LogicMonitor

LogicMonitor hosted monitoring platform:

Security Whitepaper

Table of Contents

Introduction:

LogicMonitor is a Software-as-a-Service (SaaS) based hybrid observability platform powered by AI, designed to simplify health and performance management for complex technology infrastructures. Helping to protect the confidentiality of your systems and data is of utmost importance to LogicMonitor, as is maintaining your trust and confidence.

This document is intended to describe the protections provided by LogicMonitor to ensure that your data is well-protected, as well as detail the controls implemented to ensure the integrity and availability of the LogicMonitor platform.

LogicMonitor's cybersecurity philosophy is based on a multi-layer cloud-centric strategy that provides controls across all levels of the platform. It uses a data-driven approach to continuously assess the effectiveness of its security capabilities and measure the program's overall maturity level. It also includes the following:

- Robust vulnerability management program
- Disaster recovery capabilities
- Employee background checks
- Sophisticated access control mechanisms
- Independent audits of LogicMonitor's security program effectiveness
- External penetration tests
- Customer feedback

At LogicMonitor, its teams strive to improve, earn, and maintain your trust. More information can be found on the Trust Center website.

Product Security

The LogicMonitor platform has been designed with a rich set of security features to ensure the privacy and security of your data.

Application Security

LogicMonitor has a robust application security program that includes a comprehensive set of industry leading best practices, a sample of which are listed below:

> *"LogicMonitor has a robust application security program that includes a comprehensive set of industry leading best practices."*

Application development security

- Software engineering teams are trained on secure coding practices.
- The LogicMonitor platform is based on a number of backend and frontend application and microservice components. These components are grouped by functional area, with a dedicated development team assigned to each function. Access to modify the code repositories belonging to any particular component is strictly limited to the security principles of least privilege and need to know.
- All modifications to component source code go through a manual review process to validate the efficacy and security of the change.
- As part of a "shift left" methodology toward product security, new feature development triggers a formal Architecture Review Board process early in the design phase, which includes threat modeling to uncover vulnerabilities that must be addressed by LogicMonitor's development team and validated by its Quality Assurance organization.
- LogicMonitor's Secure Software Development Lifecycle includes comprehensive testing via Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and Software Composition Analysis (SCA).
- All findings from SAST, DAST, and SCA scans are formally tracked, and vulnerabilities are remediated within agreed upon timeframes based on the vulnerability severity classification.
- All operationalized application code is scanned on a daily basis for vulnerabilities.
- LogicMonitor performs continuous manual penetration testing of the product software by its Quality Assurance organization.
- Regular information sharing sessions are conducted for the development organization on topics such as OWASP Top 10 security risks, OWASP secure coding best practices, effective threat modeling, security logging guidance, data classification guidance, along with many other relevant security topics.

Deployment security

- Application builds are mediated by a CI/CD system with tightly-managed access controls designed such that each component's build plan may be controlled and managed only by the lead engineers of each functional team.
- Developers are not permitted to edit the steps used to deploy components in production. This prevents them from being exposed to secret credentials and/or otherwise being able to tamper with production resources.
- Developers are not permitted to edit build plans after they have been finalized. This helps ensure that the same version of an application which was built and tested is what goes out to production environments.
- The use of digital signing tools on its build servers helps ensure the integrity of the build output.
- Employee access for maintaining the build servers is strictly controlled via RBAC and the security principle of least privilege.

- Once application security testing has been completed and a release has passed initial rounds of testing, an application component may be deployed for subsequent stages of testing. Access to manage and control application deployments is strictly limited via RBAC and the security principle of least privilege.
- Release candidate builds are deployed via automation tooling and securely transmitted to secure storage with very limited write access. Each build includes a checksum or equivalent signature technology, which is stored separately from the build artifacts. Application deployments to subsequent testing stages (alpha, beta, gamma) and then production environments are conducted via automation tooling, via a tightly-controlled process that leverages the application signature to validate the application integrity within the target environment.
- At each candidate stage, further acceptance testing is conducted with minimum bake-in times to ensure quality. Only after a release candidate has passed all testing stages is deployment approved for customer release.

Data classification and handling

All of your device data provided to LogicMonitor is classified according to sensitivity. Data LogicMonitor classifies as customer-sensitive includes essential device identification information such as hostname / IP address as well as the health and performance metric data associated with each resource. Customer-confidential data includes resource metadata (such as operating system versions, SNMP community strings, API passwords, etc.), LM Logs™ data, LM Config™ files, network flow data, and any highly sensitive information about your account holders. This confidential data is handled with the highest level of security.

LogicMonitor encrypts these elements upon receipt using industrial-strength AES encryption. Encryption keys are unique per-customer and are encrypted via Amazon's AWS Key Management Service (KMS) envelope encryption prior to storage. Monitored device credentials are not stored to disk in LogicMonitor Collectors, with the added customer-controlled option to utilize industry recognized credential vault solutions for credential storage.

Additional details can be found in LogicMonitor's support pages.

Network transport protections

Any access to the LogicMonitor platform — whether via a web browser, the LogicMonitor APIs, or a LogicMonitor Collector — is conducted exclusively over HTTPS using Transport Layer Security (TLS) encryption. TLS is a cryptographic protocol that is designed to protect you against eavesdropping, tampering, and message forgery.

LogicMonitor supports the most up-to-date versions of the protocol (TLS 1.2 or newer), long encryption keys (2048-bit), and strong ciphers. All data ingested and processed by the LogicMonitor platform — metrics, logs, configuration data, etc. — enjoys these strong protections.

End-user authentication

User accounts are authenticated to the LogicMonitor platform either using its in-built authentication system or via integration with a customer-configured Single Sign-On (SSO) provider that supports the Security Assertion Markup Language (SAML) protocol. When using stock authentication, passwords are never stored directly but instead maintained in salted one-way hashes according to industry best-practices. In addition to minimum strength requirements, the hashing algorithm LogicMonitor employs has native resistance to brute-force attacks.

Together these ensure that your passwords are safe even in a worst-case scenario. To further protect account security, two-factor authentication is available, and it is strongly recommended to be enabled at the account level.

To learn more about end user authentication you can refer to LogicMonitor's two factor authentication support page.

Alternatively, you can elect to authenticate your end-users to LogicMonitor via your in-house SSO service. Using SAML, customers sign in using existing credentials stored and managed by your Identity Provider (such as Okta, ADFS, etc.).

As a result, authentication management policies such as password strength, password aging, or the use of multi-factor or biometric systems may be controlled directly by you, using your existing identity management systems. To assist with onboarding, new users can be automatically created upon first time login from a provisioned Identity Provider.

More information can be found in LogicMonitor's support pages.

Role-based authorization

Once authenticated, end-user access is controlled by a sophisticated role-based access control (RBAC) system. In addition to the pre-built roles included as default, your custom roles should always be created to limit access based on your application of the principle of least privilege and need to know. For example, roles might be created to separate access on a device level so that a network team and server team can't view each other's devices.

Alternatively, roles can be deployed to limit individuals' access to modify monitoring modules (LogicModules) or Collector configurations. Roles can be applied such to control access to individual accounts and their associated API tokens.

Network access control lists

In addition to authentication controls, LogicMonitor allows for the creation of a "Network Allow-List." This feature allows you to provide a list of IP addresses and/or network blocks from which your account may be accessed. Any attempt to sign in from unspecified networks is blocked and logged.

Additional details can be found in LogicMonitor's support pages.

LogicMonitor Collector security

The LogicMonitor Collector has been carefully designed and developed with high-security in mind. Communication between the Collector and the LogicMonitor platform uses HTTPS/TLS with publicly-signed certificates to prevent man-in-the-middle attacks between itself and the LogicMonitor platform. Each Collector is cryptographically keyed to the LogicMonitor platform via a strong credential that undergoes regular rotation. All confidential monitored device data handled by the Collector is stored in memory and never written to disk. Additionally, you have the option to utilize industry recognized credential vault solutions for device credential storage.

Additional information about the LogicMonitor Collector can be found in its support pages.

Device least privilege

LogicMonitor's best practices dictate that the Collector be installed with the least possible privileges within your environment, avoiding running it as a root, local administrator, or domain administrator account.

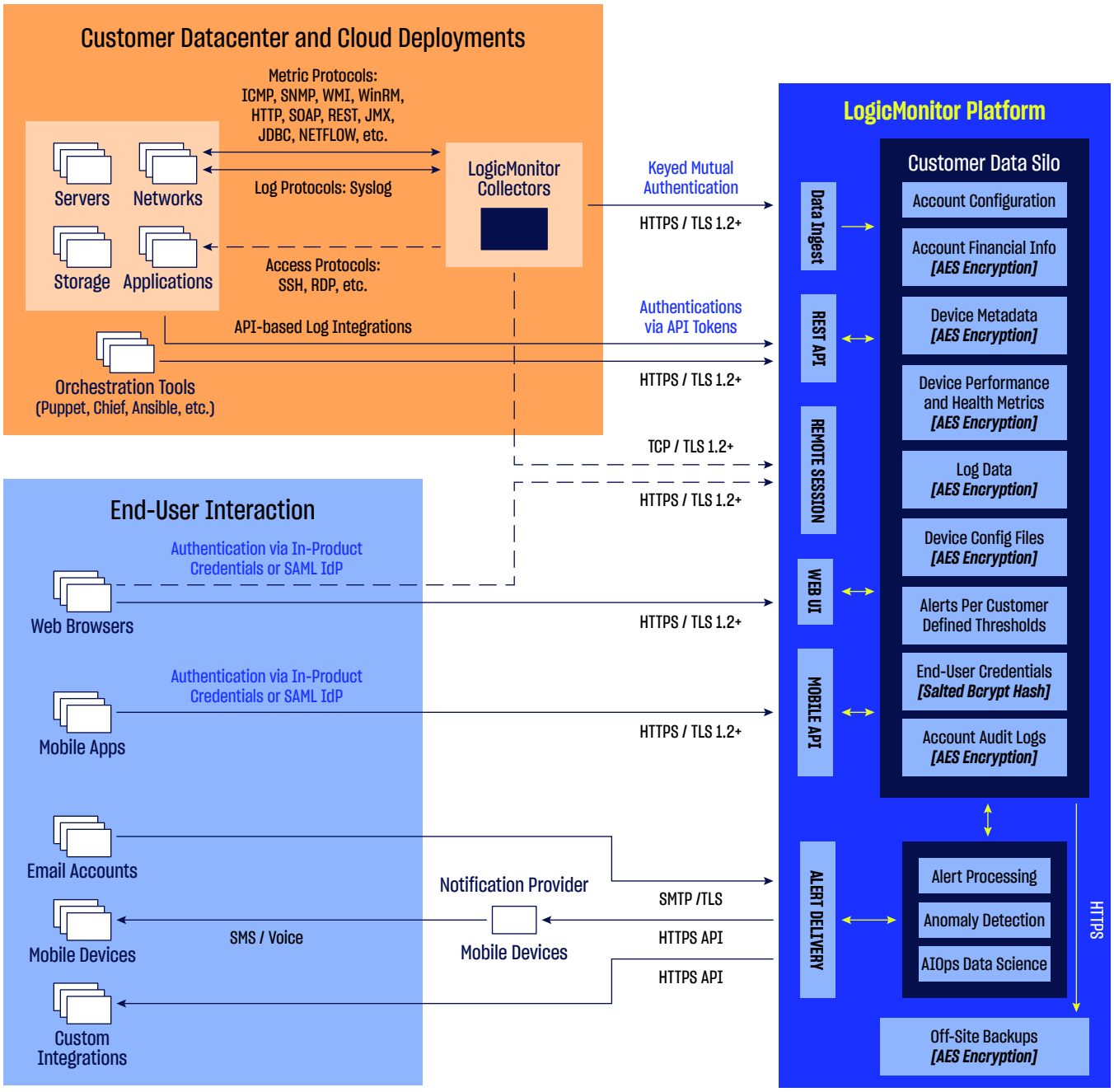
Further the Collector should be provided the least possible privileges to gather instrumentation for any given device; typically, read-only rights are sufficient. Access configuration for each device is entirely within your control, and its support documentation provides details on how to configure the minimum required permissions.

Secure alert transmission

LogicMonitor supports the transmission of alerts via email, SMS, voice message, API/webhook, as well as custom integrations. Email alerts are delivered from LogicMonitor using Simple Mail Transfer Protocol (SMTP), with TLS preferred, as determined by your email server configurations, to provide encrypted delivery of alert message content.

SMS and voice alerts are delivered to its sub-service provider's communication gateway exclusively over authenticated APIs secured with TLS encryption. Any custom integrations can leverage any security mechanisms supported by the integration service endpoint.

Figure 1. LogicMonitor Platform - Data Flow Overview



Audit logging

LogicMonitor maintains comprehensive audit logs that detail essentially all material activity within your account. Platform audit logs are searchable within the portal and can be integrated with existing SIEM or log management systems via its API. Alternatively LogicMonitor's reporting features allow for offline storage of audit logs via its automated generation of periodic activity reports.

Penetration testing

LogicMonitor regularly validates the security of its platform via third-party penetration testing. Professional cybersecurity teams are provided with its application source code as well as full platform access to validate the defensive security measures taken within its software development lifecycle.

In addition to third-party testing, LogicMonitor maintains a security defect testing regimen, This includes automated static code analysis, manual source code analysis, dynamic application security testing, as well as manual penetration testing, conducted from within the LogicMonitor Platform and Collector environment. Any security defects discovered are escalated to its development team for highest priority remediation.

Personally identifiable information

As a service targeted at IT observability, LogicMonitor is not intended to store personal data. Incidental collection of personal information however, is required for the purposes of user authentication, alert delivery, and auditing. The scope of such data stored within LogicMonitor includes only the names, login credentials, email addresses, and mobile device numbers of account holders. These elements are considered confidential to you and handled accordingly.

The nominal personal information LogicMonitor collects is used only within the context of service operation. It is owned and controlled solely by you and is never shared with other organizations. LogicMonitor operates in compliance with the European Union General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and offers a Data Protection Addendum (DPA) alongside its Service Agreement to formally memorialize these obligations.

Here is additional information on LogicMonitor's privacy policy.

Shared security responsibilities

The LogicMonitor platform provides a depth of security controls that are designed to be managed by account administrators. You are obligated to use these features effectively to ensure the security and integrity of your systems.

LogicMonitor's recommendations for security best practices for you can be found in the support pages.

As one specific example, end-user authentication — either using LogicMonitor's stock authentication or SAML — should be configured such that each individual uses a unique account. Two-factor authentication, either as provided in-product or via your SAML Identity Provider, is **strongly** recommended for ALL user accounts. Note that all customer accounts locally provisioned within the portal (i.e. not via SAML) will be required to utilize two-factor authentication by December 31st, 2024. Roles managed within its RBAC system should be created as appropriate and assigned to user accounts based on the principle of least privilege and need to know. Administrator access should be restricted to as few individuals as possible.

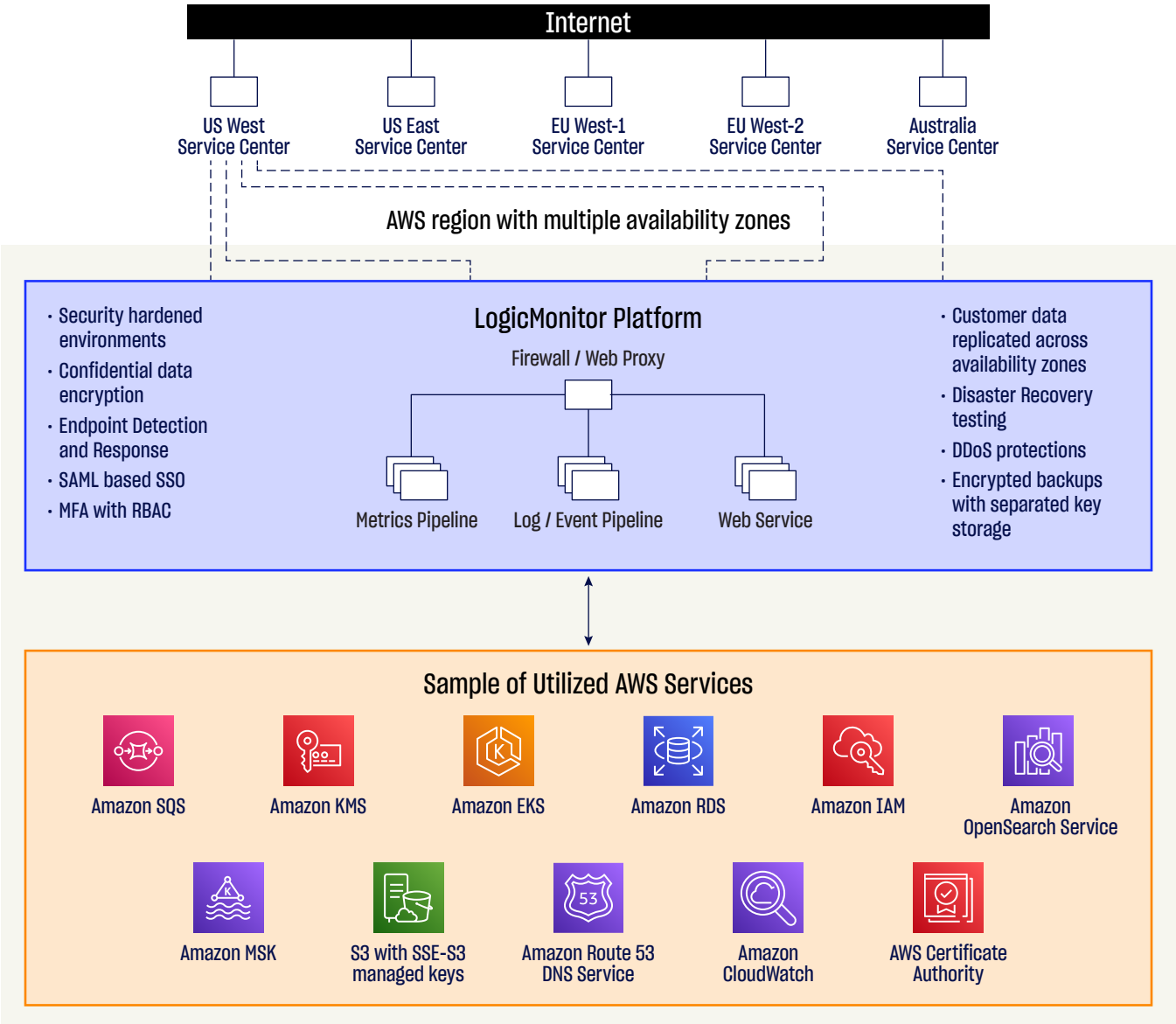
Operational Security

The operational infrastructure on which the LogicMonitor platform runs has been designed with high-security as a primary consideration, using a defense-in-depth approach to ensure comprehensive threat protection.

Platform architecture

Fundamental to the security of LogicMonitor's operational infrastructure is the design of its multi-tenancy architecture, by which each customer account is created as a completely independent entity. Each customer account is logically separated from every other, effectively isolating each customer's data footprint from one another. This ensures that in a hypothetical security breach involving any one account, all other customer accounts would remain protected.

Figure 2. LogicMonitor Platform - Network and Security Topology



Network and operating system security

For new customers, the LogicMonitor platform is operated out of the Amazon AWS service centers shown in figure 2. Each operational footprint employs intelligent packet inspection, traffic classification and filtering, and threat detection. Traffic is routed through delivery controllers which provide additional protections before sending the traffic to application servers. LogicMonitor production servers run Linux with hardening standards applied. Existing customers are being carefully migrated out of data centers and into AWS as well.

Being built on top of Amazon AWS provides additional benefits in terms of resilience to Denial of Service (DoS) attacks. As part of its overall architecture strategy, LogicMonitor leverages capabilities such as the AWS Shield Standard DDoS protection service, AWS Security Groups, and AWS Route 53 DNS service. Route 53, in particular, leverages AWS's global surface area, capable of absorbing large amounts of DNS traffic as needed.

Its intelligent network filtering capabilities within LogicMonitor's platform significantly reduce its overall attack surface. LogicMonitor only allows inbound connections using HTTPS. All traffic is inspected to ensure that it meets certain criteria, such as validating traffic routing to only the correct customer portal, detecting and blocking bot patterns, and blocking network traffic from/to sanctioned countries.

Each application server runs Endpoint Detection and Response (EDR) software which detects, reports, and stops suspicious or anomalous activity.

Vulnerability management

Vulnerability scans are conducted on an ongoing basis using commercial tools, using both an "internal" and "external" perspective. This outside-in approach ensures that any possible issue will be discovered. Once a vulnerability has been identified, it is evaluated for risk and prioritized for remediation.

Incident management

LogicMonitor has a formal incident management process for security events that may affect the confidentiality, integrity, or availability of its systems or data. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation.

When an information security incident occurs, information security staff respond by logging and prioritizing the incident according to its severity. Events that directly impact you are treated with the highest priority. Following remediation, incidents undergo post-mortem investigations as necessary to determine the root cause for single events, discover trends spanning multiple events over time, and develop new strategies to help prevent recurrence of similar incidents. LogicMonitor performs periodic tabletop exercises to evolve and refine its incident response processes.

Threat management

LogicMonitor employs a variety of sources to stay current with the evolving cyber threat landscape as it relates to its company and customers. It also receives a regular stream of informational feeds on the latest threats, including ransomware trends, malware trends, phishing methods, AI enhanced attack methods, relevant dark web activity, and various open source intelligence (OSINT) feeds. This information is then utilized to calibrate LogicMonitor's cybersecurity program to better align with the changing threat landscape.

Physical and environmental security

Historically the LogicMonitor's service platform has operated as a hybrid deployment across co-located data centers and AWS regions. While LogicMonitor still retains some legacy operations in this hybrid environment, all new customer accounts are fully deployed in AWS regions. Its service centers for legacy operations are geographically distributed to mitigate the risks of natural disasters. Both LogicMonitor's service provider for its legacy datacenters and AWS maintain stringent controls around the physical and environmental security of each site.

In its datacenter facilities, a five-step process is required to gain physical access to LogicMonitor servers, including a 24x7x365 manned security check, electronic keycards, and successive biometric scanning at each point of access. High-resolution video surveillance is maintained throughout the facilities.

Datacenter environmental controls include N+1 redundancy in generator-backed uninterruptible power, N+2 redundancy in cooling capacity, along with VESDA-based fire suppression, flood control, and earthquake resilience. Each facility is certified as compliant either with SOC 2 Type 2 or ISO 27001 standards, and LogicMonitor reviews each provider's compliance reports annually to ensure ongoing maintenance of these rigorous security controls.

Business continuity management

To minimize service interruption due to hardware failure, cloud service provider disruptions, natural disaster, or other catastrophes, LogicMonitor has Disaster Recovery (DR) principles baked-in to the foundation of its service operation. Its DR program includes multiple components to minimize the risk of any single point of failure.

Redundancy and resiliency

For legacy hybrid deployments which include physical data centers, LogicMonitor maintains a sufficient amount of redundant "warm-spare" hardware capacity in each location to absorb the failure of any other service location. Network equipment is deployed in N+1 high-availability pairs to provide for immediate failover. All devices employ redundant power supplies, each of which is connected to independent generator-backed power circuits. Internet connectivity is fully redundant at each location, with WAN links to multiple ISPs maintained across physically disparate routing hardware.

Backup and recovery

Backups of your data are conducted via customer data "snapshots" which occur every four hours. Upon generation, each snapshot is encrypted with a customer-specific key and transmitted to Amazon Web Services (AWS).

Once in AWS, each snapshot package is replicated across at least two AWS geographic regions. A rotation schedule is maintained for each snapshot package, with a maximum retention period of sixty days. The restoration of your data from a snapshot is an automated process that can be actuated only by LogicMonitor technical operations staff. Its overall backup/restore processes undergo scheduled testing prior to every release.

Organizational security

Personnel security

LogicMonitor employees are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, and professional standards. Before hiring, LogicMonitor verifies each individual's previous employment, conducts reference checks, and performs background checks where permitted by local labor laws and regulations.

Upon acceptance of employment at LogicMonitor, all employees are required to execute a confidentiality agreement and must acknowledge receipt of and compliance with policies in its Employee Handbook. As part of new-hire orientation, all employees receive baseline security training, with additional training provided based on an individual's role.

Access control

Authentication controls

LogicMonitor requires the use of a unique User ID for each of its employees, which is used to identify each person's activity on its corporate network. All LogicMonitor business systems are configured such that they are accessible only by this unique account.

Access to any systems that contain your data requires authentication via a centrally-managed Single Sign-On (SSO) service. LogicMonitor's SSO system enforces the use of strong password policies, including password expiration, restrictions on password reuse, and minimum password strength. Two-factor authentication is enforced to further protect against unauthorized access.

Upon hire, each employee is assigned an account by its Employee Success organization and is granted the minimum privileges required by their role as described below. At the end of an individual's employment with LogicMonitor, a policy-based workflow ensures that account access is disabled.

Authorization controls

Access rights and levels are based on an employee's job function and role, using the principles of least privilege and need to know, to match access privileges to defined responsibilities. LogicMonitor employees are granted only a limited set of default permissions to access common corporate resources.

Requests for additional access follow a formal process that involves a request and approval from a data or system owner, manager, or other executives. Approvals are managed by workflow tools that maintain auditable records of all changes.

Accounting

LogicMonitor's policy is to log each authentication transaction and sign-on request to each business system. These logs are maintained off-site in an immutable format and are reviewable on an as-needed basis.

Third-party audit and compliance

LogicMonitor has undergone multiple third-party audits of its information security program. The operation of its product has been certified to meet the exceptionally high standards defined by the International Standards Organization (ISO), and is certified to the ISO/IEC 27001:2013 standard for security program management, as well as the ISO/IEC 27017:2015 standard for the secure operation of cloud services and the ISO/IEC 27018:2019 standard for protection of Personally Identifiable Information (PII)

LogicMonitor also maintains an audit program against the AICPA's Service Organization Controls (SOC) Trust Services Principles. Its processes around service infrastructure, software, people, procedures, and data handling are compliant with SSAE 18 criteria, and it maintains a SOC 2 Type 2 report as certification. It is important to highlight that a Type 2 report covers the operational effectiveness of its compliance program and controls over a specified period of time.

LogicMonitor's current security and privacy compliance documentation may be accessed via its trust portal website.

Conclusion

LogicMonitor is committed to keeping the data it stewards on behalf of you safe and secure. Each of the components of its multi-layered security strategy is embraced throughout the organization.

As a key part of LogicMonitor's overall security strategy, it is important for our partners to understand our shared responsibilities as it relates to SaaS. LogicMonitor will always strive to do all we can to ensure safe and secure operation of our services, but it is equally important for you to follow security best practices at all times. Security is only as strong as the weakest link in the chain.

To assist you in this endeavor, we have established this page on our website.

Click here to learn more about LogicMonitor solutions.

About LogicMonitor®

LogicMonitor® offers hybrid observability powered by AI. The company's SaaS-based platform, LM Envision, enables observability across on-prem and multi-cloud environments. We provide IT and business teams operational visibility and predictability across their technologies and applications to focus less on troubleshooting and more on delivering extraordinary employee and customer experiences. For more information, visit logicmonitor.com and our blog, or follow us on LinkedIn, X, Facebook, and YouTube.

LogicMonitor