Service Description and SLAs for Managed Services

1. CLOUDASSURED MANAGED SERVICES (CAMS)

1.1. INTRODUCTION

The CloudAssured Cloud Management Platform, and optional Cloud Service Expense Management (CSEM) capabilities comprise the Smartronix CloudAssured Managed Services solution. CAMS gives your organization the ability to leverage the power and scalability of the cloud while reducing the cost and complexity of managing and monitoring infrastructures and applications in-house. Our experts provide complete management of cloud services from initial provisioning through the entire solution life-cycle. Our Managed Services span private, public, multicloud, and hybrid cloud offerings, allowing your organization to focus on critical business and strategic technology efforts while leaving resource-intensive IT operations to our professional team of experts.

CAMS includes the software licensing and configurations for the tools required to manage and monitor your environments to meet your Service Level Agreements.

1.2. CAMS MANAGEMENT PORTAL

The CAMS Portal ITSM framework provides the primary interface for the customer experience. The CAMS portal provides each customer a unique view of the delivered Managed Services solution and provides access into service request, event and incident ticket management systems. The back-office ITSM functionality is delivered via a Smartronix customized ServiceNow portal to ensure strict, organization-specific separation of customer data. Additionally, the CAMS Portal and supporting ServiceNow implementation can apply access governance across Smartronix personnel in case of regulatory or other customer-specific compliance requirements (special background investigations, public clearances, or other industry-specific clearance activities.) Cloud Assured Managed Services customers can create, track, manage, and report on all of their service requests from a central location 24/7/365.

1.3. MANAGED SERVICES AND SERVICE MANAGEMENT

The Core Services have been developed and integrated to provide customers with a fully instrumented Cloud experience. Optional Services in the catalog are designed to enhance customer experience and capabilities through delivery of discrete capabilities within the Smartronix Cloud Management Platform inclusive of the processes, procedures, tooling, and licensing necessary to deliver predictable results. **Table 1 and 2** below identifies the portfolio of Core, Optional, and Optional Security Services.

The Smartronix cloud management framework can also address scenarios where customers may have existing tools, interoperability or business requirements that drive custom service integrations. These custom integrations are priced separately to accommodate unique licensing costs and labor required for a tailored solution.

1.4. CLOUD RESALE AND CONSOLIDATED BILLING

The Smartronix Cloud Resale and Consolidated Billing service delivers value-added Cloud Service Expense Management (CSEM) capabilities. Customers consume Cloud Services through re-sale from Smartronix. Re-sale customers receive a single consolidated invoice of all utilized services across all managed accounts. Billing detail is tailored to support customer business and financial management requirements including organizational and divisional separation for show-back / chargeback purposes.

The CSEM Advisory service (Optional Services) is bundled into our Cloud Resale and Consolidated Billing service and is designed to optimize your cloud expense efficiency and transparency.

2. SERVICE DESCRIPTIONS

The following sections describe the Core, Optional, and Managed Security Services offerings.

Table 1. CloudAssured Core Managed Services

Core Account Services	
Account Management Services	x
Event Management and Incident Response	x
SLA Management	x
Log Aggregation	x
Boundary Management	x
Infrastructure Provisioning	x
Core Instance Services	
Monitoring and Notification	x
Operating System Patch Management	x
Anti-malware Management	x
Backup and Restoration	x

Table 2. CloudAssured Optional Services

Optional Managed Services	Optional Managed Security Services
Cloud Service Expense Management Advisory Service	Security Incident Response
Infrastructure Advisory Service	Enhanced Log Aggregation and Analysis
Disaster Recovery	Host Intrusion Detection/Prevention
Advanced Application Monitoring	Host File Integrity Monitoring
Enhanced Data Encryption	Smartronix CyberHunter
Application Management	Systems Vulnerability Scanning
Database Management	Security Compliance Advisory Services
Web and CDN Management	
Workspace Management	
Serverless - Compliance, Logging, and Real-Time Monitoring	
Container Service Monitoring	
Container Service Patching	

2.1. ACCOUNT SERVICES (REQUIRED)

2.1.1. ACCOUNT MANAGEMENT SERVICES (AMS)

The CAMS Account Management Service (AMS) is optimized to enforce and report CIS Benchmark Compliance and provide event trail aggregation and analysis. Security Benchmarks are defined and monitored in accordance with CAMS/CIS best-practices, which are made up of hundreds of industry-standard checks. Environments are audited to ensure security compliance, against relevant standards.

Scope:

- CSP Account Event Trails: AWS CloudTrail, Azure Monitor Logs, GCP StackDriver Metrics
- Object Storage Security: AWS S3, Azure Storage Accounts, GCP Cloud Storage Buckets
- AWS/Azure/GCP CIS Benchmark Compliance Implementation/Auditing/Reporting at the Account/Subscription/Project level

Standard Audited CSP Events:

- Privileged (root) Login
- Non-MFA Login
- Identity and Access Management changes to Policies, Groups, Users and Roles
- Notification of new Security Groups and changes to existing Security Groups
- Object Storage Policies/ACL changes
- Public access grant notifications for Object Storage
- Service Quota Limits

Automated Compliance Reporting:

- Reports on best practices and customer compliance with Center for Internet Security (CIS) benchmarks compared against the CSP IaaS environment and assets.
- Reports on existing Object Storage policies and potential risks (is the storage publicly accessible)

Account Management Triggers include:

*Triggers can be customized to customer workloads. Custom event types not identified below can be created/deployed and actioned directly to the customer as a professional services effort.

Root account logins	CSP Login authentication failures
Object storage policy changes	Security group changes
IAM policy changes	Network ACL changes
Logins without MFA	Change to cloud network gateway
CloudTrail configuration changes	Network route table changes

2.1.2. EVENT MANAGEMENT & INCIDENT RESPONSE

The Smartronix' Event Management and Incident Response (EM&IR) Service supports identification, classification, and filtering of Events, as well as structured response for mitigation and remediation of exception Incidents within customer environments.

Event management includes detection and notification via the CAMS Monitoring Solution (CMS) automation framework. Events are filtered via notification service topics and registered as Informational, Warning, or Exception.

Event Warnings initiate low priority Incident response workflows. Exception Events trigger high priority Incident response processes and procedures. The Smartronix' CloudAssured team employs structured processes for the identification, classification, escalation where necessary, and remediation of managed cloud infrastructure and supported operating system incidents.

2.1.3. SLA MANAGEMENT

Customer service requirements are monitored and tracked against documented Service Level Agreements (SLAs). The SLA Management Service reports service performance against standard Service Level targets identified below in Section 3. The reports are provided periodically and are designed to ensure service transparency by providing quality metrics throughout your experience. These metrics become the baseline for our ITSM Continuous Process Improvement.

2.1.4. LOG AGGREGATION SERVICE

Smartronix' Log Aggregation (LA) Service captures cloud service provider logs, guest OS logs for managed instances, and network logs. Alerts are generated for critical events and key performance indicators within the environment, which then automatically trigger an operational response.

Using the LA Service and Smartronix' change management process, the CloudAssured team monitors the IaaS environment for possible security incidents through event filters and alerts and performs change management of event filters implemented to ensure known critical events are identified and escalated. This service is filter-driven by a set of unwanted event types. These events include items such as cloud infrastructure configuration changes, instance termination, and excessive CPU utilization. These event filters are customized through-out the MSP term as patterns develop from lessons learned specific to the customer's applications.

Please note that log correlation, advanced search, and analysis is not part of this service – see Security Services – Enhanced Log Aggregation and Analysis. Technologies used in support of log aggregation include:

- CSP API Logs
- Virtual Network Flow Logs
- Object Storage Access Logs
- CSP Service Log Streams
- OS Logs (agent required for managed instances)
- GuardDuty for AWS only (Customer responsible for GuardDuty charges in their account. Alerts generated for level 5 and above.)

2.1.5. BOUNDARY MANAGEMENT

Smartronix' Boundary Management (BM) Service is a proactive monitoring and management service providing configuration management of cloud service provider components for networking, firewalls, virtual private networking (VPN), subnets, access control lists (ACLs), and virtual networks.

Our CloudAssured team will manage and monitor boundary protection and cloud environment network operations to ensure a secure and highly-available environment for customer data and applications. The BM service identifies, mitigates, and implements network level changes in response to events or customer requests. Supported change requests include VPN tunnel configuration, firewall policy changes to ACLs, IP route configurations, public IP allocation for service advertising, deployment of load balancing capabilities, and deployment of new cloud IP subnets. Technologies used in support of boundary management include:

- Network Flow Logs
- CSP API Event Logs
- M&N for ACL and Security Group changes

2.1.6. INFRASTRUCTURE PROVISIONING

Smartronix Infrastructure Provisioning (IP) services ensure consistent and repeatable deployment of cloud infrastructure. Customers submit IP requests through the CloudAssured ITSM portal for any service that requires management. Smartronix receives the requests, confirms the requirements, provisions the resource, and instruments the resource to ensure any core or additionally procured managed service is configured appropriately for M&N, SLA, ER&IR, AMS, BU, PM, and LA services.

Core Infrastructure Provisioning covers:

- Compute
- Storage
- Boundary Configuration
- Identity and Access Management Credentials
- Load Balancers
- Workspace provisioning

2.2. CORE SERVICES (INSTANCE BASED)

Smartronix core services integrate with the established Event Management and Incident Response and ITSM Portal for Service Request Management.

2.2.1. MONITORING AND NOTIFICATION SERVICE

The Smartronix M&N Service leverages the CAMS Monitoring Solution (CMS) automation framework. The CMS leverages micro services to detect all assets that are tagged for management and enables a defined set of standardized alarms/alerts. Each alarm can be customized to a tagged instance definition, allowing customer environments to have different defined alarm triggers for specific workloads. The CMS framework leverages web hooks to pull in the alarms/alerts and to automate creation of ITSM tickets.

Triggers include:

**Triggers can be customized to customer workloads. Custom event types not identified below can be created/deployed and actioned directly to the customer as a professional services effort.*

High CPU Utilization*	Instance failed health check
Disk space utilization*	Excessive network utilization*
Excessive disk IOPs*	High memory usage*
Excessive disk write queue length*	

2.2.2. OPERATING SYSTEM PATCH MANAGEMENT

Smartronix' Operating System Patch Management (PM) Service monitors the availability of and proactively applies operating system patches and updates through the use of a patch management life-cycle. Smartronix' CloudAssured team performs monthly patching of guest operating systems based on the vendor release schedule. Maintenance and patching windows are coordinated with each customer to ensure operations are not impacted by system patching. The patching capability is a scripted process that will trigger the guest OS to download and apply the identified guest OS patches. The applied patches are tracked through the CloudAssured MSP system to track system configuration. Critical or security related patches are quickly escalated to the customer for approval to deploy during an out of cycle maintenance window.

Customers can opt-in (patch and update) or opt-out (do not patch, do not update) individual systems via the instance tag.

Supported Operating Systems include:

- Amazon Linux 2015.03+
- RedHat Enterprise Linux
- CentOS 6/7
- Ubuntu 12.04/14.04 LTS
- Windows 2008-2019

2.2.3. ANTI-MALWARE MANAGEMENT SERVICE

Smartronix' Anti-malware (AMS) Management Service protects your environment against malware (viruses, trojans, spyware/grayware) by ensuring that the CAMS provided antimalware is installed, up-to-date, active, and is running current malware signatures on managed OS instances. When malware is detected, we proactively ensure quarantine and automatically create an incident ticket for the remediation of the issue. Audits are performed to ensure individual server compliance with customer antimalware policies.

The service is provided through a consolidated management framework. Smartronix' CloudAssured MSP offering leverages distributed relays and customer policy-based isolation. The AMS functionality is currently provided by the TrendMicro Deep Security Suite (DSS). Smartronix deploys the Deep Security Agent (DSA) on the customer guest OS image. These instances are registered through the customer DSA relay and transmitted through encrypted IP-restricted transport to the CloudAssured Deep Security Manager (DSM). Through the DSM, policies are applied to customer agents to ensure signature updates are applied as soon as available to enable up-to-date protection of customer systems. Customers can request custom agent exclusions through the CloudAssured ServiceNow portal.

The anti-malware service protects against many file-based threats, including the following: Viruses (file infectors), Trojans, Backdoors, Worms, Network, Rootkits, Spyware, Grayware, packers, and keyloggers.

2.2.4. BACKUP AND RESTORATION

Smartronix' Backup (BU) Services include system, configuration, environment and cloud services backup and restore. Backups are created and stored in the customer's cloud environment and data storage costs associated with backups are part of the customer cloud environment operating costs.

BU Services includes scheduled point in time disk volume snapshots to backup iterations of the storage volume. The service can be customized to retain backups for a customer-specified duration. The duration of backup retention will have an impact on cloud storage costs. Through the ITSM process, the CloudAssured team can restore system volumes to a customer-specified point-in-time. Prior to restoration of the requested volumes, a new snapshot will be captured to ensure a rollback is available if the restore is unsuccessful. Backup and restore testing is performed annually to ensure backup consistency.

2.3. OPTIONAL MANAGED SERVICES

2.3.1. CSEM ADVISORY

The Smartronix Cloud Service Expense Management (CSEM) Advisory Service facilitates environmental cost optimization based on actual usage data aggregation and correlation. Recommendations are based on analysis of CSEM actuals; application of advanced tool sets to model future spend as a function of utilization and execution of "what-if" scenarios; familiarity with customer workloads and environments; and, extensive experience across customer cloud environments. The CSEM Advisory Service is included as an integrated component of the Cloud Resale and Consolidated Billing Service.

Examples of cost optimization opportunities include:

- Resource utilization (Throttling under-utilized instances; Parking off-period resources)
- Right-sizing instance type
- Selection of workload-appropriate pricing models
- Resource tagging
- Reclamation of orphaned resources
- Optimization of BYOL (Bring-your-own-license)
- Storage life-cycle management
- Cost Monitoring and Alerting

This service requires deployment of the Smartronix CSEM tool which requires read only access to the CSP billing data and optional read only access to performance data (for service utilization optimization.)

2.3.2. INFRASTRUCTURE ADVISORY

Smartronix' Infrastructure Advisory (IA) Services provides prescriptive guidance on cloud services optimization, including capacity management reviews, architectural reviews and best practices reviews, auto scaling tuning, and migration paths for on premise workloads. These reviews leverage our CloudAssured - Well Architected guidelines and ITSM process.

The CloudAssured - Well Architected Review is a detailed analysis of your infrastructure, a thorough review of security practices, application integration architectures, and sizing of resources. This review enables Smartronix' CloudAssured team to ensure customers are leveraging cloud services in line with CSP best practices while delivering cost effective and secure service delivery.

2.3.3. DISASTER RECOVERY

Smartronix' Disaster Recovery (DR) Service defines a DR architecture and processes to provide full planning, annual testing and execution of a managed disaster recovery solution encompassing applications, systems, and environments. Our CloudAssured team will work with you to ensure your Recovery Time Objective/Recovery Point Objective (RTO/RPO) are appropriate to your mission and to architect the solution to fulfill the requirements at the lowest cost.

2.3.4. ADVANCED APPLICATION MONITORING

Smartronix' Advanced Application Monitoring (AAM) Service provides deeper visibility into your entire environment. Using header tags, synthetic transactions, agent-based health tools, and state-of-the-art tools, processes, and best practices, the Smartronix CloudAssured team will configure advanced monitoring to discover and optimize a comprehensive suite of availability and performance metrics.

2.3.5. ENHANCED DATA ENCRYPTION

Smartronix' Enhanced Data Encryption (EDE) Service is a custom solution. Smartronix' CloudAssured team works with the customer to define a service architecture compliant with their regulatory or policy requirements, and then implements the architecture with encryption built-in. The CAMS team provides all support for encryption key management and rotation, encryption of volumes and data, and implementation and management of service encryption certificates.

Areas of applicable support include:

- Use of cloud or collocated hardware security modules
- Database, disk volume, object store, and/or application level encryption
- End-to-end security – data ingestion, data at rest, data in transit, data in use, and data extraction
- Certificate management for secure protocols (SSL, HTTPS, TLS, etc.)
- Key lifecycle management (creation, deployment, expiration, rotation, invalidation)

2.3.6. APPLICATION MANAGEMENT

Smartronix' Application Management (AM) Service delivers COTS and custom-built applications under the managed Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS) model. This includes monitoring, maintenance, backup and restore, configuration management, patching and security assessments, and is designed to meet specific availability and/or performance SLAs.

2.3.7. DATABASE MANAGEMENT

Smartronix' Database Management (DBM) Service is a full-lifecycle capability available for industry-leading RDBMSs. This includes monitoring, maintenance, backup and restore, configuration management, patching and security assessments, and is designed to meet specific availability and/or performance SLAs.

2.3.8. WEB MANAGEMENT AND CDN

Smartronix' Web Management and CDN (WMC) Service provides monitoring, availability, maintenance, security and configuration management for web applications and frameworks, including the operations and management of third party CDN services. We provide proactive security monitoring of the site distribution, availability monitoring, maintenance, configuration management, patching and security of the environment and applications. External availability and performance monitoring is also available.

2.3.9. WORKSPACES MANAGEMENT

Smartronix' Workspaces Managed Services (WMS) brings server-class management and assurance to virtual desktop users. WMS includes operating system patch and update management, software packaging, and software lifecycle management (deployment, configuration management, updating, and deprovisioning). Workspaces Management Services Backups let you choose an RPO that's right for your organization and know that your virtual workstation data is protected. Antivirus and antimalware are included, and compliance is enforced. Integration with your existing directory service means organizational configurations, policies, and controls are applied to your Workspaces and managed by Smartronix WMS the same as they are for your servers.

2.3.10. SERVERLESS COMPLIANCE, LOGGING, AND REAL-TIME MONITORING (SCLRM)

The CAMS SCLRM is optimized to monitor CSP Serverless implementations and enforce and report CIS Benchmark Compliance. Security Benchmarks are defined and monitored in accordance with CAMS/CIS best-practices, which are made up of hundreds of industry-standard checks. All serverless environments are audited to ensure security compliance, against relevant standards.

Scope:

- Serverless Monitoring and Notification: AWS Lambda, GCP Cloud Functions, Azure Function Apps
- AWS/Azure/GCP CIS Benchmark Compliance Implementation/Auditing/Reporting at the Account/Subscription/Project level
-

Serverless Event Monitoring and Notification:

- Captures all (CSP) events, logs, audit information, and monitoring information provided by in-scope services.
- Alerts are defined for key events within the environment to trigger further analysis or incident response.
- Monitored Metrics include:
    - Number of invocations
    - Failed executions (permissions, timeouts, exceptions)
    - Concurrent executions
    - Execution throttling

2.3.11. CONTAINER SERVICE MONITORING (ECSM)

The CAMS ECSM is a monitoring capability designed specifically for AWS Elastic Container Services.

The CAMS Monitoring Service (CMS) has been extended to support monitoring of tagged ECS clusters. The following metrics are automatically enabled across the cluster and services:

ECS Supported Metrics (Dimension)

❖ Cluster →

- CPUUtilization
- MemoryUtilization
- CPUReservation
- MemoryReservation
- GPUReservation

- Service →
    - CPUUtilization
    - MemoryUtilization

These metrics tie into the Event Management and Incident Response service for effective identification, classification, and remediation of metrics that exceed allowable thresholds.

2.3.12. CONTAINER SERVICE PATCH MANAGEMENT (ECSP)

The CAMS ECSP is a custom patching capability designed specifically for AWS Elastic Container Services.

AWS recommends updating your ECS containers instance fleet with the latest AMI whenever possible. This solution is triggered via a Set Schedule (time based Patch Window) or the AWS Event that is triggered whenever a new AMI is provided by AWS.

Both Events cause a change to the launch configuration to use the newest AMI ID. The new AMI is automatically placed into service and the old AMI is drain stopped and removed from service. This process is repeated until all nodes are using the latest AMI. Upon successful completion of the Patching the service provides an SNS notification indicating success. If a failure event occurs the solution rolls back to the previous launch configuration and a SNS notification is provided for further remediation.

2.4. MANAGED SECURITY SERVICES

2.4.1. SECURITY INCIDENT RESPONSE

Smartronix' Security Incident Response (SIR) Service provides analysis, tracking, and corrective actions for issues impacting customer environments. Smartronix' CloudAssured team will support the incident response process through incident escalation, break/fix remediation of infrastructure and guest operating systems, support of in-scope disaster recovery, system restore, instance isolation, and event information reporting related to the cloud environment and guest operating systems. The CloudAssured IR capability can also be leveraged by customer application teams to help identify application-impacting problems related to the environment or guest operating systems.

2.4.2. ENHANCED LOG AGGREGATION AND ANALYSIS

Smartronix' Enhanced Log Aggregation and Analysis (ELAA) Service is captures events, logs, audit information and monitoring information provided by operating systems, platforms, networks, applications and infrastructure. Alerts are defined for key events within the environment to trigger further analysis or incident response.

ELAA extends the core *Log Aggregation* service by integrating search capabilities, counters, and proactive log review analysis. The *Analysis* capability enables the correlation of events by generating a process chain. For example, a web site health check failure can be linked to a john.doe login and a john.doe action of stopping the web service. The standard Log Aggregation event filter service will only identify the user logged on, the user stopped a service, or the web health check failed, but the causality link between events would be a manual process. The search capability also enhances the ability of the customer's applications teams to quickly identify underlying system events linked to a service incident.

2.4.3. HOST INTRUSION DETECTION/PREVENTION

Smartronix' Managed Host IDS/IPS service provides 24 x 7 security event alerting, investigation and response to potential security incidents identified by our endpoint HIDS/HIPS capability. The CAMS HIDS/HIPS service leverages industry partner-maintained and updates signature sets. The CAMS security team ensures the most appropriate sets of signatures are applied to customer endpoints. With systems and security managed services engineers, we provide immediate on-call and after-hours assistance to extend the IT security capability of your team.

2.4.4. HOST FILE INTEGRITY MONITORING

Smartronix' Host File Integrity monitoring service can alert you when changes happen to key operating system and application files, as well as essential processes and ports. Integrity monitoring detects unauthorized changes that introduce operational as well as security risks by identifying system incompatibilities and potential indicators of compromise (IOCs). The service leverages our FIM capability to provide alerts and response to identified events 24x7. The identification of protected files can be customized to meet customer security concerns.

2.4.5. SMARTRONIX CYBERHUNTER™

A common challenge for system administrators and security analysts is determining if an instance has malware present or has been compromised. This may be due to many reasons, such as a security event detection, concerns that a "coin miner" is impacting instance CPU load, a security misconfiguration that may have resulted in instance compromise, or leadership seeking assurances that the environment has not be compromised by a recent threat. Performed manually, live system triage is time consuming, requires specialty knowledge, and is prone to error. Common methods of triage look for indicators of compromise that always lag behind the threat and often miss the most concerning attacks.

CyberHunter is a Smartronix developed capability for performing non-service impacting live system triage and compromise assessment. Our innovative detection techniques were developed based on our years of defending high value environments from the most sophisticated threat actors. CyberHunter merges our unique memory analysis methods with our knowledge of other key points of system analysis with automation of the collection and triage of systems. Proprietary, multi-faceted analytic and triage methods are then leveraged to provide our seasoned analysts with rich, high quality information to enable an accurate and prompt threat identification. Together our tools and analysts provide our customers assurance that their environment is threat free of malicious code. And when things go wrong and an adversary gains access, the Smartronix CyberHunter capability provides the advanced skills to help push the threat out.

2.4.6. SYSTEMS VULNERABILITY SCANNING

Smartronix' Systems Vulnerability Scanning Service utilizes Tenable's Nessus Security Scanner and Nessus Security Manager. The scanning service enables the assessment of networks and connected IT systems against regulatory compliance standards and identifies any known system vulnerabilities, the solution offers automated network vulnerability scanning, configuration assessment, application vulnerability scanning, device configuration assessment, and network discovery.

Note: The standard template supported by the vulnerability scanning service is from the Center for Internet Security (CIS) benchmarks. Additional standards and templates may be supported based on customer regulatory requirements.

2.4.7. SECURITY AND REGULATORY COMPLIANCE ADVISORY SERVICES

Smartronix' Security and Regulatory Compliance Advisory (SRCA) Service leverages Smartronix' security compliance experts to provide clients guidance in meeting regulatory requirements and recommend mitigation of threats that have potential to impact client-specific environments as they appear and evolve. The service will help document and update control documentation in support of maintaining customer regulatory compliance.

Examples of compliance activities include:

- Creation of System Security Plan documentation
- Support of internal compliance audits
- Tracking Plans of Action and Milestones (POAMs)
- Risk assessment and planning
- Monitoring and responding to industry regulatory changes

1. SERVICE LEVEL AGREEMENTS

1.1. SLA 1: SYSTEM AVAILABILITY

SLA 1: "System" Availability	
Description	This SLA applies to "system availability" of a service. A system is considered a series of components that make up the infrastructure service that hosts and provides the compute and storage capabilities consumed by the customer applications and services. System availability applies to the following products and services: • Virtual Compute Instances (AWS EC2 and Azure Virtual Machines deployed in the same availability set) • Block Storage (AWS EBS, Azure System/Data Disks) Smartronix SLA incorporates the AWS and Azure SLA terms defined below which are subject to change in accordance with the AWS and Azure Agreements. • AWS Compute SLA: https://aws.amazon.com/ec2/sla/ • Microsoft Azure Compute SLA: https://azure.microsoft.com/en-us/support/legal/sla/virtual-machines/v1_6/ • GCP SLAs will be negotiated per customer
Measurement	Smartronix will measure system infrastructure availability by using tools that will access the cloud infrastructure compute availability at 5 minute intervals to analyze cloud IaaS regional compute availability.
Calculation	NUMERATOR Uptime (Seconds) ÷ DENOMINATOR= Total amount of time (seconds) for the monitoring period = RESULT Service Level (%) Attained.

SLA 1: “System” Availability	
Success Criteria	Smartronix will be considered successful if the system is fully available for use 99.95% of the time.
Exceptions / Conditions	Instances scheduled to occur during the following periods are excluded from the Numerator and Denominator for calculation purposes: Downtime approved by customer; and Downtime due to events outside Smartronix control and approved as such by customer. Examples of these type of exception events include: Force majeure events; and Outages determined to be caused by customer or customer contractor-developed application code provided by customer. Systems must be implemented in a functional high availability configuration.

1.2. SLA 2: BACKUP AND RESTORATION

SLA 2: Backup and Restoration	
Description	This SLA measures the percent of times that the platform is restored to last agreed and documented state and last transactional dataset after failure, data loss or user request for restoration.
Measurement	Initiation of restore for individual file or database requests within 8 hours of receipt of request or notification of failure Backup retention periods are defined by Client.
Calculation	NUMERATOR: Number of successful restore initiations within 8 hours or Number of full restoration within 48 hours ÷ DENOMINATOR: Number of Requests for Restores = RESULT Service Level (%) Attained.
Success Criteria	Smartronix will be considered successful if successfully restored 95% of the time as measured on a Monthly basis.
Exceptions / Conditions	SLA’s may not be met during Client Disaster Recovery and Client Disaster Recovery exercises, during those periods best effort will replace the SLA.

1.3. SLA 3: INCIDENT RESPONSE

SLA 3: Incident Response Time	
Description	This SLA measures Smartronix’ response time, per the Exceptions/Conditions in this SLA, following issue identification.

SLA 3: Incident Response Time	
Measurement	SLA attainment is validated by 100% inspection of reporting documentation.
Calculation	NUMERATOR: Number of incidents receiving response within time for given severity level ÷ DENOMINATOR: Total number of Incidents = RESULT: Service Level (%) Attained.
Success Criteria	Smartronix is successful if 95% of incidents receive a response within response time for given severity level, as measured on a monthly basis.
Exceptions / Conditions	Severity 1 - Critical - An entire service is down. All users affected. Within 1 hour of incident occurring 24x7x365. Severity 2 - High - Operation of the service is severely degraded, or major components of the services are not available. Significant user impact. Within 2 hours of incident occurring 24x7x365. Severity 3 - Medium - Some non-essential features of the service are impaired or subject to interruptions while most vital components of the service remain functional. Minimal user impact. Within 24 hours of incident occurring during business hours. (8am-8pm EST M-F). Severity 4 - Low - Errors that are minor and clearly have little to or no impact on the normal operation of the service. No or minimal user impact. Within 1 business day of incident occurring during business hours. (8am-8pm EST M-F). Exception: Impending events; notification will happen; incident response will be initiated before follow-up notification; as clients will be previously notified (SLA 5) of the likelihood of the event.

1.4. SLA 4: OPERATING SYSTEM PATCHING AND UPDATING

SLA 4 – Operating System Patching	
Description	This SLA measures Smartronix' ability to patch all operating systems protecting on a planned schedule. All critical patches will be applied in accordance to the client planned schedule that will be defined in the Concept of Operations document. All other patches will be executed upon a customer pre-approved schedule.
Measurement	All operating systems will be up to date with critical patches within 10 days of release and measured by scanning with vulnerability software.
Calculation	NUMERATOR: Total number of patched systems within 10 calendar days of critical patch release ÷ DENOMINATOR: Number of systems requiring patches = RESULT: Service Level (%) Attained.

SLA 4 – Operating System Patching	
Success Criteria	Smartronix is considered successful when 95% of critical patches are applied to the initial environment within 10 calendar days of release from vendor and subsequent patches are applied per the customer patch schedule. Patches must be approved by customer. This will be measured on a monthly basis.
Exceptions / Conditions	Ten (10) day SLA applies to the initial environment patched. Patching of subsequent environments follow customer patch schedule. Smartronix failure to execute patching of subsequent environments per customer patch schedule shall also be considered an SLA failure for purposes of the Calculation. Any patches not approved by customer or Smartronix' CCB are excluded from the SLA Calculation.

1.5. SLA 5: IMPENDING EVENT NOTIFICATION

SLA 5 – Impending Event Notifications	
Description	Smartronix will notify the customer of the possibility of an impending event or events that have occurred which might affect system operation. Examples include cloud service provider notifying Smartronix of service degradation, service unavailability, or service termination.
Measurement	Smartronix will measure impending event notification based on reporting within 1 hour of detection of the event or impending event.
Calculation	Best Effort. Availability SLA ultimately determines client access to the system or service.
Success Criteria	N/A
Exceptions / Conditions	Events outside of Smartronix control are not included.

1.6. SLA 6: DATABASE MANAGEMENT SERVICE REQUEST

SLA 6 – Service Request – Database Management	
Description	Smartronix will initiate requested support on-demand functions for Database support made by the customer within one business day. Examples include request for database refresh from prod to Test or development, launching database instances, preforming performance analysis.
Measurement	Smartronix will measure request response based on the time requested as documented in the ITSM reporting system and the request initiation being within 1 business day.
Calculation	NUMERATOR: Number of successful request initiations within 1 business day ÷ DENOMINATOR: Number of Requests =

	RESULT Service Level (%) Attained.
Success Criteria	Smartronix will be considered successful if successfully initiated responses 95% of the time as measured on a Monthly basis.
Exceptions / Conditions	SLA's may not be met during Client Disaster Recovery and Client Disaster Recovery exercises, during those periods best effort will replace the SLA.

1.7. SLA 7: IMPENDING SECURITY THREAT NOTIFICATION

SLA 7: Impending Security Threat Notifications	
Description	Smartronix will notify the Client of the possibility of an impending Security Threat or events that have occurred which may impact system operation. Examples include global intelligence sources identifying new threats in the environment that may impact OS, Applications, or services used by Client.
Measurement	Smartronix will measure impending event notification based on reporting within 1 hour of detection of the event or impending threat
Calculation	Best Effort. Availability SLA ultimately determines client access to the system or service.
Success Criteria	N/A
Exceptions / Conditions	Events outside of Smartronix control are not included.

*SLA usage can vary dependent on services purchased.

2. COMMERCIAL PRICING

Table 3. Account Services

Service Title	Monthly Price
Account Management Service	$X/Account
SLA Management	
Event Management & Incident Response	
Boundary Management	
Log Aggregation (Basic)	
Infrastructure Provisioning Service	$X/Provisioning Request

Table 4. Core Managed Services

Service Title	Monthly Price
Monitoring and Notification	$X/instance
Operating System Patch Management	
Anti-malware Management	
Backup and Restoration Service	

Table 5. Cluster Managed Services

Service Title	Monthly Price
Container Service Monitoring and Notification	$X/cluster
Container Service Patch Management	

*CAMS has a monthly minimal commitment of $2,500 across account, core, and cluster managed services.

Table 6. Optional Services

Service Title	Price
Cloud Service Expense Management Advisory Service	X% of Invoice monthly
Infrastructure Advisory Services	Priced based on scope
Disaster Recovery Service	Price based on request
Advanced Application Monitoring	Priced based on scope
Enhanced Data Encryption	Price based on request
Application Management Services	Price based on request
Database Management Services	$X / instance
Web Management Services and CDN	$X/ per site distribution
Workspaces Management Services	Tier per Workspace Instance Fee $X Per less than 150 Instances $X for 150 through 300 $X for 300 through 700 $X Greater than 700
Serverless Environment – Compliance, Logging, and Real-time monitoring	$X per application or service mesh

Table 7. Optional Security Services

Service Title	Price
Security Incident Response	Priced based on scope.
Enhanced Log Aggregation and Analysis	Log Monitoring and Analysis - $320/per GB of indexed data, based on average daily consumption in a calendar month.
Host Intrusion Detection/Prevention	$X per instance
Host File Integrity Monitoring	$X per instance
Smartronix CyberHunter	Based on blocks of 400 collections per day $X per month
Security Systems Vulnerability Scanning	$X per instance
Security & Regulatory Compliance Advisory Service	Professional Services Priced based on scope

*ELAA has a monthly minimal commitment of $8,000 per month or the total of cost based on average GB indexed per day in a one-month measurement period (based on calendar), whichever is higher.

Notes:

- Customized service/pricing for customer environments that have reduced requirements, e.g. Development, Test, Quality Assurance, or Labs is available.
- CAMS is deployed to customer CSP accounts via Terraform infrastructure as code templates. This enables Smartronix to expedite customer onboarding and to ensure quality through a templatized, tested, and automated workflow.
- AWS Clients are required to enable Config, CloudTrail, CloudWatch, network flow logs, and allow SMX to install AWS CloudWatch agent, AWS SSM agent, and AWS Inspector Agent on managed instances in regions that run services supported by Smartronix.
- Smartronix CAMS will leverage a centralized IdP with MFA enabled login to gain access the customer CSP account. All actions performed in the customer CSP account will be logged and retained in the customer account for audit purposes.
- Micro services will execute service automation tasks within the account to enable instance monitoring, snapshots/backups, and creation of alarms to create event notifications.
- Smartronix will reserve one resource tag for use in the management of the resources.

2.1. DISCOUNT SCHEDULE

Monthly Cost	Discount Tier
$0 - $25,000	0%
$25,001 - $50,000	2.5%
$50,001 - $100,000	5%
$100,001 - $150,000	7.5%
$150,001 - $200,000	10%
$200,001 - $500,000	12.5%
$500,001 -$1,000,000	15%
Over $1,000,001	20%

NOTE: The Version History table below is for internal reference only.

Version History

Version	Date	By	Description of Changes
00	4/5/2018	R. Jones	Added doc number and Version History table.
01	9/25/2018	T. Hobiena	Updated Title
02	9/30/2019	A. Vultaggio	Updated service definitions
03	10/29/2019	R. Groat	Broke out Account Managed Services and added container managed services
04	11/13/2019	R. Groat / A. Vultaggio	Updated pricing. Changed RapidScan to CyberHunter per Rick Schutz.