TRINITYCYBER

USE CASE

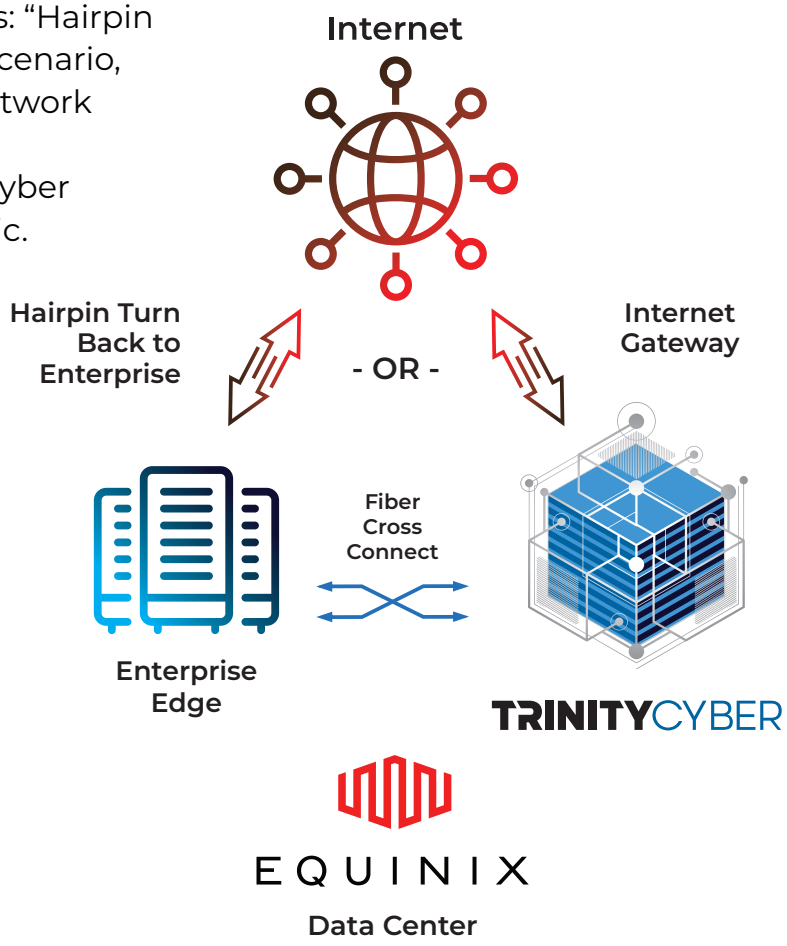
Enterprise

Connect to Trinity Cyber and Receive Full Content Inspection for All Internet-Facing Services

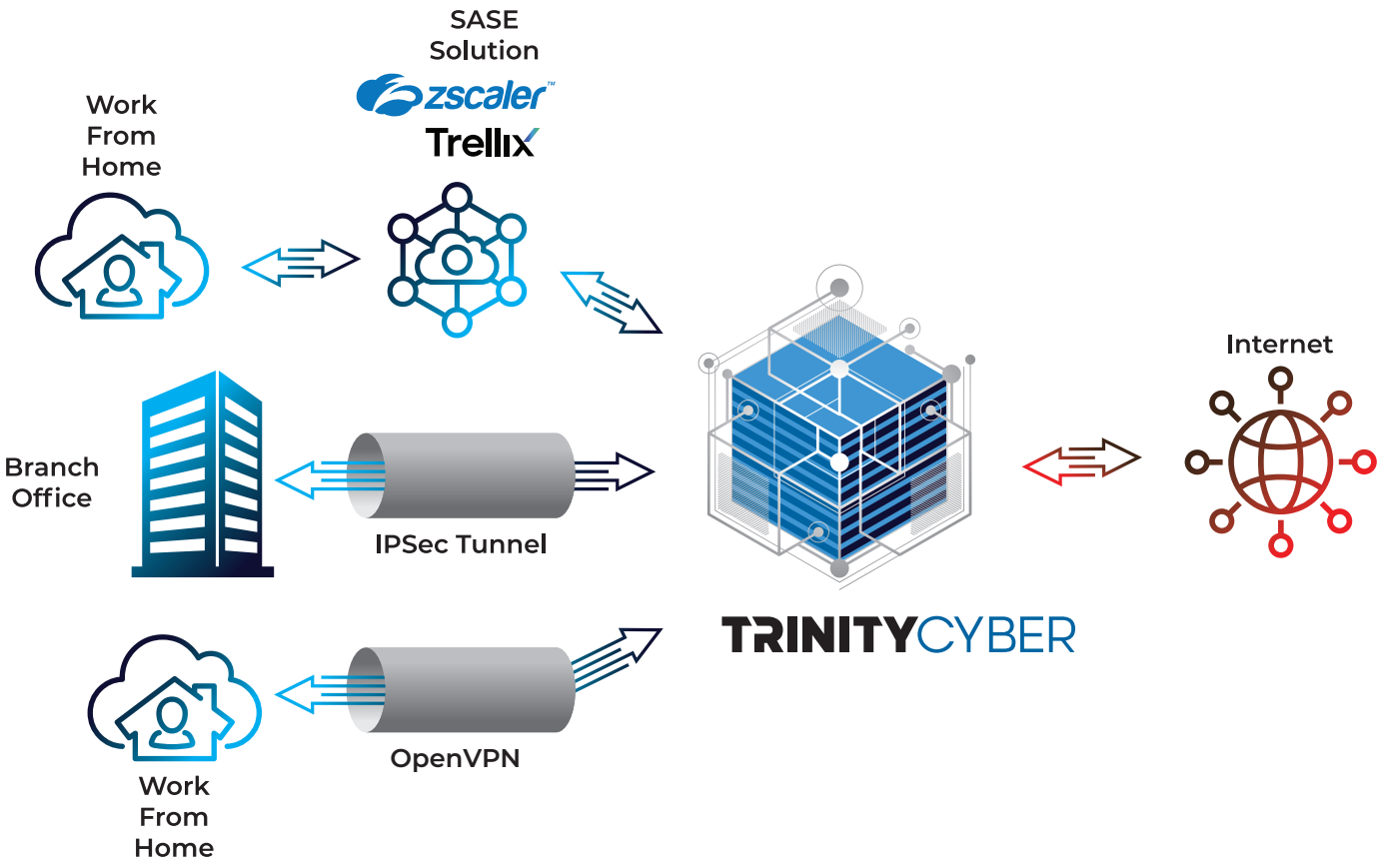
Unleash the power of Trinity Cyber's cutting-edge full content inspection technologies and team of world-class experts to protect your enterprise. Trinity Cyber's award-winning capability delivers unparalleled deep, content-based, full session inspection and real-time active cyber threat mitigation – all operated for you by an expert team of seasoned professionals.

For enterprises hosted in Equinix data centers, a fiber cross connect offers a high-performance, low-latency solution to place Trinity Cyber in the path between your edge and the internet. This connection establishes a local, high-speed physical cable connection between server racks, facilitating seamless and lightning-fast data transmission. Network technicians ensure the shortest possible distance between your network stack and Trinity Cyber, reducing latency to an absolute minimum. Cross connects allow data transfer through Layer 2 using MAC address identification (with optional MACSec encryption), or Layer 3 via IP address routing. Customers can also opt for a custom on-premises solution. Whether your network requires a gigabit system or one that processes terabits per second with less than a millisecond latency, Trinity Cyber has a solution for you.

When Trinity Cyber completes its full content inspection, traffic follows one of two paths: "Hairpin Turn" or "Gateway." In the "Hairpin Turn" scenario, processed data returns directly to your network stack before continuing to its destination. Alternatively, with the "Gateway", Trinity Cyber acts as the internet gateway for your traffic. Outgoing data passes through Trinity Cyber before reaching the internet, while incoming traffic first encounters Trinity Cyber's full content inspection, significantly reducing performance loads on your systems and easing the administrative workload.



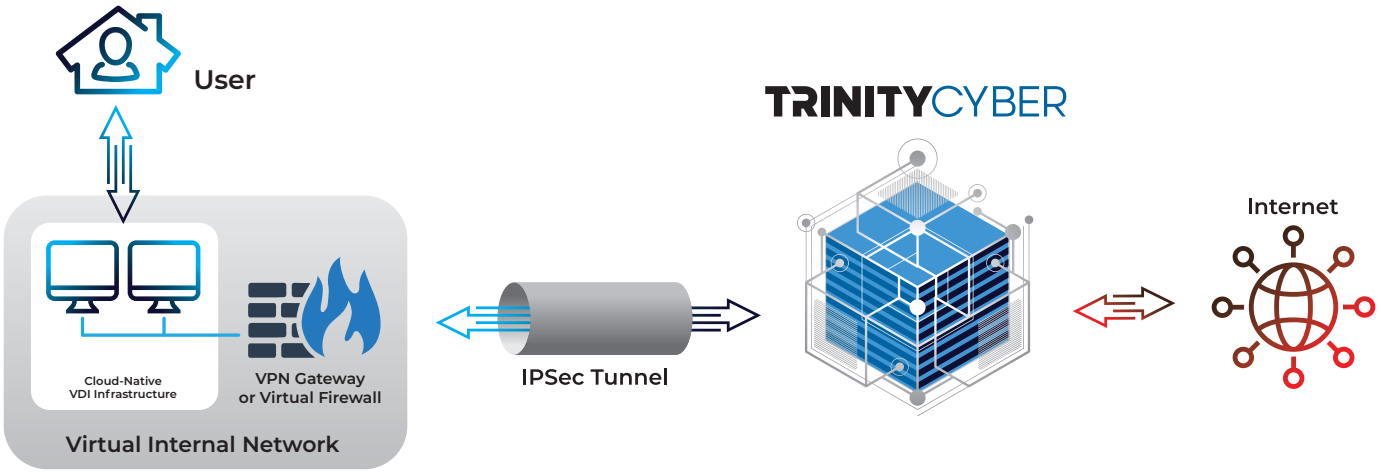
If you have branch offices, just tunnel your branch internet traffic to one of Trinity Cyber's closest internet gateways. For your remote users, either install Trinity Cyber's VPN client for direct access to Trinity Cyber or add the Trinity Cyber technology into the service chain of your existing Secure Access Service Edge (SASE) infrastructure. You get a massive boost to your security and 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 workload.



If your users leverage cloud-native VDI infrastructure, such as AWS Workspaces, traffic originating inside the VDI instance can be protected by Trinity Cyber. A cloud-native VPN Gateway offering or a virtual firewall from the vendor of your choosing will be used to establish an IPSec tunnel to Trinity Cyber and be the internet gateway for the virtual network connected to VDI infrastructure.

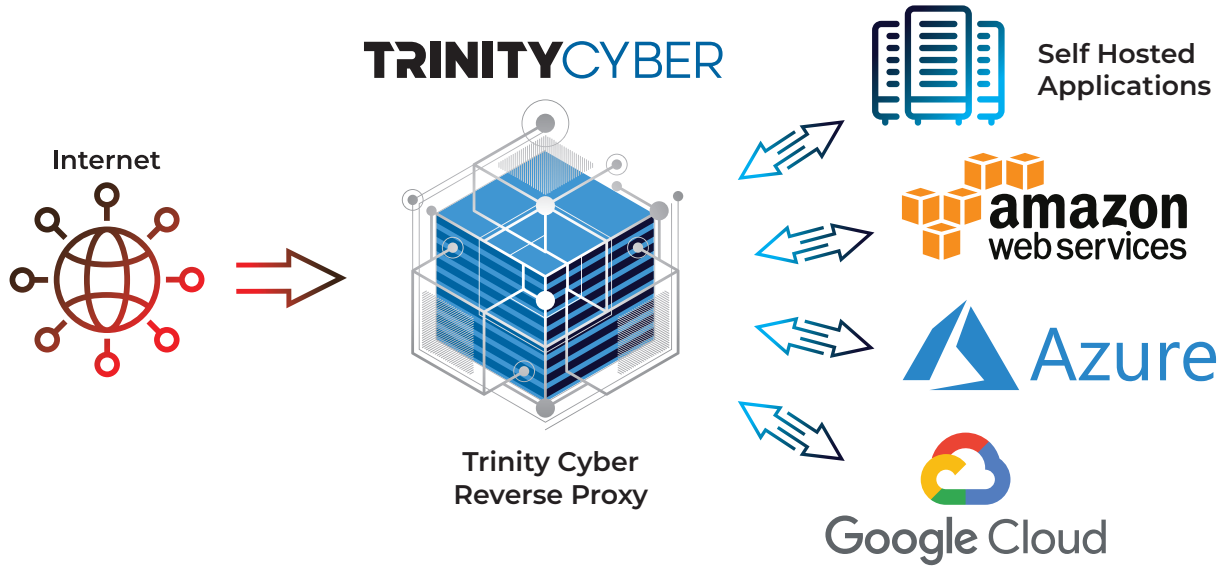
This configuration enables full utilization of Trinity Cyber's full content inspection offering, including:

- Inline protection by Trinity Cyber
- L4-L7 Advanced Firewalling and Policy Configuration
- BPF and Threat Event related Packet Capture
- SSL Decryption
- Agentless Inspection and Mitigation

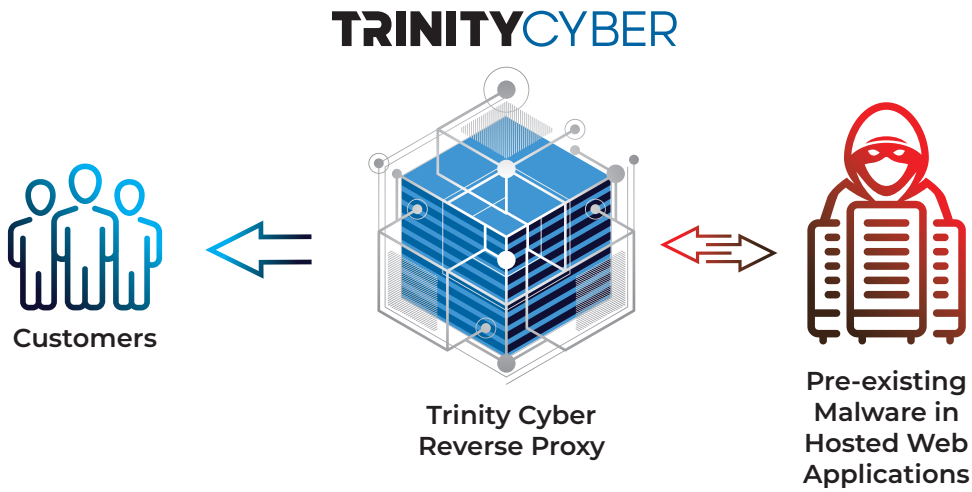


If you host web applications in the cloud, protect these applications and your customers by leveraging Trinity Cyber's secure reverse proxy feature, operating full content inspection between your applications and the internet.

While traditional web application firewall (WAF) services tied to Content Delivery Networks (CDNs) are convenient, these technologies use the same inadequate security components and antiquated processes that have been around for decades. While there are many vulnerabilities in CISA's Known Exploited Vulnerabilities (KEV) list, none are more important than the ones our partners at GreyNoise say are actively being exploited this minute. **We stop them all.** No alert aggregation. No follow up. No blinking lights. No triage.



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. Your customers will find out much later that their credit card information has been stolen and it's a bad day for both of you. Since the technology operates in both directions, it can "see" and remove malicious code directly from live web sessions. The entire process happens so fast, your customers won't even notice. And through this method, Trinity Cyber continues to expose hidden threats, ensuring that attackers cannot exploit new vulnerabilities in your applications, while simultaneously protecting customers from threats that would otherwise be undetectable.



With minimal effort and Trinity Cyber at your side, you gain access to a groundbreaking, fully-managed, enterprise-level security capability without complexity and overhead - an ideal solution for anyone looking to reduce their cyber risk and increase their cybersecurity posture.

The Trinity Cyber Core Technology

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. When the technology encounters a threat on your traffic - which it does more accurately and with a more enduring approach than any competitor in 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.

As soon as you are connected, your internet content is actively inspected to protect you against the ever-evolving threat landscape. The technology is backed by a suite of cybersecurity services like content-based threat hunting and emerging threat analysis – all made better through the 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 customer portal where you can see and drill into each and 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 that 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. This means you get a complete picture, analyzing even the most subtle threats and anomalies. The 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. Customers can 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.

The vast majority of your web traffic is encrypted with Transport Layer Security (TLS) between your browser and the web sites you visit. It is in these encrypted channels where most cyber adversaries lurk. Trinity Cyber decrypts this traffic; performs its full content inspection to neutralize the threats; and re-encrypts the traffic before releasing it to the internet. The entire process happens so fast, you won't even notice. 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 TLS Exemption Management, you may identify specific segments of traffic that should remain encrypted and inaccessible.

With Trinity Cyber managing your SSL decryption, you not only receive world-class protection, but through the customer portal, your digital forensics and incident response (DFIR) teams also get SSL-decrypted PCAP at their fingertips. Trinity Cyber guides you through the easy process of installing a root certificate into the trust store of your devices to make SSL decryption possible. Trinity Cyber's integrated PCAP solution enables your security team to use standard Berkeley Packet Filtering (BPF) syntax during a rolling 72-hour window, making it a breeze to search and retrieve SSL-decrypted packet captures to support thorough analysis and investigations. Your IT team will appreciate the ability to use SSL-decrypted PCAP to troubleshoot technology integration.

As a complement to Trinity Cyber's patented technologies, the company also offers standard L3 (source/destination IP) and L4 (stateful port and protocol inspection) firewall functionality as an additional security service, allowing you to save money by simplifying and offloading network security management. This feature is only available for customers using Trinity Cyber as an internet gateway (cross connect without hairpin and/or IPSec tunnel) with traffic egress to the internet through Trinity Cyber.

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), 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.