TRINITYCYBER

USE CASE

PROTECT YOUR WEB APPLICATIONS AND YOUR CUSTOMERS

Place Trinity Cyber in Front of Your Hosted Applications to Protect Your Infrastructure and Your Customers with Full Content Inspection

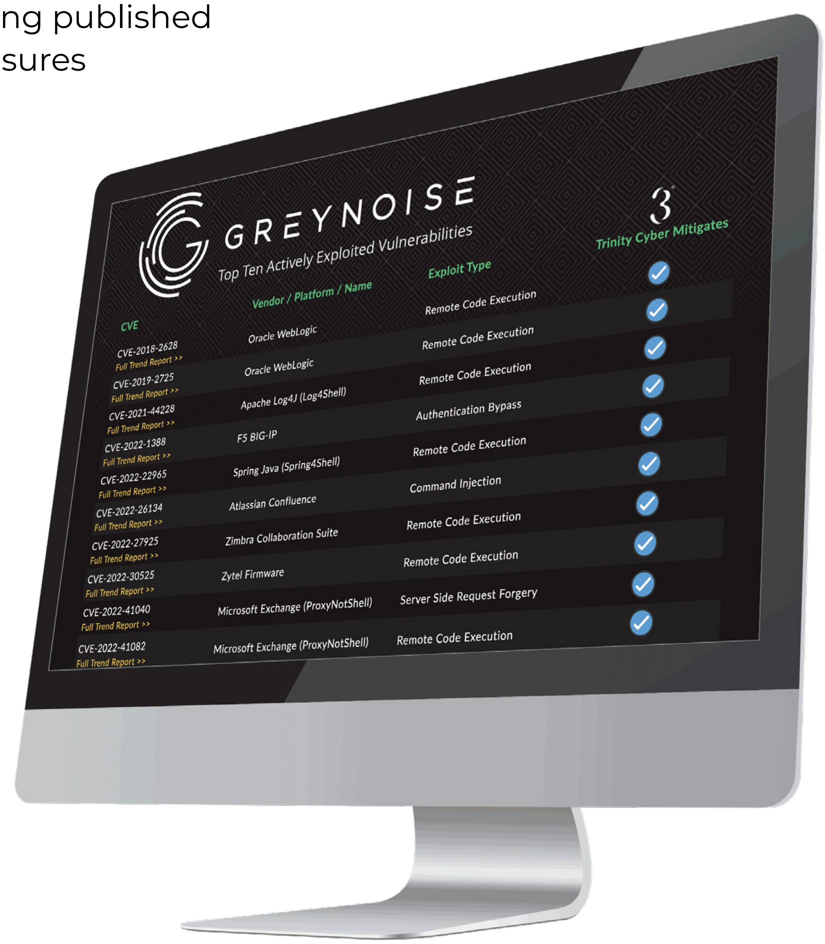
Unleash the power of Trinity Cyber's cutting-edge full content inspection technologies and team of world-class experts to protect your applications and customers.

To connect an application through Trinity Cyber Service, all you have to do is point a CNAME entry in your DNS to Trinity Cyber, placing full content inspection in the path between your applications and the internet.

The CNAME record provided to you is geo-distributed and a highly available pointer to the Trinity Cyber technologies, and is enabled as a reverse proxy for your web applications. By limiting inbound access to Trinity Cyber's IP Prefixes, the only path between your web applications and the internet will be protected.

As soon as you are connected, your internet content is actively inspected to protect you against the ever-evolving threat landscape, including inspection and mitigation of threats in file uploads. At the same time, your customers are protected against any threats that were already lurking on your site.

Traditional web application firewall (WAF) services tied to Content Delivery Networks (CDNs) are convenient, but these technologies use the same inadequate security components and antiquated processes that have been around for decades. They are easily evaded and cannot rapidly protect you from the ever-increasing published Common Vulnerabilities and Exposures (CVEs) flooding your security team. Trinity Cyber partners with GreyNoise, who tracks all actively exploited CVEs around the globe. While there are many vulnerabilities in CISA's Known Exploited Vulnerabilities (KEV) list, none are more important than the ones GreyNoise says are actively being exploited this minute. **Trinity Cyber stops them all.** No alert aggregation. No follow up. No blinking lights. No triage.

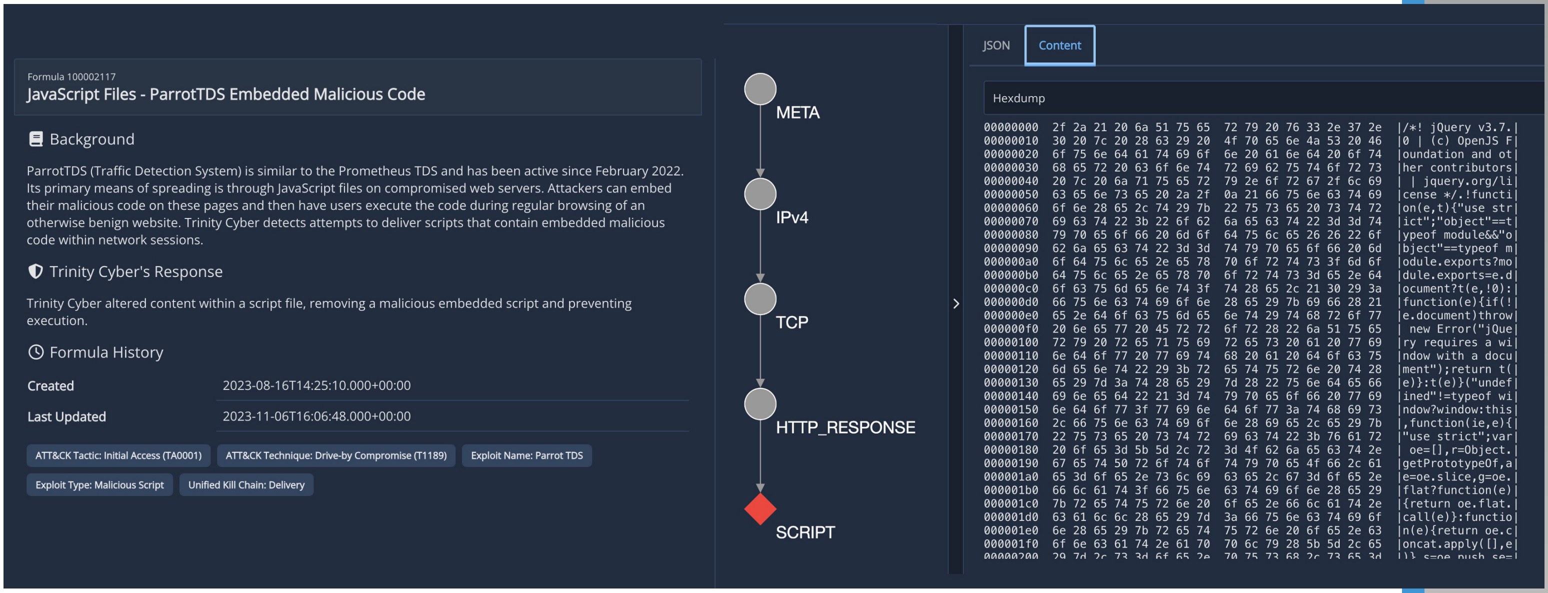


GREYNOISE

Top Ten Actively Exploited Vulnerabilities

CVE	Vendor / Platform / Name	Exploit Type	Trinity Cyber Mitigates
CVE-2018-2628 Full Trend Report >>	Oracle WebLogic	Remote Code Execution	✓
CVE-2019-2725 Full Trend Report >>	Oracle WebLogic	Remote Code Execution	✓
CVE-2021-44228 Full Trend Report >>	Apache Log4J (Log4Shell)	Remote Code Execution	✓
CVE-2022-1388 Full Trend Report >>	F5 BIG-IP	Authentication Bypass	✓
CVE-2022-22965 Full Trend Report >>	Spring Java (Spring4Shell)	Remote Code Execution	✓
CVE-2022-26134 Full Trend Report >>	Atlassian Confluence	Command Injection	✓
CVE-2022-27925 Full Trend Report >>	Zimbra Collaboration Suite	Remote Code Execution	✓
CVE-2022-30525 Full Trend Report >>	Zytel Firmware	Remote Code Execution	✓
CVE-2022-41040 Full Trend Report >>	Microsoft Exchange (ProxyNotShell)	Server Side Request Forgery	✓
CVE-2022-41082 Full Trend Report >>	Microsoft Exchange (ProxyNotShell)	Remote Code Execution	✓

Trinity Cyber gives you peace of mind and active risk reduction by removing CVE conditions right out of the internet session.



Formula 100002117

JavaScript Files - ParrotTDS Embedded Malicious Code

Background

ParrotTDS (Traffic Detection System) is similar to the Prometheus TDS and has been active since February 2022. Its primary means of spreading is through JavaScript files on compromised web servers. Attackers can embed their malicious code on these pages and then have users execute the code during regular browsing of an otherwise benign website. Trinity Cyber detects attempts to deliver scripts that contain embedded malicious code within network sessions.

Trinity Cyber's Response

Trinity Cyber altered content within a script file, removing a malicious embedded script and preventing execution.

Formula History

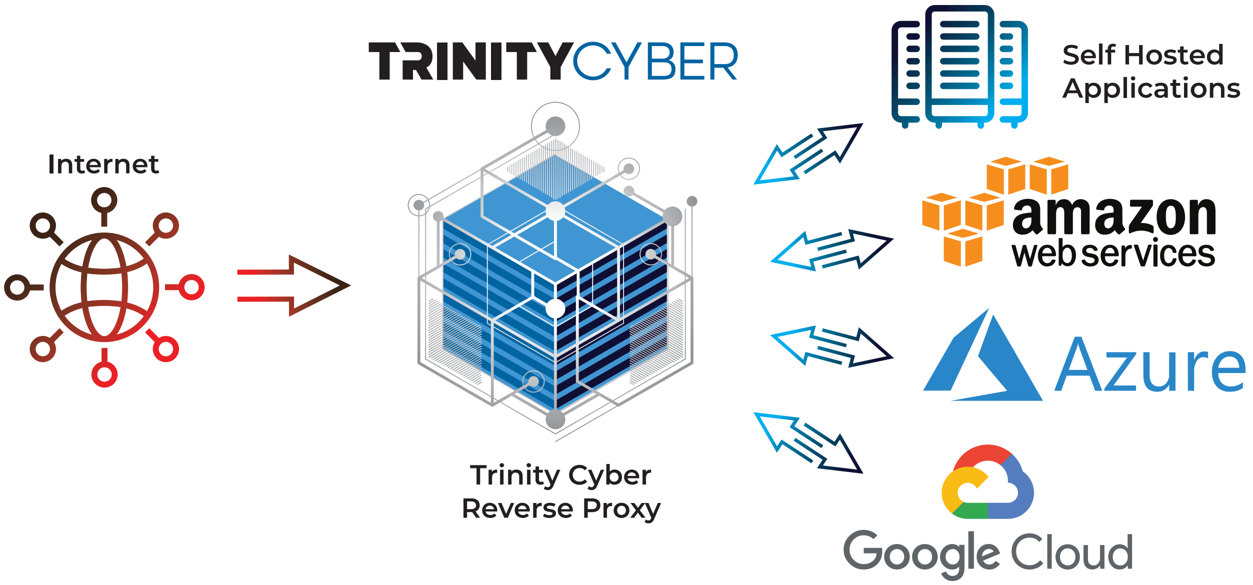
Created	2023-08-16T14:25:10.000+00:00
Last Updated	2023-11-06T16:06:48.000+00:00

ATT&CK Tactic: Initial Access (TA0001)
ATT&CK Technique: Drive-by Compromise (T1189)
Exploit Name: Parrot TDS
Exploit Type: Malicious Script
Unified Kill Chain: Delivery

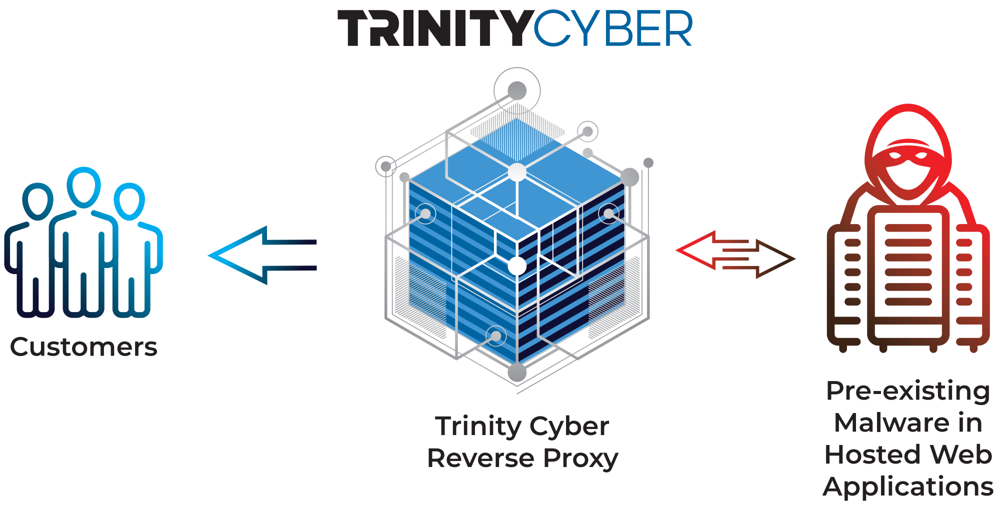
```
00000000  2f 2a 21 20 6a 51 75 65  72 79 20 76 33 2e 37 2e  |/*! jQuery v3.7.|
00000010  30 20 7c 20 28 63 29 20  4f 70 65 6e 4a 53 20 46  |0 | (c) OpenJS F|
00000020  6f 75 6e 64 61 74 69 6f  6e 20 61 6e 64 20 6f 74  |oundation and ot|
00000030  68 65 72 20 63 6f 6e 74  72 69 62 75 74 6f 72 73  |her contributors|
00000040  20 7c 20 6a 71 75 65 72  79 2e 6f 72 67 2f 6c 69  | | jquery.org/li|
00000050  63 65 6e 73 65 20 2a 2f  0a 21 66 75 6e 63 74 69  |cense */.!functi|
00000060  6f 6e 28 65 2c 74 29 7b  22 75 73 65 20 73 74 72  |on(e,t){"use str|
00000070  69 63 74 22 3b 22 6f 62  6a 65 63 74 22 3d 3d 74  |ict";"object"==t|
00000080  79 70 65 6f 66 20 6d 6f  64 75 6c 65 26 26 22 6f  |ypeof module&&"o|
00000090  62 6a 65 63 74 22 3d 3d  74 79 70 65 6f 66 20 6d  |bject"==typeof m|
000000a0  6f 64 75 6c 65 2e 65 78  70 6f 72 74 73 3f 6d 6f  |odule.exports?mo|
000000b0  64 75 6c 65 2e 65 78 70  6f 72 74 73 3d 65 2e 64  |dule.exports=e.d|
000000c0  6f 63 75 6d 65 6e 74 3f  74 28 65 2c 21 30 29 3a  |ocument?t(e,!0):|
000000d0  66 75 6e 63 74 69 6f 6e  28 65 29 7b 69 66 28 21  |function(e){if(!|
000000e0  65 2e 64 6f 63 75 6d 65  6e 74 29 74 68 72 6f 77  |e.document)throw|
000000f0  20 6e 65 77 20 45 72 72  6f 72 28 22 6a 51 75 65  | new Error("jQue|
00000100  72 79 20 72 65 71 75 69  72 65 73 20 61 20 77 69  |ry requires a wi|
00000110  6e 64 6f 77 20 77 69 74  68 20 61 20 64 6f 63 75  |ndow with a docu|
00000120  6d 65 6e 74 22 29 3b 72  65 74 75 72 6e 20 74 28  |ment");return t(|
00000130  65 29 7d 3a 74 28 65 29  7d 28 22 75 6e 64 65 66  |e)}:t(e)}("undef|
00000140  69 6e 65 64 22 21 3d 74  79 70 65 6f 66 20 77 69  |ined"!=typeof wi|
00000150  6e 64 6f 77 3f 77 69 6e  64 6f 77 3a 74 68 69 73  |ndow?window:this|
00000160  2c 66 75 6e 63 74 69 6f  6e 28 69 65 2c 65 29 7b  |,function(ie,e){|
00000170  22 75 73 65 20 73 74 72  69 63 74 22 3b 76 61 72  |"use strict";var|
00000180  20 6f 65 3d 5b 5d 2c 72  3d 4f 62 6a 65 63 74 2e  | oe=[],r=Object.|
00000190  67 65 74 50 72 6f 74 6f  74 79 70 65 4f 66 2c 61  |getPrototypeOf,a|
000001a0  65 3d 6f 65 2e 73 6c 69  63 65 2c 67 3d 6f 65 2e  |e=oe.slice,g=oe.|
000001b0  66 6c 61 74 3f 66 75 6e  63 74 69 6f 6e 28 65 29  |flat?function(e)|
000001c0  7b 72 65 74 75 72 6e 20  6f 65 2e 66 6c 61 74 2e  |{return oe.flat.|
000001d0  63 61 6c 6c 28 65 29 7d  3a 66 75 6e 63 74 69 6f  |call(e)}:functio|
000001e0  6e 28 65 29 7b 72 65 74  75 72 6e 20 6f 65 2e 63  |n(e){return oe.c|
000001f0  6f 6e 63 61 74 2e 61 70  70 6c 79 28 5b 5d 2c 65  |oncat.apply([],e|
00000200  29 7d 2c 73 3d 6f 65 2e  70 75 73 68 2c 73 65 3d  |)},s=oe.push,se=|
```

Without Trinity Cyber, you wouldn't know if one of your applications was compromised to steal data from your customers until it was too late. If you're already a victim of Magecart or ParrotTDS, for example, these threats are explicitly designed to evade traditional WAF technologies. The depth of the JavaScript obfuscation makes these exploits otherwise undetectable. Your customers find out much later that their credit card information has been stolen and it's a bad day for both of you. Since Trinity Cyber's capability operates in both directions, the technology can "see" and render obfuscated JavaScript, easily identifying it as malicious. Your customers experience a safe and clean web experience, completely unaware of the danger that was lurking and the malicious content your site would have delivered.

When malicious content in web sessions is removed, the Customer Portal notification tells you everything you need to know to clean up your server. This entire process happens so fast, your customers won't even notice. Through this method, Trinity Cyber is always exposing hidden threats, ensuring that attackers cannot exploit new vulnerabilities in your applications while simultaneously protecting your customers from threats that would otherwise be undetectable.



Let Trinity Cyber set up a reverse proxy for all your hosted web application domains. This connection option places Trinity Cyber's capabilities and services in front of all requests destined for your hosted applications. Since the full content inspection technologies operate in both directions, Trinity Cyber simultaneously protects your infrastructure, your applications, and your customers. Enablement is based on DNS records, making turn-up fast and easy. You get real-time protection for your websites and web applications hosted using public cloud providers such as Amazon Web Services (AWS), Google Cloud Platform (GCP), Azure or in private cloud environments, and is compatible with any other services in use, including global load-balancers, CDNs, and more.

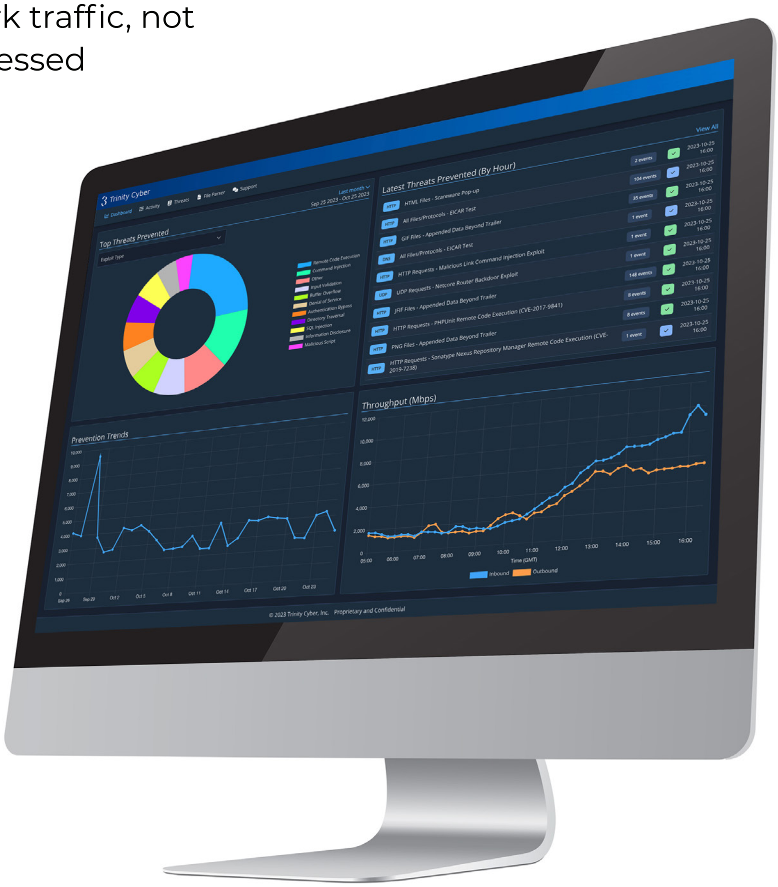


The Trinity Cyber Core Technology

Trinity Cyber's award-winning capability delivers unparalleled deep, content-based, full session inspection and real-time active cyber threat mitigation – all operated for you by an expert team. In an ecosystem overoptimized to support alert aggregation and incident response, Trinity Cyber's patented technology empowers a wide spectrum of *real-time* corrective actions – each meticulously crafted to match a CVE, threat actor group, ransomware gang, and entire families of threats. No alerts to aggregate. Near zero false positives.

The technology is backed by a suite of additional cybersecurity services like content-based threat hunting and emerging threat analysis. Trinity Cyber operates on your behalf, defends you against the latest threats, manages all the systems, and provides you with a context-rich, interactive information portal where you can see and drill into every threat stopped by Trinity Cyber. Each event is fully triaged so that your security team can rest assured that not only are you protected, but also every notification in the portal is legitimate with more than 99.99% accuracy.

The portal is home to additional analytics tools: Packet capture (PCAP) and File Parser. Trinity Cyber offers comprehensive PCAP results, capturing all network traffic, not just the events detected and processed by the Trinity Cyber platform. Trinity Cyber's integrated PCAP solution enables your security team to use standard Berkeley packet filtering (BPF) syntax on a rolling 72-hour basis, making it a breeze to search and retrieve SSL-decrypted packet captures to support thorough analysis and investigations. This means you get a complete picture, analyzing even the most subtle threats and anomalies.



Latest Threats Prevented (By Hour)

View All

HTTP	HTML Files - Scareware Pop-up	2 events	✓	2023-10-25 16:00
HTTP	All Files/Protocols - EICAR Test	104 events	✓	2023-10-25 16:00
HTTP	GIF Files - Appended Data Beyond Trailer	35 events	✓	2023-10-25 16:00
DNS	All Files/Protocols - EICAR Test	1 event	✓	2023-10-25 16:00
HTTP	HTTP Requests - Malicious Link Command Injection Exploit	1 event	✓	2023-10-25 16:00
UDP	UDP Requests - Netcore Router Backdoor Exploit	1 event	✓	2023-10-25 16:00
HTTP	JFIF Files - Appended Data Beyond Trailer	148 events	✓	2023-10-25 16:00
HTTP	HTTP Requests - PHPUnit Remote Code Execution (CVE-2017-9841)	8 events	✓	2023-10-25 16:00
HTTP	PNG Files - Appended Data Beyond Trailer	8 events	✓	2023-10-25 16:00
HTTP	HTTP Requests - Sonatype Nexus Repository Manager Remote Code Execution (CVE-2019-7238)	1 event	✓	2023-10-25 16:00

Additionally, Trinity Cyber's File Parser tool puts the power of advanced file analytics at your fingertips. This feature in the customer portal enables security analysts to drag and drop a file and see an immediate breakout of all the file components. Customers use it to aid in analysis, threat intelligence, and incident response. File Parser is an indispensable file submission tool designed to unearth and depict file exploits, malware, and obfuscation techniques concealed within file content.

About Trinity Cyber

Trinity Cyber runs a high-availability cybersecurity countermeasure capability as a service and triages all events as a service. You get clean traffic and less noise. It radically reduces risk and false positives. Trinity Cyber doesn't offer a secure web gateway (SWG), web application firewall (WAF), or intrusion prevention system (IPS), but rather outperforms and replaces every SWG, WAF, and IPS on the market.

Trinity Cyber sells in subscription tiers to accommodate all budgets and risk appetites. The annoying price models have died along with the old technologies that Trinity Cyber replaces. Unlimited seats for your SWG. Unlimited domains for your WAF. Internet gateway security that matches your usage. Put Trinity Cyber in your path to the internet. Pick as many connection options as you need. Only pay for what you use. Pick your tier and pay the price you see plus an additional consumption fee if applicable.

Contact us today at **Info@TrinityCyber.com** to learn more.