# The Future of Cybersecurity

- Better security results with automated controls
- Fewer false positives
- Reduced alert fatigue

Gartner

COOL
VENDOR
2020™

# Abstract:

Existing network security technology cannot achieve the depth, context or accuracy at the speed needed to prevent threats at the edge. The traditional Intrusion Prevention Systems (IPS), Next Generation Firewalls (NGFW) and Secure Web Gateways (SWG) use static indicators of compromise (IOC) that are regularly evaded, generate alerts based on inferences and produce high false positive rates. All of these require time-consuming and costly manual response by customers, not to mention constant tuning.

Trinity Cyber took a new approach and invented technology that can deeply inspect full session Internet traffic and modify it inline to remove exploits and malware or prevent them from functioning. It is the first technology that can parse, scan and rebuild full session Internet traffic in both directions to expose and mitigate actual threat content and do so with an average processing latency of *less than a millisecond*. It offers a profound new capability to the information security community. The Trinity Cyber technology's precise session inspection and editing capabilities deliver better detection and defeat attacker tactics, techniques and procedures (TTPs), which is vital to finding, beating and actually preventing modern cyber threats.

Trinity Cyber has two service lines. The **TC:Edge** service is a private cloud offering that is operated and maintained by Trinity Cyber's experts for the customer. This saves them time and money and produces better detection with automated prevention, cleaner traffic and an array of useful metadata, traffic analysis and advanced network hunting capabilities. **TC:File** services provide extremely accurate and fast file-based threat discovery. They are offered as an OEM into partner platforms as well as an API service for threat analysts.

Both service lines uniquely address today's complex security challenges and rapidly deliver superior, tangible results in ways others cannot. Trinity Cyber's team is world-class, its service lines are expanding and the tech is turning heads. Most importantly, Trinity Cyber's preventive controls address the three biggest problems in the cyber industry, delivering:

- Better security
- Fewer false positives
- Reduced alert fatigue

# Strained and Stressed Security Response

Security teams are drowning in a sea of alert fatigue, incident response workload, false positives, and a host of associated problems that are worsening steadily. They are stretched continuously, working in a highly reactive, "always on" mode. They are frustrated their security stacks fail to accurately identify and stop cyber threats but still produce an enormous number of alerts. Many alerts are ultimately determined to be false positives, but actions are still required. These critical groups are being stretched to a breaking point, as a recent Simon Hayhurst report[1] found:

- More than 90% of cybersecurity professionals are stressed in their role
- 40% feel their existing security solution stack is inadequate
- Nearly half (46%) of the respondents have thought about quitting the industry

Many organizations already feel they do not have the SOC team staff to do the job properly.[2] Hiring and retaining these highly skilled, valued and difficult-to-replace professionals remains a major challenge. According to ISACA's "State of Cybersecurity 2022" report, 60% of respondents are having difficulty retaining qualified cybersecurity professionals, a 7% increase from 2021.[3]

## The Security Service Edge Isn't Always Secure

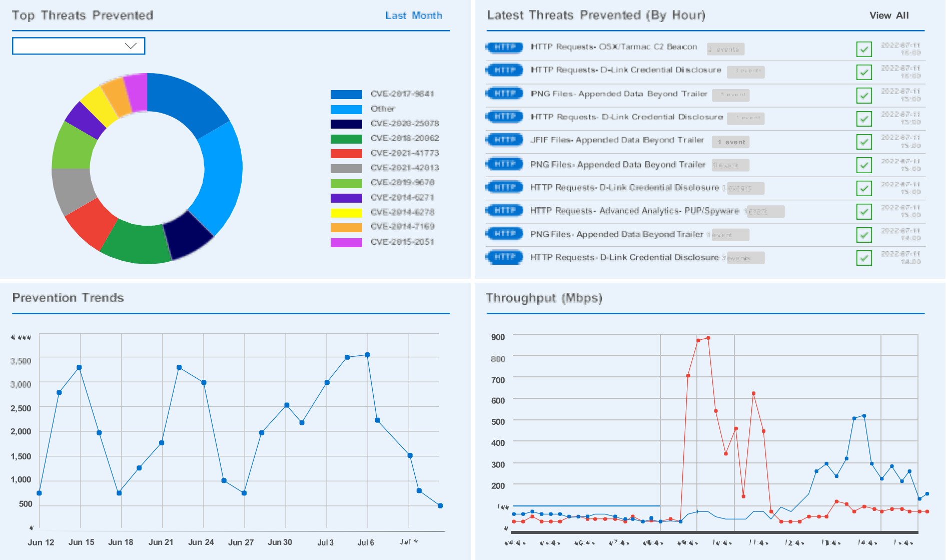
Most Security Service Edge (SSE) offerings rely upon traditional IPS and SWG products to deter cyber attacks. These technologies fail to provide adequate protection because they cannot examine network traffic, protocols and embedded files with the depth and speed required to prevent threats before they enter or leave the customer's network. While some threats are blocked based upon domains, IP addresses and hash values, most threats still penetrate defenses. To make matters worse, these technologies produce a nearly *one in two false positive rate*[4] for daily security alerts.

## Trinity Cyber Takes a Different Approach and Invented a New Technology

Trinity Cyber has the solution to these thorny customer challenges with two managed service lines, both built upon the groundbreaking Trinity Cyber Engine:

**TC:EDGE**
AUTOMATED THREAT PREVENTION

**TC:Edge** services replace or augment significantly the antiquated and ineffective security components of SSE and provide superior, automated threat detection and prevention against advanced attacks. Shortly after deploying the **TC:Edge** service, customers experience reduced incident response workloads by over 30%



Latest Threats Prevented (By Hour) View All

| | | | | |
|---|---|---|---|---|
| HTTP | HTTP Requests- OSX/Tarmac C2 Beacon | 3 events | ✓ | 2022-07-11<br>16:00 |
| HTTP | HTTP Requests- D-Link Credential Disclosure | 3 events | ✓ | 2022-07-11<br>16:00 |
| HTTP | PNG Files- Appended Data Beyond Trailer | 1 event | ✓ | 2022-07-11<br>15:00 |
| HTTP | HTTP Requests- D-Link Credential Disclosure | 1 event | ✓ | 2022-07-11<br>15:00 |
| HTTP | JFIF Files- Appended Data Beyond Trailer | 1 event | ✓ | 2022-07-11<br>15:00 |
| HTTP | PNG Files- Appended Data Beyond Trailer | 1 event | ✓ | 2022-07-11<br>15:00 |
| HTTP | HTTP Requests- D-Link Credential Disclosure | 3 events | ✓ | 2022-07-11<br>15:00 |
| HTTP | HTTP Requests- Advanced Analytics- PUP/Spyware | 1 event | ✓ | 2022-07-11<br>15:00 |
| HTTP | PNG Files- Appended Data Beyond Trailer | 1 event | ✓ | 2022-07-11<br>14:00 |
| HTTP | HTTP Requests- D-Link Credential Disclosure | 3 events | ✓ | 2022-07-11<br>14:00 |

Example Dashboard from Trinity Cyber Customer Portal

By deploying the Trinity Cyber technology inline at the Internet-facing network edge, **TC:Edge**'s deep, contextual, full session inspection and automated preventive controls reveal and modify malicious traffic to remove exploits and malware (or prevent them from functioning), interfere with command and control (C2) and deny inappropriate exfiltration of outbound data. Instead of alerts that must be actioned, customers receive cleaner traffic and event notifications that a threat was detected and mitigated, along with a wealth of valuable metadata useful to threat analysts. Trinity Cyber event notifications and metadata are delivered to customers via a web-based portal and can be easily ingested into a customer's Security Information and Event Management (SIEM) tool through direct integration of an API. Each notification includes information on the threat, the technique used by the adversary, the preventive action executed by the Trinity Cyber Engine on the customer's behalf, and a rich, extensible compilation of session metadata and threat intelligence.

## TC:FILE

FILE PARSING, INSPECTION AND VERDICT ASSESSMENT *IN FRACTIONS OF A SECOND*

**TC:File** services are for customers requiring protection from file-based threats. They are a faster and more precise choice for identifying file-based threats compared to traditional alternatives such as sandboxing, content disarm and reconstruction (CDR) and forensic tools. Powered by the Trinity Cyber Engine, **TC:File** services conquer obfuscation techniques as well as parse and interrogate files contextually to reveal malicious content. This exposes the actual exploitive conditions hidden by the attacker.

### TC:File Verdict

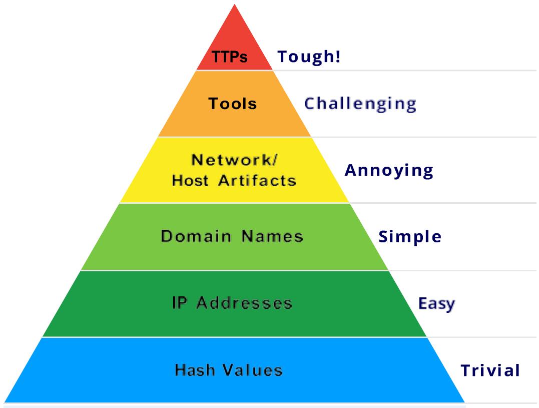
Through a web server interface, customer platforms can OEM the power of the Trinity Cyber file inspection engine into their tools and platforms to deliver to their customers accurate verdicts on file maliciousness plus highly valuable metadata for every parsed object and sub object.

**TC:File Forensics**

Via a web-based API, customers submit their suspect files to the Trinity Cyber Engine. In less than a second, the **TC:File Forensics** service returns accurate verdicts on file maliciousness, highly valuable metadata for every parsed object and sub object, a parsed view of the file for forensics, and rich threat intelligence.

# The Trinity Cyber Engine Stops Attacker Methods

The foundation for both **TC:File** and **TC:Edge** services is the Trinity Cyber Engine and its unique, automated abilities to expose and neutralize attacker methods. Identifying and stopping the techniques used by attackers is crucial to defeating and preventing cyber attacks. Attackers spend years developing the tools and TTPs they use. Until now, security teams could only detect tools and TTPs after an incident. Detecting these artifacts inline and at speed is difficult, but Trinity Cyber has invented the ability to do so reliably and at scale. Customers receive and benefit from superior, enduring security because adversaries will often change their payloads and infrastructure, but they will rarely change their TTP.



David Bianco's pyramid illustrates the relationship between types of indicators used to detect an adversary's activities and how much pain it will cause them when those indicators are denied

Many cybersecurity technologies can only operate at the lower sections of David Bianco's Pyramid of Pain.[5] These characteristics are easy to detect and even easier for adversaries to modify. Attackers employ an ever-changing landscape of hash values, IP addresses, domains, and superficial network and file artifacts. They change these values faster than existing technologies can update, illustrating yet another reason why the security provided by products based upon these technologies is lacking.

The Trinity Cyber Engine operates at the top of the pyramid, leveraging its advanced capabilities beyond block and alert to remove, replace or modify any content necessary to precisely neutralize attacker TTPs and prevent threats. As a result, *entire categories and families of individual threats and many Common Vulnerabilities and Exposures (CVEs), regardless of their placement in content, are defeated and prevented from fully executing at their root*. Also, because many individual attacks share similar techniques for delivery, both known and unknown payloads are neutralized and prevented.

# Example Threats Prevented by Stopping TTPs

| Name | Description |
|---|---|
| Follina<br>(CVE-2022-30190) | CVE-2022-30190 is a vulnerability in the Microsoft Support Diagnostic Tool, allowing attackers to remotely attack victims with a crafted malicious document or web page. Follina is typically exploited by spearphishing or drive-by-download attacks and is often an initial access method. The Trinity Cyber Engine removes Follina inline automatically. |
| Winnti Backdoor | An evasive backdoor that targets Linux environments, known to be used by the Winnti Group (APT41) to perform financially motivated attacks. This threat is capable of establishing and maintaining persistence on a targeted system. The Trinity Cyber Engine removes Winnti Backdoor threats inline automatically. |
| BoomMic (aka VaporRage) | A malicious downloader that can be part of a phishing campaign by the Russian APT 29. BoomMic is capable of file execution, terminating processes and downloading additional malware. The Trinity Cyber Engine removes BoomMic threats inline automatically. |
| BeatDrop | A malicious downloader observed to be part of a phishing campaign by the Russian APT 29. When successfully downloaded and executed, BeatDrop is capable of file execution, data encryption and downloading additional malware. The Trinity Cyber Engine removes BeatDrop inline automatically. |
| PHPUnit<br>RCE Exploit | A remote code execution (RCE) vulnerability, known as CVE-2017-9841, exists in the PHPUnit Programmer-Oriented platform. The vulnerability exists in the Util/ PHP/eval-stdin.php script, which, when successfully exploited, allows an attacker to run malicious code on a victim's system. The Trinity Cyber Engine removes the PHPUnit - RCE Exploit inline automatically. |
| MaxOfferDeals | MaxOfferDeals is adware that has been observed to be part of the Shlayer MacOS Trojan package. Shlayer is malware that masquerades as a legitimate web player plugin. By downloading the fake plugin, users infect their computer with malicious adware, such as MaxOfferDeals, that gathers information about their system and can retrieve other malware packages. These components periodically beacon and send encrypted commands and data to adversary-controlled infrastructure. The Trinity Cyber Engine removes MaxOfferDeals inline automatically. |
| Blackcat Ransomware | BlackCat is ransomware that is being sold in underground forums as Ransomware-as-a-Service (RaaS), supporting both Windows and Linux operating systems. BlackCat is known to target a wide variety of industries, including energy, transportation and utilities. When successfully delivered and executed, BlackCat will attempt to delete any volume shadow copies and enumerate any accessible drives for encryption. The Trinity Cyber Engine removes Blackcat ransomware inline automatically. |
| Confluence OGNL Injection<br>Vulnerability<br>CVE-2022-26134 | A vulnerability exists within Atlassian Confluence software which allows attackers to insert arbitrary commands via the OGNL syntax to achieve RCE on vulnerable Internet-facing servers. The Trinity Cyber Engine detects and removes attempts to exploit CVE-2022-26134 inline automatically. |
| AvosLocker Ransomware | Avos is a Ransomware as a Service (RaaS) affiliate-based group. Avos RaaS affiliates and attackers commonly focus on known vulnerabilities in other areas as an intrusion vector to deploy AvosLocker ransomware. Once their AvosLocker malware is delivered on a targeted system, AvosLocker encrypts files and then demands payment to restore them. The Trinity Cyber Engine detects and stops AvosLocker ransomware attacks before they can begin. |

# Eliminating False Positives and Mitigating TTPs

A recent ESG Research study of leaders across 500 organizations found that 45% of all daily security alerts are false positives and that 75% of their organizations spend an equal amount of time (or more) on false positives as on legitimate attacks.[6] The problem is so acute that, in a multi-continent survey of security experts, 74% claimed their volume of false positives was steady or rising while 26% shared they “turn off alerts because they are too noisy.”[7] In contrast, the Trinity Cyber Engine’s threat detection is far more accurate – 10,000 times more precise, with a False Positive Rate that is better than 0.03%.

To consistently deliver this level of precision inline, at line speed and scale, the Trinity Cyber Engine invisibly stages every Internet session, pairing request and response bodies for supreme fidelity in both directions. It then fully and contextually inspects all content before it enters or leaves a customer’s control. During this inspection phase, it automatically removes any obfuscation that often allows threats to proceed undetected by other security products.

The Trinity Cyber Engine parses the traffic’s protocol fields and files, revealing a contextually rich view of the session content, its protocols and payloads. This deep, contextual level of inspection exposes the attacker TTPs, specific tools, obfuscation, CVEs and other content critical to not just alerting but also neutralizing the attack.

Since attacker TTPs cannot be “blocked,” once identified, more precise and nuanced approaches are necessary beyond “block” and “alert” to neutralize what makes the TTP successful. Trinity Cyber has a created repertoire of actions that do what no other inline security technology can: modify, remove and replace content to neutralize attacker tools, TTPs and malware.

**Modify: alter exploits in flight**

- Alters content of remote code exploits to disable them inline
- Neutralizes tailored payloads from APT groups

**Remove: make it disappear**

- Drops malware/exploits/C2 out of network sessions
- Removes web-based exploit delivery mechanisms from response bodies
- Removes malicious content hidden deeply within files – or removes them

**Replace: swap corrupted or malicious for benign**

- Replaces files, sub objects within files and protocol content
- Replaces nearly anything with artifacts findable by defenders

These precisely applied actions, executed automatically and bidirectionally with an average processing latency of <1ms, undermine the malicious tools and TTPs used by adversaries. Attacks are consistently identified, thwarted and prevented, providing customers protection and security that others cannot.

## Trinity Cyber's Unequaled Expertise and Commitment

Trinity Cyber's award-winning threat analysis and operations teams skillfully manage, operate and maintain the Trinity Cyber Engine for the **TC:Edge** and **TC:File** service lines. They are the most talented cybersecurity professionals in the industry, with decades of experience designing, managing and operating the most sensitive and demanding networks in both public and private sector. They apply their expertise to protect customers, reduce false positives and slash the need for incident response.

Trinity Cyber's team continuously monitors and analyzes customer traffic for threat activity and for vulnerabilities that would be viewed as attractive targets by adversaries. The Trinity Cyber Engine empowers threat hunting and threat analysis teams to employ deep, contextual threat intelligence to identify and defeat the latest cyber threats. This level of threat hunting is far superior to log entry analysis, and the knowledge acquired is immediately applied to continuously improve the automated threat detection and prevention provided to customers.

## Conclusion

With an original, innovative approach, Trinity Cyber invented a transformational technology called the Trinity Cyber Engine. Trinity Cyber's fully managed service lines, **TC:Edge** and **TC:File**, are built upon the Trinity Cyber Engine and provide customers the protections they seek. With almost no false alarms and at line speed, the Trinity Cyber Engine is unrivaled in detecting, neutralizing and preventing threats automatically. Because it defeats attacker TTPs, it finds, mitigates and prevents modern cyber threats and drives significant incident response reductions. Customers are already benefiting from the automated prevention of threats that evade discovery by their other security products as well as reduced incident response workloads of more than 30%. Trinity Cyber is the future of cybersecurity, and we are ready to help you achieve your security goals.

### About Trinity Cyber

Trinity Cyber, Inc. is a US-based corporation that invents and operates technology to solve the most difficult cyber security challenges. The company's products and services range across several multi-billion dollar market segments. The company's founders, management team and technologists are all award-winning, recognized leaders in their field.

# Endnotes

1. “Voice of Secops” 3rd edition, 2022, Simon Hayhurst, Hayhurst Consultancy, 2022 (commissioned by Deep Instinct)
2. Ibid
3. “State of Cybersecurity 2022, Global Update on Workforce Efforts, Resources and Cyberoperations”, ISACA, 2022
4. “Tool Sprawl and False Positives Hold Security Teams Back”, Kelly Sheridan, Dark Reading, July 12, 2021
5. “The Pyramid of Pain”, David Bianco, Enterprise Detection and Response, January 17, 2014
6. “Tool Sprawl and False Positives Hold Security Teams Back”, Kelly Sheridan, Dark Reading, July 12, 2021
7. “Voice of Secops” 3rd edition, 2022, Simon Hayhurst, Hayhurst Consultancy, 2022 (commissioned
8. by Deep Instinct)

Trinity Cyber

Gartner
COOL
VENDOR
2020

Trinity Cyber was named a Cool Vendor in Gartner's Cool Vendors in Network and Endpoint Security, Mark Harris, Rob Smith, et al., Sept. 30, 2020.

The GARTNER COOL VENDOR badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

trinitycyber.com