Uplevel Your Defenses: Intrusion Prevention at Network Speed Meets Full Packet Capture

Break the Perpetual Cycle of Only Chasing Attacks and Take Back Command and Control

Whether you are already a SentryWire customer or in the consideration stage, Trinity Cyber adds an active layer of threat response and prevention outside of your network edge that enables defenders to gain the upper hand against advanced threats.

A Truly Unique and Powerful Capability

1. 2020 Gartner Cool Vendor for Network and Endpoint Security
2. Every Internet session is parsed and inspected in flight before it reaches or leaves network
3. Patent pending technology enables in flight response actions (we interfere with your adversaries)
4. Operated for you by the brightest minds in cybersecurity committed to stopping the bad guys

We Solve a Fundamental Challenge in Network Defense: Deep Security at Line Speed

Network speed and security have been in tension for the past decade. The tradeoff between the two has led to compromises in the effectiveness of security technology. As a result, network security technologies have been limited to cursory security inspection and automated rules that guess whether traffic is malicious based on indicators of compromise and then allow intrusion while enabling hurried incident response. Taking the time to perform a more careful and accurate inspection of network traffic in flight has not been technologically possible without introducing significant latency. But, Trinity Cyber has solved this with Advanced Intrusion Prevention as a Service.

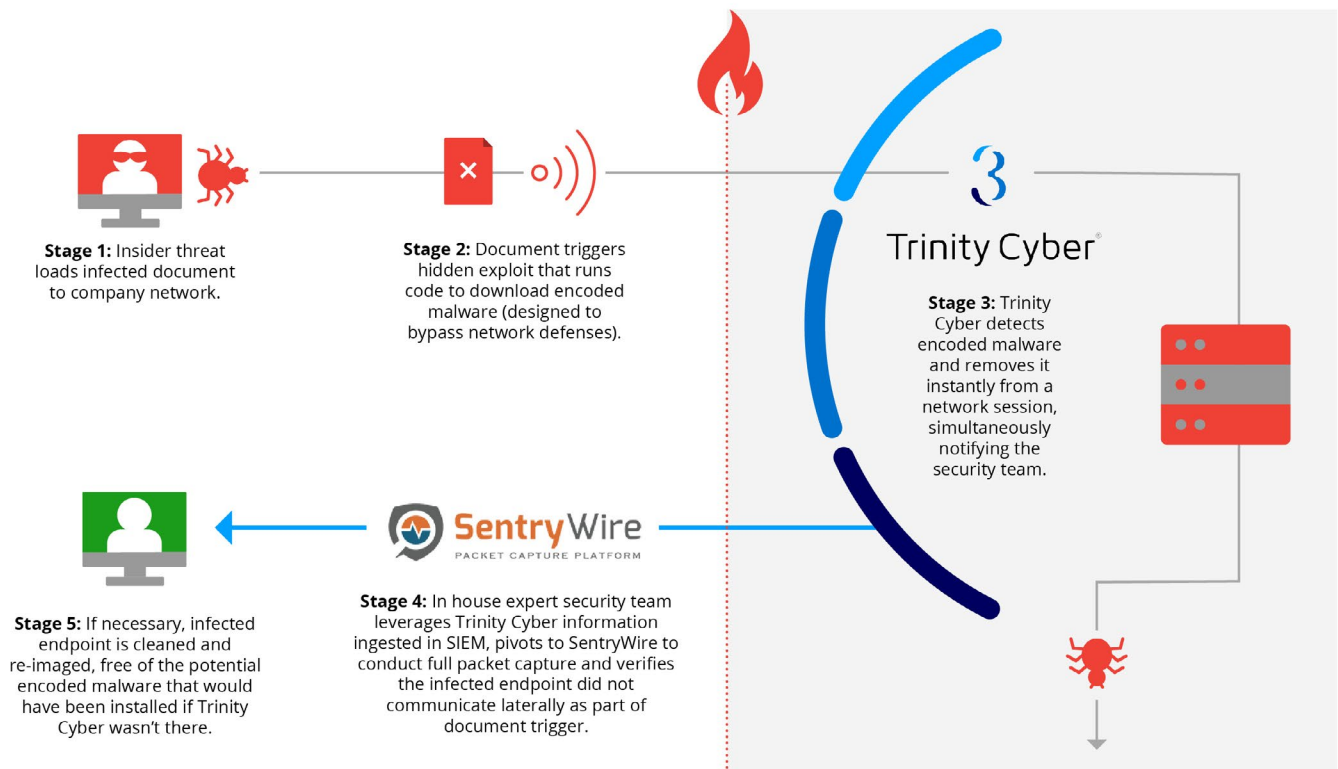## We Operationalize "Man-in-the-Middle" for the Good Guys

Trinity Cyber is a fully managed service that actively neutralizes threats before they breach or leave your network (bidirectional protection). We deliver our technology as a service using a **private cloud-based model** in multiple US datacenters, which allows for scalability, geographic flexibility, and **near-zero deployment effort** for our clients.

Trinity Cyber delivers truly preventive controls at line rate speed by deeply and accurately inspecting and modifying full session network traffic in flight **to remove, alter, or replace malicious content** without interrupting customer operations or notifying the attacker. Not all organizations are ready to interact with adversaries, which is why we calibrate our preventative controls to match your risk profile (ranging from simple to complex actions).

Trinity Cyber

Sentry Wire
PACKET CAPTURE PLATFORM

SentryWire Together with Trinity Cyber Delivers Holistic Network Security

Organizations who subscribe to our Intrusion Prevention as a Service access real-time notification on what is being actively prevented from happening on their networks. Rich metadata on every threat we prevent, and on-call experts for technical questions and collaboration. With this information, organizations deploying SentryWire Packet Capture for internal networks can better focus their investigations to expedite resolution with confidence. With Trinity Cyber acting outside the network edge, and SentryWire illuminating traffic inside of it, network defenders can finally take a breath.

Malware Delivery Scenario Featuring Trinity Cyber and SentryWire

Stage 1: Insider threat loads infected document to company network.

Stage 2: Document triggers hidden exploit that runs code to download encoded malware (designed to bypass network defenses).

Stage 3: Trinity Cyber detects encoded malware and removes it instantly from a network session, simultaneously notifying the security team.

Stage 4: In house expert security team leverages Trinity Cyber information ingested in SIEM, pivots to SentryWire to conduct full packet capture and verifies the infected endpoint did not communicate laterally as part of document trigger.

Stage 5: If necessary, infected endpoint is cleaned and re-imaged, free of the potential encoded malware that would have been installed if Trinity Cyber wasn't there.

Can Your Business Benefit From SentryWire/Trinity Cyber Partnership?

- Are your resources overextended trying to address increasing amount of threats?
- Is security a critical part of your business?
- Are you concerned about SolarWinds?
- Do you currently lack external-to-internal network visibility combined with active prevention controls?

Contact us today at:

SentryWire.com
Info@SentryWire.com
(410) 712-0270