Trinity Cyber Service & Technology

Gartner COOL VENDOR 2020™

Advanced Network Threat Prevention

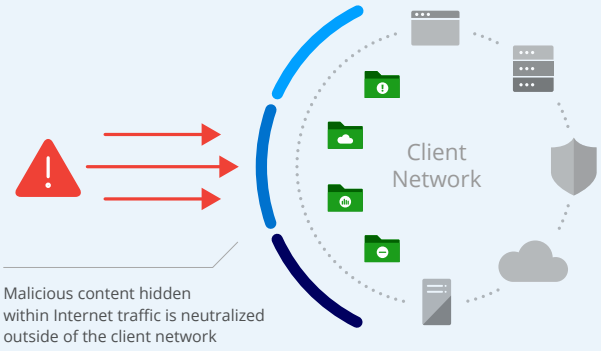
Trinity Cyber delivers an active threat prevention layer outside of your existing security without any disruption to your business. Our 24x7x365 Security Operations Center (SOC) operates a trusted man-in-the-middle proxy technology that acts on and thwarts advanced techniques and threats that other companies and products miss. We accomplish this by focusing on the methodologies behind the threats, instead of waiting for a sign that an attack has already happened. These signs, known as indicators of compromise (IOCs), change as quickly as they are discovered. Our approach is different and better. In fact, **Gartner recently named Trinity Cyber as a Cool Vendor for Network and Endpoint Security**.[1]

Trinity Cyber's managed threat prevention technology invisibly disrupts cyber attacks without disrupting your business operations. Our service is powered by a suite of high end processors installed in our private cloud. This extreme processing capability drives our patented technology to operate with imperceptible latency and near zero false positives. Our cutting-edge combination of detection logic and threat-mitigating actions that we call Formulas, examine Internet-session traffic and detect malicious exploits, polymorphic payloads, and protocol abuses based on their underlying structure. Our Formulas represent a dynamic, multi-dimensional, application level analysis of an entire network session, enabling us to target threats based on attributes that even the attackers don't consider. With Formulas and our unparalleled detection capability, prevention actions are immediately taken in-line, keeping attackers one step behind.

Outside Your Network

Trinity Cyber operates outside your perimeter, in the fabric of the Internet, as opposed to sitting inside your network. From this defense-in-the-middle position, Trinity Cyber is able to evaluate your Internet traffic before it becomes your network traffic. This unique vantage point gives Trinity Cyber an unparalleled view of the cyber-threat landscape and will also protect your edge-based defensive perimeter.

Stopping the Attack No Matter the Protocol or System



Threat Prevention as a Service

The reality is that any device on your network that can reach the Internet is a potential target. Trinity Cyber's advanced threat prevention technology is agnostic to the type and number of devices on your network. Our proprietary session-aware scan engine allows us to parse protocols and applications in real time to identify and neutralize malicious methodologies. This threat-centric, active approach, coupled with our location sitting between you and the Internet, gives you trusted defense regardless of the devices, protocols, systems, or architecture of your network.

Active
Trinity Cyber actively thwarts the adversary's tactics and protocols while ensuring business continuity—adding significant threat prevention to any customer.

Trusted
Our 24x7x365 Security Operations Center (SOC) operates a trusted man-in-the-middle proxy that acts on advanced adversary techniques.

Precise
With a .03% false detection rate, we accurately defeat would-be attackers before they can touch your infrastructure.

[1]Gartner, Cool Vendors in Network and Endpoint Security, Mark Harris, Rob Smith, et al., 30 September 2020.

Trinity Cyber

Features and Benefits

Subscription-Based Predictable Pricing

Trinity Cyber offers a cutting-edge technology service on a subscription basis. Our pricing model is based on the size of your Internet circuit, not the size of your network. As a result, price will never vary based on how many devices or users you add. This provides predictability and linearity to any company, especially those growing and transforming during mergers or acquisitions.

Easy to Manage

Trinity Cyber complements your existing security operations and works regardless of the complexity of your network, the age of your systems, or the types and number of devices. Our advanced threat prevention seamlessly enables an extra layer of security for firewalls, routers, Internet of Things (IoT) devices, and control systems—anything that touches the Internet. No hardware or software installation is required, giving you unencumbered, hassle-free security.

Active Prevention Without Generating Tickets

Trinity Cyber not only offers superior detection, but immediate and active mitigation. By exposing the entire session to Trinity Cyber's application layer, man-in-the-middle parsing and processing, we can react in real time, with extreme precision, rather than feeding an orchestration engine or event manager to take a post-detection action.

Invisible to Business Operations

Our operations ensure business continuity while delivering unmatched security. Users who would be victimized by a watering hole attack (or get duped into opening a malicious document) can do so safely with the attackers' code neutralized or removed by Trinity Cyber before it reaches them. Traffic isn't unnecessarily blocked. Emails aren't randomly quarantined. Threats are absolutely removed.

Ensuring Security Amid Transformation

Companies growing through mergers and acquisitions can leave themselves vulnerable as they attempt to combine and secure different networks. Protecting an acquisition before corporate integration enables true and consistent security across multiple enterprises. Sometimes you simply cannot patch or upgrade a legacy system without disrupting business operations. Attackers know this and look for weak spots in such systems. Trinity Cyber ensures you never expose your weaknesses—both the ones you know about and the ones you don't.

Security for Your Unique Needs: Industrial Control Systems • IoT Custom Protocols • Custom File Types

Every modern enterprise faces their own unique security challenges. They must deal with an ever-increasing variety of new and novel devices connecting to the Internet. They may have designed their own types of files or communication protocols or perhaps an IT enterprise controls infrastructure. Whether a threat targets an IoT device, a control system, a custom communication protocol, or a unique file type, we provide constant vigilance by examining Internet protocols and the objects (files) within them.

sales@trinitycyber.com • (240) 842-9900 • trinitycyber.com

Trinity Cyber

Trinity Cyber's Value Proposition

Trinity Cyber is your first line of defense for mitigating threats outside your network. Thanks to our patented technology and precise operations, we reduce the volume of alerts and false positives generated by your legacy products—eliminating many threats before they reach your perimeter. That frees up your most valuable assets, your highly trained and overextended security professionals, to focus on higher-value tasks such as proactive threat-hunting within your network.

Trinity Cyber's advanced threat prevention technology delivers unmatched accuracy with less than 1-ms average latency, ensuring normal, unencumbered operation for your business. Our operators neutralize a vast range of known and emerging threats. Our analysts are immersed in studying the latest vulnerabilities, malware campaigns, and exploits, enabling them to identify new and developing dangers that target our clients and community. Our service boasts a false-detection rate near zero, which is falling every day thanks to our cutting-edge approach.

Trinity Cyber gives you the resources of a nation state-level Security Operations Center (SOC) that integrates with your existing team to augment your capabilities with our proactive, defense-in-the-middle threat mitigation. Each and every time we actively remove a threat from Internet traffic, a summary is generated and immediately available for review on our client-specific, API-driven portal. Your staff have instant visibility into Trinity Cyber operations, and our SOC is always available and ready to support you, 24x7x365.

Capabilities	Trinity Cyber	Managed Security Service Provider	Event Correlation and Orchestration	Traditional Security Products
OPERATIONAL				
Installation Required		X	X	X
Focused Inside Network		X	X	X
Operates Outside Enterprise	X			
Client Managed			X	X
THREAT PREVENTION				
IOC-Based Threat Prevention		X	X	X
Non–IOC-Based Threat Prevention	X			
Correlation Detection	X	X	X	X
Adversary Interference	X			
Deception Technology	X			
Invisible to the Adversary	X			
SERVICE				
24x7 Security Operations Center	X	X		
24x7 Threat Hunting	X			
24x7 On-Call Support	X	X		
Intuitive and Informative Client Portal	X	X		
Proactive Operations	X			
Adaptive Countermeasures	X			
Forensic Capabilities	X	X		X
Client-Focused Intelligence	X			
Reduced Alert Fatigue	X	X		

sales@trinitycyber.com • (240) 842-9900 • trinitycyber.com

Trinity Cyber