TRINITYCYBER

USE CASE

REMOTE USERS: VPN CONNECTIONS

Protect Your Company from the Threats Posed by Your Remote Workforce with Trinity Cyber's Full Content Inspection

The shift towards a remote workforce has brought about unparalleled flexibility and efficiency. However, when your staff can work from anywhere and even use their own devices, it's vital to apply consistent protection across all threat surfaces.

The very nature of remote work introduces new vulnerabilities to the enterprise that include unsecured home networks and potential device compromise. Without protection, susceptibility to phishing attacks increases. When an employee visits a website compromised by previous attacks, they fall prey to drive-by attacks at massive scale. Addressing this new normal places a massive strain on the scant security resources available within most companies.

Unleash the power of Trinity Cyber's cutting-edge full content inspection technologies to protect your company from the threats inherent from a remote workforce.

Simply install an OpenVPN-compatible endpoint client on your devices and connect them to Trinity Cyber's internet gateway. Device traffic is routed through Trinity Cyber's protection systems, catching and neutralizing malicious traffic and phishing content in real time, *before an incident occurs*. Drive-by attacks – like those used by ParrotTDS and Magecart – embed obfuscated malicious JavaScript into legitimate websites and slip past other security solutions. Trinity Cyber defeats these threats by stripping malicious JavaScript and other bad content directly from the intended victim's web session. The Trinity Cyber technology prevents the credential theft and the cleanup aftermath, while the user simply enjoys a safe and otherwise normal web experience.

Trinity Cyber's remote workforce infrastructure employs OpenVPN, a popular and trusted open-source secure tunneling protocol. Trinity Cyber provides a default configuration that works optimally for most network configurations. Should your needs require customization, customers may choose from a number of software downloads that support the OpenVPN protocol. The Trinity Cyber team can make personalized recommendations based on your existing network configuration and provide default configurations.

To connect to the internet gateway, Trinity Cyber provides a VPN destination – provisioned and unique to your organization – to be used on all endpoint connections. You can enter connection details into your client manually, import the connection via URL download, or download an OpenVPN configuration file from the Trinity Cyber portal.

Once the VPN connection is active, all traffic for the device is protected as it is routed to the internet through Trinity Cyber. Internet content is actively inspected to protect your enterprise against the ever-evolving threat landscape.

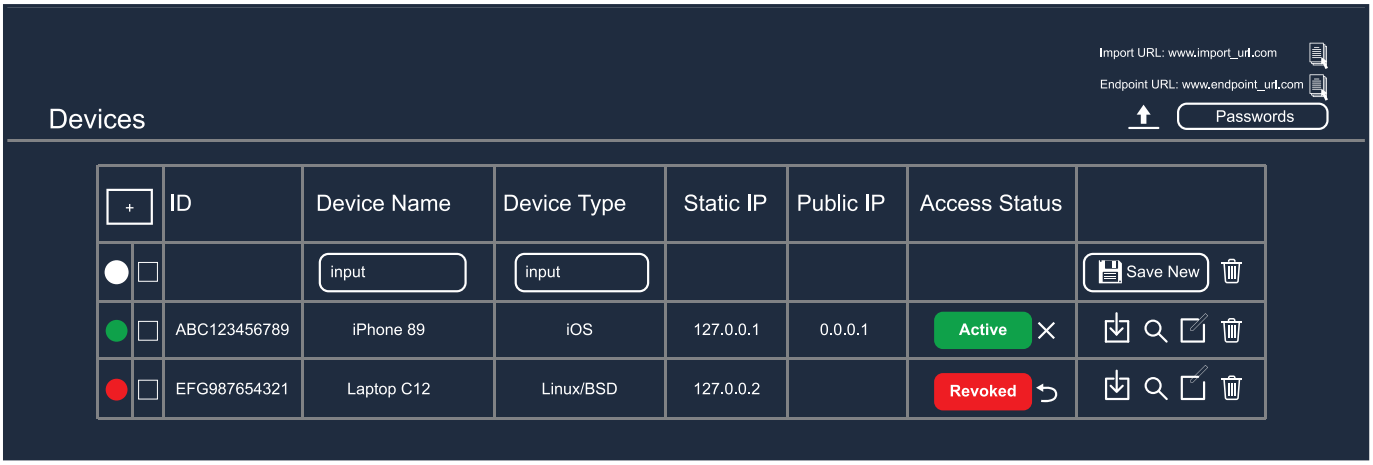
The vast majority of your remote workforce's web traffic is encrypted with Transport Layer Security (TLS) between their browser and the websites they visit. It is in these encrypted channels where most cyber adversaries lurk. Trinity Cyber protects against attackers hiding in your encrypted traffic by performing TLS Inspection, a three-step process:

1. Incoming encrypted traffic is identified and decrypted
2. Full content inspection neutralizes the threats
3. Traffic is re-encrypted and released to its destination

The entire process happens so fast, you won't even notice: 90% of all traffic is processed in less than 5 ms. Through this method, Trinity Cyber exposes hidden threats, ensuring that attackers cannot exploit protected channels to infiltrate your network. Trinity Cyber guides you through the easy process of installing a root certificate into the trust store of your devices to make TLS inspection possible.

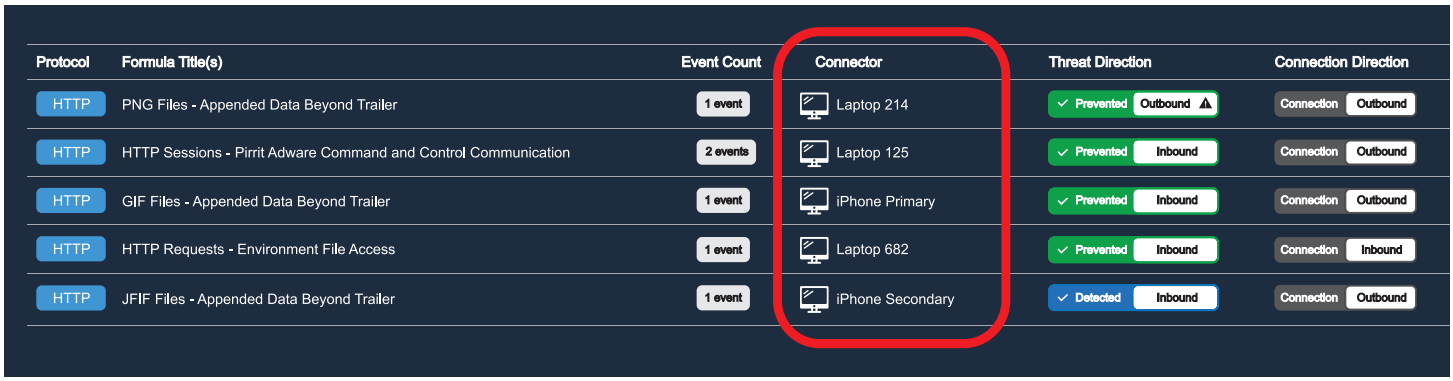
In cases where sensitive traffic cannot or should not be decrypted, Trinity Cyber manages a decryption exemption policy for you. With TLS Exemption Management, you may identify specific segments of traffic that should remain encrypted and inaccessible. This feature is essential for preserving the functionality of certain apps in 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 portal is your primary interface to review and manage the devices on your network, and their connections to the internet. You can view a complete list of VPN-connected devices, with the ability to filter and sort results, as well as perform a variety of administrative functions.

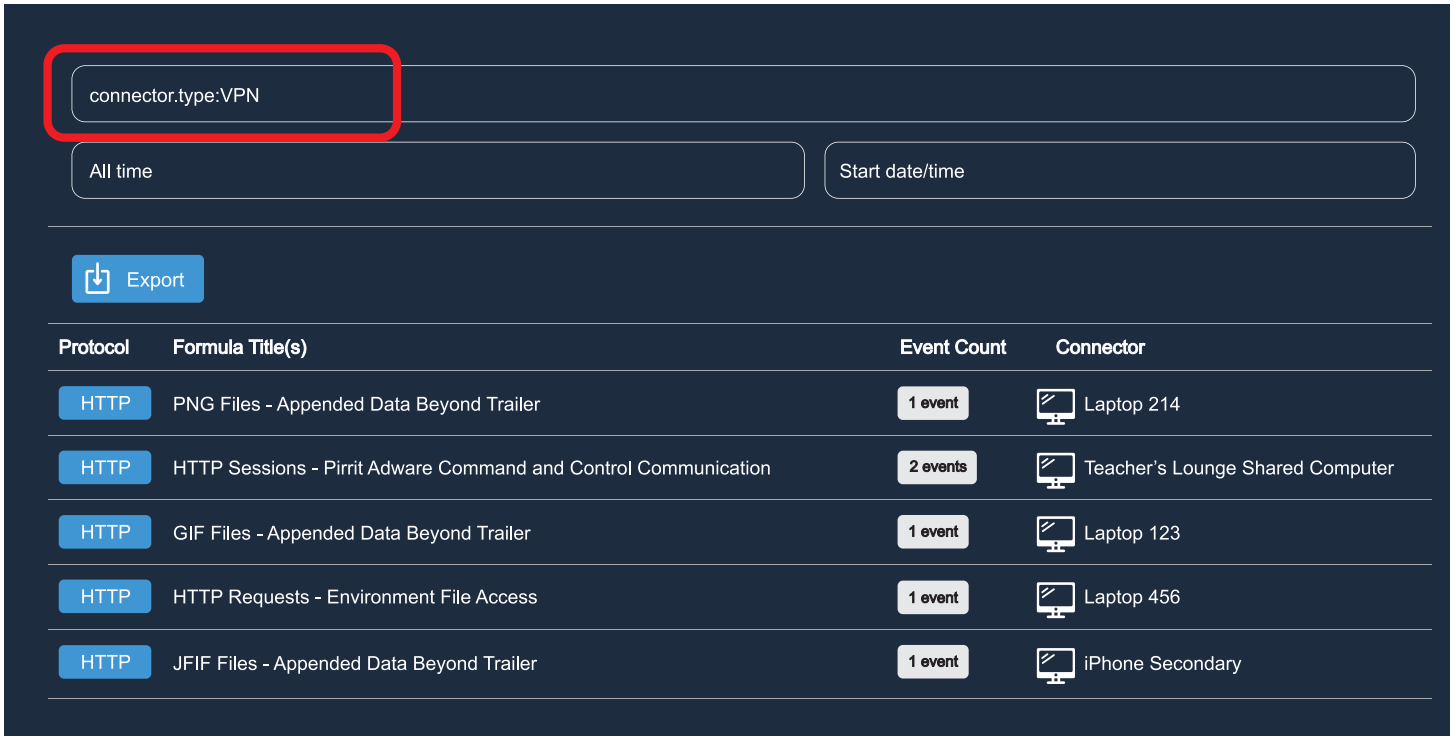


Additionally, you can add new devices to the list to grant immediate access to the VPN configuration file. This is ideal for situations in which the endpoint is disconnected from the internet. Many VPN clients can also download configuration details directly via URL. The URL for this download and its authorization password are also available from the Device page for your convenience.

Furthermore, the portal enables you to see the malicious events identified and mitigated by Trinity Cyber across all connection interfaces (e.g., VPN, IPSec tunnels, forward proxy, reverse proxy). Events originating from a VPN connection are called out, including the unique device name, allowing security and network personnel to take corrective action on the endpoint and/or follow up with the affected end user. Each event is already validated with extreme precision so you can rest assured of your protection.



You can also query keywords specific to your endpoint devices, allowing you to search for activity for a specific device or collection of devices.



All activities are available via API, allowing you to review the data within your company's Security Information and Event Management (SIEM) appliance.

Trinity Cyber offers multiple deployment options to suit customers' needs:

- **Manual Per Endpoint:** For companies that have a limited number of devices to connect, you can download and install the VPN client, and then set up the internet connection manually. Trinity Cyber offers three ways to create a new connection: 1 - import the connection from a URL and password that is unique to your company; 2 - import the connection from a configuration file that is then fed to the VPN client; and 3 - enter the configuration details manually (however, this increases the risk for human error).
- **Isolated Deployment:** You can set up your secure connection in air-gapped situations, when security parameters require that a new endpoint never access the internet directly without going through a VPN connection first. Simply download the configuration file and deliver it to the endpoint device via approved means.
- **Automated Deployment via Remote Management:** VPN installation and configuration is commonly automated. If your system administrators manage endpoints using tools like Mobile Device Management (MDM), Group Policy Objects (GPO), or third-party deployment software like Jamf or Munki, you should consider adding Trinity Cyber's internet gateway connections to your suite of remotely managed applications.

While exact implementations can vary significantly, Trinity Cyber will work with your systems and network staff to provide a smooth automation process.

The Trinity Cyber Core Technology

Trinity Cyber's cutting-edge full content inspection technologies protect your company from the threats posed by your remote workforce. Connecting your remote workers to Trinity Cyber's internet gateway is easy and simple to manage. The company's award-winning capabilities provide real-time active cyber threat mitigation backed by a suite of enhanced cybersecurity services operated on your behalf by world-class security experts.

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 CVEs, threat actor groups, ransomware gangs, and entire families of threats. No alerts to aggregate. Near zero false positives.

When the technology encounters a threat in the network traffic – which it does more accurately and with a more enduring approach than any competitor on the market – it seamlessly mitigates that threat on the wire, 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 that include content-based threat hunting and emerging threat analysis. Trinity Cyber operates on your behalf, defends you against the latest threats, manages all the systems, and provides you with a context-rich, interactive web 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 also every notification in the portal is legitimate with more than 99.99% accuracy.

As a complement to Trinity Cyber's patented technologies, the company offers Layer 3 (source/destination IP) and Layer 4 (stateful port and protocol inspection) firewall functionality as an additional security service, allowing you to save money by simplifying and offloading network security management. 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, making it an ideal solution for enterprises looking to reduce their cyber risk and increase their cybersecurity posture. Trinity Cyber's elite team of experts serve as an extension of your security team and manage a low-risk firewall posture for all of your connections, protecting your local and cloud-based resources.

Trinity Cyber's web portal is home to analytics tools as well: Packet capture (PCAP) and File Parser. Trinity Cyber offers comprehensive PCAP results, capturing all SSL-decrypted network traffic from your users, 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. Use Trinity Cyber's PCAP to support digital forensics and incident response (DFIR), aid in information technology (IT) troubleshooting, and help expose insider threats.

Trinity Cyber's File Parser tool puts the power of advanced file analytics at your fingertips. With this feature in the portal, security analysts can drag and drop a file, get an immediate maliciousness verdict, and see a graphical and data-rich breakout of all the file components. Use it to aid in analysis, threat intelligence, and incident response.

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.