Service Level Agreement

This Service Level Agreement ("SLA") is part of the Commercial Subscription Agreement ("CSA") between Company and Trinity Cyber. Capitalized terms used herein that are not defined in this SLA shall have the meaning attributed to them in the Terms of Service ("ToS").

Trinity Cyber is committed to providing effective, reliable, highly accurate and available security services without negatively affecting the availability or latency of Company's internet service. As a part of this commitment, Trinity Cyber personnel will install new customers quickly and effectively, and provide support in a timely and professional manner. Our service is designed to remain available and highly performant, and not to interrupt customer internet services or business operations.

1. SERVICE COMMITMENTS

1.1. Installation Commitment. Trinity Cyber will install its service within 60-90 business days measured from the effective date of a Commercial Subscription Agreement. If Trinity Cyber fails to meet this commitment, Company will receive one-month Service Credit for every month of delay. Trinity Cyber's Installation Commitment is subject to the condition that Company or its representatives must cooperate with Trinity Cyber in the installation process, which includes providing timely and accurate information about Company network, timely access to network configuration information and traffic, and cooperates in making any necessary network infrastructure configuration changes. This commitment does not apply to on-premise deployments.

1.2. Trinity Cyber System Availability and Performance Commitments. Trinity Cyber services and technologies are designed to be highly available and low latency, and its preventive security controls are designed not to be visible to hackers or disruptive to customer operations.

1.2.1. Trinity Cyber System Availability. Trinity Cyber guarantees 99.999% availability of its service over the period of each full calendar month (the "System Availability Target"), excluding occasional scheduled maintenance outages, which will be coordinated in a manner mutually acceptable and approved in advance by the Company and Trinity Cyber. On occasion, Trinity Cyber may place the inline components of Trinity Cyber services in bypass for the purpose of trouble shooting Company network issues. The time during which Trinity Cyber has intentionally placed its inline components into bypass for the purpose of trouble shooting is not included in the calculation of system availability.

System Availability	Service Credit
>= 99.999%	N/A
< 99.999% but >= 99.99%	3 days
< 99.99% but >= 99.00%	7 days
< 99.00% but >= 98.00%	15 days
< 98.00%	30 days

1.2.2. Trinity Cyber System Processing. Trinity Cyber commits to processing Company internet traffic with an average latency of 3 milliseconds or less, measured as an average of all Company Internet traffic processed by Trinity Cyber over the course of a 90-day period corresponding to the four quarters of the calendar year. Trinity Cyber processing latency will be measured from the time data arrives at a Trinity Cyber processing stack until the data leaves it. This includes all load balancing, switching, and routing components in addition to the actual security processing. It does NOT include any transport latency to or from Trinity Cyber's point of presence, transfer latencies for protocols layers above the data link layer, or latencies introduced due to the dynamic nature of the Internet. As a full-session store-and-forward proxy, latency cannot be measured at a packet level for all traffic. Some protocols, e.g. ICMP, can be measured at a per-packet layer. Others, e.g. HTTP, are proxied such that packets and segments are turned into data streams and objects before being processed and then forwarded.

1.2.3. Trinity Cyber System Security Controls. Trinity Cyber maintains a False Detection Rate[1] (FDR) less than 1% for all Formulas, averaged over the course of a 90-day period corresponding to the four quarters of the calendar year. Trinity Cyber will routinely implement new preventive Formulas on behalf of Company, and will maintain the same levels of accuracy and efficacy of these updates. Automated actions taken on Company's Internet Traffic by Trinity Cyber's Solution are tailored to minimize business impact and maximize business continuity. Every action taken will be communicated to Company, as appropriate, through Trinity Cyber's Customer Portal, or via its Application Programming Interface (API). Customer Portal information will provide necessary timestamps and any telemetry exposed to Trinity Cyber that will aid in tracing a threat or Formula event.

[1] False Detection Rate is calculated as the number of times a false detection occurred divided by the number of times the detection of a particular event was attempted. This value is in sharp contrast to the more commonly used and less revealing False Positive Rate, which is typically calculated as the number of times a false detection occurred divided by the number of times detection processing occurred. The use of a low FPR is more easily achievable and can often lull cyber defenders into a false sense of security. If calculated as a False Positive Rate, the typical average Trinity Cyber False Positive Rate would have more than 10 zeros to the right of the decimal point.

1.3. Commitment Not to Interrupt Company Internet Service. Most of Trinity Cyber's services utilize inline technology. For Company's receiving inline services, Trinity Cyber represents very little risk to Company internet availably and reliability. While using Trinity Cyber services, excluding all things outside the control or fault of Trinity Cyber, Company will experience at least 99.999% internet service availability at up to the data rate Company purchased from its Internet Service Provider (ISP) averaged across an aggregate of typical network traffic over the period of one calendar month (the "Internet Service Availability Target"). No guarantees are made about individual connections or specific protocols. Trinity Cyber will make every effort practicable to maintain the availability of Company's network services up to and including bypassing the inline components of the Trinity Cyber Solution for the purpose of trouble shooting, to prevent or limit internet service interruption, or both. Trinity Cyber will proactively monitor its Solution as it relates to Company's network performance to proactively mitigate potential fault conditions, and will respond to Company notices of suspected interruption promptly (see Severity 1 Response below).

Internet Availability	Service Credit
>= 99.999%	N/A
< 99.999% but >= 99.00%	3 days
< 99.00% but >= 98.00%	7 days
< 98.00% but >= 95.00%	15 days
< 95.00%	30 days

2. CUSTOMER ACKNOWLEDGMENTS AND RESPONSIBILITIES

Company recognizes that the Internet is a diverse collection of independently operated networks, equipment, and service providers. Transit from Company's point(s) of presence to Trinity Cyber's point(s) of presence will be designed for mutually agreed upon optimal computer network and financial attributes, but is outside the control of either Company or Trinity Cyber. No attributes of performance described herein that cannot be controlled by Trinity Cyber will be attributed to it. It is incumbent upon Company personnel to also do their due diligence and ensure fail-safes and automated bypass capabilities are in place to mitigate any failures outside the control of either Company or Trinity Cyber.

Trinity Cyber can provide engineering design support and documentation sufficient to ensure Company is comfortable with their recourse options should Trinity Cyber be unable, for reasons outside of their control, to alleviate an availability or performance issue in a timely manner.

3. ADDITIONAL DEFINITIONS

3.1. Formula. Trinity Cyber defines a Formula to be a combination of 1) complex detection logic (part of a powerful new syntax developed to interrogate fully parsed and indexed network content that Trinity Cyber scanning engines, decoders, and parsers expose) and 2) automated mitigation syntax that employs tailored mitigation actions to prevent or modify a threat inline.

3.2. Error. Error means a material deviation in the performance of the Solution from the then-current description.

4. TERMINATION FOR AVAILABILITY FAILURES

In the event that (i) the System Availability Target is not met for 3 months in a rolling 12 month period, or (ii) the Internet Service Availability Target is not met for 3 months in a rolling 12 month period, then Company may terminate the CSA and/or the applicable Order by providing written notice to Trinity Cyber, and Trinity Cyber shall refund to Company a pro-rata portion of any prepaid Subscription Fees for the remaining paid period after the effective date of such termination.

5. SERVICE CREDIT AND CLAIM PROCESS

5.1. Service Credit. In the specific circumstances set forth in Sections 1.1, 1.2.1 and 1.3., and only in those circumstances, monetary payment for violations of this SLA will be provided in the form of a credit to the Company ("Service Credits") upon review by Trinity Cyber following the Service Credit Claim Process in Section 5.2. Service Credits will be proportional to the period impacted and monthly billable service prices, in accordance with circumstances described in Section 1.1 and the Service Credits listed in the tables in Sections 1.2.1 and 1.3.

5.2. Service Credit Claim Process. In order to initiate a claim for a Service Credit, Company must contact Trinity Cyber within thirty (30) days after the incident has been resolved, for which credit is requested. Claims should be initiated at ServiceCredit@TrinityCyber.com. The Service Credit request must be made in writing and must provide: (a) the Company name and contact information; (b) the date and beginning/end time of the claimed outage or failed metric; and (c) a brief description of the characteristics of the claimed outage or failed metric.

6. SOLE AND EXCLUSIVE REMEDY

The Service Credits and the termination rights set forth in Section 4 above are Company's sole and exclusive remedies, and Trinity Cyber's sole and exclusive obligations and liabilities, for any failure of Trinity Cyber to meet the System Availability Target or the Internet Service Availability Target or to install the service.

7. THE TRINITY CYBER SUPPORT AND SUPPORT ENGAGEMENT PROCESS

Trinity Cyber support services are available through the Trinity Cyber online Customer Portal 24x7x365. Response times will vary based on the severity level of the reported issue and subscription tier. Details are set forth in the chart below. Trinity Cyber support services also are available via telephone at 1-240-842-9930 for severity level 1 issues.

Upon reporting the issue or inquiry, reported issues and inquiries will be assigned a unique Case ID number and such number must be used in all future correspondence until the issue or inquiry is resolved. Trinity Cyber will respond to Company personnel according to the severity and support levels below:

Trinity Cyber Support	**Advanced**	**Premium**	**Elite**
Customer Portal Access 24 x 7 x 365	✓	✓	✓
Phone: 1-240-842-9930	Severity L1 Only	Severity L1 Only	✓
Monthly / Quarterly Performance Review	X	✓	✓
Annual Review	✓	✓	✓
Severity Level Response Times			
Severity L1 Response – An issue that prevents operation of critical documented functions with high frequency or duration (e.g., issues involving network availability or significant throughput disruptions)	2 hrs	30 min	15 min
Severity L2 Response – An issue that consistently prevents operation of non-critical documented functions or occasionally impacts critical documented functions or a critical issue for which a temporary work around has been provided (e.g., Company believes that false detections or Formula updates are disrupting the availability of their networks or services)	4 hrs	1 hr	30 min
Severity L3 Response – An issue that has some impact on administration, non-critical operation or other secondary functions or a major issue for which a temporary work around has been provided (e.g., system errors, certificate issues)	12 hrs	3 hrs	2 hrs
Severity L4 Response – Company requests product related technical advice or general information and feature questions related to the services.	48 hrs	6 hrs	4 hrs
Support Contact Information			

- Customer Portal Access: https://portal.trinitycyber.com/support
- Telephone: +1-240-842-9930 (Severity Level 1 issues only)

Special Notes:

- In order for Trinity Cyber to best support Premium and Elite subscribers, Premium and Elite companies agree to attend and support regularly scheduled monthly or quarterly business reviews with Trinity Cyber
- Cases in a status of "Customer Hold" with no update from Company after 5 business days will be closed, except those related to Monitoring Alerts requiring Company housekeeping
- Government entities may only subscribe to Elite service