LogicMonitor Security Overview

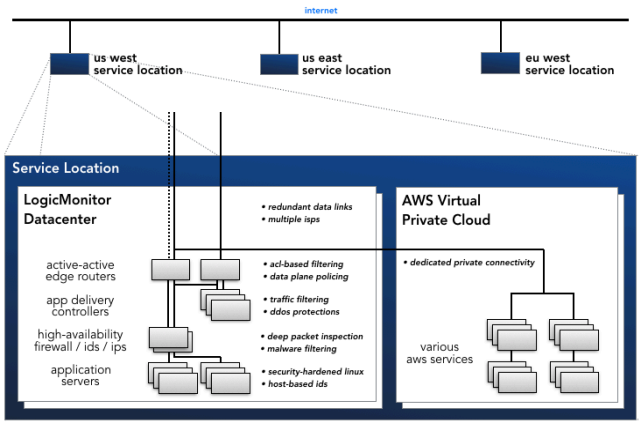
LogicMonitor maintains many layers of security controls across our service platform. Our rigorous defense-in-depth approach ensures that your data is strongly protected.

Platform Security

- TLS 1.2 encryption – with only the strongest keys and ciphers – is used to secure all communication between your environment and LogicMonitor
- Automatic encryption-at-rest is employed for device access credentials, user account information, LM Config™ data, and all other sensitive information
- Strong authentication using either our built-in two-factor system or integration with your SAML Identity Provider
- Robust access management via fine-grained role-based access control
- IP Whitelisting prevents unauthorized third-parties from accessing your account

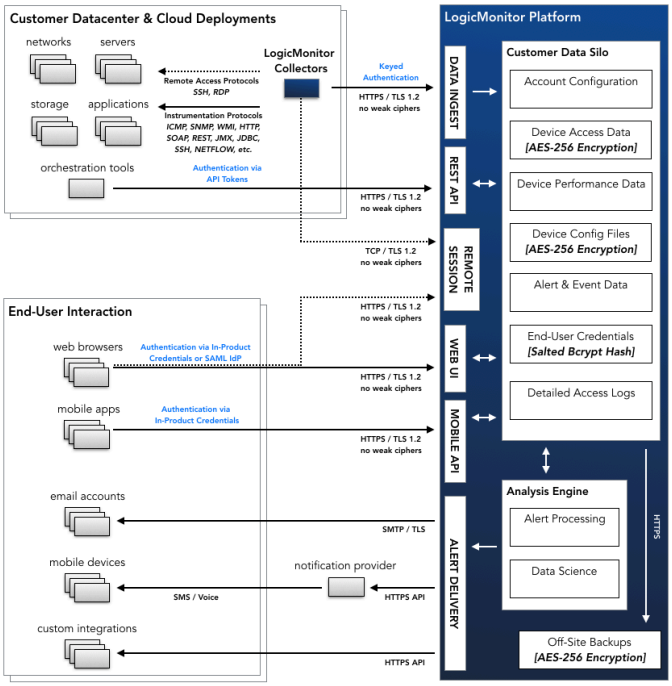
Operational Security

- Built on security-hardened Linux servers with both perimeter & host-based intrusion prevention systems
- Redundancy is integrated throughout the service platform to ensure high-availability
- Multi-factor authentication coupled with roles assigned based on least-privilege prevent unauthorized access



Collector Security

- Each LM Collector is uniquely keyed to a customer account using modern cryptographic techniques
- All communication is initiated outbound by the Collector itself – no inbound connectivity ensures that the Collector is resistant to attack
- Device access credentials are stored only in memory and never written to disk



Auditing & Compliance

- Formally audited against SOC2 principles of security, confidentiality, and availability
- Regular source-code assisted penetration testing of our service platform by professional information security firms
- Personal information handled in compliance with EU GDPR requirements

For more details on LogicMonitor's security stance see the LogicMonitor Security Whitepaper available at www.logicmonitor.com/security.