TRINITYCYBER

USE CASE

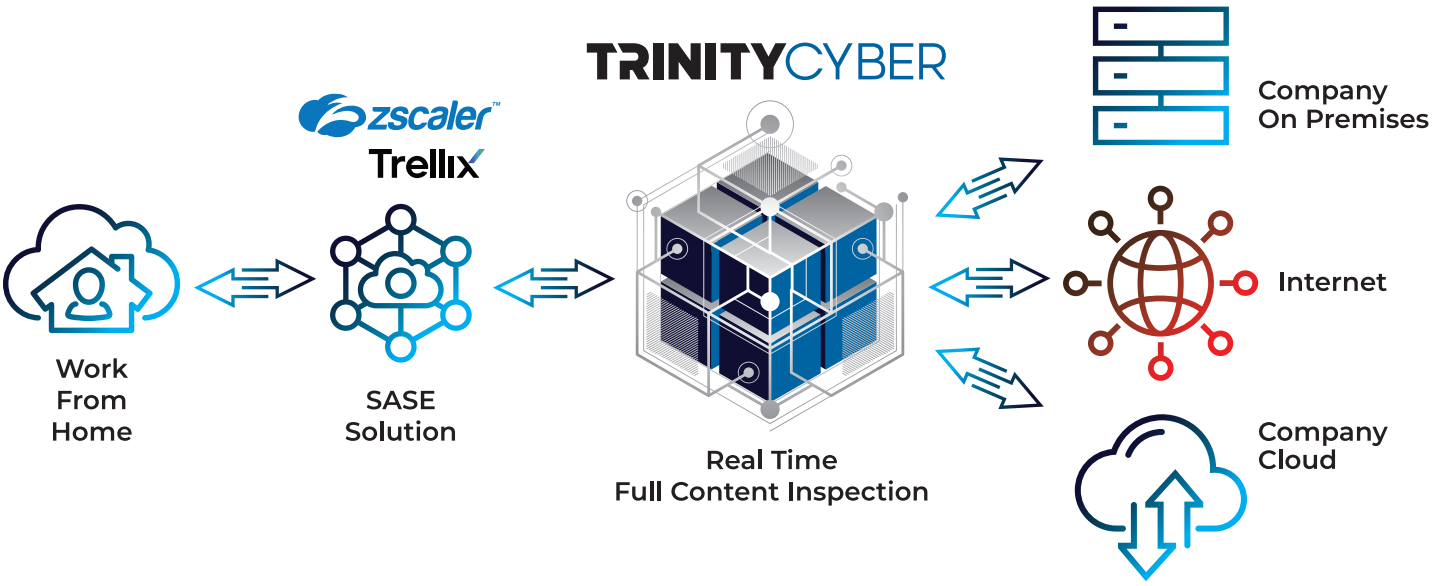
REMOTE USERS: SASE CONNECTIONS

Protect Your Company from the Threats Posed by Your Remote Workforce with Trinity Cyber's 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 enterprise from the threats inherent to a remote workforce.

All you have to do is instruct your existing Secure Access Service Edge (SASE) infrastructure to make Trinity Cyber the next hop to the internet - It's a simple service chain configuration. As soon as your endpoints are connected, your remote workforce's internet content is actively inspected to protect your enterprise against the ever-evolving threat landscape. You get added protection and the tremendous visibility that comes with Secure Sockets Layer (SSL)-decrypted Packet Capture (PCAP) at your fingertips.

Most SASE and Security Service Edge (SSE) offerings, while necessary to secure remote workers, use the same inadequate security components and antiquated processes that have been around for decades. Trinity Cyber is far superior. Other vendors sell Secure Web Gateways (SWGs) that block known bad URLs and hashes, but do not deeply inspect web traffic for malicious content the way Trinity Cyber does. For example, obfuscated JavaScript (like that used by ParrotTDS and Magecart) slips past SWGs, but not Trinity Cyber. The Trinity Cyber capability defeats these threat actors by finding and neutralizing their tactics. Trinity Cyber doesn't rely on ever-changing indicators of compromise (IOCs) that would just block a user from an otherwise legitimate experience. Rather, the technology parses, inspects, and strips malicious JavaScript and other nefarious content directly from the user's session.



The same is true for Intrusion Prevention Systems (IPSs) that SASE providers employ. These technologies are easily evaded, rely on IOCs and pattern matching, are limited to block and alert actions, and produce mountains of false positives – all requiring more work by the customer to triage and remediate. Even browser isolation technologies are defeated once a user downloads a file.

By adding Trinity Cyber into the service chain of your SASE infrastructure, you get a massive boost to your security and you significantly reduce the strain on your security workforce.

Trinity Cyber works with the most popular SASE vendors, including Zscaler and Trellix (formerly McAfee), to greatly improve your security posture and reduce workloads. With gateway locations in Washington, D.C., New York, Chicago, Dallas, and San Jose, your remote workers will enjoy responsive and secure internet from anywhere in the United States. Trinity Cyber's internet gateway – powered by full content inspection – will be the last stop for traffic going to the internet and the first stop for traffic coming from the internet.

The vast majority of your remote workforce's web traffic is encrypted with Transport Layer Security (TLS) between their browser and the websites they visit. Commonly referred to as SSL encryption, it is in these channels where most cyber adversaries lurk. Trinity Cyber's technology decrypts this traffic, performs full content inspection to neutralize the threats, and re-encrypts the traffic before releasing it to the internet. This entire process happens so fast, you won't even notice. Through this method, Trinity Cyber is always exposing hidden threats, while ensuring that attackers cannot exploit protected channels to infiltrate your network.

In cases where sensitive traffic cannot or should not be decrypted, Trinity Cyber manages a decryption exemption policy for you. With SSL Exemption Management, you may identify specific segments of traffic that should remain encrypted and inaccessible. This feature also is essential for preserving the functionality of certain mobile devices. Trinity Cyber brings a wealth of experience to this process and offers advice on the exemptions necessary to help you run and maintain your enterprise without disruptions.

Trinity Cyber's integrated, SSL-decrypted PCAP solution enables your security team to use standard Berkeley packet filtering (BPF) syntax on a rolling 72-hour basis, making it simple to search and retrieve SSL-decrypted packet captures to support thorough analysis and investigations. With Trinity Cyber managing your SSL decryption, you receive world-class protection while your digital forensics and incident response (DFIR) teams get access to SSL-decrypted PCAP through Trinity Cyber's customer portal.

If you're using Zscaler, Trellix, or other leading vendors, forwarding your remote workforce's web traffic to one of Trinity Cyber's internet gateways delivers deeper, more content-aware protection with a more enduring solution that significantly reduces risk well beyond hash matching, URL filtering, and simple pattern matching.

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 of seasoned professionals. 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, a threat actor group, a ransomware gang, and entire families of threats. No alerts to aggregate. No false positives. When the technology encounters a threat on your traffic (which it does more accurately and with a more enduring approach than any competitor on the market), it mitigates that threat on the wire, seamlessly and in real-time while delivering a context-rich notification. With average processing times of less than 1ms, neither you nor the opposition will even know the technology is there.

The technology is backed by a suite of additional cybersecurity services like content-based threat hunting and emerging threat analysis – all made better through our patented technology. 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 analytic tools: PCAP and File Parser. Trinity Cyber offers comprehensive PCAP results, capturing all network traffic, not just the events detected and processed by the platform. This means you get a complete picture, analyzing even the most subtle threats and anomalies. Trinity Cyber's File Parser tool puts the power of advanced file analytics at your fingertips. File Parser is a feature in the customer portal where security analysts can drag and drop a file and see an immediate breakout of all the file components. 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. Powered by the same technology that delivers inline full content inspection, File Parser offers unparalleled file inspection in split-second speeds.

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. We are not an SWG, web application firewall (WAF), or IPS, but we outperform and replace every SWG, WAF, and IPS on the market.

We accommodate all budgets and risk appetites. Trinity Cyber sells in subscription tiers. 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.