MANAGED SERVICES

Compliance is a Journey, not a Destination

Your compliance status is only as good as your ability to demonstrate that security controls are operating effectively. Reliant offers infrastructure and security services to manage installations of our patented Redbox Platform and more.

While Reliant's Redbox Platform supports PCI technical requirements, it is the merchants themselves who are ultimately responsible for operating the controls and ensuring that the technology is maintained in a state in which security controls are demonstrably effective.

The Managed Services Program is based on ensuring compliance with ongoing PCI DSS control objectives and is facilitated though the use of the Redbox Platform. We manage all aspects of the platform, including its health, status and ongoing maintenance, and review and resolve security events and alerts.

WHY MANAGED SERVICES?

IT departments face multiple challenges in operating and maintaining network infrastructure, while also managing enterprise-wide applications. At a time when PCI mandates would otherwise require increased staffing for data-security functions, IT departments have fewer resources to devote to this compliance function. As a result, our customers have increasingly turned to Reliant to manage the Redbox Platform, including associated PCI technical controls and hosted applications.

Our Managed Services Program addresses the gaps that many merchants face when they are understaffed and/or lack the knowledge, skill set and expertise to manage their own PCI compliance. The service combines our extensive knowledge of PCI Requirements with our years of experience managing retail technology environments in the field.

For merchants with limited staff, the responsibility of ongoing PCI compliance requirements adds a level of operational scale and PCI expertise that may be challenging to maintain. Compliance requires continued involvement from a merchant's IT and security staff to ensure that controls remain in place and are demonstrably effective. Merchants are also responsible for managing the health, status and ongoing maintenance of the Redbox Platform installations.

Benefits of our Managed Services Program

- Helps reduce capital costs
- Provides access to Reliant's specialized skills and expertise
- Provides internal resource flexibility
- Frees existing IT resources to be invested strategically to increase revenue and competitive advantage

Operational Support

- Manage configuration changes and overall health of the Redbox Platform infrastructure
- Perform capacity planning and major system upgrades
- Support operational incidents and diagnose issues that may involve multiple network components and telecommunication services
- Manage compliance of mission-critical applications with complex PCI requirements, such as credit card processing

RELIANT

MANAGED SERVICES

MANAGED SERVICES PROGRAM COMPONENTS

Reliant's Managed Services Program includes multiple options and levels of service. This flexible service accommodates many retailers' existing in-house capabilities, fills the gaps where skills or staffing may be lacking and can be customized as necessary to meet your needs. Typical service program components include:

I. Base Redbox Platform Device Monitoring

This Level 1 support program is designed to monitor the status of each Redbox Platform deployed in your retail chain. Key support features include:

- Automated event detection, incident creation and notification
- Incident evaluation and root-cause analysis
- Resolution of known issues and notification
- Referral to the appropriate resolver group
- Informing client when Level 2 & 3 Support is required

II. Redbox Platform Device Management

This service includes responsibility for the client Redbox Platform operating environment, including the overall health of the Redboxes, configuration changes and program-level monitoring of security controls. Support features include:

- Dedicated Reliant Redbox Platform program manager PCI Requirements
- Redbox Platform infrastructure management, including system maintenance, capacity planning, updates and upgrades
- Access and firewall rules management in conformance with client policy and PCI DSS requirements, including execution of all firewall rule changes
- Executing quarterly internal network vulnerability scans

III. Redbox Platform Log Capture, Management and Alerting

Includes the monitoring of log data and security events from the Redbox Platform and related systems. Reliant will notify client of suspicious activity or violations of predefined security policies. Responsibilities include:

- Monitoring all security events collected from cardholder data network and host systems
- Reviewing all alerts of suspicious activities across the enterprise, and communication of potential issues to client
- Managing syslog online storage, offline backup and management

IV. PCI Security Account Management

Reliant operates Redbox Platform controls on behalf of our client and provides ongoing PCI compliance consulting to meet objectives in client PCI policy, including:

- Analysis of alerting trends and incidents in conformance with Incident Response Policy
- Analysis of vulnerability scanning reports and results
- Regular rotation and changes of account access controls and keys, according to the client's PCI policy
- Conducting Security Operations Reviews which are attended by both the client and Reliant
- Maintaining a Security Calendar (Scans, Access Reviews, Firewall Rule Reviews and more)
- Maintaining Redbox Platform infrastructure documentation in an "audit-ready" state, including troubleshooting documentation, run-books and the Redbox Platform Auditor's Guide

PCI Requirements

- Manage scheduled activities such as internal and external network scans, wireless scans, access reviews, firewall rules and log file reviews
- Manage system-wide changes, release of new software upgrades and employee access to card-data environments
- Respond to unplanned incidents resulting from non-technology means or Redbox Reporting and Logging
- Service PCI audits, including gathering data for audit
- Meet changes to PCI requirements issued by the PCI Security Standards Council
- Meet changes to PCI compliance resulting from changes in customer infrastructure