

Security Whitepaper: LogicMonitor Hosted Monitoring Platform

Security Whitepaper

LogicMonitor Hosted Monitoring Platform

Table of Contents

Introduction	2
Overview	2
Product Security	3
Operational Security	7
Physical & Environmental Security	9
Business Continuity Management	10
Organizational Security	10
Conclusion	12

For more information on LogicMonitor visit www.logicmonitor.com

Introduction

LogicMonitor is a Software-as-a-Service based IT operations monitoring system designed to simplify health and performance management for complex technology infrastructures. Helping to protect the confidentiality of our customers' systems and data is of utmost importance to LogicMonitor, as is maintaining the trust and confidence of our customers. This document is intended to describe the protections provided by LogicMonitor to ensure that our customers' data is well-protected, as well as describe the controls we've implemented to ensure the integrity and availability of the LogicMonitor platform.

Overview

LogicMonitor's security stance is based upon a multi-layered strategy that provides controls across all levels of our platform: from design and implementation of the LogicMonitor product through the transmission, storage, and access of customer data and all the way down through the operation of our technical infrastructure. Our comprehensive security strategy includes the following components:

- Product Security
- Operational Security
- Physical & Environmental Security
- Business Continuity Management
- Organizational Security

Product Security

The LogicMonitor platform has been designed with a depth of security features to ensure the privacy and security of our customers' data.

Data Classification and Handling

All customer device data provided to LogicMonitor is classified according to sensitivity. Data we classify as non-sensitive includes device identification info such as hostname / IP address as well as the health and performance data associated with each device. Sensitive data includes device metadata – such as operating system versions, SNMP community strings, API passwords – device configuration files, NetFlow data, and all personally identifying information about your account-holders. Such data is considered customer confidential and treated with the utmost security. LogicMonitor encrypts these elements upon receipt using industrial-strength AES encryption using the strongest possible key size (256 bits). Encryption keys are unique per-customer and generated in-memory such that they are never stored to disk. This design ensures that decryption of sensitive data is virtually impossible by even the most sophisticated attacker.

Network Transport Protections

All access to the LogicMonitor platform – whether by browser, LogicMonitor API, or LogicMonitor Collector – is conducted exclusively over HTTPS using Transport Layer Security (TLS) encryption. TLS is a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery. LogicMonitor uses the most up-to-date version of the protocol (TLS 1.2), long encryption keys (2048-bit), and strong ciphers.

End-User Authentication

User-accounts are authenticated to the LogicMonitor platform either using our in-built authentication system or via integration with a customer-configured Identity Provider via Security Assertion Markup Language (SAML). When using stock authentication, passwords are never stored directly but instead maintained in salted one-way hashes according to industry best-practice. In addition to minimum strength requirements, the hashing algorithm we employ has native resistance to brute-force attacks. Together these ensure that our customer's passwords are safe even in a worst-case scenario. To further protect account

security, two-factor authentication is available either on a per-account or per-role basis.

Alternately our customers can elect to authenticate their end-users to LogicMonitor via their own SAML Identity Provider. Using SAML, our customers sign-in using existing credentials stored within their own in-house systems. As a result, authentication management policies such as password strength, password aging, or the use of multi-factor or biometric systems are directly controlled by the customer's existing systems.

Role-Based Authorization

Once authenticated, end-user access is controlled by a sophisticated role-based access control (RBAC) system. Using RBAC, custom roles can be created to limit access to any area of the LogicMonitor platform. For example, roles might be created to separate access on a device level so that a network team and server team can't view one another's devices. Alternately, roles can be deployed to limit individuals' access to modify monitoring LogicModules or Collector configurations. Roles can be applied such that they control access to an individual account and its associated API tokens.

Network Whitelisting

In addition to authentication controls, LogicMonitor allows for the creation of a "Network Whitelist." This feature allows our customers to provide a list of IP network blocks from which their account may be accessed. Any attempt to sign-in from unspecified networks is blocked.

Collector Security

The LogicMonitor Collector has been carefully designed and developed with high-security in mind. All communications made by the collector are outbound: either within your LAN to the devices it's been assigned to monitor, or outbound to the LogicMonitor platform. This design is specifically intended to limit the Collector's attack surface.

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 which undergoes regular rotation. All sensitive device data handled by the Collector is always stored in-memory and never written to disk.

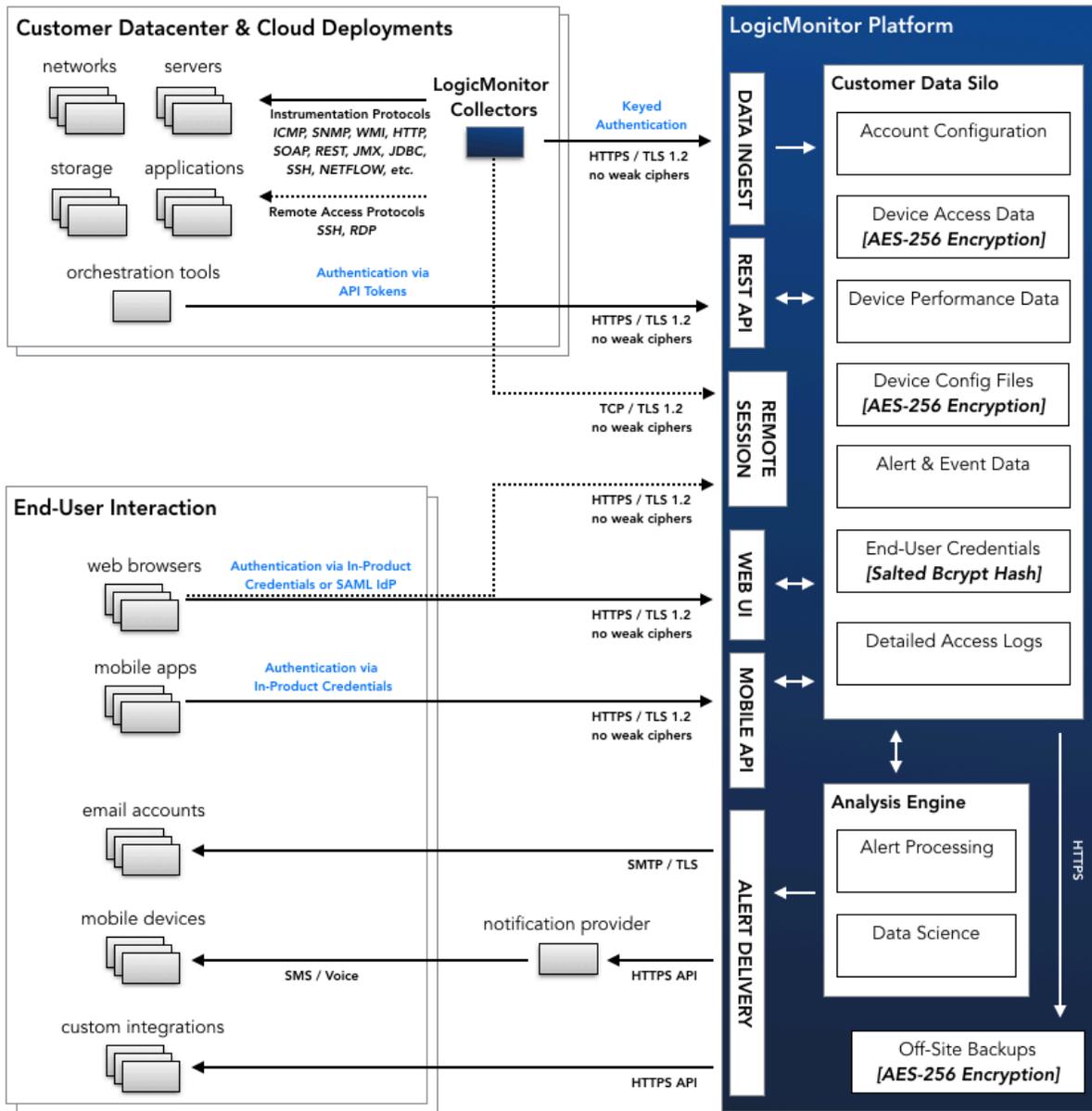


Figure 1. LogicMonitor Platform – Data Flow Overview

Device Least Privilege

LogicMonitor's best practices dictate that the Collector have 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 our customers' control, and our support documentation provides details on how to configure the minimum required rights.

Secure Alert Transmission

LogicMonitor supports the transmission of alerts via email, SMS, voice message, and API/webhook. Email alerts are delivered from LogicMonitor using Simple Mail Transfer Protocol (SMTP) with TLS to provide encrypted delivery of alert message content. SMS and voice alerts are delivered to our sub-service provider's communication gateway exclusively over authenticated APIs secured with TLS encryption. Any custom alerts configured via a webhook can employ any security mechanisms supported by the service endpoint.

Access Logging

LogicMonitor maintains comprehensive audit logs which detail actions taken within your account by end-users and API calls. Audit log retention is based on pricing package (3 months / 1 year / 2 years) and all content is searchable. Our reporting features allow for offline storage of access logs via automatic report generation.

Penetration Testing

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

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

Personally Identifiable Information

As a service targeted at IT operations performance monitoring, LogicMonitor is not intended to store personal data. Incidental collection of personal information 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 (optionally) mobile device numbers of accountholders. These elements are considered confidential to our customers and handled accordingly.

The nominal personal information we collect is used only within the context of service operation. It is owned and controlled solely by the customer and is never shared with other organizations. We operate LogicMonitor in compliance with the European Union General Data Protection Regulation (GDPR) and offer a Data Protection Addendum (DPA) alongside our Service Agreement in testament to these obligations.

Shared Security Responsibilities

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

Specifically, end-user authentication – either using our 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. Roles should be created as appropriate and assigned to user accounts based on the principle of least-privilege. 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 our multi-tenancy architecture, by which each customer account is created as a completely independent entity. Each customer account is logically

and/or physically separated from every other, effectively isolating each customer from one another. This ensures that in a security breach involving any one account all other customer accounts remain protected.

Network & Operating System Security

The LogicMonitor platform is operated out of three geographically-distributed datacenters. Each operational footprint is secured by modern firewall systems that employ intelligent packet inspection, traffic classification and filtering, and malware identification/blocking. Traffic is routed through delivery controllers which provide additional protections before sending the traffic to application servers. LogicMonitor production servers run non-virtualized Linux and are hardened according to defense-grade standards.

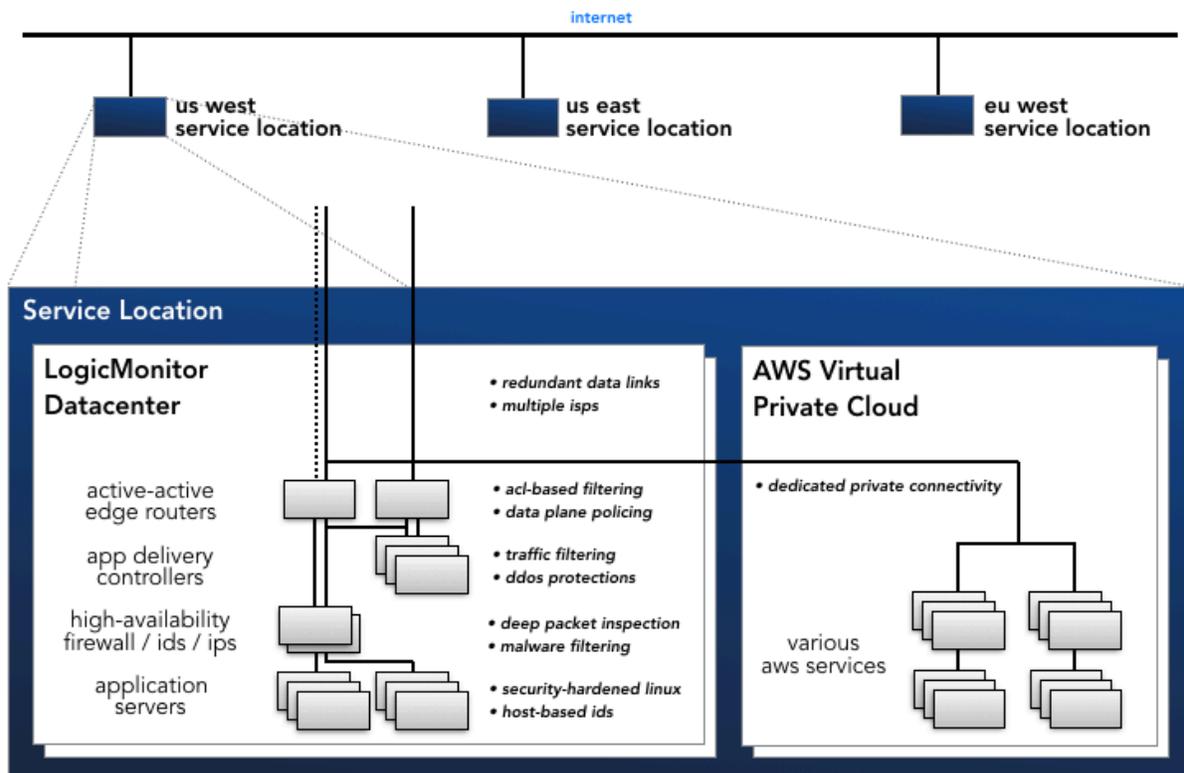


Figure 2. LogicMonitor Platform – Network & Security Topology

Vulnerability Management

Each application server runs intrusion detection software which scans for system vulnerabilities from within the production network. 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 customers are treated with the highest priority. Following remediation, incidents undergo post-mortem investigations as necessary to determine the root cause for single events, trends spanning multiple events over time, and to develop new strategies to help prevent recurrence of similar incidents.

Physical & Environmental Security

LogicMonitor's service platform is operated as a hybrid deployment across co-located datacenters and AWS resources. Our service center locations are geographically-distributed to mitigate the risks of natural disasters. Both our datacenter sub-service provider and AWS maintain stringent controls around the physical and environmental security of each site. In our 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.

Environmental controls include N+1 redundancy in generator-backed uninterruptable power, N+2 redundancy in cooling capacity, along with VESDA-based fire suppression, flood control, and earthquake resiliency. Each facility is certified as compliant either with SOC 2 Type 2 or ISO 27001 standards, and LogicMonitor reviews their compliance reports annually to ensure ongoing maintenance of sufficient security controls.

Business Continuity Management

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

Redundancy & Resiliency

In addition to maintaining operations across geographically-distributed service 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 & Recovery

Backups of LogicMonitor customer 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 one year.

The restoration of customer data from a snapshot is an automated process that can be actuated only by LogicMonitor technical operations staff. Our overall backup/restore processes undergo scheduled testing once per quarter.

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 our 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 our employees, which is used to identify each person's activity on our corporate network. All LogicMonitor business systems are configured such that they are accessible only by this unique account.

Access to any systems that contain customer 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, an employee is assigned an account by our People Operations unit 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 concepts 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 an 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 individual business system. These logs are maintained off-site in an immutable format and are reviewable on an as-needed basis.

Third-Party Auditing & Compliance

LogicMonitor has undergone multiple third-party audits of our information security program. The operation of our product has been certified meet the exceptionally high standards defined by the International Standards

Organization, 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. We also maintain an audit program against the AICPA's Service Organization Controls (SOC) Trust Services Principles. Our processes around service infrastructure, software, people, procedures, and data handling are compliant with SSAE 18 criteria, and we maintain a SOC 2 Type 2 report as certification.

Conclusion

LogicMonitor is committed to keeping the customer data we steward on behalf of our customers safe and secure. Each of the components of our multi-layered security strategy is embraced throughout the organization.

Thousands of customers trust LogicMonitor to assist with the management of their technology infrastructure, and we invest in that trust every day. Our customers can rest assured that LogicMonitor values the confidentiality, integrity, and availability of their data.