogDNA web application, LogDNA's Security team operates continuous automated static analysis using advanced tools and techniques. Significant defects identified by this process are reviewed and followed to resolution by the Security Team.

PROTECTING CUSTOMER DATA

The focus of LogDNA's security program is to prevent unauthorized access to customer data. To this end, our team of dedicated security practitioners, working in partnership with peers across all of our teams, take exhaustive steps to identify and mitigate risks, implement best practices, and constantly evaluate ways to improve.

DATA ENCRYPTION IN TRANSIT AND AT REST

LogDNA transmits data over public networks using strong encryption. This includes data transmitted between LogDNA clients and the LogDNA service. LogDNA supports the latest recommended secure cipher suites to encrypt all traffic in transit, including the use of TLS protocols, encryption, and hashing algorithms, as supported by the clients. This applies to all types of data at rest within LogDNA's systems.

NETWORK SECURITY

Customer data submitted into the LogDNA services is only permitted to exist in LogDNA's production network, its most tightly controlled network. Administrative access to systems within the production network is limited to those engineers with a special business need.

Only those network protocols essential for delivery of LogDNA's service to its users are open at LogDNA's perimeter. Changes to LogDNA's production network configuration are restricted to authorized personnel.

In LogDNA's hosted production environment, control of network devices is retained by the hosting provider. For that reason, LogDNA logs, monitors, and audits system calls and has developed alerts for system calls that indicate a potential intrusion.

AUTHORIZING ACCESS

To minimize the risk of data exposure, LogDNA adheres to the principle of least privilege—workers are only authorized to access data that they reasonably must handle in order to fulfill their current job responsibilities. To ensure that users are so restricted, LogDNA employs the following measures:

- All systems used at LogDNA require users to authenticate, and users are granted unique identifiers for that purpose.
- Each user's access is reviewed at least quarterly to ensure the access granted is still appropriate for the user's current job responsibilities.

Workers may be granted access to a small number of internal systems, such as the corporate LogDNA instance, by default upon hire. Requests for additional access follow a documented process and are approved by the responsible owner or manager.

AUTHENTICATION

To further reduce the risk of unauthorized access to data, LogDNA employs multi-factor authentication for administrative access to systems with more highly classified data. Where possible and appropriate, LogDNA uses public and private keys combination for authentication. For example, at this time, administrative access to production servers requires operators to connect using both an SSH key. Where passwords are used, multi-factor authentication is enabled for access to higher data classifications.

SYSTEM MONITORING, LOGGING AND ALERTING

LogDNA monitors servers, workstations, and mobile devices to retain and analyze a comprehensive view of the security state of its corporate and production infrastructure. Administrative access, use of privileged commands, and system calls on all servers in LogDNA's production network are logged.

LogDNA's Security Team collects and stores internal (non-customer) production logs for analysis. Logs are protected and retained for at least one year. Analysis of logs is automated to the extent practical to detect potential issues and alert responsible personnel. Alerts are examined and resolved based on documented priorities.

RESPONDING TO SECURITY INCIDENTS

LogDNA has established policies and procedures for responding to potential security incidents. All incidents are managed by LogDNA's dedicated Computer Security Incident Response Team. LogDNA defines the types of events that must be managed via the incident response process. Incidents are classified by severity. Incident response procedures are tested and updated at least annually.

DATA AND MEDIA DISPOSAL

Customer data is removed immediately upon deletion or log retention expiration. LogDNA hard deletes all information from currently running production systems.

LogDNA's hosting provider is responsible for ensuring the removal of data from disks allocated to LogDNA's use before they are repurposed.

PROTECTING SECRETS

LogDNA has implemented appropriate safeguards to protect the creation, storage, retrieval, and destruction of secrets such as encryption keys and service account credentials.

WORKSTATION SECURITY

All workstations issued to workers are configured by LogDNA to comply with our standards for security. These standards require all workstations to be properly configured, kept updated, and run monitoring software. LogDNA's default configuration sets up workstations to encrypt data, have strong passwords, and lock when idle.

CONTROLLING SYSTEM OPERATIONS AND CONTINUOUS DEPLOYMENT

We take a variety of steps to combat the introduction of malicious or erroneous code to our operating environment and protect against unauthorized access.

Controlling change

To minimize the risk of data exposure, LogDNA controls changes, especially changes to production systems, very carefully. LogDNA applies change control requirements to systems that store data at higher levels of sensitivity. These requirements are designed to ensure that changes potentially impacting Customer Data are documented, tested, and approved before deployment.

Server hardening

New servers deployed to production are hardened by disabling unneeded and potentially insecure services, removing default passwords, and applying LogDNA's custom configuration settings to each server before use.

DISASTER RECOVERY

Non-Log Production data are replicated among discrete operating environments to protect the availability of LogDNA's service in the event of catastrophic events. LogDNA performs restoration testing annually to ensure the completeness and accuracy of backup data. The LogDNA data archiving service provides the mitigation of data loss for customer logs in the event of catastrophic events.

CONCLUSION

We take security seriously at LogDNA because every person and team using our service expects their data to be secure and confidential. Safeguarding this data is a critical responsibility we have to our customers and we work hard to maintain that trust.

logdna

Sales Contact:	outreach@logdna.com
Support Contact:	support@logdna.com
Media Inquiries:	press@logdna.com