MANAGED SECURITY SERVICE LEVEL AGREEMENT

This Managed Security Service Level Agreement ("SLA") is incorporated into the Quote executed by C Spire Business and Customer for Managed Security Services and sets forth the specific terms and conditions under which C Spire Business shall supply the Security Information and Event Management Services described herein to Customer. The general terms applicable to such Services are contained in the Master Terms and Conditions ("MTC") and the Master Service Level Agreement ("MSLA") incorporated into the Quote by reference. Capitalized terms used but not defined herein shall have the meanings set forth in the MTC and MSLA.

TERMINOLOGY

The following are service-specific definitions. Common definitions are already defined in our Master Service Level Agreement.

- Device – The Customer server, router, switch, firewall, VPN, or other legacy device receiving Service.
- Operating System – The base software running on Customer Device.

SERVICE DESCRIPTION

C Spire Business' cloud-powered security tools fully integrate software solutions, security operations, and monitoring into one solution to keep resources secure and compliant. We monitor, analyze, educate, and protect networks with intrusion detection, vulnerability assessments, threat monitoring, content filtering, multifactor authentication, and log management solutions.

SERVICE OFFERINGS

THREAT MONITORING

C Spire Business' Threat Monitoring solution combines two essential security capabilities into one. Our bundled approach saves you time and money while still providing the most thorough approach on the market. This service can also allow our team of certified security experts to quickly and efficiently detect threats in your environment.

INCIDENT RESPONSE AND REMEDIATION

During any disruption of Services, including but not limited to disruptions caused by a cyber security event, C Spire's investigation and response is limited to restoring only those Services being provided. C Spire is not responsible for preserving forensic artifacts in the course of such investigation and response, and C Spire expressly disclaims all related liability. C Spire Business does not provide or perform (a) identification, collection, examination, and analysis of data for purposes other than restoration of Services ("Digital Forensic Services") or (b) containment and recovery from an incident outside of the work necessary to restore Services

("Incident Response Services"). As such, and notwithstanding anything to the contrary, Digital Forensic Services and Incident Response Services are specifically excluded from all Services purchased by Customer.

Incident Remediation is not a service provided through any of C Spire Business's Threat Monitoring platforms. Any incident remediation provided by C Spire Business will be scoped through a Statement of Work with associated pricing, through Professional Services block hours, or billed through Time, Travel, and Materials at standard market rates.

C Spire business provides this service through two different platforms depending on customer need:

1. Arctic Wolf

The Arctic Wolf Platform is comprised of 3 major components that are contracted separately:

1. MDR (Managed Detection & Response)

a. Continuous monitoring and threat hunting with broad visibility across the environment
b. Investigation & response with Log Retention and Search (optional add-on)
c. Guided remediation (Professional Services) with root cause analysis

2. Managed Risk

a. Dynamic asset discovery & attack surface coverage with account takeover risk detection
b. Classification & contextualization of risk with a Risk Scoring report
c. On Demand reporting & guided remediation

3. Managed Security Awareness

a. Train & prepare employees to stop social engineering attacks like phishing.
b. Identify threat topics that need reinforcement.
c. Transform to a culture of security.

OPTIONS

LOG RETENTION

Logs may be retained for up to one year.

DATA EXPLORATION

Search of retained logs

SENSOR HARDWARE

Threat Monitoring requires that a sensor be installed at all egress points where internet traffic leaves the network and is also required to collect SIEM logs. There are multiple options depending on network size and what is needed of the sensor, and sensors may be deployed as hardware or as virtual appliances.

2. ConnectWise (Perch) Security

The two essentials of this threat monitoring solution:

- SIEM – Correlates and analyzes security event data from across your cloud and on-premise environments.

- Intrusion Detection – Continuously monitors traffic between devices and protection of critical assets and systems in your cloud and on-premise environments.

C Spire's Threat Monitoring service is not a prevention or remediation service, but rather alerts C Spire Business and Customer to threats detected in the environment. Customer is responsible for remediation of the threat and vulnerability. C Spire Business Professional Services can be engaged through block hours to provide remediation services.

OPTIONS

NETWORK IDS

The Network IDS coverage is based on total number of IP addresses on the network that are being monitored. There are options to add 8x5 or 24x7 SOC coverage and both come with four-hour SLAs.

SIEM

SIEM can be added to a device on the network to collect logs for correlation with NIDS as well as store them for compliance purposes. This is added to the Network IDS license for that device. SIEM storage comes with the following storage lengths:

- 30 Days Storage
- 180 Days Storage
- 365 Days Storage

SENSOR HARDWARE

Threat Monitoring requires that a sensor be installed at all egress points where internet traffic leaves the network and is also required to collect SIEM logs. There are multiple options depending on network, size of the sensor, and what is needed.

WORKSTATION ENCRYPTION

C Spire can provide end-user endpoint encryption via a combination of BitLocker and Intune. Customer must purchase Intune, or a Microsoft 365 package that includes Intune, through C Spire Business's Microsoft 365 offering.

WORKSTATION ENCRYPTION FEATURES

C Spire Business will perform initial provisioning of the account.
C Spire Business will modify policies to match customer needs.
C Spire Business will update policies per customer requests. Requests for such changes must be approved by authorized customer contact.

WORKSTATION ENCRYPTION DEPENDENCIES

C Spire Business requires that the customer purchase Intune through Microsoft 365 and C Spire's Encryption Management SKU.

ADVANCED ENDPOINT PROTECTION (AEP) – ENDPOINT DISCOVERY & RESPONSE (EDR)

SentinelOne Singularity Complete uses deep learning to detect new and unseen malware files without relying on signatures like a traditional antivirus solution.

AEP-EDR FEATURES

- C Spire Business will perform initial provisioning of the account.
- C Spire Business will modify policies to match customer needs.
- C Spire Business will update policies, whitelists, and blacklists per customer requests. Requests for such changes must be approved by authorized customer contact.
- This service can be sold for workstations or servers separately.

AEP-EDR DEPENDENCIES AND LIMITATIONS

C Spire Business requires the installation of the C Spire-managed SentinelOne agent on customer servers. Additionally, performance is limited to the technical capability of the SentinelOne platform.

MULTIFACTOR AUTHENTICATION

Our Multifactor Authentication solution will drastically lower the risk of compromised credentials by associating a user's cell phone to their user account. When they attempt to log in, they will be provided with a second factor of authentication. This can be a prompt from the Duo app on their mobile phone.

WEB FILTERING

Web Filtering through Cisco Duo provides a layer of cloud-delivered protection in the network security stack, both on and off the corporate network, preventing command and control callbacks, malware, and phishing over any port or protocol.

MANAGED WEB FILTERING FEATURES

- C Spire Business will perform initial provisioning of the account.
- C Spire Business will modify policies to match customer needs.
- C Spire Business will update policies, whitelists, and blacklists per customer requests. Requests for such changes must be approved by authorized customer contact.

ADD-ON OPTION

The following option may be added to Web Filtering Service for an additional cost.

ACTIVE DIRECTORY INTEGRATED AND MOBILE DEVICE

With this option, C Spire Business provides user- or group-based policies for content filtering. Reporting can also be tracked at a specific level as opposed to the global settings. Requires virtual appliance to be installed.

Availability Dependency

Customer must have a virtual platform (managed, hybrid, private, virtual private cloud) and domain controller(s) if they are using the Active Directory Integrated and Mobile Device option.

WEB FILTERING LIMITATIONS

C Spire Business will only install client/agents if the Customer has a Managed Infrastructure agreement. Otherwise, Customer can purchase a Block of Hours.

AVAILABILITY DEPENDENCIES

The availability of Service is dependent on the following:

- Existence of a suitable network transport from C Spire Business to User(s). C Spire Business also reserves the right to limit Service availability in the event that necessary Service Components are either unavailable or unattainable at a reasonable cost to C Spire Business.

- It is Customer's responsibility to ensure that all devices are able to connect to the Service and are configured properly. This includes, but is not limited to, Ethernet switches, Ethernet cabling, workstations, servers, operating systems, and software.

- Customer is responsible for assisting in the configuration of Log Sources, Collection Policies, Log Correlation Policies, Saved Views / Reports, Blocking Policies, Scans, Manually Generated Incidents, Alerts, and Cases in the Services User Interface.

- Customer will work with C Spire Business to install and configure equipment for the purpose of enabling the Services including, but not limited to, appliances, network taps, Firewalls, routers, switches, and Operating Systems.

SERVICE LEVEL METRICS

Service availability and Service performance goals are 99.9% for the cloud services offered in the solution. Appliances, agents, or any other services deployed with the client environment are not included in 99.9% cloud SLA. Client onsite services are response-based SLA only.

SERVICE DELIVERY

Upon receipt of the signed Quote, C Spire Business will coordinate installation services with the Customer and our security services vendor.

WORKSTATION ENCRYPTION

- C Spire Business will need access or assistance deploying to all necessary client workstations.
- C Spire Business will configure all necessary portal access and policies.

ADVANCED ENDPOINT PROTECTION (AEP) – ENDPOINT DISCOVERY & RESPONSE (EDR)

- C Spire Business will need access or assistance deploying the SentinelOne agent to all necessary client servers.
- C Spire Business will configure all necessary portal access and policies.

MULTIFACTOR AUTHENTICATION

- C Spire Business will need access or assistance installing the Duo application on any necessary servers.
- C Spire Business will provision the vendor portal.
- C Spire Business will provide basic access and setup instructions.

THREAT MONITORING

- Physical Server(s)
- Threat Monitoring software
- Integration with the C Spire Business Security Operation Center

WEB FILTERING

- C Spire Business will need assistance modifying DNS forwarding. Server firewall access will be needed.
- If the AD integration option is purchased, Customer must provide the environment to set up the virtual appliance. C Spire Business will help with setup and will need Customer to provide IP addresses on their internal network and assist with setup.

If additional configuration work is required due to limitations of the Customer network, C Spire Business reserves the right to bill Customer at current hourly rates for additional configuration time.

C Spire Business is not responsible for, and will not be obligated to provide, any support or assistance in configuration, installation, administration, troubleshooting, maintenance, repair, or integration of customer equipment, software, or network application into the Customer's internal network. C Spire Business is not responsible for any failure of tools or services to detect or prevent security events within the environment and C Spire Business will be held harmless for any security event, system compromise, data loss, corruption, theft, or intrusion to customer environment.